MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Rekomendacje dotyczące bezpieczeństwa technologii operacyjnych (OT)

NIST SP 800-82r3_wer. 2.0_PL

NIST SP 800-82r3_wer. 2.0_PL

25 czerwca 2024

Rekomendacje dotyczące bezpieczeństwa technologii operacyjnych (OT)

Publikacja dostępna pod adresem:

Rekomendacje cyberbezpieczeństwa

NIST Special Publication
NIST SP 800 82r3

Guide to Operational Technology (OT) Security

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Victoria Pillitteri
Suzanne Lightman
Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800 82r3

Guide to Operational Technology (OT) Security

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Smart Connected Systems Division
Communications Technology Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST SP 800-82r3_wer. 2.0_PL, *Rekomendacje dotyczące bezpieczeństwa technologii operacyjnych (OT)***, stanowi tłumaczenie publikacji *NIST SP 800-82 rev. 3, Guide to Operational Technology (OT) Security,* i zostało opracowane za zgodą National Institute of Science and Technology.

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

W publikacji posłużono się pojęciami zdefiniowanymi w oryginalnej (angielskiej) wersji dokumentu, na podstawie którego powstały niniejsze zalecenia.
Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim.
Pozostałe role i funkcje zostały przedstawione w języku angielskim[1]. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.
Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.**

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie. Taka identyfikacja nie stanowi rekomendacji, poparcia ani nie ma na celu sugerowania, że dane podmioty, materiały lub urządzenia są bezwzględnie najlepsze z dostępnych dla osiągnięcia danego celu.

[1] Kluczowi uczestnicy zarządzania ryzykiem – patrz: Narodowe Standardy Cyberbezpieczeństwa

W niniejszym dokumencie zostały wymienione nazwy wybranych dostępnych na rynku urządzeń, narzędzi, programów lub innych materiałów, zarówno o charakterze komercyjnym, jak i niekomercyjnym. Wykorzystanie takich nazw służy wyłącznie przedstawieniu odpowiednich opisów procedur eksperymentalnych. Wskazanie to nie stanowi reklamy ani promocji jakiegokolwiek produktu lub usługi przez NIST, jak również nie oznacza, że wskazane materiały lub urządzenia stanowią najlepsze dostępne rozwiązania służące osiągnięciu danego celu. Niniejsza publikacja może zawierać odniesienia do innych publikacji opracowywanych przez NIST zgodnie z obowiązkami statutowymi przypisanymi tej organizacji. Informacje zawarte w niniejszej publikacji, w tym koncepcje i metodologie, mogą znaleźć zastosowanie w agencjach federalnych nawet przed ukończeniem wszelkich publikacji towarzyszących. W związku z tym, do czasu zakończenia prac nad każdą publikacją, istniejące wymagania, wytyczne i procedury pozostają w mocy. W związku z celami dotyczącymi planowania i zmian, agencje federalne powinny uważnie śledzić rozwój nowych publikacji NIST. Zachęcamy organizacje do zapoznawania się z publikowanymi wersjami roboczymi publikacji udostępnionymi w celu zgłaszania uwag oraz przekazywania swoich opinii do NIST. Wiele publikacji NIST dotyczących cyberbezpieczeństwa, poza publikacjami wymienionymi powyżej, są dostępne w witrynie internetowej https://csrc.nist.gov/publications.

KLAUZULA PRAWNA

Niniejszy dokument został przygotowany na podstawie dokumentu opracowanego przez amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) zgodnie z jego ustawowymi obowiązkami wynikającymi z ustawy rządu federalnego Stanów Zjednoczonych dotyczącej modernizacji zasad bezpieczeństwa informacji (*ang. Federal Information Security Modernization Act - FISMA*) z 2014 roku [44 U.S.C. § 3551 i n.], Public Law (P. L.) 113-283. Obszar odpowiedzialności NIST obejmuje opracowywanie norm oraz wytycznych w zakresie bezpieczeństwa informacji, w tym minimalnych wymagań dotyczących federalnych systemów informatycznych. Opracowane normy i wytyczne nie mogą być jednak stosowane w odniesieniu do krajowych systemów bezpieczeństwa bez wyraźnej zgody stosownych urzędników federalnych odpowiedzialnych za ustalanie zasad dotyczących tych systemów. Wytyczne zawarte

w niniejszym dokumencie są zgodne z wymogami opisanymi w okólniku A-120 Biura ds. Zarządzania i Budżetu (*ang. Office of Management and Budget – OMB*).

Żadna część niniejszej publikacji nie może stanowić podstawy do uznania za nieobowiązujące normy i wytyczne dotyczące agencji federalnych, ustanowionych przez Sekretarza ds. Handlu na mocy stosownych uprawnień ustawowych. Wytyczne zawarte w niniejszej publikacji nie zmieniają ani nie powinny być uznawane za nadrzędne względem uprawnień Sekretarza ds. Handlu, Dyrektora Biura ds. Zarządzania i Budżetu (OMB) lub jakiegokolwiek innego urzędnika federalnego. Niniejsza publikacja może być wykorzystywana przez organizacje pozarządowe na zasadzie dobrowolności i nie jest objęta prawami autorskimi na terytorium Stanów Zjednoczonych. NIST uprasza jednak o wskazanie autorstwa dokumentu.

Spis treści

Tłumaczenie

Tłumaczenie

Spis ilustracji

Tłumaczenie

Spis tabel

STRESZCZENIE

Niniejszy dokument przedstawia rekomendacje dotyczące wdrażania środków bezpieczeństwa w zakresie technologii operacyjnych (*ang. Operational Technology - OT*), które uwzględniają szczególne wymogi dotyczące osiągów, wydajności, niezawodności i bezpieczeństwa. Systemy i urządzenia wchodzące w zakres technologii operacyjnych to rozwiązania, które wchodzą w interakcje ze środowiskiem fizycznym lub zarządzają urządzeniami wchodzącymi w interakcje ze środowiskiem fizycznym. Takie systemy oraz urządzenia wykrywają lub wywołują zmiany poprzez monitorowanie lub kontrolowanie urządzeń, procesów i zdarzeń. Przykłady takich rozwiązań obejmują systemy sterowania przemysłowego, systemy automatyki budynków, systemy transportowe, systemy kontroli dostępu fizycznego, systemy monitorowania i systemy pomiarowe działające w środowiskach fizycznych. Niniejszy dokument obejmuje omówienie technologii operacyjnych oraz typowych topologii systemów, wskazuje typowe zagrożenia oraz podatności występujące w tych systemach, a także zawiera zalecane środki przeciwdziałania pozwalające na ograniczenie związanego z nimi ryzyka.

SŁOWA KLUCZOWE

bezpieczeństwo komputerowe; rozproszone systemy sterowania (*ang. computer security; distributed control systems – DCS*); przemysłowe systemy sterowania (*ang. industrial control systems – ICS*); bezpieczeństwo informacji; bezpieczeństwo sieci (*ang. network security)*; technologia operacyjna (*ang. operational technology – OT*); programowalne sterowniki logiczne (*ang. programmable logic controllers – PLC*); zarządzanie ryzykiem (*ang. risk management*); środki bezpieczeństwa/zabezpieczenia (*ang. security controls*); systemy kontroli nadzorczej i pozyskiwania danych (SCADA) (*ang. supervisory control and data acquisition (SCADA) systems – SCADA*).

SPRAWOZDANIA DOTYCZĄCE TECHNOLOGII SYSTEMÓW KOMPUTEROWYCH

Laboratorium Technologii Informacyjnych (*ang. Information Technology Laboratory – ITL*) przy Narodowym Instytucie Standaryzacji i Technologii (*ang. National Institute of Standards and Technology – NIST*) działa na rzecz gospodarki USA i dobra publicznego poprzez zapewnienie technicznego wsparcia krajowej infrastruktury pomiarowej i normalizacyjnej. ITL opracowuje testy, metody testowe, dane referencyjne, weryfikacje koncepcji (*ang. proof of concept*) oraz analizy techniczne, mające na celu rozwój i produktywne wykorzystanie technologii informacyjnych. Zakres zadań ITL obejmuje opracowywanie norm i wytycznych w zakresie zarządzania, administracji, a także aspektów technicznych i fizycznych w celu zapewnienia bezpieczeństwa i prywatności informacji innych niż związane z bezpieczeństwem narodowym w federalnych systemach informacyjnych przy zachowaniu efektywności kosztowej. Niniejsza publikacja specjalna oznaczona numerem 800 zawiera sprawozdanie dotyczące badań, wytycznych oraz działań ITL w zakresie komunikacji, bezpieczeństwa systemów informacyjnych oraz o współpracy z przemysłem, jednostkami rządowymi oraz organizacjami akademickimi.

UWAGA DLA CZYTELNIKÓW

Na potrzeby opracowania niniejszego dokumentu wykorzystano poprzednie wydania publikacji NIST SP 800-82. Nowe informacje uwzględnione w tym wydaniu obejmują:

- rozszerzenie zakresu stosowania wytycznych z przemysłowych systemów sterowania na systemy technologii operacyjnej;
- aktualizacje zagrożeń i podatności związanych z technologią operacyjną;
- aktualizacje dotyczące zarządzania ryzykiem związanym z technologią operacyjną, a także zaleceń w zakresie dobrych praktyk i stosowanych architektur;
- aktualizacje dotyczące bieżących działań w zakresie bezpieczeństwa technologii operacyjnej;
- aktualizacje dotyczące narzędzi oraz zdolności do ochrony technologii operacyjnych;

- zmiany dostosowujące treść publikacji do innych norm i wytycznych dotyczących bezpieczeństwa technologii operacyjnych, w tym ram cyberbezpieczeństwa;
- nowe wytyczne ujednolicające treść publikacji z informacjami dotyczącymi zabezpieczeń opisanych w dokumencie NIST SP 800-53, Rev. 5 / NSC 800-53 [NSC 800-53];
- dodatkowe informacje dotyczące technologii operacyjnych na potrzeby zabezpieczeń opisanych w dokumencie NIST SP 800-53, Rev. 5 / NSC 800-53 [NSC 800-53], które zapewniają dostosowanie do poziomu minimalnych zabezpieczeń systemów technologii operacyjnej o niskim, umiarkowanym i wysokim poziomie wpływu.

INFORMACJA O UJAWNIENIU PATENTÓW

INFORMACJA: Laboratorium Technologii Informacyjnych (ITL) NIST zwróciło się do właścicieli patentów, których wykorzystanie może być wymagane w celu zapewnienia zgodności z wytycznymi lub wymogami określonymi w treści niniejszej publikacji, o udostępnienie stosownych zastrzeżeń patentowych. Należy jednak pamiętać o tym, że właściciele patentów nie są zobowiązani do ujawnienia patentów na prośbę ITL; co więcej, ITL nie przeprowadziło analiz patentowych w celu wskazania patentów, które mogą być związane z zakresem niniejszej publikacji.

W dniu publikacji i po wystosowaniu próśb o wskazanie zastrzeżeń patentowych, których wykorzystanie może być wymagane w celu zapewnienia zgodności z wytycznymi lub wymogami zawartymi w niniejszej publikacji, ITL nie otrzymało informacji o takich zastrzeżeniach patentowych.

Niniejszy dokument nie stanowi oświadczenia ani zapewnienia ze strony ITL, że w celu uniknięcia naruszeń ochrony patentowej przy korzystaniu z niniejszej publikacji nie jest wymagane uzyskanie licencji.

PODSUMOWANIE

Niniejszy dokument przedstawia rekomendacje dotyczące skutecznego wdrażania środków bezpieczeństwa w zakresie technologii operacyjnych (OT)[2], które uwzględniają wymogi dotyczące osiągów, wydajności, niezawodności i bezpieczeństwa. Systemy i urządzenia należące do kategorii technologii operacyjnych to rozwiązania, które wchodzą w interakcje ze środowiskiem fizycznym lub zarządzają urządzeniami powodującymi takie interakcje. Takie systemy oraz urządzenia wykrywają lub wywołują zmiany poprzez monitorowanie lub kontrolowanie urządzeń, procesów i zdarzeń. Przykłady takich rozwiązań obejmują systemy sterowania przemysłowego, systemy automatyki budynków, systemy transportowe, systemy kontroli dostępu fizycznego, systemy monitorowania i systemy pomiarowe działające w środowiskach fizycznych. Niniejszy dokument obejmuje omówienie technologii operacyjnych oraz typowych topologii systemów, wskazuje typowe zagrożenia oraz podatności występujące w tych systemach, a także wymienia zalecane środki przeciwdziałania pozwalające na ograniczenie związanego z nimi ryzyka. Technologie operacyjne mają kluczowe znaczenie dla funkcjonowania infrastruktury krytycznej, którą często charakteryzuje wysoki stopień powiązań i wzajemnych zależności. W tym kontekście warto nadmienić, że choć organy rządowe odpowiadają za zarządzanie i obsługę wielu elementów infrastruktury krytycznej państwa, część takich systemów znajduje się w rękach prywatnych, a za ich utrzymanie odpowiadają ich właściciele i operatorzy. Ponadto infrastruktura krytyczna często jest określana mianem systemu systemów ze względu na współzależności istniejące między różnymi sektorami przemysłu i wzajemne powiązania między partnerami biznesowymi.

Pierwsze systemy technologii operacyjnej w niewielkim stopniu przypominały tradycyjne systemy technologii informacyjnej, były bowiem odizolowane, wykorzystywały zastrzeżone protokoły sterowania i opierały się na specjalistycznych urządzeniach sprzętowych oraz wyspecjalizowanym oprogramowaniu. Obecnie systemy te coraz częściej wykorzystują

[2] Zobacz także:https://csrc.nist.gov/Projects/operational-technology-security.

rozwiązania z zakresu technologii informacyjnej, które umożliwiają komunikację z systemami biznesowymi organizacji oraz zdalny dostęp; ponadto są one projektowane i wdrażane przy użyciu standardowych komputerów, systemów operacyjnych oraz protokołów sieciowych, w wyniku czego w coraz większym stopniu upodabniają się do systemów informacyjnych. Takie połączenie rozszerza ich możliwości, jednak wiąże się też ze zmniejszeniem poziomu odizolowania systemów OT od świata zewnętrznego względem tradycyjnych rozwiązań, co przekłada się na wzrost potrzeb w zakresie zabezpieczeń tych systemów. Popularyzacja sieci bezprzewodowych naraża systemy technologii operacyjnej na szereg zagrożeń ze strony atakujących znajdujących się w stosunkowo bliskiej odległości fizycznej, a jednocześnie nie mających bezpośredniego fizycznego dostępu do urządzeń. Ze względu na to, że zabezpieczenia oraz rozwiązania zapewniające bezpieczeństwo zostały zaprojektowane z myślą o typowych systemach teleinformatycznych, wdrażanie ich w środowiskach technologii operacyjnych wymagają zachowania szczególnej ostrożności. Niektóre przypadki wymagają nowych rozwiązań i zabezpieczeń dostosowanych do wymogów środowisk OT.

Pomimo wielu podobieństw, współczesne technologie operacyjne charakteryzuje szereg cech, które odróżniają je od tradycyjnych systemów przetwarzających informacje. Wiele z tych różnic wynika z faktu, że elementy logiczne wykonywane w systemach OT mają bezpośredni wpływ na środowisko fizyczne. W praktyce może oznaczać to znaczące ryzyko i zagrożenie dla zdrowia i ludzkiego życia, ryzyko wystąpienia poważnych szkód środowiskowych oraz ryzyko poważnych strat finansowych w wyniku zatrzymania produkcji, negatywnego wpływu zdarzenia na gospodarkę państwa oraz ujawnienie wrażliwych informacji. Co więcej, rozwiązania technologii operacyjnej charakteryzują się szczególnymi wymaganiami w zakresie wydajności i niezawodności. W wielu przypadkach takie urządzenia i systemy działają pod kontrolą systemów operacyjnych i aplikacji, które administratorzy technologii informacyjnych mogą uważać za nietypowe i niekonwencjonalne. Dodatkowe wyzwanie stanowi fakt, że wymogi w zakresie bezpieczeństwa i wydajności bywają sprzeczne z wymogami w zakresie bezpieczeństwa wdrażanymi na etapie projektowania systemów OT oraz w czasie ich obsługi.

Inicjatywy w zakresie cyberbezpieczeństwa technologii operacyjnych powinny zawsze stanowić element szerszych programów dotyczących bezpieczeństwa i niezawodności OT zarówno w zakładach przemysłowych, jak i w przedsiębiorstwach – cyberbezpieczeństwo ma bowiem zasadnicze znaczenie dla bezpiecznego i niezawodnego działania nowoczesnych procesów przemysłowych. Zagrożenia dla systemów technologii operacyjnej mogą pochodzić z wielu źródeł. Obejmują one wrogie rządy, ugrupowania terrorystyczne, niezadowolonych pracowników, złośliwych napastników, klęski żywiołowe, złośliwe działania pracowników organizacji oraz niezamierzone działania, takie jak błędy ludzkie lub nieprzestrzeganie ustalonych zasad i procedur. Podstawowe cele dotyczące bezpieczeństwa technologii operacyjnych zwykle stawiają na pierwszym miejscu ich integralność i dostępność, a następnie poufność, jednak nadrzędnym priorytetem jest każdorazowo bezpieczeństwo fizyczne.

Lista incydentów, które mogą dotyczyć systemów technologii operacyjnej, obejmuje:

- przerwanie lub opóźnienie przepływu informacji przez sieci OT, które może zakłócić działanie technologii operacyjnych, prowadząc do utraty wglądu w działanie oraz kontroli nad systemami;
- nieautoryzowane zmiany instrukcji, poleceń lub wartości alarmowych, które mogą doprowadzić do uszkodzenia lub wyłączenia urządzeń, wpłynąć na środowisko lub spowodować zagrożenie życia ludzkiego;
- przekazywanie niedokładnych danych operatorom systemu w celu ukrycia nieautoryzowanych zmian, lub w celu skłonienia operatorów do podjęcia niewłaściwych działań, które mogą nieść za sobą różne negatywne skutki;
- modyfikacje oprogramowania OT lub jego ustawień konfiguracyjnych, a także zakażenie oprogramowania OT złośliwym oprogramowaniem, co może nieść za sobą różne negatywne skutki;
- zakłócenie działania systemów ochronnych, co może stanowić zagrożenie dla kosztownych i trudno dostępnych urządzeń;
- zakłócenie działania systemów zabezpieczających, które może stanowić zagrożenie dla życia ludzi.

Główne cele w zakresie bezpieczeństwa systemów technologii operacyjnej powinny obejmować następujące zagadnienia:

- **Ograniczenie logicznego dostępu do sieci oraz systemów OT, aktywności sieciowej i systemów.** Zabezpieczenia mogą obejmować wdrożenie jednokierunkowych bram, wykorzystywanie architektury sieci DMZ z zaporami ogniowymi, aby zapobiec przenikaniu ruchu sieciowego między siecią organizacji i siecią OT, a także wdrożenie oddzielnych mechanizmów uwierzytelniania i poświadczeń dla użytkowników sieci organizacji oraz systemów OT. System technologii operacyjnej powinien również opierać się na wielowarstwowej topologii sieci, przy czym najbardziej krytyczna komunikacja winna odbywać się w najbardziej bezpiecznej i niezawodnej warstwie.
- **Ograniczenie fizycznego dostępu do sieci i urządzeń OT.** Nieautoryzowany dostęp fizyczny do elementów systemu może stanowić poważne ryzyko dla funkcjonowania systemów OT. W celu zapewnienia bezpieczeństwa należy stosować połączenie środków kontroli dostępu, takich jak: zamki, czytniki kart lub pracownicy ochrony.
- **Ochrona poszczególnych komponentów OT przed kompromitacją.** Zabezpieczenia w tym zakresie obejmują instalowanie poprawek bezpieczeństwa w jak najkrótszym czasie po ich uprzednim przetestowaniu w rzeczywistych warunkach, wyłączenie wszystkich nieużywanych portów i usług oraz zadbanie o to, by pozostały wyłączone, ograniczenie uprawnień użytkowników systemów OT wyłącznie do tych, które są wymagane w związku z wykonywaną pracą, śledzenie i monitorowanie ścieżek audytu oraz stosowanie środków bezpieczeństwa, takich jak oprogramowanie antywirusowe i oprogramowanie weryfikujące integralność plików w sytuacjach, w których jest to technicznie wykonalne, aby skutecznie zapobiegać instalacji złośliwego oprogramowania, odstraszać potencjalnych napastników, wykrywać przypadki infekcji, a także łagodzić ich skutki. Klucze do elementów systemów OT, w tym programowalnych sterowników logicznych (PLC) i systemów bezpieczeństwa, powinny być zawsze w pozycji włączonej, z wyjątkiem sytuacji, w której są programowane.

- **Ograniczenie nieautoryzowanej modyfikacji danych.** Zabezpieczenie dotyczy danych we wszystkich stanach (w tym w stanie spoczynku, w tranzycie, w użyciu) oraz strumieni danych wychodzących poza granice sieci.
- **Wykrywanie zdarzeń i incydentów związanych z bezpieczeństwem.** Wykrywanie zdarzeń związanych z bezpieczeństwem, które nie przerodziły się jeszcze w incydenty, może pomóc w przerwaniu łańcucha ataku, zanim napastnicy osiągną swoje cele. Zabezpieczenia te obejmują możliwość wykrywania uszkodzonych komponentów systemów OT, niedostępnych usług i wyczerpanych zasobów, które są ważne dla zapewnienia prawidłowego i bezpiecznego funkcjonowania systemu.
- **Utrzymanie funkcjonalności w niesprzyjających warunkach.** Zabezpieczenie to wymaga projektowania systemów OT w sposób umożliwiający realizację kluczowych działań w przypadku zakłóceń. Wszystkie krytyczne komponenty systemu powinny posiadać nadmiarowe odpowiedniki. Awarie komponentu nie powinny wiązać się z generowaniem niepotrzebnego ruchu w systemach OT ani w innych sieciach, nie powinny także powodować problemów w innych obszarach, które mogą doprowadzić do kaskadowej awarii. Systemy OT powinny również przewidywać degradację poziomów działania, na przykład przejście ze stanu normalnego z pełną automatyzacją do stanu awaryjnego wymagającego większego zaangażowania operatorów i ograniczenia automatyzacji, a następnie do trybu ręcznego, w którym automatyzacja jest wyłączona.
- **Przywracanie i uruchamianie systemu po incydencie.** Incydenty są nieuniknione – z tego powodu konieczne jest opracowanie planu odpowiedzi na incydent. Jedną z najważniejszych cech dobrego (skutecznego) programu bezpieczeństwa jest szybkość przywrócenia systemu po wystąpieniu incydentu.

Zespół do spraw cyberbezpieczeństwa obejmujący przedstawicieli wielu działów i jednostek organizacyjnych może wykorzystać zróżnicowaną wiedzę oraz doświadczenie w celu przeprowadzenia oceny ryzyka dla systemu OT i jego ograniczenia. Zespół ds. cyberbezpieczeństwa powinien obejmować co najmniej jednego przedstawiciela działu IT organizacji, inżyniera ds. nadzoru technicznego, operatora systemu sterowania, specjalisty ds. bezpieczeństwa sieci i systemów,

przedstawiciela kadry zarządzającej oraz przedstawiciela działu bezpieczeństwa fizycznego. W celu zapewnienia ciągłości podejmowanych działań oraz kompleksowego podejścia, zespół ds. cyberbezpieczeństwa powinien również skonsultować się z producentem systemu sterowania bądź integratorem systemu. Zespół ds. cyberbezpieczeństwa powinien ściśle współpracować z kierownictwem organizacji (np. kierownikiem obiektu), a także z osobami na stanowiskach[3] Chief Information Officer (CIO), Chief Information Security Officer (CISO), które wraz z dyrektorem generalnym (*ang. Chief Executive Officer – CEO*) lub dyrektorem ds. operacyjnych (*ang. Chief Operating Officer – COO*) ponoszą pełną odpowiedzialność za cyberbezpieczeństwo systemów OT oraz za wszelkie incydenty bezpieczeństwa, incydenty związane z niezawodnością lub uszkodzenia urządzeń spowodowane bezpośrednio lub pośrednio przez cyberincydenty. Skuteczny program cyberbezpieczeństwa dotyczący systemów OT powinien opierać się na strategii „obrony w głąb", która wymaga stosowania warstw zabezpieczeń w taki sposób, aby zminimalizować potencjalne skutki awarii dowolnego z nich. Przedsiębiorstwa i organizacje nie powinny opierać się na strategii bezpieczeństwa opartej na niejawności informacji.

W przypadku typowego systemu OT strategia obrony w głąb obejmuje:

- Opracowywanie zasad bezpieczeństwa, procedur, szkoleń i materiałów szkoleniowych dotyczących danego systemu OT.
- Uwzględnienie strategii bezpieczeństwa oraz procedur opartych na Krajowym Systemie Informacji dot. Terroryzmu (*ang. National Terrorism Advisory System*) oraz wdrażanie środków bezpieczeństwa odpowiadających poziomowi zagrożenia.
- Uwzględnienie wymogów w zakresie bezpieczeństwa w całym cyklu życia systemu OT, począwszy od etapów projektowania architektury, nabycia urządzeń i oprogramowania, montażu, eksploatacji, konserwacji i wycofania z eksploatacji.
- Wdrożenie wielowarstwowej topologii sieci systemu OT, przy czym najbardziej krytyczna komunikacja winna odbywać się w najbardziej bezpiecznej i niezawodnej warstwie.

[3] Opis kluczowych ról – patrz: NSC 7298.

- Zapewnienie separacji logicznej między siecią organizacji i siecią OT, opartej na przykład na zaporach sieciowych kontrolujących przepływ pakietów pomiędzy sieciami oraz jednokierunkowych bramach sieciowych.
- Uwzględnienie sytuacji, w których może być konieczne zapewnienie separacji fizycznej, gdy separacja logiczna może okazać się niewystarczająca.
- Wdrożenie architektury sieci opartej na strefie zdemilitaryzowanej (DMZ), na przykład w celu zapobiegania wymianie pakietów między sieciami organizacji i siecią OT.
- Wdrożenie uwierzytelniania wieloskładnikowego na potrzeby zdalnego dostępu do systemów OT.
- Zapewnienie nadmiarowości kluczowych komponentów systemu oraz nadmiarowych połączeń sieciowych.
- Uwzględnienie zasad stopniowej degradacji w architekturze kluczowych systemów w celu zapobiegania katastrofalnym w skutkach awariom kaskadowym.
- Wyłączenie nieużywanych portów i usług urządzeń OT po zweryfikowaniu, że takie działanie nie wpłynie negatywnie na ich działanie.
- Ograniczenie fizycznego dostępu do sieci i urządzeń OT.
- Ograniczenie uprawnień użytkowników OT wyłącznie do tych, które są wymagane do wykonywania pracy przez każdego użytkownika (np. ustanowienie kontroli dostępu opartej na rolach, skonfigurowanie ról w oparciu o zasadę minimalnych uprawnień).
- Wykorzystywanie oddzielnych mechanizmów uwierzytelniania i poświadczeń dla użytkowników sieci OT i sieci organizacji – konta umożliwiające dostęp do systemu OT nie powinny być wspólne z kontami użytkowników uprawniających do dostępu do sieci organizacji.
- Korzystanie z nowoczesnych rozwiązań, takich jak inteligentne karty pozwalające na uwierzytelnianie użytkowników.

- Wdrażanie zabezpieczeń, na przykład oprogramowania wykrywającego włamania, oprogramowania antywirusowego, oprogramowania weryfikującego integralność plików wszędzie tam, gdzie jest to technicznie możliwe, aby ograniczyć możliwość wprowadzenia złośliwego oprogramowania, powstrzymać jego rozprzestrzenianie się, zmniejszyć narażenie systemów OT na złośliwe oprogramowanie i uniemożliwić wykorzystanie ich w celu dalszego rozprzestrzeniania złośliwego oprogramowania w ramach systemu, a także pomiędzy systemami oraz do innych systemów.
- Stosowanie zabezpieczeń takich jak szyfrowanie bądź skróty kryptograficzne w przypadku przechowywania danych OT i komunikacji.
- Szybkie wdrażanie poprawek bezpieczeństwa po ich przetestowaniu w rzeczywistych warunkach na systemie testowym przed instalacją w systemie OT, jeśli jest to możliwe.
- Śledzenie i monitorowanie ścieżek audytu w krytycznych obszarach systemu OT.
- Stosowanie niezawodnych i bezpiecznych protokołów i usług sieciowych tam, gdzie jest to możliwe.

Współpraca między NIST i specjalistami zajmującymi się technologiami operacyjnymi w sektorze publicznym i prywatnym zaowocowała opracowaniem szczegółowych wytycznych dotyczących stosowania zabezpieczeń opisanych w publikacji NIST (SP) 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* [SP800-53r5] w systemach OT. Niniejszy dokument stanowi próbę przeniesienia tych wytycznych na grunt polski w ramach Narodowych Standardów Cyberbezpieczeństwa. Wytyczne zostały opisane w Załączniku F do niniejszego dokumentu.

Choć wiele zabezpieczeń opisanych w dokumencie NSC 800-53 [NSC 800-53]może zostać zastosowane do systemów OT w istniejącej formie, niektóre z nich wymagają interpretacji dostosowanej do wymogów systemów OT lub zastosowania rozszerzenia, które może przybrać jedną z poniższych form:

- **Omówienie kontekstu systemów OT** jest źródłem dodatkowego bezpieczeństwa na temat stosowania środków bezpieczeństwa oraz zabezpieczeń rozszerzonych w systemach OT oraz środowiskach, w których działają te wyspecjalizowane

systemy. Wytyczne zawierają również informacje o tym, dlaczego dany środek bezpieczeństwa lub dane zabezpieczenie rozszerzone mogą nie być przeznaczone do wdrożenia w niektórych środowiskach OT lub mogą wymagać dodatkowego przystosowania, tj. zastosowania procedury ustalania zakresu działania systemu lub zabezpieczeń kompensacyjnych. Omówienie kontekstu systemów OT nie zastępuje wytycznych uzupełniających zawartych w dokumencie NSC 800-53 [NSC 800-53].

- **Zabezpieczenia rozszerzone** stanowią rozszerzenia podstawowych środków bezpieczeństwa, których wdrożenie może być wymagane w przypadku niektórych systemów OT.

Najskuteczniejszą metodą zabezpieczenia systemów OT jest wykorzystanie zalecanych przez podmioty branżowe praktyk oraz wdrożenie proaktywnych, opartych na współpracy działań kadry kierowniczej, inżynierów i operatorów systemów OT, specjalistów IT oraz zaufanego doradcy OT. Zespół ten powinien w swoich działaniach wykorzystywać informacje oparte na źródłach rządowych, branżowych, informacjach przekazywanych przez dostawców oraz standardach wymienionych w Załączniku D do niniejszego dokumentu.

1. WPROWADZENIE

1.1. CEL I ZAKRES

Celem niniejszego dokumentu jest przedstawienie wytycznych dotyczących skutecznego wdrażania środków bezpieczeństwa w zakresie technologii operacyjnych (OT)[4], które uwzględniają wyjątkowe wymogi dotyczące osiągów, wydajności, niezawodności i bezpieczeństwa. Dokument obejmuje omówienie systemów technologii operacyjnej oraz typowych topologii systemów, wskazuje typowe zagrożenia oraz podatności występujące w tych systemach, a także wymienia zalecane środki przeciwdziałania pozwalające na ograniczenie związanego z nimi ryzyka. Ponadto obejmuje on rozszerzenie zabezpieczeń opisanych w publikacji specjalnej NIST (SP) 800-53, Rev. 5 [SP800-53r5] oraz dokumencie NSC 800-53 [NSC 800-53], które pozwalają na dostosowanie ich do wyjątkowych cech technologii operacyjnych. Pomimo tego, że treść niniejszego dokumentu opisuje kontekst dotyczący zabezpieczeń, poszczególne zabezpieczenia zostały opracowane w taki sposób, by zapoznanie się z jego treścią nie było konieczne do ich wdrożenia.

Ze względu na fakt, że istnieje wiele rodzajów technologii operacyjnych charakteryzujących się różnymi poziomami potencjalnego ryzyka i wpływu, niniejszy dokument zawiera listę wielu metod i technik zabezpieczania systemów OT. Niniejszy dokument nie powinien być wykorzystywany wyłącznie w roli listy kontrolnej zabezpieczeń określonego systemu. Zachęcamy czytelników do przeprowadzenia ocen ryzyka dotyczących wykorzystywanych systemów i dostosowania zaleceń, wytycznych i rozwiązań do indywidualnych wymogów w zakresie bezpieczeństwa, a także biznesowych i operacyjnych. Zakres stosowania podstawowych koncepcji związanych z zabezpieczaniem systemów OT przedstawionych w niniejszym dokumencie jest stale rozszerzany.

[4] Skrót „OT” może odnosić się zarówno do „technologii operacyjnej” lub „technologii operacyjnych”. Właściwe rozwinięcie skrótu w treści niniejszego dokumentu wynika z kontekstu, w jakim został użyty, zwłaszcza słów w liczbie pojedynczej lub mnogiej.

1.2. ODBIORCY

Niniejszy dokument zawiera szczegółowe informacje dotyczące systemów OT. Czytelnicy tego dokumentu powinni być zaznajomieni z ogólnymi koncepcjami dotyczącymi obszaru bezpieczeństwa komputerowego i protokołami komunikacyjnymi wykorzystywanymi między innymi w sieciach, ze względu na to, że dokument ten jest dokumentem technicznym. Jego treść obejmuje jednak informacje kontekstowe niezbędne do zrozumienia omawianych zagadnień.

Wśród odbiorców i czytelników niniejszego dokumentu znajdują się następujące osoby:

- Inżynierowie ds. nadzoru technicznego, integratorzy i architekci, którzy projektują lub wdrażają systemy OT.
- Administratorzy systemów, inżynierowie i inni specjaliści ds. technologii informacyjnych, którzy pełnią rolę administratorów systemów OT, a także odpowiadają za instalowanie poprawek lub wdrażanie zabezpieczeń w tych systemach.
- Konsultanci ds. bezpieczeństwa, którzy przeprowadzają oceny bezpieczeństwa i testy penetracyjne systemów OT.
- Przedstawiciele kadr kierowniczych odpowiedzialni za systemy OT.
- Przedstawiciele kierownictwa wyższego szczebla, którzy muszą zrozumieć zagrożenia dotyczące systemów OT, aby skutecznie uzasadnić i przeprowadzić wdrożenie programu cyberbezpieczeństwa OT.
- Badacze i analitycy, którzy badają unikalne potrzeby w zakresie bezpieczeństwa systemów OT.
- Dostawcy opracowujący produkty wdrażane w ramach systemów OT.

1.3. STRUKTURA DOKUMENTU

Treść niniejszego dokumentu jest podzielona na następujące główne rozdziały:

- Rozdział 2 zawiera omówienie zagadnienia technologii operacyjnych, w tym porównanie systemów OT i IT.

- W rozdziale 3 omówiono proces opracowania i wdrożenia programu cyberbezpieczeństwa OT w celu ograniczenia ryzyka związanego z podatnościami opisanymi w Załączniku C.
- Rozdział 4 opisuje zagadnienia zarządzania ryzykiem w obszarze bezpieczeństwa technologii operacyjnych oraz stosowania ram zarządzania ryzykiem do systemów OT.
- Rozdział 5 opisuje zalecenia dotyczące integracji zabezpieczeń z architekturami sieci typowymi dla systemów OT, kładąc szczególny nacisk na praktyki segmentacji i separacji sieci.
- Rozdział 6 zawiera wskazówki dotyczące stosowania ram cyberbezpieczeństwa do systemów OT.
- Rozdział Referencje zawiera listę publikacji wykorzystanych w procesie opracowywania niniejszego dokumentu.

Niniejsze wytyczne obejmują także szereg załączników, które zawierają następujące informacje pomocnicze:

- Załącznik A przedstawia listę akronimów i skrótów wykorzystywanych w treści niniejszego dokumentu.
- Załącznik B zawiera glosariusz terminów wykorzystywanych w treści niniejszego dokumentu.
- Załącznik C zawiera omówienie źródeł zagrożeń dla systemów OT, a także podatności oraz uwarunkowań zwiększających narażenie, zdarzenia powodujące zagrożenia oraz incydenty.
- Załącznik D obejmuje listy i opisy organizacji, badań i działań związanych z bezpieczeństwem OT.
- Załącznik E obejmuje omówienie zabezpieczeń oraz narzędzi zwiększających zdolność do ochrony systemów OT.
- Załącznik F zawiera rozszerzenia zabezpieczeń opisanych w dokumentach NIST SP 800-53, Rev. 5 [SP800-53r5] oraz NSC 800-53 [NSC 800-53] w zakresie technologii operacyjnych, w tym listę środków bezpieczeństwa oraz zabezpieczeń rozszerzonych, a także dodatkowe wytyczne odnoszące się do systemów OT.

2. OMÓWIENIE SYSTEMÓW OT

Pojęcie technologii operacyjnej (OT)[5] odnosi się do systemów i urządzeń, które wchodzą w interakcje ze środowiskiem fizycznym lub zarządzają urządzeniami wchodzącymi w interakcje ze środowiskiem fizycznym. Takie systemy oraz urządzenia wykrywają lub wywołują zmiany poprzez monitorowanie lub kontrolowanie urządzeń, procesów i zdarzeń. Przykłady takich rozwiązań obejmują przemysłowe systemy sterowania, systemy automatyki budynków, systemy transportowe, systemy kontroli dostępu fizycznego, systemy monitorowania i systemy pomiarowe działające w środowiskach fizycznych.

Systemy OT obejmują urządzenia sterujące (na przykład elektryczne lub mechaniczne), zgodne ze specyfikacjami dotyczącymi pożądanych efektów lub oczekiwanej wydajności. Tego rodzaju systemy sterowania mogą zostać skonfigurowane na jeden z trzech sposobów:

- *Sterowanie w pętli otwartej*: Rezultat jest uzależniony od ustalonych ustawień.
- *Sterowanie w pętli zamkniętej*: Rezultat wpływa na działania w taki sposób, by osiągnąć założony cel działania.
- *Sterowanie w trybie ręcznym*: System jest w całości kontrolowany przez operatorów.

W tym rozdziale znajduje się omówienie kilku rodzajów popularnych systemów OT, w tym systemów kontroli nadzorczej i pozyskiwania danych (SCADA), rozproszonych systemów sterowania (DCS), programowalnych sterowników logicznych (PLC), systemów automatyki budynków (BAS), systemów kontroli dostępu fizycznego (PACS) oraz systemów przemysłowego Internetu rzeczy (IIoT). Zawarte w treści rozdziału schematy przedstawiają topologię sieci, połączenia, komponenty i protokoły, które są zwykle wykorzystywane w powiązaniu z poszczególnymi systemami. Celem przedstawienia tych przykładów jest próba ustalenia zakresów pojęć dotyczących topologii. Rzeczywiste wdrożenia takich systemów sterowania mogą obejmować kombinacje przedstawionych koncepcji, które powodują zacieranie granic pomiędzy

[5] Zobacz także: https://csrc.nist.gov/Projects/operational-technology-security.

nimi. W czasie lektury należy mieć na uwadze, że diagramy przedstawione w rozdziale 2 nie dotyczą zagadnienia zabezpieczenia systemów OT. Architektura bezpieczeństwa oraz środki bezpieczeństwa zostały omówione odpowiednio w rozdziale 5 i Załączniku F do niniejszego dokumentu.

2.1. ROZWÓJ SYSTEMÓW OT

Wiele współczesnych systemów OT zawdzięcza swój kształt oraz wykorzystywaną architekturę łączeniu nowych możliwości z dziedziny technologii informacyjnych z istniejącymi systemami fizycznymi, co skutkowało zastępowaniem lub uzupełnianiem fizycznych mechanizmów sterowania. W ten sposób wbudowane cyfrowe elementy sterujące zastąpiły analogowe mechaniczne elementy sterujące w maszynach wirujących i silnikach. Zmniejszenie kosztów przy jednoczesnym zwiększeniu wydajności przyczyniły się do popularyzacji tych rozwiązań, co zaowocowało powstaniem wielu „inteligentnych" technologii, takich jak: inteligentne sieci elektryczne, inteligentne rozwiązania transportowe, inteligentne budynki, inteligentne linie produkcyjne czy urządzenia Internetu rzeczy. Choć takie działania doprowadziły do poprawy łączności między tymi systemami, zwiększyły ich krytyczność i oczekiwania związane z możliwościami adaptacji, odporności oraz bezpieczeństwa.

Rozwój systemów OT wciąż prowadzi do opracowywania nowych rozwiązań i możliwości, jednocześnie zapewnia długie cykle życia, które stanowią jeden z wyróżników tych systemów. Połączenie możliwości systemów informacyjnych z systemami fizycznymi powoduje jednak konieczność uwzględnienia szeregu zjawisk mających wpływ na bezpieczeństwo. Modele inżynieryjne i analizy są stale rozwijane, by uwzględnić te nowe możliwości oraz zależności dotyczące bezpieczeństwa, prywatności i wpływu na środowisko.

2.2. SYSTEMY OPARTE NA OT I ICH WSPÓŁZALEŻNOŚCI

Technologie operacyjne (OT) są wykorzystywane w wielu sektorach i stanowią element wielu infrastruktur. Niektóre z nich są uznawane za sektory i infrastruktury krytyczne – ich lista znajduje się poniżej. OT stanowią element wszystkich infrastruktur krytycznych, tworzą też ważny element sektorów, których nazwy zostały zapisane pogrubioną czcionką.

- **Sektor chemiczny**
- **Sektor obiektów komercyjnych**
- Sektor łączności
- **Sektor produkcji krytycznej**
- **Sektor zapór wodnych**
- **Sektor przemysłu obronnego**
- **Sektor służb ratowniczych**
- **Sektor energetyczny**
- Sektor usług finansowych
- **Sektor żywności i rolnictwa**
- **Sektor obiektów rządowych**
- **Sektor opieki zdrowotnej i zdrowia publicznego**
- Sektor technologii informacyjnych
- **Sektor reaktorów jądrowych, materiałów i odpadów nuklearnych**
- **Sektor systemów transportowych**
- **Sektor systemów wodno-kanalizacyjnych**

Technologie operacyjne mają kluczowe znaczenie dla funkcjonowania infrastruktury krytycznej państwa, często charakteryzującej się wysokim stopniem wzajemnych połączeń i współzależności. Dotyczy to zarówno połączeń fizycznych, jak i realizowanych za pośrednictwem szeregu technologii informacyjnych i komunikacyjnych. W tym kontekście warto nadmienić, że choć organy rządowe odpowiadają za zarządzanie i obsługę wielu wymienionych powyżej elementów infrastruktury krytycznej państwa, część takich systemów znajduje się w rękach prywatnych, a za ich utrzymanie odpowiadają ich właściciele i operatorzy. Ponadto infrastruktura krytyczna często jest określana mianem „systemu systemów” ze względu na współzależności istniejące między różnymi sektorami przemysłu i wzajemne powiązania między partnerami biznesowymi. [Peerenboom], [Rinaldi]

Wystąpienie incydentu dotyczącego jednej z tych infrastruktur może w związku z tym bezpośrednio i pośrednio wpłynąć na inne infrastruktury poprzez kaskadowe i eskalujące awarie.

Przykładem mogą być sektory przesyłu i dystrybucji energii elektrycznej, które wykorzystują geograficznie rozproszone systemy sterowania SCADA w celu obsługi ściśle połączonych i dynamicznych systemów należących do tysięcy publicznych i prywatnych dostawców energii oraz spółdzielni energetycznych dostarczających energię elektryczną użytkownikom końcowym. Niektóre z tych systemów SCADA monitorują i kontrolują dystrybucję energii elektrycznej dzięki gromadzonym danym i poleceniom przesyłanym z centrali do oddalonych geograficznie terenowych stacji sterowania. Systemy SCADA są również wykorzystywane do monitorowania i kontrolowania systemów dystrybucji wody, ropy naftowej i gazu ziemnego, w tym rurociągów, statków, pojazdów ciężarowych, pojazdów szynowych i kanalizacji.

Zarówno systemy SCADA, jak i rozproszone systemy sterowania, są często połączone w sieci. Za przykład mogą posłużyć stacje kontroli mocy oraz elektrownie. Pomimo tego, że praca elektrowni jest kontrolowana przez rozproszony system sterowania, musi on komunikować się z systemem SCADA w celu dostosowania wytwarzanej mocy do wymogów systemów przesyłowych i dystrybucyjnych.

Energia elektryczna jest uznawana za źródło większości problemów powodujących zakłócenia w działaniu współzależnych infrastruktur krytycznych. Skutkiem mogą być awarie kaskadowe zainicjowane na przykład przez zakłócenie mikrofalowej sieci komunikacyjnej używanej w systemie SCADA odpowiadającym za obsługę sieci przesyłowej energii elektrycznej. Brak możliwości monitorowania i sterowania może spowodować wyłączenie dużej elektrowni i doprowadzić do utraty zasilania w stacji przesyłowej. Taka awaria może z kolei spowodować poważne zaburzenie równowagi w sieci, wywołując kaskadową awarię w całej sieci energetycznej skutkującej przerwami w dostawie prądu na dużym obszarze, które mogą potencjalnie wpłynąć na produkcję ropy naftowej i gazu ziemnego, działanie rafinerii i systemów uzdatniania wody, działanie systemów odprowadzania ścieków i rurociągów, które wykorzystują energię elektryczną.

2.3. DZIAŁANIE, ARCHITEKTURY I KOMPONENTY SYSTEMÓW OT

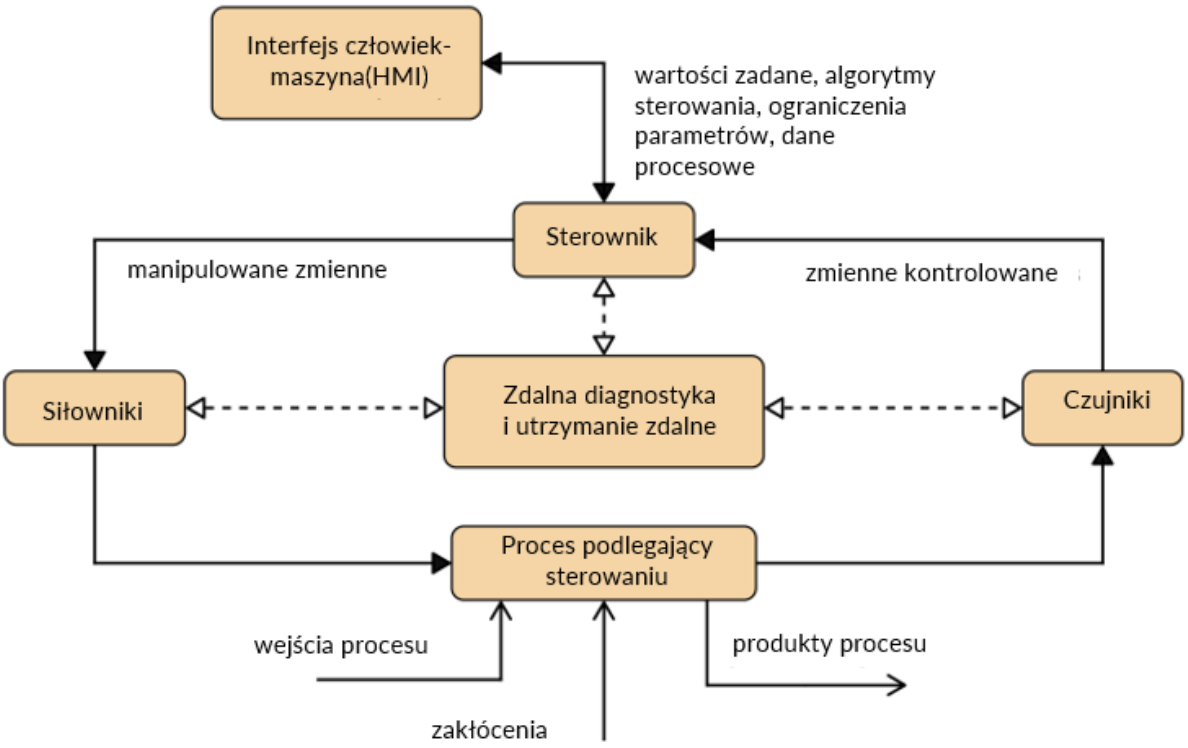
Przedstawiona na **rysunku 1** typowa architektura systemu OT obejmuje liczne pętle sterowania, interfejsy człowiek-maszyna oraz narzędzia do zdalnej diagnostyki i konserwacji. System opiera się na szeregu protokołów sieciowych wykorzystywanych w ramach wielowarstwowych architektur sieciowych. Niektóre procesy krytyczne mogą również obejmować systemy bezpieczeństwa.

Pętla sterowania wykorzystuje czujniki, siłowniki i sterowniki do sterowania procesem. *Czujnik* to urządzenie, które dokonuje pomiaru pewnej właściwości fizycznej, a następnie wysyła te informacje w formie *kontrolowanych zmiennych* do sterownika. Sterownik interpretuje pomiary i generuje odpowiednie *zmienne manipulowane* w oparciu o algorytm sterowania i docelowe wartości zadane, które przekazuje do siłowników. *Siłowniki* – na przykład zawory sterujące, wyłączniki, przełączniki i silniki – są używane do bezpośredniego wpływania na kontrolowany proces na podstawie poleceń przekazywanych przez sterownik.

W typowym systemie monitorowania zwykle nie występują bezpośrednie połączenia między czujnikami a siłownikami. Wartości z czujników są przesyłane do stacji monitorującej i analizowane przez człowieka. Tego rodzaju systemy nadal można zaklasyfikować do grona systemów OT (pomimo tego, że nadal ich część stanowią ludzie), ponieważ celem systemu monitorowania jest wykrycie i ograniczenie skutków zdarzenia lub stanu. Przykładem takiego rozwiązania mogą być drzwi z czujnikiem ostrzegającym o ich sforsowaniu, który spowoduje wysłanie pracowników działu ochrony w celu sprawdzenia sytuacji. Inne przykłady obejmują czujniki środowiskowe wykrywające wysoką temperaturę w serwerowni, dzięki którym pracownicy centrum sterowania mogą włączyć dodatkowy klimatyzator.

Operatorzy i specjaliści używają *interfejsów człowiek-maszyna (ang. human-machine interfaces – HMI)* w celu monitorowania i konfigurowania wartości zadanych, algorytmów sterowania oraz dostosowywania i ustalania parametrów sterownika. Interfejsy wyświetlają także informacje o stanie procesu i dane historyczne. *Narzędzia diagnostyczne i konserwacyjne* pozwalają na zapobieganie awariom, a także ich wykrywanie oraz usuwanie.

W niektórych przypadkach pętle sterowania mogą być zagnieżdżone bądź kaskadowe – w takich sytuacjach wartość zadana jednej z nich jest oparta na zmiennej procesowej wynikającej z innej pętli. Pętle poziomu nadzorczego i pętle niższego poziomu działają w sposób ciągły przez cały czas trwania procesu z czasami cyklu wynoszącymi od kilku milisekund do kilku minut.



Rysunek 1. Podstawowy mechanizm działania typowego systemu OT

2.3.1. ZAGADNIENIA ZWIĄZANE Z PROJEKTOWANIEM SYSTEMU OT

Kształt projektu systemu OT jest uzależniony od wielu czynników, między innymi od tego, czy stosowana topologia jest oparta na rozwiązaniach typu SCADA, rozproszonych systemach sterowania lub sterownikach PLC. W tym rozdziale zostały opisane najważniejsze czynniki, które wpływają na decyzje projektowe dotyczące sterowania, komunikacji, niezawodności i redundancji w systemach OT. Ze względu na fakt, że czynniki te mają duży wpływ na projekt systemu OT, pozwalają one także na określenie wymogów systemu w zakresie bezpieczeństwa.

- **Bezpieczeństwo fizyczne.** Systemy muszą być w stanie wykrywać wystąpienie niebezpiecznych warunków i uruchamiać działania w celu przywrócenia

bezpieczeństwa. W przypadku większości procesów o krytycznym znaczeniu dla bezpieczeństwa niezbędny jest ludzki nadzór i sterowanie potencjalnie niebezpiecznym procesem.

- **Wymagania dotyczące sterowania czasem (*ang. control timing*).** Cechą procesów systemowych jest szeroki zakres wymagań związanych z czasem, w tym dotyczących szybkości, regularności, ciągłości i synchronizacji. Ze względu na to, że ludzie nie są w stanie niezawodnie i konsekwentnie spełniać tych wymagań, konieczne może być zastosowanie zautomatyzowanych sterowników. Niektóre systemy mogą wymagać wykonywania obliczeń w bliskiej odległości od czujników i siłowników, aby zmniejszyć opóźnienia w komunikacji i wykonywać niezbędne działania w odpowiednim czasie.
- **Rozmieszczenie geograficzne.** Systemy charakteryzują się różnym stopniem rozproszenia – obejmują zarówno systemy o ograniczonym zasięgu (na przykład lokalne procesy sterowane przez sterownik PLC), jak i duże, rozproszone systemy (na przykład rurociągi transportujące ropę naftową czy sieci elektroenergetyczne). Większe rozproszenie zwykle wiąże się z zapotrzebowaniem na wykorzystanie rozległych sieci komunikacyjnych, opartych na dzierżawionych liniach, komutacji kanałów[6] bądź pakietów, a także technologiach komunikacji mobilnej.
- **Hierarchia.** Celem kontroli nadzorczej jest zapewnienie centralnej lokalizacji, która może gromadzić dane z wielu jednostek w celu wspierania decyzji w zakresie sterowania opartych na aktualnym stanie systemu. Systemy hierarchicznego lub scentralizowanego sterowania są często stosowane w celu zapewnienia operatorom kompleksowego wglądu w działanie całego systemu.
- **Złożoność sterowania.** Proste sterowniki i wstępnie skonfigurowane algorytmy mogą często realizować funkcje sterowania. Bardziej złożone systemy (na przykład system kontroli ruchu lotniczego) wymagają udziału ludzi, których celem jest zapewnianie, że wszystkie działania prowadzą do osiągnięcia celów systemu.

[6] Także: komutacja łączy lub komutacja obwodów.

- **Dostępność.** Systemy o wysokich wymaganiach w zakresie dostępności i czasu pracy mogą wymagać większego poziomu nadmiarowości lub alternatywnych rozwiązań we wszystkich obszarach związanych z komunikacją i sterowaniem.
- **Skutki awarii.** Awaria sterowania może mieć bardzo różny wpływ na różne obszary. Od systemów charakteryzujących się większym wpływem lub wyższym poziomem krytyczności oczekuje się odporności na awarie, realizowanej dzięki nadmiarowym urządzeniom sterującym oraz możliwości działania w stanie zdegradowanym.

2.3.2. SYSTEMY SCADA

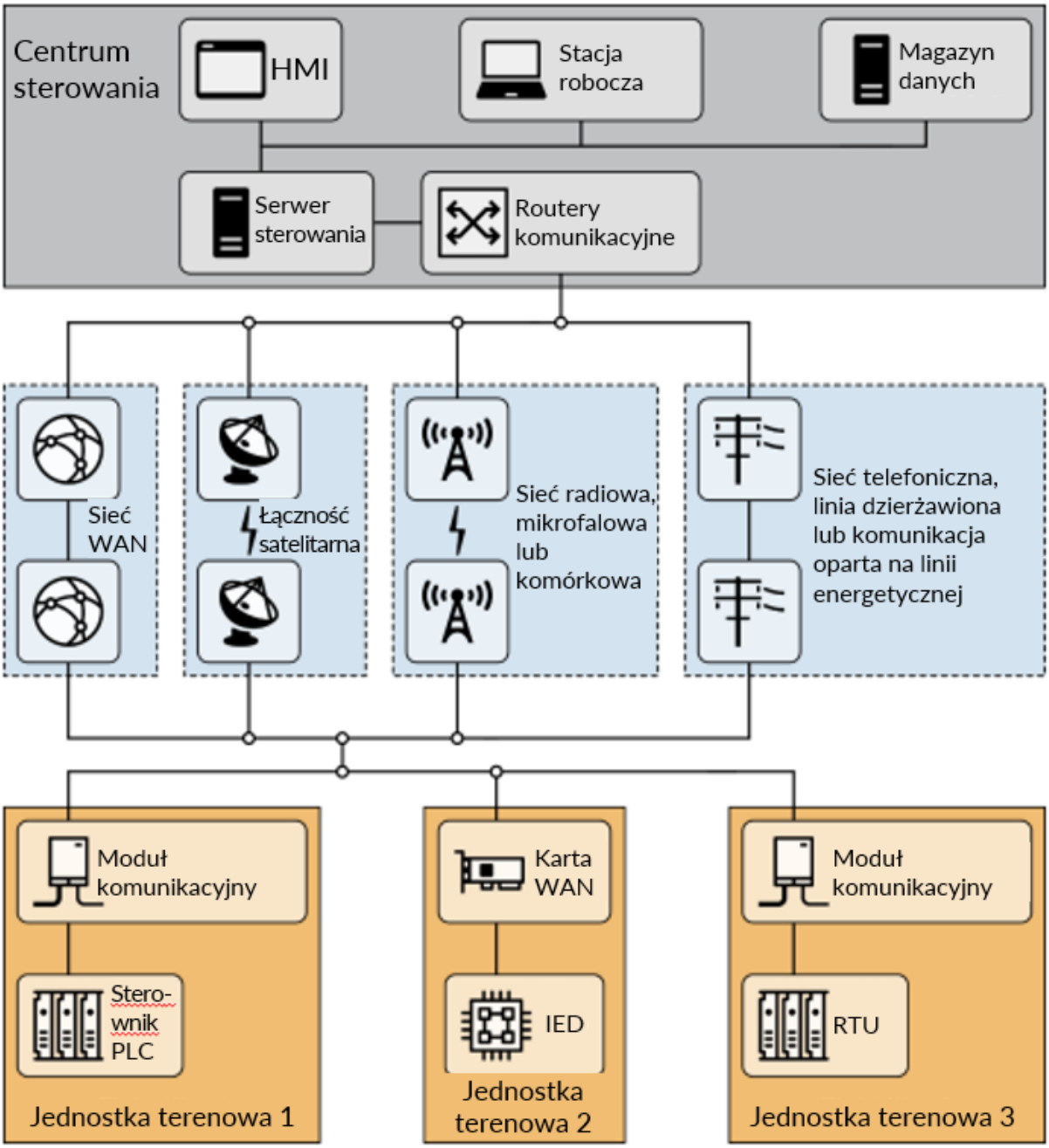
Systemy kontroli nadzorczej i pozyskiwania danych (*ang. Supervisory control and data acquisition – SCADA*) są wykorzystywane do sterowania rozproszonymi zasobami, w przypadku których scentralizowane gromadzenie danych jest równie ważne jak procesy sterowania. [Bailey] [Boyer] Systemy te mają zastosowanie w systemach dystrybucji wody i odprowadzania ścieków, rurociągach transportujących ropę naftową i gaz ziemny, systemach przesyłu i dystrybucji energii elektrycznej oraz systemach transportu kolejowego i transportu publicznego. W skład systemów SCADA wchodzą systemy gromadzenia i przesyłania danych, a także oprogramowanie HMI, które pozwalają na zbudowanie scentralizowanego systemu monitorowania i kontroli wielu elementów wejściowych i wyjściowych procesu. Systemy SCADA są wykorzystywane w celu zbierania informacji z urządzeń zainstalowanych w zdalnych lokalizacjach, przesyłania ich do centrum sterowania i prezentowania informacji operatorowi w formie graficznej lub tekstowej, co umożliwia monitorowanie lub kontrolowanie całego systemu z centralnej lokalizacji w czasie zbliżonym do rzeczywistego. w zależności od stopnia zaawansowania i konfiguracji danego systemu, sterowanie każdym systemem, procesem lub zadaniem może odbywać się automatycznie lub na podstawie poleceń operatora.

Typowe urządzenia sprzętowe wykorzystywane w takich systemach obejmują serwer sterowania umieszczony w centrum sterowania, urządzenia komunikacyjne (na przykład oparte na: częstotliwościach radiowych, liniach telefonicznych, kablach lub łączności satelitarnej) oraz jedno lub wiele rozproszonych geograficznie urządzeń zainstalowanych w zdalnych lokalizacjach, wśród których można wymienić zdalne

urządzenia końcowe (*ang. remote terminal units – RTU*) oraz sterowniki PLC, które służą do sterowania siłownikami bądź monitorowania czujników. Serwer sterowania przechowuje i przetwarza dane wejściowe i wyjściowe przekazywane przez zdalne urządzenia końcowe, które (podobnie jak sterownik PLC) mogą odpowiadać za sterowanie procesem na poziomie lokalnym. Urządzenia komunikacyjne umożliwiają przesyłanie informacji i danych między serwerem sterowania a urządzeniami RTU lub sterownikami PLC. Oprogramowanie jest skonfigurowane w taki sposób, by przekazywać informacje na temat elementów wymagających monitorowania, dopuszczalnych zakresów parametrów oraz czynności, które należy wykonać w przypadku pomiaru zmiennej procesowej poza zakresem dopuszczalnych wartości. Inteligentne urządzenia elektroniczne (*ang. intelligent electronic device – IED*), takie jak przekaźniki zabezpieczające, mogą komunikować się bezpośrednio z serwerem sterującym. Lokalne urządzenie RTU może także gromadzić dane z urządzenia IED w celu przekazania ich do serwera sterującego. Urządzenia IED zapewniają możliwości bezpośredniego monitorowania sprzętu i czujników oraz sterowania. Urządzenia IED mogą być bezpośrednio odpytywane i kontrolowane przez serwer sterujący. Ponadto większość takich urządzeń jest wyposażona w lokalne oprogramowanie, które umożliwia działanie w przypadku braku bezpośrednich poleceń z centrali sterowania. Systemy SCADA są zwykle projektowane w sposób zapewniający odporność na awarie dzięki dużemu poziomowi nadmiarowości, który może jednak nie zapewnić wystarczającej ochrony w przypadku złośliwego ataku.

Rysunek 2 przedstawia elementy oraz omówienie konfiguracji typowego systemu SCADA. Centrala sterowania przedstawiona w górnej części schematu obejmuje serwer sterowania oraz routery odpowiedzialne za komunikację. Inne elementy występujące w centrali sterowania obejmują interfejs człowiek-maszyna, stacje robocze i serwer danych połączone siecią lokalną (*ang. local area network – LAN*). Centrala sterowania gromadzi i rejestruje dane zbierane przez urządzenia zdalne, wyświetla informacje na interfejsie HMI i może inicjować działania w oparciu o wykryte zdarzenia. Centrala sterowania odpowiada także za scentralizowane alarmowanie, analizę trendów i sprawozdawczość.

Urządzenia zdalne przedstawione w dolnej części **Rysunku 2** odpowiadają za sterowanie siłownikami i monitorowanie czujników. Takie urządzenia są często wyposażone w funkcję zdalnego dostępu, aby umożliwić operatorom przeprowadzanie zdalnej diagnostyki oraz napraw, zwykle za pośrednictwem oddzielnego modemu lub połączenia z rozległą siecią informatyczną (*ang. wide area network – WAN*). Zarówno standardowe, jak i własnościowe protokoły komunikacyjne realizowane za pośrednictwem połączeń szeregowych i sieciowych, są wykorzystywane do przesyłania informacji między centralą sterowania a urządzeniami zdalnymi przy użyciu rozwiązań komunikacyjnych takich jak: linie telefoniczne, kable miedziane, światłowody lub częstotliwości radiowe (na potrzeby transmisji rozsiewczej, komunikacji mikrofalowej lub połączeń satelitarnych).

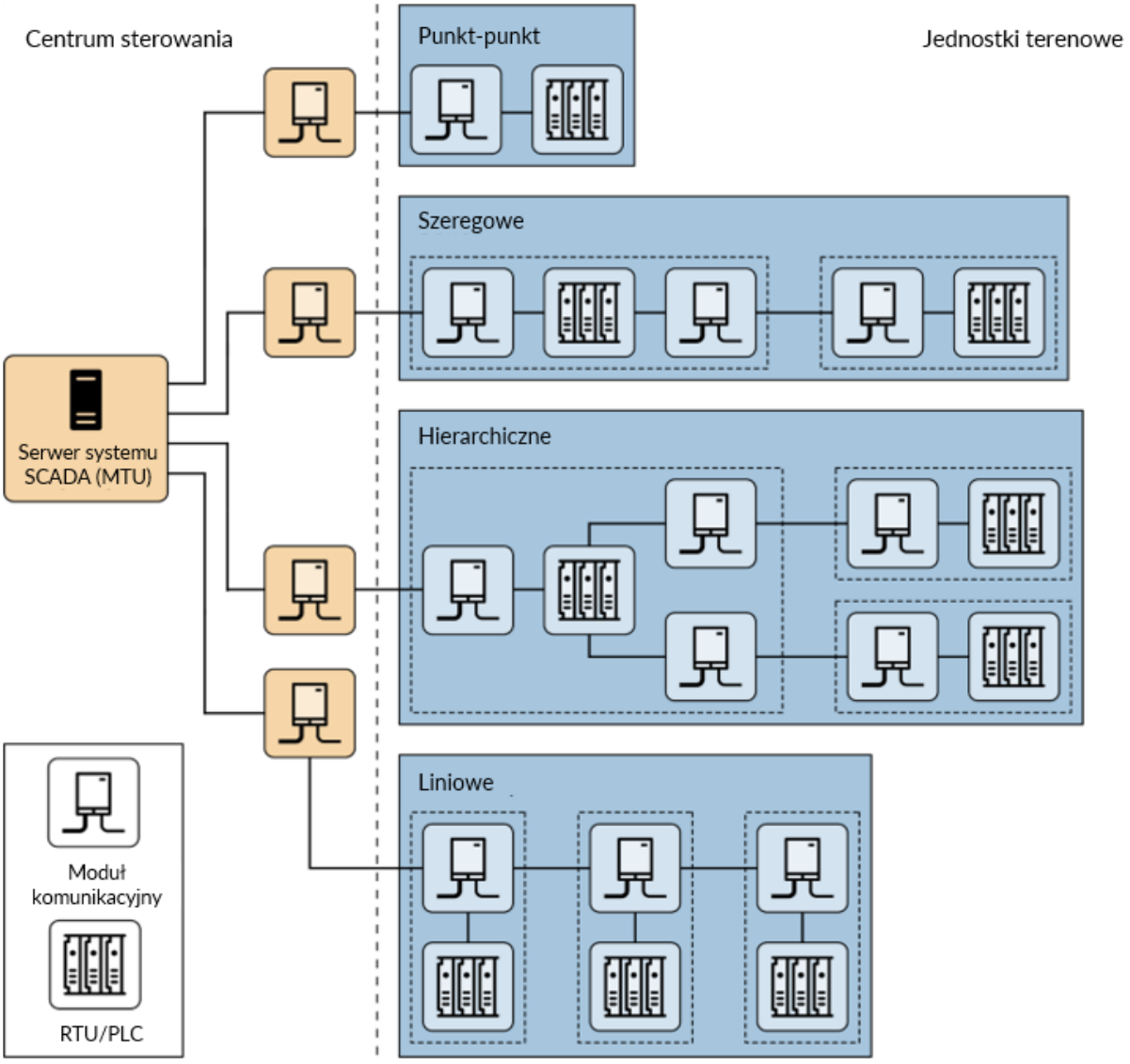


Rysunek 2. Konfiguracja typowego systemu SCADA przedstawiająca urządzenia centrali sterowania, urządzenia komunikacyjne oraz zdalne

Topologie systemów komunikacji wykorzystywanych w systemach SCADA różnią się w zależności od potrzeb danego rozwiązania. Przykłady topologii stosowanych w takich systemach zostały przedstawione na **Rysunku. 3**, który przedstawia topologie punkt-punkt, szeregowe, hierarchiczne oraz liniowe (wielopunktowe) [AGA12]. Z punktu widzenia funkcjonalności, połączenia punkt-punkt są najprostsze, jednak mogą być kosztowne ze względu na fakt, że każde połączenie wymaga

osobnego kanału. w topologii szeregowej liczba używanych kanałów jest zmniejszona, choć współdzielenie kanałów wpływa na wydajność i złożoność działania systemów SCADA. Wykorzystanie jednego kanału dla każdego urządzenia w topologiach hierarchicznych i liniowych skutkuje zmniejszoną przepustowością i zwiększoną złożonością systemu.

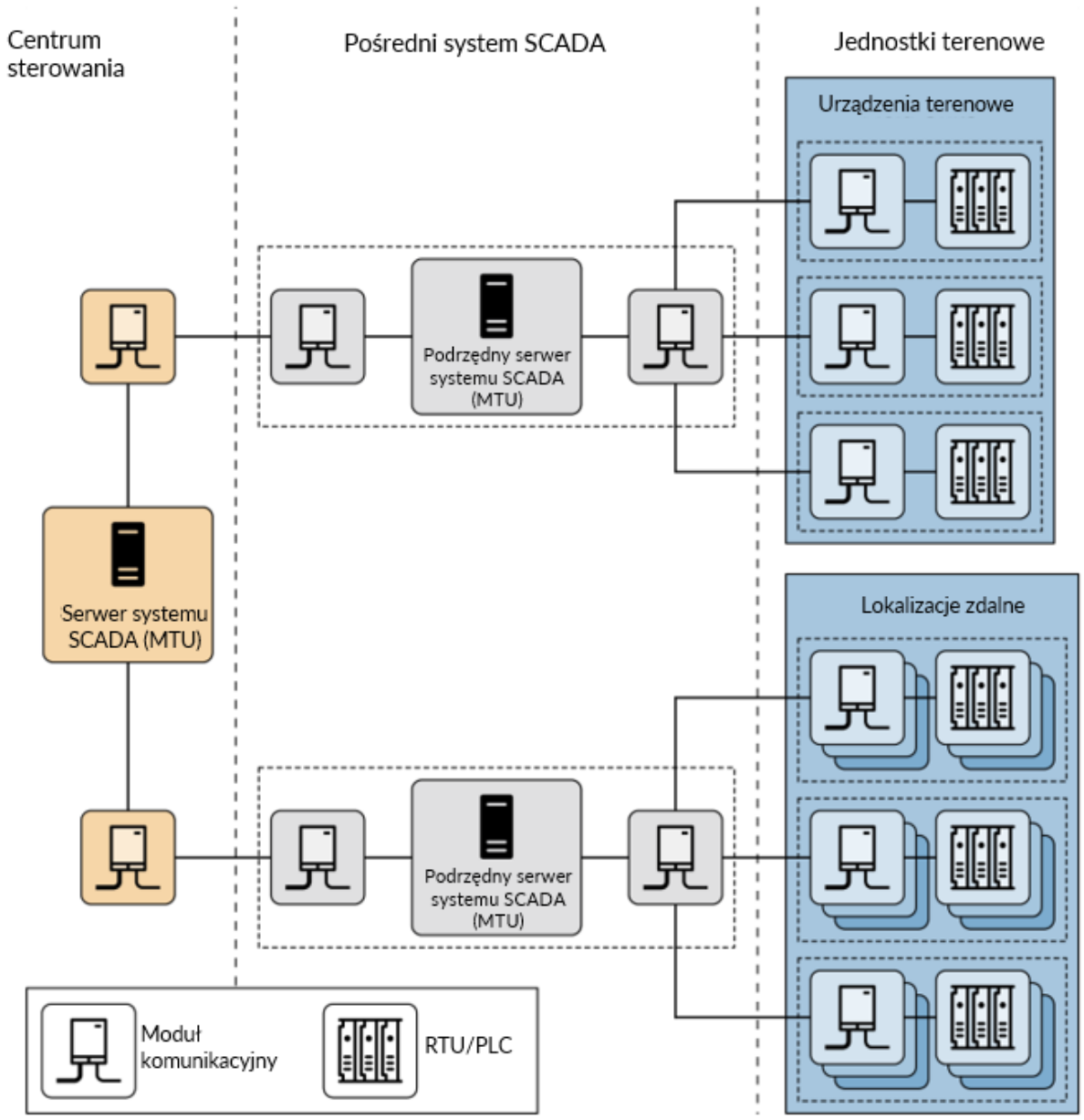
Cztery podstawowe topologie połączeń wykorzystywanych w systemach SCADA przedstawione na **Rysunku 3** mogą być dodatkowo rozszerzone dzięki wykorzystaniu urządzeń pozwalających na zarządzanie komunikacją oraz przełączanie i buforowania komunikatów.



Rysunek 3. Przykłady topologii komunikacji punkt-punkt, szeregowej, hierarchicznej oraz liniowej w systemach SCADA

Tłumaczenie

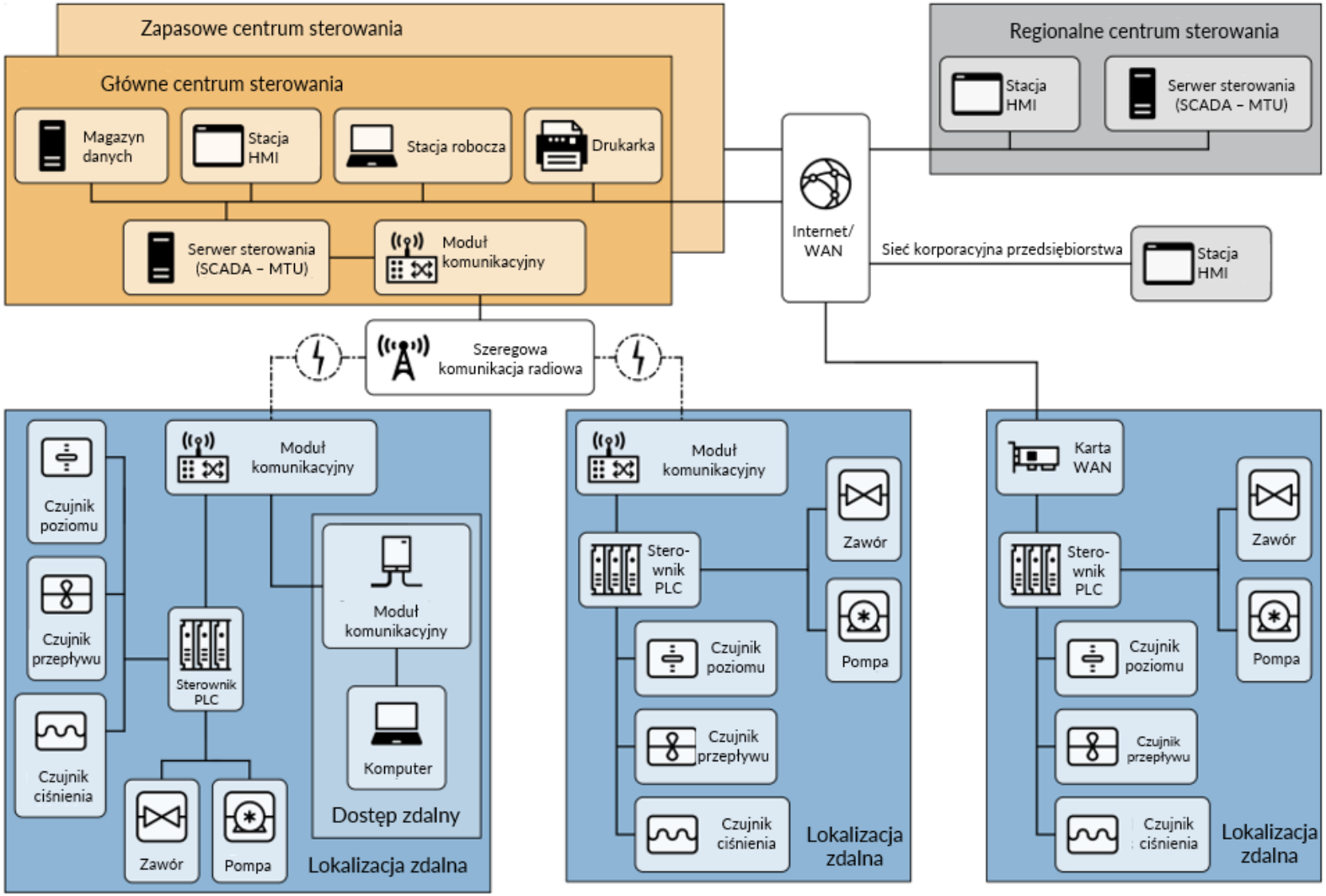
Rozległe systemy SCADA obejmujące setki urządzeń RTU często wykorzystują serwer podrzędny, który pozwala na odciążenie głównego serwera. Przykład tego rodzaju topologii został przedstawiony na **Rysunku 4**.



Rysunek 4. Przykładowa topologia systemu SCADA obsługującego dużą liczbę zdalnych urządzeń końcowych.

Rysunek 5 przedstawia przykładowe wdrożenie systemu SCADA, który składa się z głównej centrali sterowania i trzech urządzeń zdalnych. Zapasowa centrala sterowania zapewnia nadmiarowość na wypadek awarii centrali głównej. Do komunikacji między centralą sterowania a urządzeniami zdalnymi wykorzystywane są

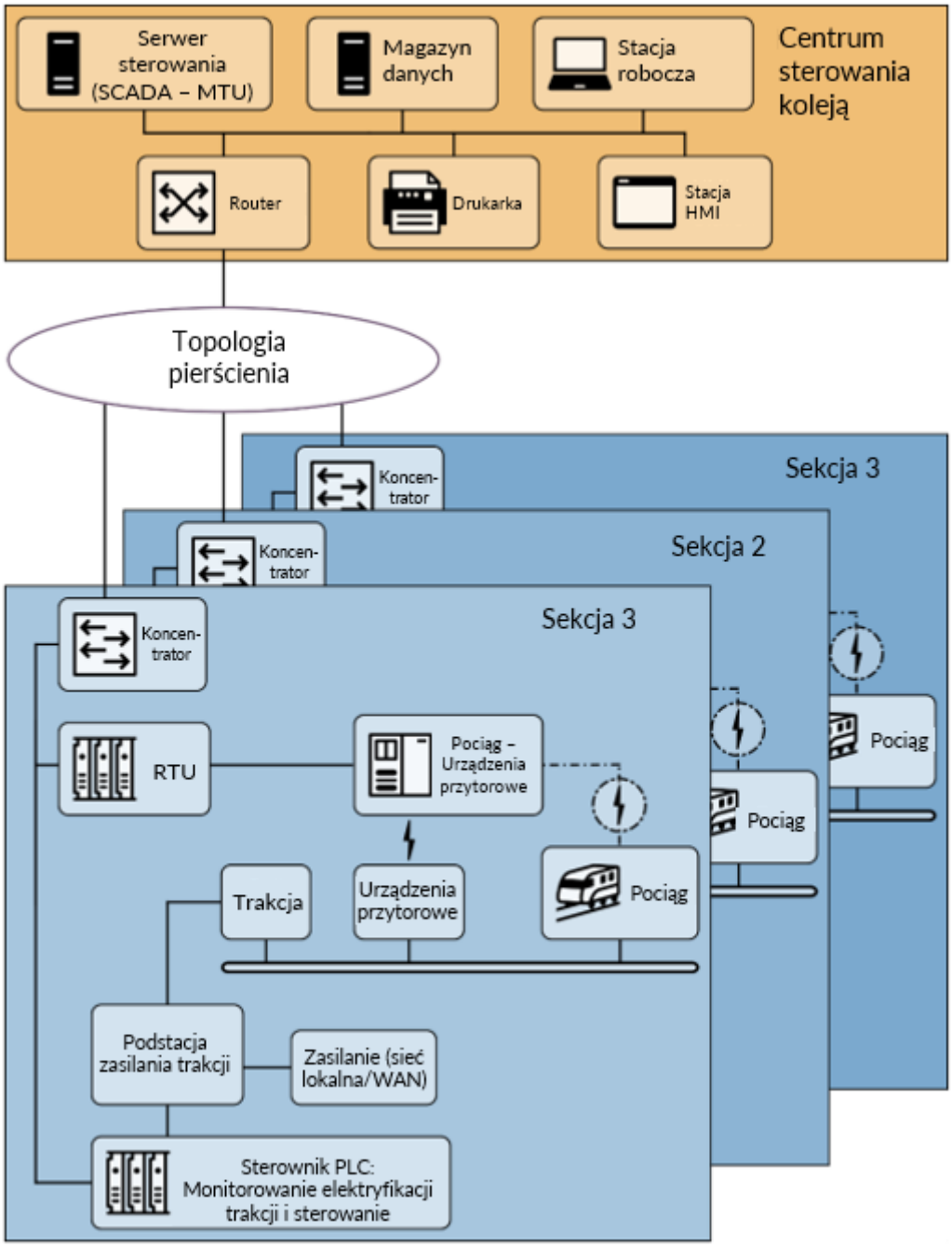
połączenia typu punkt-punkt; ponadto dwa połączenia opierają się na łączności radiowej w celu przekazywania danych telemetrycznych. Trzecie urządzenie zdalne znajduje się w pobliżu centrali sterowania i wykorzystuje sieć WAN na potrzeby komunikacji. Regionalna centrala sterowania znajduje się powyżej głównej centrali sterowania i zapewnia wyższy poziom kontroli nadzorczej. Za pośrednictwem sieci WAN możliwy jest dostęp do wszystkich centrali sterowania z poziomu sieci organizacji; ponadto istnieje możliwość uzyskania dostępu zdalnego do urządzeń zdalnych w celu rozwiązywania problemów i konserwacji. Główna centrala sterowania odpytuje zdalne urządzenia końcowe o dane w określonych odstępach czasu (na przykład co 5 sekund lub co minutę) i może wysyłać nowe ustawienia urządzeniom zgodnie z wymaganiami. Oprócz odpytywania i przesyłania poleceń wysokiego poziomu serwer sterowania śledzi również priorytetowe przerwania z rozproszonych systemów alarmowych.



Rysunek 5. Przykład wdrożenia kompleksowego systemu SCADA

Tłumaczenie

Rysunek 6 przedstawia przykładowe wdrożenie systemu SCADA wykorzystywanego na potrzeby monitorowania urządzeń kolejowych i sterowania ich działaniem. Przykład przedstawia centrum sterowania ruchem kolejowym, w którym znajduje się system SCADA, a także trzy odcinki systemu kolejowego. System SCADA odpytuje urządzenia działające wzdłuż odcinków systemu kolejowego w celu uzyskania informacji na temat stanu pociągów, systemów sygnalizacyjnych, systemów trakcyjnych oraz automatów biletowych. Informacje te są również przekazywane do konsol operatorów wyposażonych w interfejsy człowiek-maszyna w centrum sterowania ruchem kolejowym. System SCADA monitoruje polecenia wysokiego poziomu wydawane przez operatorów w centrum sterowania ruchem kolejowym i przesyła je do poszczególnych urządzeń. Ponadto system SCADA monitoruje warunki na poszczególnych odcinkach torów i wydaje polecenia w oparciu o te warunki (na przykład zatrzymanie pociągu, aby zapobiec wjazdowi na tory, które zostały zalane lub które są zajęte przez inny pociąg).



Rysunek 6. Przykład realizacji systemu SCADA na potrzeby monitorowania ruchu kolejowego oraz sterowania jego działaniem.

2.3.3. ROZPROSZONE SYSTEMY STEROWANIA

Rozproszony system sterowania (DCS) pozwala na sterowanie systemami produkcyjnymi znajdującymi się w tej samej lokalizacji geograficznej. Wykorzystuje się je w obiektach takich jak: rafinerie ropy naftowej, stacje uzdatniania wody i oczyszczalnie ścieków, elektrownie, zakłady chemiczne, zakłady motoryzacyjne oraz

zakłady wytwarzające leki. Systemy te są zazwyczaj wykorzystywane w celu sterowania procesami lub elementami dyskretnymi.

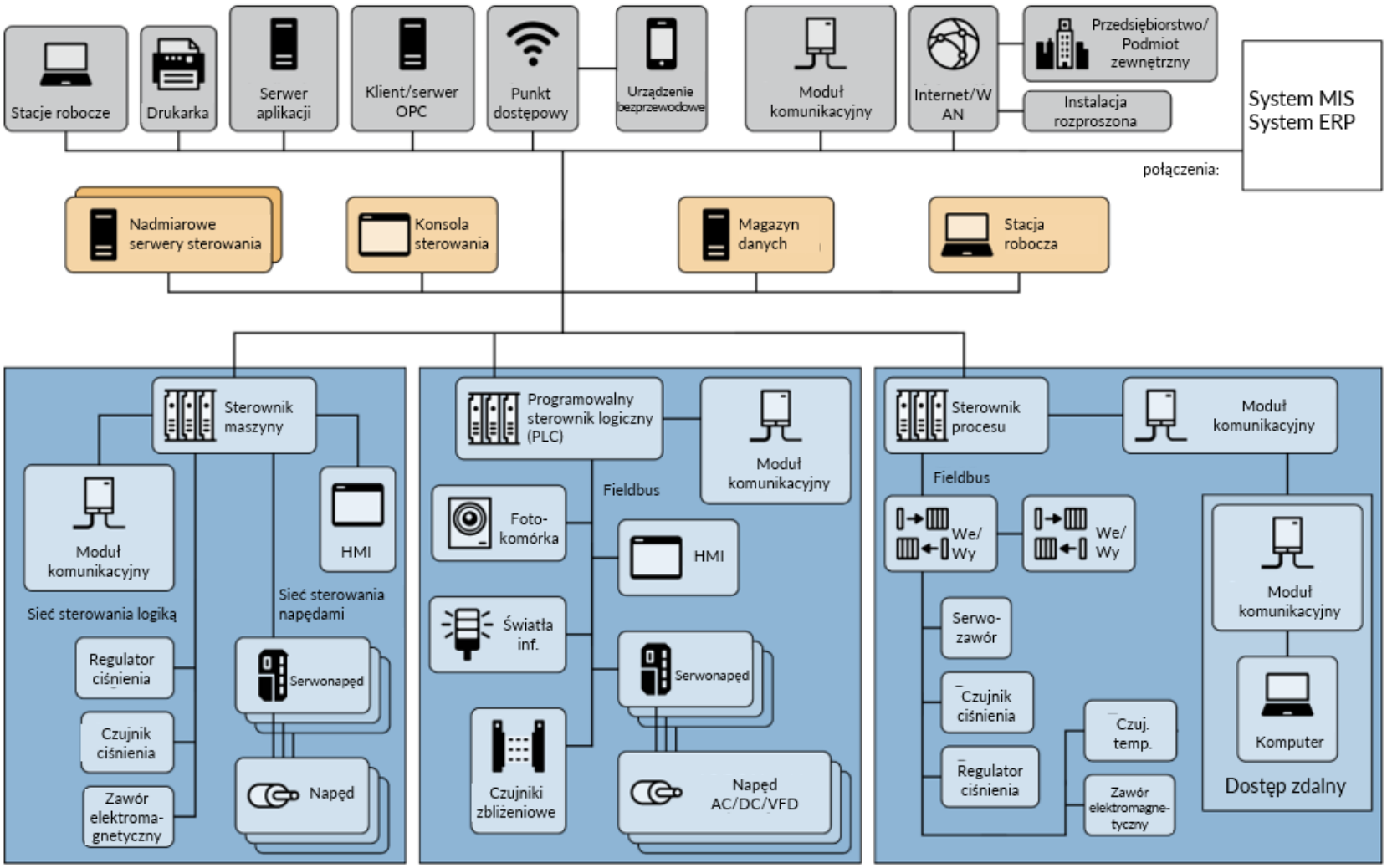
Rozproszone systemy sterowania stanowią kompleksowe architektury sterowania obejmujące poziom kontroli nadzorczej pozwalający na kontrolowanie wielu zintegrowanych podsystemów, które odpowiadają z kolei za sterowanie działaniem lokalnego procesu. Rozproszone systemy sterowania opierają się na scentralizowanej pętli kontroli nadzorczej w celu sterowania zbiorem lokalnych sterowników realizujących zadania związane z realizacją całego procesu produkcyjnego. [Erickson] Kontrola produktów oraz sterowanie procesem jest zwykle osiągana poprzez wdrożenie pętli sterowania ze sprzężeniem zwrotnym lub wyprzedzającym, które pozwalają na automatyczne utrzymanie kluczowych parametrów produktu lub procesu w pobliżu określonej wartości zadanej. Na poziomie poszczególnych urządzeń wykorzystywane są sterowniki procesu lub sterowniki PLC, które są konfigurowane w celu zapewnienia pożądanej tolerancji oraz szybkości automatycznej poprawy w przypadku zakłócenia przebiegu procesu. Dzięki modułowej budowie systemu produkcyjnego, rozproszone systemy sterowania ograniczają wpływ pojedynczej usterki na cały system. W wielu nowoczesnych systemach, rozproszone systemy sterowania są połączone z siecią organizacji, aby zapewnić wgląd w procesy produkcyjne pracownikom odpowiedzialnym za operacje.

Rysunek 7 przedstawia elementy oraz podstawową konfigurację przykładowego rozproszonego systemu sterowania. Przedstawiony system obejmuje cały zakład – od podstawowych procesów produkcyjnych aż po warstwę organizacji. W przedstawionym przykładzie kontroler nadzorujący (serwer sterujący) komunikuje się z podrzędnymi urządzeniami za pośrednictwem sieci sterowania. Serwer sterowania wysyła wartości zadane do rozproszonych sterowników i gromadzi przekazywane przez nie dane. Rozproszone sterowniki odpowiadają za kontrolowanie siłowników w oparciu o polecenia serwera sterującego i informacje zwrotne z czujników.

Rysunek 7 przedstawia również przykłady sterowników niskiego poziomu, które stanowią część rozproszonego systemu sterowania. Przedstawione urządzenia sterujące obejmują sterownik maszyny, sterownik PLC i sterownik procesu. Sterownik maszyny jest połączony z czujnikami i siłownikami za pomocą połączeń punkt-punkt,

z kolei pozostałe trzy urządzenia wykorzystują sieci Fieldbus w celu łączenia się z czujnikami procesowymi i siłownikami. Zastosowanie sieci Fieldbus eliminuje potrzebę stosowania połączeń punkt-punkt między sterownikiem a poszczególnymi czujnikami i siłownikami. Ponadto magistrala Fieldbus pozwala na realizację dodatkowych funkcji, obejmujących między innymi diagnostykę urządzeń. Może także umożliwić realizację algorytmów sterowania w ramach magistrali, co pozwala na uniknięcie konieczności przesyłania sygnałów do sterownika PLC w przypadku każdej operacji sterowania. Standardowe przemysłowe protokoły komunikacyjne zaprojektowane przez grupy przemysłowe, w tym Modbus i Fieldbus [Berge], są często wykorzystywane w sieciach sterowania i sieciach Fieldbus.

Oprócz pętli sterowania na poziomie nadzorczym i terenowym, w niektórych realizacjach występują poziomy pośrednie. Na przykład, w przypadku rozproszonego systemu sterowania odpowiadającego za sterowanie zakładem produkcyjnym wytwarzającym zróżnicowane elementy, mogą istnieć pośrednie warstwy nadzoru dla każdej komórki produkcyjnej wchodzącej w skład organizacji. Obejmują one komórki produkcyjne, w skład których wchodzą sterowniki maszyn obrabiających daną część, a także sterownik robota, który podaje materiały i odbiera produkty końcowe. W zakładzie może istnieć szereg takich komórek, które odpowiadają za zarządzanie sterownikami w ramach głównej pętli kontroli nadzorczej rozproszonego systemu sterowania.



Rysunek 7. Przykład kompleksowego wdrożenia rozproszonego systemu sterowania

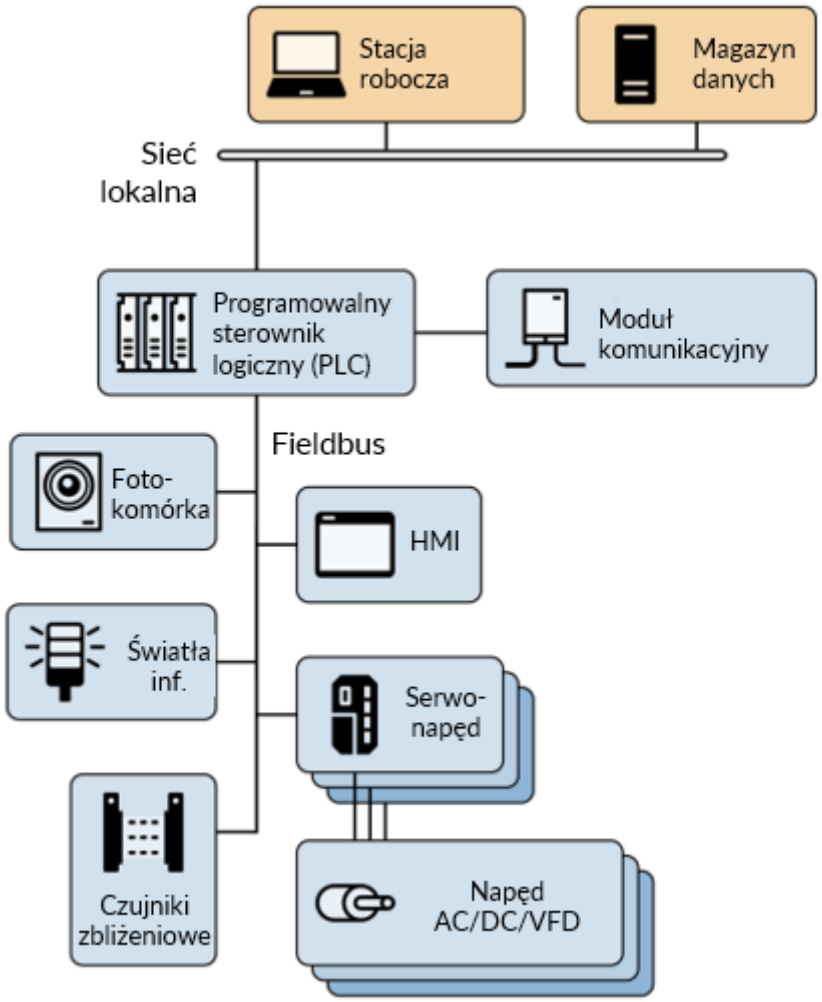
Tłumaczenie

2.3.4. TOPOLOGIE OPARTE NA PROGRAMOWALNYCH STEROWNIKACH LOGICZNYCH

Programowalne sterowniki logiczne (*ang. Programmable Logic Controller – PLC*) są wykorzystywane zarówno w systemach SCADA, jak i rozproszonych systemach sterowania (*ang. Distributed Control System – DCS*), w których pełnią funkcję elementów sterujących systemu hierarchicznego. Służą do sterowania procesami na szczeblu lokalnym dzięki pętli sterowania ze sprzężeniem zwrotnym, opisanej w poprzednich podrozdziałach. W przypadku systemów SCADA mogą zapewniać funkcjonalność zbliżoną do urządzeń RTU. W rozproszonych systemach sterowania (DCS), sterowniki PLC są wdrażane w roli sterowników lokalnych w ramach programu kontroli nadzorczej.

Sterowniki PLC mogą być również wykorzystywane w roli głównego sterownika w mniejszych systemach OT, w przypadku których umożliwiają zabezpieczenie operacyjne procesów i urządzeń (na przykład linii montażowych samochodów lub sterowników procesów). Tego rodzaju topologie odbiegają od rozwiązań stosowanych w przypadku systemów SCADA i rozproszonych systemów sterowania, ponieważ zwykle nie obejmują centralnego serwera sterowania lub interfejsu człowiek-maszyna, w związku z czym zapewniają przede wszystkim sterowanie w pętli zamkniętej przy minimalnym udziale człowieka. Sterowniki PLC są wyposażone w moduł pamięci programowalnej przez użytkownika, która pozwala na przechowywanie poleceń umożliwiających realizację określonych funkcji, takich jak sterowanie sygnałami wejściowymi i wyjściowymi, realizację logiki, synchronizację, zliczanie, sterowanie proporcjonalno-całkująco-różniczkujące (*ang. proportional-integral-derivative - PID*) w trzech trybach, komunikację, arytmetykę oraz przetwarzanie danych i plików.

Rysunek 8 przedstawia sterownik PLC połączony z siecią Fieldbus sterujący procesem produkcyjnym. Sterownik PLC jest dostępny za pośrednictwem interfejsu programowania na stacji roboczej, a dane są przechowywane w archiwum danych. Wszystkie te urządzenia są połączone lokalną siecią komputerową LAN.



Rysunek 8. Przykład realizacji systemu sterowania opartego na programowalnych sterownikach logicznych

2.3.5. SYSTEMY AUTOMATYKI BUDYNKOWEJ

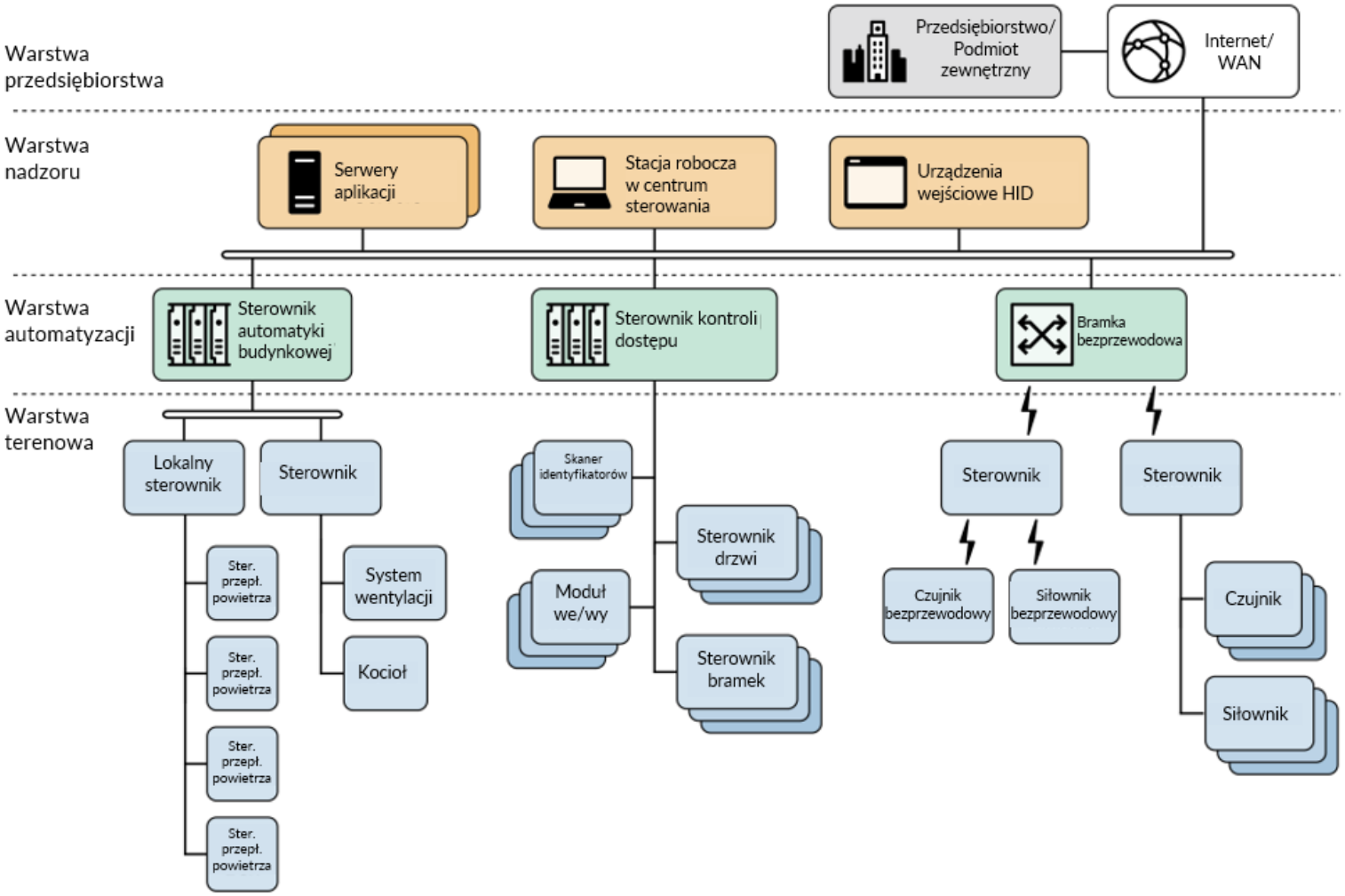
System automatyki budynkowej (*ang. Building Automation Systems – BAS*) to rodzaj systemu OT służący do sterowania wieloma urządzeniami wykorzystywanymi w budynkach, w tym systemami ogrzewania, wentylacji i klimatyzacji, systemem przeciwpożarowym, elektrycznym, oświetleniowym, kontroli dostępu, bezpieczeństwa fizycznego i innymi systemami użytkowymi. Większość nowoczesnych budynków jest wyposażona w różne formy systemów automatyki budynkowej. Starsze budynki i urządzenia mogą wymagać modernizacji, które pozwolą na wykorzystanie ich zalet i możliwości.

Niektóre z najczęstszych funkcji realizowanych przez systemy automatyki budynkowej obejmują utrzymywanie warunków środowiskowych w celu zapewnienia

wygody użytkownikom budynków, zmniejszanie zużycia energii, zmniejszanie kosztów operacyjnych i konserwacji, zapewnianie bezpieczeństwa, rejestrowanie danych (na przykład dotyczących temperatury lub wilgotności powietrza) oraz ogólne monitorowanie urządzeń (na przykład w celu informowania pracowników o awarii urządzeń lub alarmach).

Przykład systemu BAS został przedstawiony na **Rysunku 9**. System BAS może opierać się na komunikacji przewodowej bądź bezprzewodowej ze sterownikami i bramami. Na przykład czujniki środowiskowe mogą przekazywać dane dotyczące temperatury i wilgotności powietrza sterownikowi budynku. Jeśli wartości zgłaszane przez czujniki wyjdą poza zadane wartości skrajne, sterownik może wysłać sygnał do systemu sterowania zmiennym przepływem powietrza, by ten zwiększył lub ograniczył przepływ powietrza i uregulował temperaturę do zadanej wartości. Z kolei użytkownik budynku skanujący swój identyfikator przy pomocy czytnika może spowodować wysłanie danych uwierzytelniających do kontrolera systemy kontroli dostępu i serwera kontroli aplikacji w celu ustalenia, czy dostęp powinien zostać przyznany.

Choć niniejszy dokument zawiera zalecenia, które mogą być stosowane jako punkt odniesienia dla wdrażania zabezpieczeń systemów BAS przed zagrożeniami dotyczącymi cyberbezpieczeństwa, zachęcamy czytelników do przeprowadzenia oceny ryzyka systemów i dostosowania zaleceń i wytycznych do specyficznych wymagań w zakresie bezpieczeństwa, a także biznesowych i operacyjnych.



Rysunek 9. Przykład wdrożenia systemu automatyki budynkowej

Tłumaczenie

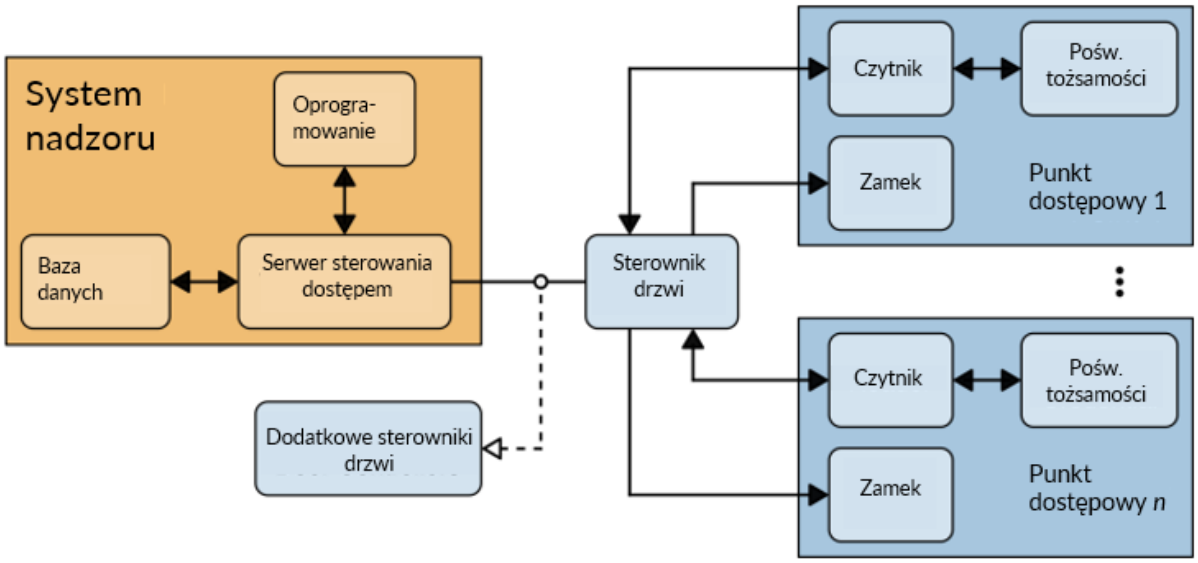
2.3.6. SYSTEMY KONTROLI DOSTĘPU FIZYCZNEGO

Systemy kontroli dostępu fizycznego (*ang. Physical Access Control Systems – PACS*) to rodzaj systemów będących częścią fizycznych środków bezpieczeństwa, zaprojektowanych w celu kontrolowania dostępu do danego obszaru.
W przeciwieństwie do standardowych barier fizycznych, systemy kontroli dostępu fizycznego mogą wpływać na to, jakie osoby otrzymują dostęp, kiedy jest on przyznawany i jak długo powinien trwać.

Punkt dostępu to wejście lub bariera, która wymaga kontroli dostępu. Niektóre powszechnie występujące przykłady punktów dostępu związanych z systemami kontroli dostępu fizycznego to drzwi i zamki, bramki bezpieczeństwa, kołowroty i szlabany.
W zależności od rodzaju budynku liczba punktów dostępu może być zróżnicowana.
W przypadku obiektów o wysokim poziomie bezpieczeństwa może być ograniczona do jednego, z kolei duży budynek biurowy może mieć wiele punktów dostępu.

Identyfikator lub osobiste dane uwierzytelniające służą do potwierdzania tożsamości upoważnionego użytkownika próbującego uzyskać dostęp do obszaru lub budynku. Systemy kontroli dostępu fizycznego często wymagają od użytkownika posiadania poświadczeń w celu uzyskania dostępu do obiektu lub wrażliwych danych. Przykłady poświadczeń obejmują uproszczone zabezpieczenia, takie jak na przykład kody PIN, hasła, breloki, karty dostępu, a także bardziej zaawansowane poświadczenia, w tym szyfrowane identyfikatory oraz aplikacje mobilne. Poświadczenia identyfikacyjne wskazują, które osoby próbują uzyskać dostęp i umożliwiają rejestrowanie prób uzyskania dostępu.

W punktach dostępu znajdują się zwykle czytniki bądź klawiatury. Czytnik odczytuje dane i wysyła je do sterownika drzwi w celu weryfikacji poświadczenia i sprawdzenia, czy użytkownikowi należy umożliwić dostęp. Jeśli system wymaga również klawiatury lub czujnika biometrycznego, na przykład w związku z wymogiem uwierzytelniania wieloskładnikowego, użytkownik wprowadza swój osobisty numer identyfikacyjny lub wykonuje skan biometryczny po zeskanowaniu poświadczenia. Przykład systemu kontroli dostępu fizycznego został przedstawiony na **Rysunku 10**.



Rysunek 10. Przykład wdrożenia systemu kontroli dostępu fizycznego

W przedstawionym przykładzie sterownik drzwi odbiera dane uwierzytelniające z czytnika i weryfikuje tożsamość oraz poświadczenie. Jeśli poświadczenie zostanie potwierdzone przez serwer kontroli dostępu, panel sterowania przesyła polecenie autoryzacji dostępu i odblokowania drzwi. Jeśli poświadczenie zostanie odrzucone, drzwi pozostaną zablokowane, a użytkownik nie będzie mógł uzyskać dostępu do budynku. Wszystkie próby dostępu są rejestrowane przez sterownik drzwi, a dane są przekazywane do serwera kontroli dostępu. Serwer kontroli dostępu zawiera repozytorium danych o użytkownikach, uprawnień dostępu oraz dzienników audytu. W zależności od systemu, serwer może znajdować się w lokalnym centrum danych lub w chmurze.

Choć niniejszy dokument zawiera zalecenia, które mogą być stosowane jako punkt odniesienia dla wdrażania zabezpieczeń systemów kontroli dostępu fizycznego przed zagrożeniami dotyczącymi cyberbezpieczeństwa, zachęcamy czytelników do przeprowadzenia oceny ryzyka systemów i dostosowania zaleceń i wytycznych do specyficznych wymagań w zakresie bezpieczeństwa, a także biznesowych i operacyjnych.

2.3.7. SYSTEMY BEZPIECZEŃSTWA FIZYCZNEGO

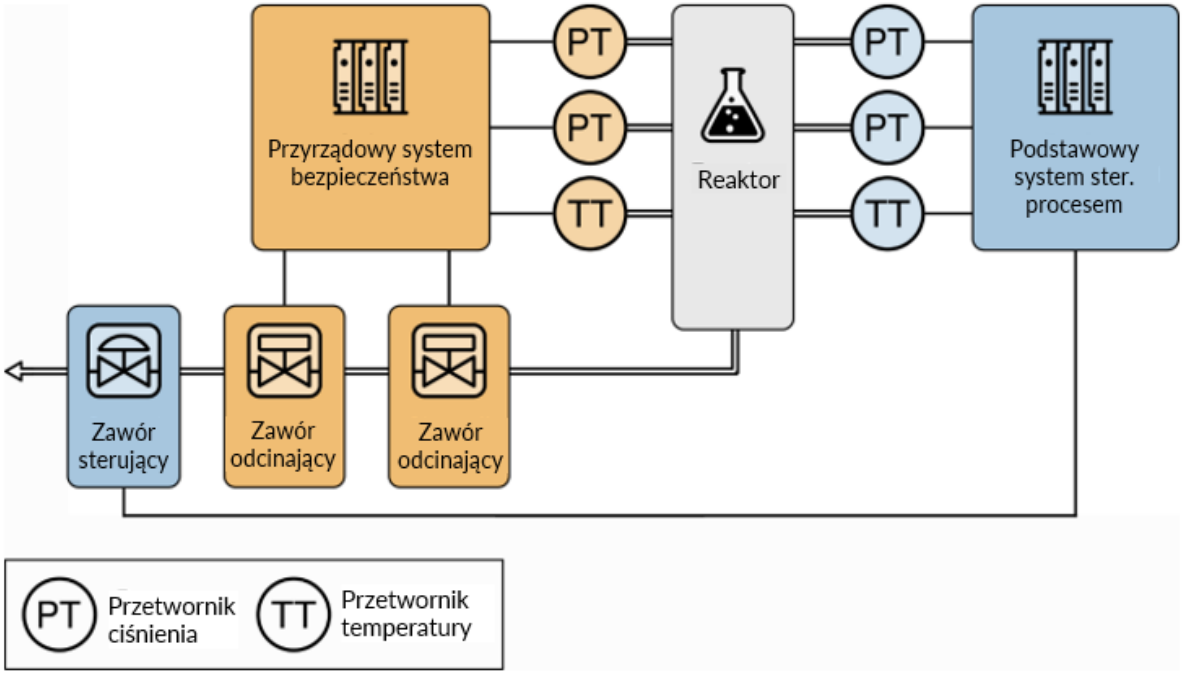
Wiele procesów fizycznych kontrolowanych przez systemy OT może doprowadzić do zaistnienia sytuacji zagrażających zdrowiu i życiu ludzi, a także skutkujących zniszczeniem mienia i środowiska. Systemy bezpieczeństwa fizycznego mają na celu zmniejszenie prawdopodobieństwa bądź ograniczenie negatywnych skutków niebezpiecznych sytuacji poprzez przywrócenie systemu do bezpiecznego stanu. Istnieje kilka rodzajów systemów bezpieczeństwa fizycznego związanych ze środowiskami OT. To między innymi wyłączniki awaryjne (*ang. emergency shut down – ESD*), wyłączniki bezpieczeństwa (*ang. process safety shutdown – PSS*) oraz systemy przeciwpożarowe i przeciwgazowe (*ang. fire and gas systems – FGS*).

Jednym z podstawowych rodzajów systemów bezpieczeństwa fizycznego są systemy automatyki zabezpieczeniowej (*ang. safety instrumented system – SIS*), które składają się z jednego lub wielu elementarnych przyrządowych systemów bezpieczeństwa (*ang. safety instrumented functions – SIFs*). Elementarne przyrządowe systemy bezpieczeństw to systemy, w których skład wchodzą zazwyczaj czujniki, elementy logiczne oraz elementy sterujące (takie jak siłowniki), których celem jest przywrócenie systemu do bezpiecznego stanu w przypadku przekroczenia wstępnie skonfigurowanych wartości progowych. Systemy automatyki zabezpieczeniowej stanowią element ogólnej strategii ograniczania ryzyka w celu zmniejszenia prawdopodobieństwa bądź potencjalnych skutków uprzednio opisanego zdarzenia do poziomu mieszczącego się w granicach ryzyka tolerowanego przez podmiot. Pomimo istnienia wielu zróżnicowanych norm, zgodnie z którymi projektowane są systemy bezpieczeństwa fizycznego, systemy automatyki zabezpieczeniowej są projektowane zgodnie z wymogami normy [IEC61511].Tego rodzaju systemy zwykle stosuje się w zakładach przetwórstwa chemicznego, rafineriach i obiektach jądrowych.

Systemy automatyki zabezpieczeniowej działają często niezależnie od wszystkich pozostałych systemów sterowania; dzięki temu awaria podstawowego systemu sterującego procesem (*ang. basic process control system – BPCS*) nie wpłynie negatywnie na jego funkcjonalność. Tradycyjne systemy automatyki zabezpieczeniowej były projektowane w formie rozwiązań samodzielnych, fizycznie

i logicznie odseparowanych od reszty systemu sterowania. W przypadku przykładowej konfiguracji zaprezentowanej na **Rysunku 11**, systemy automatyki zabezpieczeniowej oraz podstawowy system sterujący procesem działają całkowicie niezależnie od siebie – nie dochodzi do bezpośredniej komunikacji między systemami. Niektóre nowoczesne systemy tego rodzaju zostały zaprojektowane w taki sposób, by umożliwiały komunikację z systemem sterowania. Tego typu systemy nazywamy zintegrowanymi systemami sterowania i bezpieczeństwa (*ang. Integrated Control and Safety Systems – ICSS*). Tego rodzaju rozwiązania mogą być urządzeniami typu „wszystko w jednym" dostarczanymi przez jednego producenta, mogą także obejmować wiele urządzeń wytwarzanych przez wielu producentów. Choć zintegrowane systemy sterowania i bezpieczeństwa łączą funkcje obu systemów, komponent odpowiedzialny za automatykę zabezpieczeniową nadal musi spełniać wymogi normy [IEC61511].Jedną z zalet tego rozwiązania jest możliwość przekazywania informacji między systemem automatyki zabezpieczeniowej i podstawowym systemem sterującym procesem.

Choć niniejszy dokument zawiera zalecenia, które mogą być stosowane jako punkt odniesienia dla wdrażania zabezpieczeń systemów kontroli bezpieczeństwa fizycznego przed zagrożeniami dotyczącymi cyberbezpieczeństwa, zachęcamy czytelników do przeprowadzenia oceny ryzyka systemów i dostosowania zaleceń i wytycznych do specyficznych wymagań w zakresie bezpieczeństwa, systemów bezpieczeństwa fizycznego, biznesowych i operacyjnych.



Rysunek 11. Przykład wdrożenia systemu automatyki zabezpieczeniowej

2.3.8. PRZEMYSŁOWY INTERNET RZECZY

Kategoria urządzeń przemysłowego Internetu rzeczy (*ang. Industrial Internet of Things – IIoT*) obejmuje czujniki, przyrządy, maszyny oraz inne urządzenia połączone w sieć i wykorzystujące łączność internetową w celu usprawnienia procesów biznesowych i działania rozwiązań w zakładach przemysłowych i produkcyjnych. [Berge] Pomimo postępującego ujednolicania i rozwoju połączeń między systemami IT oraz OT, sterowanie procesami fizycznymi pozostaje stosunkowo wyjątkową i kluczową koncepcją dotyczącą obszaru technologii operacyjnych.

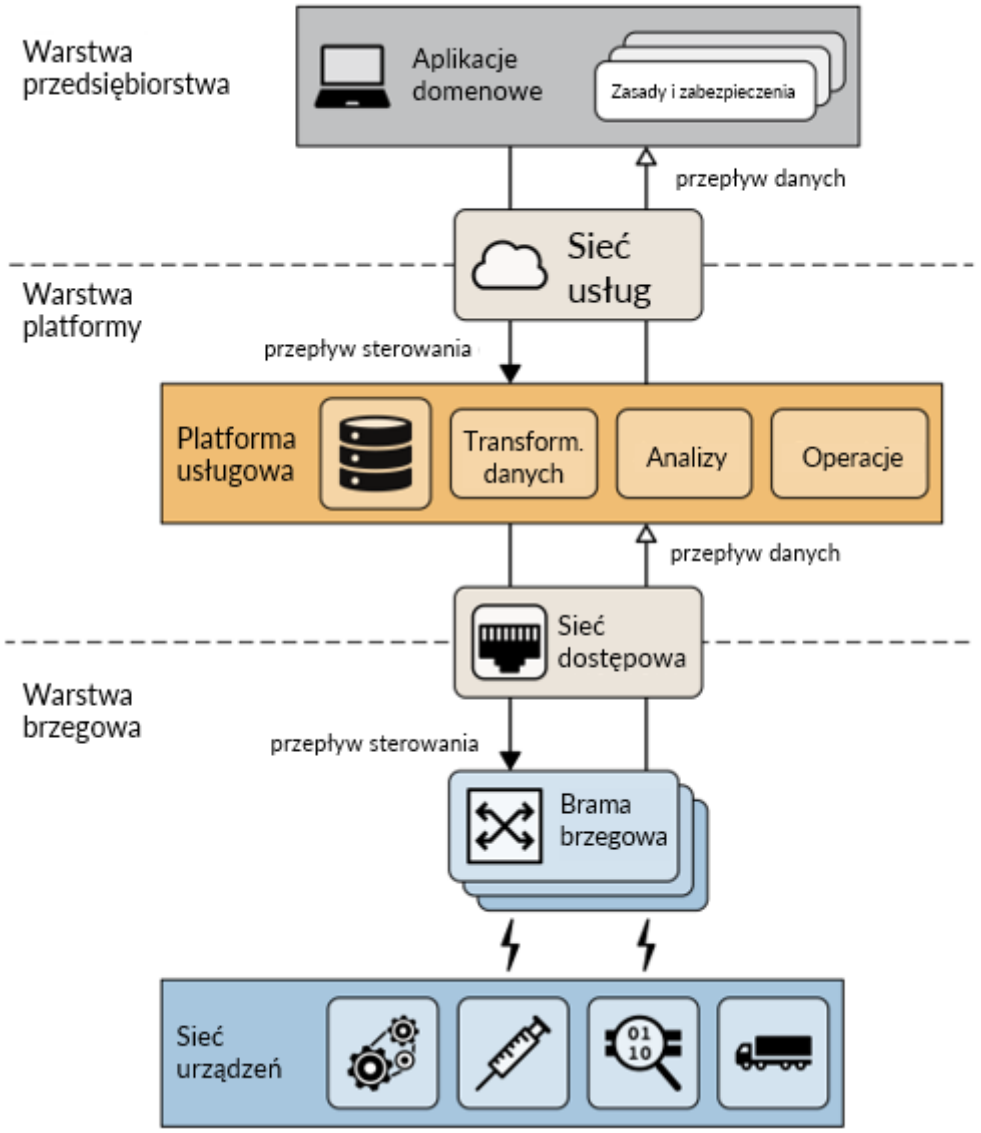
Konsorcjum Przemysłowego Internetu Rzeczy (*ang. Industry IoT Consortium*) przedstawiło propozycję trzywarstwowego modelu architektury systemów do wykorzystania na potrzeby rozwiązań IIoT [IIRA19]: warstwę brzegową (*ang. Edge Tier*), warstwę platformy (*ang. Platform Tier)* i warstwę organizacji (*ang. Enterprise Tier)*. Każda warstwa odgrywa określoną rolę w przetwarzaniu danych i poleceń sterowania związanych z działaniem procesów. Według tego modelu, poszczególne warstwy są połączone trzema sieciami – siecią bliskiego zasięgu (*ang. Proximity Network*), siecią dostępową (*ang. Access Network*) oraz siecią usług (*ang. Service Network*). Przykładowa architektura została przedstawiona na **Rysunku 12**.

Warstwa organizacji obejmuje aplikacje dotyczące poszczególnych obszarów i systemy wspomagania decyzji, oferuje interfejsy dla użytkowników końcowych, gromadzi dane z pozostałych warstw i przekazuje polecenia sterujące do pozostałych warstw.

Warstwa platformy odbiera, przetwarza i przekazuje polecenia sterujące przekazywane z warstwy organizacji do warstwy brzegowej. Łączy procesy i analizuje dane przekazywane przez pozostałe warstwy, realizuje funkcje zarządzania urządzeniami i zasobami oraz usługi niezwiązane z danym obszarem, takie jak zapytania i analizy danych. W zależności od wymogów danej realizacji poszczególne funkcje mogą być realizowane za pośrednictwem platformy przemysłowego Internetu rzeczy wdrożonej w lokalnym centrum danych, zewnętrznym centrum danych lub w chmurze.

Sieć usług umożliwia łączność między usługami działającymi w warstwach platformy i organizacji oraz pomiędzy usługami działającymi w ramach poszczególnych warstw. Łączność w ramach takiej sieci może być realizowana w formie sieci prywatnej opartej na publicznej sieci Internet lub za pośrednictwem otwartego Internetu, zapewniając bezpieczeństwo łączności między użytkownikami końcowymi a usługami.

Warstwa brzegowa gromadzi dane z urządzeń brzegowych przy pomocy sieci krótkiego zasięgu. Architektura tej warstwy jest uzależniona od wymogów danego projektu, w tym od rozmieszczenia geograficznego, lokalizacji fizycznej oraz zakresu zarządzania. W tym wypadku można mówić o warstwie logicznej, nie zaś rzeczywistym podziale fizycznym. Z punktu widzenia działalności organizacji, lokalizacja warstwy brzegowej jest uzależniona od celów biznesowych.



Rysunek 12. Trzywarstwowa architektura systemu przemysłowego Internetu rzeczy

W przypadku przetwarzania brzegowego mówimy o zdecentralizowanej infrastrukturze obliczeniowej, w ramach której zasoby obliczeniowe i usługi aplikacji mogą być dystrybuowane wzdłuż ścieżki komunikacyjnej między źródłem danych a chmurą. Takie rozwiązania występują zarówno w płaszczyźnie pionowej (tj. od urządzenia do chmury), jak i w poziomej w podsystemach IIoT. Urządzenia brzegowe nie tylko stanowią sposób na zbieranie danych w celu przesłania ich do centrum danych lub chmury; lecz także przetwarzają i analizują zgromadzone dane na brzegu, a także mogą podejmować na ich podstawie działania, w związku z czym są nieodzowne z punktu widzenia optymalizacji danych przemysłowych we wszystkich obszarach.

Architektura systemu IIoT jest w pełni rozproszona i może obsługiwać szeroki zakres interakcji i paradygmatów komunikacji, w tym:

- Połączenia peer-to-peer (np. kamery bezpieczeństwa przekazujące sobie informacje o zidentyfikowanych obiektach).
- Współpracę urządzeń brzegowych (np. turbin wiatrowych w odległych lokalizacjach).
- Rozproszone zapytania dotyczące danych przechowywanych na urządzeniach, w chmurze i w dowolnej lokalizacji pomiędzy nimi.
- Rozproszone systemy zarządzania danymi, które określają, gdzie i jak długo dane powinny być przechowywane.
- Systemy zarządzania danymi dotyczące ich jakości, gromadzenia, użyteczności, prywatności i bezpieczeństwa.

Sieci bliskiego zasięgu łączą urządzenia brzegowe (takie jak: czujniki, siłowniki, urządzenia, systemy OT i zasoby) z architekturą. Urządzenia brzegowe są zwykle przyłączane jako jeden lub więcej klastrów do bramy, która umożliwia łączność z innymi sieciami. Sieć dostępowa umożliwia łączność na potrzeby przesyłu danych i poleceń sterujących między warstwami brzegową i platformy. Połączenie to może opierać się na sieci organizacji lub sieci prywatnej realizowanej za pośrednictwem publicznego Internetu bądź sieci 4G/5G.

Choć niniejszy dokument zawiera zalecenia, które mogą być stosowane jako punkt odniesienia dla wdrażania zabezpieczeń systemów przemysłowego Internetu rzeczy przed zagrożeniami dotyczącymi cyberbezpieczeństwa, zachęcamy czytelników do przeprowadzenia oceny ryzyka systemów i dostosowania zaleceń i wytycznych do specyficznych wymagań w zakresie bezpieczeństwa, a także biznesowych i operacyjnych.

2.4. PORÓWNANIE ZAGADNIEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM SYSTEMÓW OT I IT

Systemy technologii operacyjnej (systemy OT) charakteryzują się wieloma cechami, które odróżniają je od tradycyjnych systemów teleinformatycznych (systemów IT). Wśród nich można wymienić zróżnicowane rodzaje zagrożeń oraz priorytety. Niektóre z nich obejmują znaczące ryzyko i zagrożenie dla zdrowia i ludzkiego życia, ryzyko wystąpienia poważnych szkód środowiskowych oraz ryzyko poważnych strat finansowych w wyniku zatrzymania produkcji. Rozwiązania technologii operacyjnej charakteryzują się w związku z tym szczególnymi wymaganiami w zakresie wydajności i niezawodności. W wielu przypadkach takie systemy działają pod kontrolą systemów operacyjnych i aplikacji, które zwykle nie występują w typowych środowiskach sieciowych. Wszelkie zabezpieczenia muszą w związku z tym być wdrożone w sposób, który zapewnia integralność systemu podczas normalnego działania, jak również podczas cyberataków. [Knapp]

Pierwsze systemy technologii operacyjnej w niewielkim stopniu przypominały tradycyjne systemy teleinformatyczne, były bowiem odizolowane, wykorzystywały zastrzeżone protokoły sterowania i opierały się na specjalistycznych urządzeniach sprzętowych oraz wyspecjalizowanym oprogramowaniu. Popularyzacja tanich urządzeń wykorzystujących sieci Ethernet, protokół internetowy oraz rozwiązania bezprzewodowe powoduje stopniowe wypieranie starszych, własnościowych technologii, jednak prowadzi to do zwiększenia prawdopodobieństwa wystąpienia podatności dotyczących cyberbezpieczeństwa i incydentów. Systemy technologii operacyjnej w coraz większym stopniu przypominają systemy teleinformatyczne, ponieważ wykorzystują technologie informacyjne w celu umożliwiania łączności z sieciami organizacji oraz zdalnego dostępu, w oparciu o standardowe komputery, systemy operacyjne oraz protokoły sieciowe. Takie połączenie rozszerza ich możliwości, jednak wiąże się też ze zmniejszeniem poziomu odizolowania systemów OT od świata zewnętrznego względem tradycyjnych rozwiązań, co przekłada się na wzrost potrzeb w zakresie zabezpieczeń tych systemów. Ze względu na to, że zabezpieczenia oraz rozwiązania zapewniające bezpieczeństwo zostały

zaprojektowane z myślą o typowych systemach teleinformatycznych, wdrażanie ich w środowiskach technologii operacyjnych wymagają zachowania szczególnej ostrożności. Niektóre przypadki wymagają nowych rozwiązań i zabezpieczeń dostosowanych do wymogów środowisk OT.

Wybrane wymogi, które należy wziąć pod uwagę w przypadku zabezpieczania systemów OT, obejmują:

- **Wymagania dotyczące terminowości i osiągów.** Zwyczajowo przyjęło się uważać, że systemy OT wymagają precyzji czasowej; dopuszczalne poziomy opóźnień wynikają z wymogów dla poszczególnych realizacji. Niektóre systemy wymagają niezawodnych, deterministycznych reakcji. Z drugiej strony, dzięki temu zwykle nie jest wymagana wysoka przepustowość, przeważnie niezbędna w przypadku systemów informatycznych, które w związku z tym charakteryzują się pewną odpornością na zakłócenia i opóźnienia. W przypadku wybranych systemów OT, kluczowe znaczenie mają czasy automatycznej reakcji lub odpowiedzi systemu na polecenia wydane przez człowieka. Wiele systemów OT wykorzystuje systemy operacyjne czasu rzeczywistego (*ang. real time OSs – RTOS*) – w przypadku tych rozwiązań pojęcie czasu rzeczywistego odnosi się do wymagań dotyczących czasu działania. Jednostki czasu rzeczywistego są wysoce zależne od wybranego obszaru zastosowania i muszą być wyraźnie określone.
- **Wymogi dotyczące dostępności.** Wiele procesów realizowanych przez systemy OT ma charakter ciągły. Nieoczekiwane awarie systemów sterujących procesami przemysłowymi są w związku z tym niedopuszczalne, a wszelkie przestoje muszą być często planowane z kilkudniowym lub kilkutygodniowym wyprzedzeniem. Zapewnienie wysokiej dostępności i niezawodności systemów OT wymaga przeprowadzenia wyczerpujących testów przed wdrożeniem nowych komponentów. Dzieje się tak dlatego, że zatrzymanie i wznowienie pracy takich systemów jest zwykle niemożliwe bez wpływu na produkcję, a w niektórych przypadkach wytwarzane produkty lub wykorzystywane urządzenia są ważniejsze niż przekazywane dane. Z tego powodu strategie i działania typowe dla systemów teleinformatycznych (na przykład ponowne uruchomienie komponentu) są zwykle niemożliwe do

wykorzystania w systemach technologii operacyjnej ze względu na niekorzystny wpływ na realizację wymogów dotyczących dostępności, niezawodności i łatwości konserwacji. Niektóre systemy OT wykorzystują komponenty nadmiarowe (często działające równolegle) w celu zapewnienia ciągłości działania, gdy podstawowe komponenty są niedostępne z dowolnego powodu.

- **Wymogi w zakresie zarządzania ryzykiem.** W typowym systemie teleinformatycznym główne obszary ryzyka dotyczą poufności i integralności danych. W przypadku systemów technologii operacyjnej główne obszary ryzyka obejmują bezpieczeństwo fizyczne, odporność na awarie, ochrona zdrowia, życia, zdrowia publicznego oraz zaufania, zgodność z przepisami, zniszczenie urządzeń, utratę własności intelektualnej lub zniszczenie bądź uszkodzenie produktów. Pracownicy odpowiedzialni za obsługę, zabezpieczenie i utrzymanie systemów technologii operacyjnej muszą być świadomi związku między bezpieczeństwem (ochroną) i bezpieczeństwem fizycznym. Z tego powodu wszelkie zabezpieczenia zmniejszające poziom bezpieczeństwa fizycznego są niedopuszczalne.
- **Skutki fizyczne.** Urządzenia końcowe, w tym sterowniki PLC, stanowiska operatorów oraz sterowniki rozproszonych systemów sterowania, wpływają bezpośrednio na procesy fizyczne. Systemy i urządzenia technologii operacyjnej mogą wchodzić w złożone interakcje z procesami fizycznymi, a ich konsekwencje mogą prowadzić do występowania zdarzeń fizycznych. Zrozumienie tych potencjalnych skutków często wymaga komunikacji między specjalistami zajmującymi się obszarem technologii operacyjnej oraz specjalistami odpowiedzialnymi za dany obszar fizyczny.
- **Działanie systemu.** Systemy operacyjne i sieci sterowania wykorzystywane w systemach technologii operacyjnej często różnią się od swoich odpowiedników w sieciach teleinformatycznych. W związku z tym wymagają różnych zestawów umiejętności, innego doświadczenia oraz innych zasobów wiedzy specjalistycznej. Sieci sterowania są zazwyczaj zarządzane przez inżynierów ds. nadzoru technicznego, nie zaś przez pracowników działu IT. Przyjęcie założenia, że różnice między tymi systemami są pomijalne i nieistotne, może nieść za sobą katastrofalne skutki dla ich działania.

- **Ograniczone zasoby.** Systemy technologii operacyjnej oraz systemy operacyjne czasu rzeczywistego (*ang. real-time operating systems – RTOSs*) zwykle dysponują ograniczonymi zasobami i nie obejmują zabezpieczeń oraz zdolności do ochrony typowych dla współczesnych systemów teleinformatycznych. Co więcej, starsze systemy często nie dysponują zasobami powszechnymi we współczesnych systemach teleinformatycznych. Wiele z nich nie jest wyposażonych w potrzebne funkcje, takie jak: szyfrowanie, rejestrowanie błędów czy ochrona hasłem. Bezkrytyczne stosowanie praktyk w zakresie zabezpieczenia systemów teleinformatycznych w przypadku systemów technologii operacyjnej może doprowadzić do ograniczenia ich dostępności oraz precyzji działania. Komponenty systemów OT mogą nie dysponować wystarczającymi zasobami obliczeniowymi do obsługi współczesnych zabezpieczeń, z kolei rozbudowa zasobów lub dodanie obsługi nowych zabezpieczeń może nie być możliwe.
- **Komunikacja.** Protokoły komunikacyjne i media wykorzystywane w środowiskach OT na potrzeby komunikacji między urządzeniami końcowymi oraz sterownikami są zazwyczaj inne niż w środowiskach IT i mogą być zastrzeżone.
- **Zarządzanie zmianą.** Zarządzanie zmianą ma kluczowe znaczenie dla zapewnienia integralności systemów teleinformatycznych oraz technologii operacyjnej. Brak aktualizacji oprogramowania stanowi zwykle jedną z największych podatności w zabezpieczeniach systemu. Aktualizacje oprogramowania w systemach teleinformatycznych, w tym poprawki zabezpieczeń, są zazwyczaj instalowane w krótkim czasie na podstawie stosownych zasad i procedur bezpieczeństwa. Ponadto ich realizacja jest często zautomatyzowana dzięki zastosowaniu narzędzi serwerowych. Aktualizacje oprogramowania składników systemów technologii operacyjnej nie zawsze mogą być instalowane wkrótce po ich publikacji. Dzieje się tak dlatego, że muszą zostać dokładnie przetestowane zarówno przez producenta, jak i użytkownika końcowego systemu sterowania przemysłowego przed instalacją. Ponadto osoby odpowiedzialne za zarządzanie systemami OT muszą planować wszelkie przestoje i przerwy w działaniu z kilkudniowym lub kilkutygodniowym wyprzedzeniem. Dodatkowo, systemy technologii operacyjnej mogą wymagać ponownej walidacji w ramach procesu aktualizacji. Kolejny

problem jest związany z faktem, że wiele rozwiązań OT wykorzystuje starsze wersje systemów operacyjnych, w przypadku których producenci nie wydają już poprawek bezpieczeństwa. Proces zarządzania zmianą dotyczy także urządzeń i oprogramowania układowego. Proces zarządzania zmianą wymaga dokonania starannej oceny przez specjalistów odpowiedzialnych za systemy OT (na przykład inżynierów ds. nadzoru technicznego) współpracujących z pracownikami odpowiedzialnymi za bezpieczeństwo systemów teleinformatycznych.

- **Obsługa zarządzana.** Typowe systemy teleinformatyczne umożliwiają stosowanie wielu rodzajów i podejść do obsługi i wsparcia dzięki wykorzystaniu zróżnicowanych, jednak wzajemnie połączonych architektur technologicznych. W przypadku systemów technologii operacyjnej za obsługę serwisową oraz wsparcie odpowiada czasem zaledwie jeden producent lub usługodawca. W określonych sytuacjach zabezpieczenia innych producentów nie mogą zostać zastosowane ze względu na umowy licencyjne i umowy serwisowe, a przypadki instalacji oprogramowania innych producentów bez zgody producenta danego rozwiązania mogą doprowadzić do utraty prawa do wsparcia serwisowego i obsługi rozwiązania.
- **Okres eksploatacji komponentów.** Okres eksploatacji komponentów systemów teleinformatycznych wynosi zwykle od trzech do pięciu lat ze względu na szybkie tempo rozwoju technologii. W przypadku systemów technologii operacyjnej, gdzie wiele rozwiązań powstaje z myślą o konkretnych zastosowaniach i projektach, okres eksploatacji technologii często wynosi dziesięć, piętnaście lub więcej lat.
- **Rozmieszczenie komponentów.** Większość komponentów systemów teleinformatycznych oraz wybrane komponenty systemów technologii operacyjnej znajdują się w obiektach biznesowych i komercyjnych, które są dostępne za pośrednictwem lokalnych środków transportu. Zdalne lokalizacje mogą być wykorzystywane jako obiekty zapasowe lub miejsca przechowywania kopii zapasowych. Elementy systemów OT mogą znajdować się w dużych odległościach, mogą być także odizolowane, a dostęp do nich może nastręczać wielu trudności. Lokalizacja komponentu musi również uwzględniać niezbędne środki bezpieczeństwa fizycznego i środowiskowego.

Tabela 1 zawiera podsumowanie najważniejszych różnic pomiędzy systemami teleinformatycznymi i technologii operacyjnej.

Tabela 1. Podsumowanie najważniejszych różnic pomiędzy systemami teleinformatycznymi i technologii operacyjnej

Kategoria	Technologia informacyjna	Technologia operacyjna
Wymogi dotyczące osiągów	• Brak wymogu działania w czasie rzeczywistym • Wymóg stabilnego działania. • Wymóg wysokiej przepustowości. • Wysokie opóźnienia i zakłócenia mogą być akceptowalne. • Interakcja w sytuacjach awaryjnych jest mniej krytyczna. • Istnieje możliwość wdrożenia ścisłej kontroli dostępu w stopniu niezbędnym do zapewnienia bezpieczeństwa.	• Działanie w czasie rzeczywistym. • Kluczowe znaczenie ma czas reakcji. • Ograniczona przepustowość jest dopuszczalna. • Wysokie opóźnienia i zakłócenia są niedopuszczalne. • Reakcja na sytuacje awaryjne i wypadki ma kluczowe znaczenie. • Wymaga ścisłej kontroli dostępu, która nie może utrudniać ani zakłócać interakcji człowieka z maszyną.
Wymogi dotyczące dostępności (niezawodności)	• Działania takie jak ponowne uruchomienie są dopuszczalne. • Przerwy w dostępności bywają dopuszczalne, w zależności od wymagań dotyczących systemu.	• Działania takie jak ponowne uruchomienie mogą być niedopuszczalne ze względu na wymogi dotyczące dostępności procesów. • Wymagania dotyczące dostępności mogą wymagać zastosowania nadmiarowych systemów. • Przestoje muszą być planowane z kilkudniowym lub kilkutygodniowym wyprzedzeniem. • Wymóg wysokiej dostępności wymaga wyczerpujących testów przed wdrożeniem.
Wymogi w zakresie zarządzania ryzykiem	• Systemy zarządzają danymi i je przetwarzają. • Najważniejszym obszarem jest poufność i integralność danych. • Odporność na awarie jest mniej istotna.	• Systemy wpływają na środowisko fizyczne. • Najważniejszym obszarem jest bezpieczeństwo ludzi, a następnie ochrona procesu. • Odporność na awarie jest kluczowa – nawet chwilowe przestoje mogą być niedopuszczalne.

Kategoria	Technologia informacyjna	Technologia operacyjna
	• Chwilowe przestoje nie stanowią poważnego zagrożenia. • Głównym czynnikiem ryzyka jest możliwość opóźnienia operacji biznesowych.	• Główne czynniki ryzyka to naruszenie przepisów, wpływ na środowisko oraz zagrożenie zdrowia, życia, sprzętu lub produkcji.
Działanie systemu	• Praca pod kontrolą powszechnie występujących i popularnych systemów operacyjnych. • Prosta instalacja poprawek i aktualizacji dzięki dostępności zautomatyzowanych mechanizmów i narzędzi.	• Praca pod kontrolą zróżnicowanych, własnościowych systemów operacyjnych pozbawionych wbudowanych zabezpieczeń. • Zmiany w oprogramowaniu muszą być wprowadzane z zachowaniem szczególnej ostrożności, zwykle przez producentów oprogramowania, ze względu na wyspecjalizowane algorytmy sterowania i możliwość występowania modyfikacji urządzeń oraz oprogramowania.
Ograniczone zasoby	• Systemy są wyposażone w wystarczającą ilość zasobów pozwalającą na instalację rozwiązań innych producentów, w tym zabezpieczeń.	• Systemy są projektowane z myślą o obsłudze określonego procesu przemysłowego i mogą nie być wyposażone w ilość pamięci i zasobów obliczeniowych wystarczającą do obsługi dodatkowych zabezpieczeń.
Komunikacja	• Systemy wykorzystują standardowe protokoły komunikacji. • Komunikacja oparta głównie na sieciach przewodowych z lokalnymi urządzeniami bezprzewodowymi. • Zarządzanie oparte na powszechnych praktykach stosowanych w sieciach IT.	• Systemy wykorzystują wiele własnościowych i standardowych protokołów komunikacyjnych. • Komunikacja oparta na różnych rodzajach połączeń przewodowych i bezprzewodowych, w tym wykorzystujących częstotliwości radiowe i łączność satelitarną. • Działanie w złożonych sieciach, które czasami wymagają specjalistycznej wiedzy inżynierów ds. nadzoru technicznego.
Zarządzanie zmianą	• Zmiany w oprogramowaniu są wprowadzane wkrótce po publikacji, zgodnie z dobrymi praktykami i procedurami bezpieczeństwa, proces często jest zautomatyzowany.	• Zmiany w oprogramowaniu muszą być dokładnie testowane i wdrażane stopniowo w całym systemie, aby zagwarantować utrzymanie integralności systemu.

Kategoria	Technologia informacyjna	Technologia operacyjna
		• Wszelkie przestoje muszą być często planowane z kilkudniowym lub kilkutygodniowym wyprzedzeniem. Systemy OT często opierają się na systemach operacyjnych, które nie otrzymują już poprawek producenta. • Systemy OT często wykorzystują niestandardowe aplikacje.
Obsługa zarządzana	• Systemy pozwalają na wykorzystywanie różnych usług wsparcia.	• Wsparcie serwisowe jest zazwyczaj zapewniane przez jednego dostawcę.
Okres eksploatacji komponentów	• Okres eksploatacji wynoszący od trzech do pięciu lat	• Okres eksploatacji wynoszący od dziesięciu do piętnastu lat
Rozmieszczenie komponentów	• Poszczególne komponenty są zwykle łatwo dostępne i znajdują się na miejscu.	• Poszczególne komponenty mogą znajdować się w dużych odległościach, a dostęp do nich może wymagać dużego wysiłku fizycznego.

Słowem podsumowania, różnice dotyczące sposobów działania oraz zagrożeń i ryzyka pomiędzy systemami teleinformatycznymi oraz technologii operacyjnej prowadzą do powstania potrzeby dostosowania działań ukierunkowanych na wdrażanie strategii cyberbezpieczeństwa i strategii operacyjnych. Z tego powodu zapewnienie bezpieczeństwa wymaga ścisłej współpracy międzywydziałowego zespołu obejmującego inżynierów ds. nadzoru technicznego, operatorów systemów sterowania i specjalistów ds. bezpieczeństwa IT, aby kompleksowo zrozumieć możliwe konsekwencje instalacji, obsługi i konserwacji zabezpieczeń w kontekście systemu sterowania. Specjaliści zajmujący się systemami teleinformatycznymi, którzy pracują z systemami technologii operacyjnej muszą zrozumieć wpływ rozwiązań w zakresie bezpieczeństwa informacji na niezawodność przed ich wdrożeniem. Co więcej, ze względu na wyjątkowe wymogi, niektóre systemy operacyjne oraz aplikacje, na których opierają się systemy OT, mogą nie być kompatybilne z produktami komercyjnymi w zakresie cyberbezpieczeństwa systemów teleinformatycznych.

3. OPRACOWANIE PROGRAMU CYBERBEZPIECZEŃSTWA OT

W celu ograniczenia ryzyka związanego z cyberbezpieczeństwem systemów OT, podmioty winny opracować i wdrożyć stosowny program cyberbezpieczeństwa OT. Rzeczony program winien być spójny i zintegrowany z istniejącymi programami i praktykami cyberbezpieczeństwa IT, ale także uwzględniać szczególne wymagania i cechy systemów i środowisk OT. Należy dokonywać regularnych przeglądów oraz aktualizacji planów i programów cyberbezpieczeństwa OT, aby uwzględnić zmiany w obszarach technologii, operacji, norm, przepisów oraz zmienne potrzeby w zakresie bezpieczeństwa poszczególnych obiektów.

Skuteczne połączenie zagadnień cyberbezpieczeństwa i działania systemu OT wymaga opracowania i wdrożenia kompleksowego programu, który obejmuje wszystkie aspekty cyberbezpieczeństwa. Proces ten winien obejmować określenie celów i zakresu programu; ustanowienie zespołu osób rozumiejących zagadnienia technologii operacyjnych oraz cyberbezpieczeństwa; ustanowienie zasad i procedur; określenie możliwości zarządzania ryzykiem związanym z cyberbezpieczeństwem, które obejmują ludzi, procesy i technologie; a także wskazanie codziennych działań w zakresie monitorowania zdarzeń i audytu w celu zapewnienia zgodności i wdrażania usprawnień.

W przypadkach projektowania i wdrażania nowych systemów konieczne jest poświęcenie czasu na uwzględnienie kwestii bezpieczeństwa w całym cyklu życia na poziomach architektury, zamówień, montażu, utrzymania oraz wycofania systemu z eksploatacji. Wdrażanie systemów w terenie w oparciu o założenie, że systemy te zostaną zabezpieczone w późniejszym czasie, jest źródłem znaczącego ryzyka dla systemów i organizacji. Jeśli nie ma wystarczająco dużo czasu i zasobów, aby odpowiednio zabezpieczyć system przed wdrożeniem, prawdopodobieństwo uwzględnienia zabezpieczeń na późniejszym etapie eksploatacji jest znikome. Z racji tego, że nowe systemy OT są projektowane i wdrażane rzadziej niż systemy IT, aktualizowanie, rozszerzanie lub wprowadzanie ulepszeń do istniejącego systemu OT zdarza się częściej niż projektowanie nowych rozwiązań.

Poniższy rozdział opisuje podstawowy proces opracowywania programu cyberbezpieczeństwa OT, który ma zastosowanie zarówno do nowych, jak i już

istniejących systemów OT. Dodatkowe wskazówki dotyczące opracowywania poszczególnych elementów programu cyberbezpieczeństwa systemów OT można znaleźć w podrozdziale 3.3.10.

3.1. OPRACOWANIE STATUTU PROGRAMU CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Kierownictwo wyższego szczebla musi wykazać się zainteresowaniem oraz zaangażowaniem w kwestie związane z cyberbezpieczeństwem, a także jasno komunikować znaczenie tego aspektu w całej organizacji. Cyberbezpieczeństwo to zagadnienie, za które odpowiedzialność spoczywa na wszystkich pracownikach/współpracownikach organizacji, w szczególności zaś na jej kierownictwie oraz zespołach IT i OT. Zaangażowanie w kwestie związane z cyberbezpieczeństwem można wykazać za pośrednictwem opracowania statutu programu cyberbezpieczeństwa obejmującego źródła finansowania, widoczność, zarządzanie oraz wsparcie ze strony kierownictwa wyższego szczebla. Zaangażowanie kierownictwa wyższego szczebla zapewnia większe szanse na realizację misji i celów biznesowych organizacji w zakresie cyberbezpieczeństwa.

Statut programu cyberbezpieczeństwa to napisany prostym językiem opis ogólny, który określa zakres odpowiedzialności za ochronę systemów OT oraz przyznaje stosowne uprawnienia wybranemu przedstawicielowi kierownictwa najwyższego szczebla odpowiedzialnemu za ustanowienie i utrzymanie programu cyberbezpieczeństwa (może to być na przykład CISO[7]). Niniejszy rozdział skupia się na opracowaniu programu dotyczącego systemów OT, który powinien być powiązany z ogólnym programem cyberbezpieczeństwa obowiązującym w organizacji.

Statut programu cyberbezpieczeństwa powinien określać cele i zakres programu, a także opis obowiązków. Kierownictwo wyższego szczebla opracowuje statut programu cyberbezpieczeństwa OT i wskazuje osobę odpowiedzialną za cyberbezpieczeństwo systemów OT, która posiada odpowiednie uprawnienia pozwalające na kierowanie takim

[7] Definicje ról – patrz: NSC 7298.

programem. Osoba ta powinna określić role i obowiązki osób odpowiedzialnych za poszczególne systemy, osoby odpowiedzialne za misje i procesy biznesowe oraz użytkowników. Powinna również udokumentować cele i zakres programu bezpieczeństwa systemów OT, w tym organizacje biznesowe, systemy i sieci, których dotyczy program, wymagany budżet i zasoby oraz podział obowiązków.

Organizacja może mieć już wdrożony lub opracowany program bezpieczeństwa informacji dotyczący istniejących systemów IT. Osoba odpowiedzialna za cyberbezpieczeństwo systemów OT powinna wskazać, które spośród istniejących praktyk należy wykorzystać, a które należy opracować z myślą o potrzebach systemu OT. Działanie to ma na celu zwiększenie efektywności dzięki współdzieleniu informacji i zasobów z innymi jednostkami, które mają podobne cele.

3.2. UZASADNIENIE BIZNESOWE PROGRAMU CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Cyberbezpieczeństwo systemów OT jest kluczowym elementem ogólnego bezpieczeństwa organizacji. Zdarzenia związane z cyberbezpieczeństwem mogą potencjalnie wpłynąć na realizację misji i celów organizacji, a także na środowisko, zgodność z przepisami, a nawet bezpieczeństwo ludzi. Systemy OT mogą być również wykorzystywane przez napastników w roli punktu dostępu do systemów IT i innych systemów organizacji. Ze względu na to, że systemy OT są coraz częściej podłączane do sieci IT, poleganie na tradycyjnych zabezpieczeniach (na przykład izolacji fizycznej) nie wystarcza do ochrony takich systemów przed cyberatakami. Z tego względu kompleksowa ochrona organizacji wymaga wdrożenia środków bezpieczeństwa dostosowanych do potrzeb i wymogów systemów OT. Program cyberbezpieczeństwa systemów OT uwzględnia cechy tych systemów, które wymagają szczególnej uwagi w celu przeciwdziałania zagrożeniom.

3.2.1. KORZYŚCI Z INWESTYCJI W CYBERBEZPIECZEŃSTWO SYSTEMÓW

Cyberbezpieczeństwo systemów OT umożliwia realizację misji oraz działalności biznesowej organizacji, a także zapewnia dodatkowe korzyści, w tym:

- Wzrost bezpieczeństwa, niezawodności i dostępności systemów OT.
- Wzrost wydajności systemów OT.

- Zmniejszenie obaw społeczności.
- Zmniejszenie zagrożeń prawnych.
- Zaspokojenie wymogów regulacyjnych.
- Ułatwienie uzyskania polis ubezpieczeniowych i ograniczenie kosztów.

Kompleksowy program cyberbezpieczeństwa systemów OT ma fundamentalne znaczenie dla prowadzenia zrównoważonej działalności biznesowej i może potencjalnie zwiększyć niezawodność i dostępność chronionych systemów. Dzieje się to za sprawą minimalizacji negatywnych wpływów na bezpieczeństwo informacji w systemach OT wynikających z niedostatecznie dokładnych testów, niewłaściwych zasad i reguł oraz działania błędnie skonfigurowanych systemów. Cyberataki mogą nieść za sobą szereg znaczących skutków, w tym:

- **Skutki fizyczne.** Skutki fizyczne obejmują szereg bezpośrednich konsekwencji awarii systemów OT, w szczególności obrażenia ciała i utratę życia. Inne skutki obejmują zniszczenie mienia (w tym danych) i potencjalne szkody dla środowiska.
- **Skutki gospodarcze.** Skutki gospodarcze należą do drugorzędnych skutków fizycznych incydentu obejmującego systemy OT. Obejmują straty finansowe organizacji, lub innych podmiotów zależnych od systemów OT i ich działania. Awaria infrastruktury krytycznej (na przykład sieci energetycznej czy systemu transportu) może nieść za sobą skutki gospodarcze znacząco przekraczające koszty odtworzenia uszkodzeń i przywrócenia działania po awarii. Skutki te mogą mieć negatywny wpływ na gospodarkę lokalną, regionalną, krajową lub nawet światową.
- **Skutki społeczne**. Kolejną grupą drugorzędnych skutków jest utrata zaufania państwa lub społeczeństwa wobec organizacji.

Inne przykłady potencjalnych skutków incydentu dotyczącego systemów OT zostały wymienione poniżej. Należy pamiętać, że poszczególne elementy znajdujące się na poniższej liście nie są od siebie niezależne. Wyciek niebezpiecznego materiału może doprowadzić na przykład do obrażeń lub śmierci.

- Skutki dotyczące bezpieczeństwa narodowego (na przykład umożliwienie działań grup terrorystycznych).

- Ograniczenie lub zatrzymanie produkcji w jednym zakładzie lub w wielu zakładach jednocześnie.
- Obrażenia lub śmierć pracowników.
- Obrażenia lub śmierć przedstawicieli lokalnej społeczności.
- Uszkodzenie urządzeń.
- Emisja, przekierowanie lub kradzież materiałów niebezpiecznych.
- Zniszczenia środowiska naturalnego.
- Naruszenie przepisów i wymogów regulacyjnych.
- Zanieczyszczenie produktu.
- Konsekwencje karne lub cywilne.
- Utrata wrażliwych lub poufnych informacji.
- Naruszenie wizerunku marki lub zaufania klientów.

Incydenty związane z bezpieczeństwem mogą mieć negatywny wpływ na wszystkich interesariuszy, w tym pracowników, akcjonariuszy, klientów i społeczności, w których działa organizacja, a wpływ ten może być bardziej długotrwały niż w przypadku innych rodzajów incydentów. Kierownictwo wyższego szczebla powinno wskazać i ocenić najważniejsze aspekty działalności, aby oszacować możliwy wpływ na działalność w skali roku (na przykład w przeliczeniu na finanse).

3.2.2. OPRACOWYWANIE UZASADNIENIA BIZNESOWEGO DLA PROGRAMU CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Jasne i dobrze umotywowane uzasadnienie biznesowe dla programu cyberbezpieczeństwa systemów OT jest niezbędne z punktu widzenia kierownictwa, gdyż pozwala zapewnić zaangażowanie całej organizacji w perspektywie długoterminowej oraz umożliwia przydział zasobów wymaganych do opracowania, wdrożenia i utrzymania programu. Pierwszym krokiem do opracowania programu cyberbezpieczeństwa systemów OT jest określenie celów biznesowych i misji organizacji, a także sposobu, w jaki program ten może ograniczyć ryzyko i zapewnić

zdolność organizacji do realizacji tych celów i misji. Uzasadnienie biznesowe powinno uwzględniać obawy kierownictwa wyższego szczebla oraz uzasadniać zarówno skutki biznesowe, jak i wydatki ponoszone w celu opracowania kompleksowego programu cyberbezpieczeństwa organizacji. Powinno także zawierać szczegółowe informacje na temat następujących zagadnień:

- Korzyści z utworzenia kompleksowego programu bezpieczeństwa.
- Potencjalne koszty i scenariusze awarii w przypadku niewdrożenia programu cyberbezpieczeństwa systemów OT.
- Ogólne omówienie procesu wymaganego w celu wdrożenia, obsługi, monitorowania, przeglądu, utrzymania i ulepszania programu bezpieczeństwa informacji.

Należy wziąć pod uwagę koszty i zasoby wymagane do opracowania, wdrożenia i utrzymania programu bezpieczeństwa w organizacji. Korzyści ekonomiczne płynące z programu cyberbezpieczeństwa mogą być oceniane w taki sam sposób, jak korzyści wynikające z programów bezpieczeństwa i higieny pracy. Warto jednak pamiętać, że atak na system OT może mieć znaczące konsekwencje, które mogą wykraczać znacznie poza straty finansowe.

3.2.3. MATERIAŁY POMOCNE W PROCESIE OPRACOWYWANIA UZASADNIENIA BIZNESOWEGO

Dużą pomocą w procesie opracowywania uzasadnienia biznesowego mogą być materiały udostępniane za pośrednictwem platform wymiany informacji, a także przez izby handlowe oraz organizacje normalizacyjne, firmy konsultingowe oraz interesariuszy wewnętrznych odpowiedzialnych za opracowywanie programów zarządzania ryzykiem lub inżynierii i operacji. Podmioty zewnętrzne mogą również być źródłem przydatnych informacji na temat czynników, które skłoniły kierownictwo wyższego szczebla do wspierania wysiłków oraz zasobów, które okazały się najbardziej pomocne w realizacji programu. Chociaż czynniki te mogą różnić się w zależności od branży lub sektora, mogą także występować pewne podobieństwa dotyczące ról, jakie mogą odgrywać inni specjaliści ds. zarządzania ryzykiem. Załącznik D zawiera listę niektórych bieżących działań w zakresie bezpieczeństwa systemów OT.

Pracownicy wewnętrzni zajmujący się zbliżonymi działaniami związanymi z zarządzaniem ryzykiem, na przykład pracownicy odpowiedzialni za obszary bezpieczeństwa informacji, bezpieczeństwa i higieny pracy, bezpieczeństwa środowiskowego, bezpieczeństwa fizycznego czy utrzymania ruchu, mogą zapewnić wsparcie w zakresie ustalania kluczowych zagrożeń i szacowania ich wpływu na działalność. Pracownicy ci mogą również wskazać, które osoby na stanowiskach kierowniczych koncentrują się na określonych rodzajach ryzyka, a także które osoby mogą być najbardziej otwarte na bycie twarzą takich działań.

3.2.4. PRZEDSTAWIENIE UZASADNIENIA BIZNESOWEGO PROGRAMU CYBERBEZPIECZEŃSTWA SYSTEMÓW OT KADRZE KIEROWNICZEJ

Zapewnienie skuteczności programu cyberbezpieczeństwa systemów OT wymaga aktywnego udziału kierownictwa wyższego szczebla. Kadra kierownicza na szczeblu poszczególnych organizacji, odpowiedzialna zarówno za systemy IT, jak i OT ma świadomość ryzyka, a także stosowne uprawnienia, które umożliwiają wzięcie odpowiedzialności za ten aspekt. Kierownictwo wyższego szczebla winno odpowiadać z kolei za zatwierdzanie polityk bezpieczeństwa informacji oraz wyznaczanie ich kierunków, przypisywanie ról i obowiązków związanych z obszarem bezpieczeństwa oraz wdrożenie programu bezpieczeństwa informacji w całej organizacji. Finansowanie realizacji programu może zazwyczaj odbywać się etapami. Choć rozpoczęcie prac nad programem może wymagać pewnych środków, dodatkowe fundusze można pozyskać na dalszym etapie, gdy podatności oraz potrzeby programu w zakresie bezpieczeństwa zostaną lepiej określone, a dodatkowo zostaną przygotowane szczegółowe strategie. Należy także uwzględnić koszty modernizacji systemów OT w celu zapewnienia bezpieczeństwa i zestawić je z kosztami zapewnienia bezpieczeństwa na etapie projektowania.

Często dobrym podejściem do uzyskania akceptacji kierownictwa wyższego szczebla może być oparcie uzasadnienia biznesowego na skutecznym rozwiązaniu podobnego problemu w innej organizacji. W wielu przypadkach może skłonić to przedstawicieli kierownictwa do zadania pytań o to, w jaki sposób dane rozwiązanie może mieć zastosowanie w organizacji.

Podczas przedstawiania uzasadnienia biznesowego pomocne może być również wspomnienie o konkretnych wyzwaniach związanych z zapewnianiem bezpieczeństwa systemów OT:

- Systemy OT działają w innych środowiskach i dotyczą ich wymagania inne niż w przypadku systemów IT. Przykładem może być konieczność zapewnienia dostępności i bezpieczeństwa będąca warunkiem nadrzędnym względem poufności danych.
- Rozwiązania lub narzędzia przeznaczone do systemów IT mogą nie być odpowiednie lub skuteczne w przypadku systemów OT.
- Działania kompensacyjne mogą być skutecznym rozwiązaniem zabezpieczającym system OT bez wpływu na jego wydajność.
- Ochrona systemów OT ma krytyczne znaczenie, a incydent cyberbezpieczeństwa w systemie OT może mieć katastrofalne skutki, które mogą wpłynąć na życie ludzi oraz środowisko.

3.3. TREŚĆ PROGRAMU CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Niniejszy podrozdział zawiera zalecenia dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia programu cyberbezpieczeństwa systemów OT. Zalecenia te mogą być wdrażane niezależnie, co umożliwia organizacjom dokonanie wyboru podejść i technologii najlepiej dostosowanych do ich potrzeb.

Program cyberbezpieczeństwa systemów OT jest zazwyczaj dostosowany do wymogów danego środowiska OT. W skład organizacji może wchodzić wiele zakładów obsługujących wiele zróżnicowanych środowisk OT. W takich sytuacjach należy zdefiniować program bezpieczeństwa systemów OT na poziomie organizacji uwzględniając zalecenia dostosowywane do potrzeb poszczególnych jednostek i środowisk OT.

Skuteczność programu cyberbezpieczeństwa systemów OT może być zwiększana poprzez jego koordynację lub połączenie z procesami i programem bezpieczeństwa informacji organizacji Programy bezpieczeństwa informacji zwykle skupiają się jednak kolejno na poufności, integralności i dostępności informacji w całej organizacji. Programy

bezpieczeństwa informacji nie muszą uwzględniać wszystkich potrzeb i wymogów w zakresie bezpieczeństwa i działania środowiska OT, w którym priorytetem jest bezpieczeństwo (ochrona), a dopiero potem dostępność, integralność i poufność danych. Należy uwzględnić tę różnicę w procesie opracowywania priorytetów programów bezpieczeństwa systemów IT i OT. Dokument NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)* [NSC 800-100], obejmuje omówienie elementów programu bezpieczeństwa informacji, które mogą pomoc w opracowaniu i wdrożeniu programu bezpieczeństwa informacji w organizacji.

Okres eksploatacji typowego systemu OT może przekraczać 20 lat. W rezultacie wiele starszych systemów może obejmować urządzenia i oprogramowanie, które nie są już obsługiwane przez dostawców, nie otrzymują poprawek bezpieczeństwa ani aktualizacji, a podatności ich zabezpieczeń nie są łatane. W takim przypadku program bezpieczeństwa powinien być dostosowany do wyjątkowych cech starszego systemu, a osoby odpowiedzialne za jego wdrażanie powinny sprawdzić, czy poszczególne zabezpieczenia mają zastosowanie do danego systemu. Gdy poszczególne zabezpieczenia nie są obsługiwane przez starszy system OT, należy rozważyć zastosowanie zabezpieczeń kompensacyjnych. Na przykład rozwiązania chroniące przed złośliwym oprogramowaniem mogą nie być dostępne dla sterowników PLC i systemów sterowania DCS. Oznacza to, że wymogi dotyczące ochrony przed złośliwym oprogramowaniem nie mogą być stosowane w przypadku tych urządzeń. W takim przypadku należy rozważyć możliwość wdrożenia zabezpieczeń kompensacyjnych, na przykład użycia zapory sieciowej z funkcją głębokiej inspekcji pakietów, która może monitorować i blokować zaawansowane zagrożenia, takie jak złośliwe oprogramowanie.

Głównym celem inwestycji w program cyberbezpieczeństwa jest zarządzanie ryzykiem. Ryzyko to opiera się na możliwości wykorzystania podatności aplikacji i infrastruktury przez napastników. W związku z tym decyzje dotyczące elementów programu cyberbezpieczeństwa należy podejmować przez pryzmat zarządzania ryzykiem organizacji. Pomocą w procesie opracowywania oraz wdrażania programu cyberbezpieczeństwa uwzględniającego perspektywę zarządzania ryzykiem jest dokument NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach*

informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu, który opisuje ramy zarządzania ryzykiem oraz podstawowe zadania i procesy związane z wdrażaniem programu cyberbezpieczeństwa. Proces ten został omówiony pokrótce w rozdziale 3.3.6 oraz szerzej w rozdziale 4.

Program cyberbezpieczeństwa systemów OT powinien również uwzględniać wyjątki i odstępstwa od zasad. W wymagającym środowisku OT mogą pojawić się sytuacje, które wymagają podjęcia decyzji o wprowadzeniu wyjątku od zasad bezpieczeństwa w celu umożliwienia realizacji misji lub celu systemu OT. Takie odstępstwa oraz wyjątki muszą być podejmowane z rozwagą i każdorazowo wymagają zgody kierownictwa oraz zespołu przedstawicieli wszystkich zaangażowanych działów. Program bezpieczeństwa może być źródłem zasad oraz procedur w zakresie wprowadzania tych wyjątków. Przedstawione wytyczne i dokumenty uwzględniają fakt, że nie istnieje jedno uniwersalne podejście do tych zagadnień. Dostosowując te wytyczne do wymogów danej organizacji, należy oprzeć się na wiedzy i doświadczeniu, uwzględniając ograniczenia dotyczące danej organizacji.

3.3.1. USTANOWIENIE SYSTEMU ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM SYSTEMÓW OT

Zarządzanie systemami OT powinno obejmować zasady, procedury i procesy zarządzania dotyczące wymogów prawnych i regulacji, a także wytyczne w zakresie ryzyka, ochrony środowiska oraz działalności organizacji. Proces zarządzania powinien zapewniać, że pracownicy rozumieją zasady oraz procesy, a jednocześnie służą jako podstawa procesów zarządzania ryzykiem związanym z cyberbezpieczeństwem systemów OT. Aby wypracować skuteczne metody zarządzania cyberbezpieczeństwem systemów OT, należy opracować procesy, wyznaczyć obowiązki oraz wskazać osoby odpowiedzialne na odpowiednich stanowiskach w jednostkach odpowiedzialnych za zarządzanie ryzykiem. Typowy proces zarządzania cyberbezpieczeństwem powinien obejmować następujące elementy:

- Opracowanie, ustanowienie oraz rozpowszechnienie zasad cyberbezpieczeństwa systemów OT.

- Koordynacja ról i obowiązków w zakresie cyberbezpieczeństwa systemów OT, uzgodnienie ról i obowiązków pracowników wewnętrznych i partnerów zewnętrznych.
- Zapewnienie, że wymogi prawne i regulacyjne dotyczące cyberbezpieczeństwa systemów OT, w tym przepisów dotyczących prywatności, są zrozumiałe i uwzględnione.
- Zapewnienie, że ryzyko związane z cyberbezpieczeństwem jest uwzględnione w ramach procesów zarządzania ryzykiem organizacji.

Dodatkowe rekomendacje dotyczące opracowywania wytycznych w zakresie cyberbezpieczeństwa systemów OT można znaleźć w rozdziale 6. Uzupełniające informacje wraz z przykładami ilustrującymi proces ustanawiania jednostek odpowiedzialnych za zarządzanie cyberbezpieczeństwem znajdują się również w raporcie wewnętrznym Narodowego Instytutu Standaryzacji i Technologii (NIST IR) 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.2. ZBUDOWANIE I PRZESZKOLENIE MIĘDZYWYDZIAŁOWEGO ZESPOŁU ODPOWIEDZIALNEGO ZA REALIZACJĘ PROGRAMU CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Zespół do spraw cyberbezpieczeństwa obejmujący przedstawicieli wielu działów i jednostek organizacyjnych powinien wykorzystywać swoją zróżnicowaną wiedzę oraz doświadczenie związane z różnymi sektorami i obszarami w celu przeprowadzenia oceny ryzyka dotyczącego systemów OT i jego skutecznego ograniczenia. W skład zespołu ds. cyberbezpieczeństwa systemów OT powinny wejść następujące osoby: pracownicy działu IT, inżynier ds. nadzoru technicznego, operator systemu sterowania, specjalista ds. bezpieczeństwa i zarządzania ryzykiem w podmiocie. Zespół ds. bezpieczeństwa informacji powinien również obejmować wszelkich dostawców usług w zakresie cyberbezpieczeństwa.

Z punktu widzenia bezpieczeństwa, poważne ryzyko wypadku oraz utrata szczelności spowodowana awarią sprzętu lub błędami operatora mogą nieść za sobą poważne konsekwencje. Cyberbezpieczeństwo jest kolejnym wyzwaniem dla bezpieczeństwa i niezawodności procesów przemysłowych, zatem włączenie ekspertów ds. bezpieczeństwa

do zespołu ds. cyberbezpieczeństwa jest ważne z punktu widzenia ustalania obszarów potencjalnego wpływu związanych z podatnościami dotyczącymi cyberbezpieczeństwa. Wiedza tych osób na temat projektowania systemów OT i zagadnień związanych z bezpieczeństwem pomoże również w opracowywaniu zabezpieczeń.

Choć inżynier ds. nadzoru technicznego odgrywa ważną rolę w procesie zabezpieczania systemów OT, nie jest w stanie robić tego skutecznie bez współpracy i wsparcia zarówno ze strony działu IT, jak i przedstawicieli kierownictwa. Pracownicy działu IT często dysponują wieloletnim doświadczeniem w zakresie cyberbezpieczeństwa, a wiele rozwiązań może mieć przełożenie na systemy OT. Ze względu na różnice pomiędzy sektorami inżynierii oraz i IT, połączenie kompetencji obu działów ma kluczowe znaczenie dla procesu wspólnego projektowania i wdrażania zabezpieczeń.

Organizacje charakteryzują się różnymi rozmiarami, strukturami, zasięgami geograficznymi i złożonością. Wszystkie te czynniki, podobnie jak strategie oparte na dostępnych zasobach oraz środkach finansowych, mogą skłonić organizacje do zatrudnienia pracowników zajmujących się cyberbezpieczeństwem systemów OT w roli pracowników etatowych lub wykonawców. Alternatywnym rozwiązaniem jest zlecenie zadań związanych z zapewnieniem bezpieczeństwa systemów OT podmiotowi zewnętrznemu. Niezależnie od wybranego rozwiązania, zespół odpowiedzialny za zarządzanie cyberbezpieczeństwem systemów OT powinien być powiązany z zespołem odpowiedzialnym za cyberbezpieczeństwo systemów IT i zespołem odpowiedzialnym za zarządzanie ryzykiem podmiotu.

Odpowiedzialność za wdrażanie działań w zakresie cyberbezpieczeństwa zwykle spoczywa na organizacji odpowiadającej za infrastruktury IT i OT, natomiast wskaźniki operacyjne i informacje na tematy ryzyka związanego z cyberbezpieczeństwem są przekazywane do jednostki odpowiedzialnej za zarządzanie ryzykiem. Skuteczność programu wymaga współpracy między tymi jednostkami w zakresie finansowania i oczekiwań dotyczących osiągnięć z uwzględnieniem dostępnych zasobów finansowych oraz pracowników. Jednostka odpowiedzialna za zarządzanie ryzykiem współpracuje z kierownictwem wyższego szczebla w celu określenia poziomu tolerowanego ryzyka oraz ryzyka szczątkowego.

W procesie budowania zespołu ds. cyberbezpieczeństwa należy uwzględnić następujące zadania:

- Ustanowienie oraz utrzymanie ról i obowiązków w zakresie cyberbezpieczeństwa w celu budowania, obsługi i ulepszania programu cyberbezpieczeństwa systemów OT.
- Ustanowienie ról i obowiązków w zakresie cyberbezpieczeństwa dla dostawców zewnętrznych, obejmujących dostawców usług, wykonawców i inne organizacje odpowiedzialne za rozwój i usługi systemów OT oraz zarządzanie bezpieczeństwem.

Dodatkowe rekomendacje dotyczące budowy zespołu znajdują się w rozdziale 4 oraz w Załączniku D do niniejszego dokumentu. Informacje zilustrowane przykładami znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.3. OPRACOWANIE STRATEGII CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Strategia zarządzania ryzykiem w organizacji stanowi podstawę do opracowania strategii cyberbezpieczeństwa systemów OT[8]. Strategia cyberbezpieczeństwa systemów OT opiera się na strategii zarządzania ryzykiem w organizacji, w tym na określonym poziomie tolerowanego ryzyka, opisanych zagrożeniach, założeniach, ograniczeniach, priorytetach i kompromisach. Na jej podstawie jest następnie dostosowywana do wymogów programu cyberbezpieczeństwa systemów OT.

Strategia cyberbezpieczeństwa systemów OT:

- Stanowi uzupełnienie i uszczegółowienie wytycznych zawartych w strategii zarządzania ryzykiem organizacji, uwzględnia także ograniczenia i wymagania dotyczące systemów OT,

[8] Dodatkowe informacje na temat opracowywania strategii zarządzania ryzykiem w organizacji znajdują się w dokumencie [NIST SP 800-37] w rozdziale poświęconym przygotowaniu zadań i rezultatów, zwłaszcza w zadaniu P-2 – Strategia zarządzania ryzykiem. W rozdziale 3 znajdują się także dodatkowe informacje na temat wyznaczania zadań na szczeblu organizacji i poszczególnych systemów, których celem jest przygotowanie do wdrożenia ram zarządzania ryzykiem wynikających z NIST Risk Management Framework.

- Obejmuje skład zespołu oraz wskazuje osoby odpowiedzialne za cyberbezpieczeństwo systemów OT,
- Określa model realizacji działań dotyczących cyberbezpieczeństwa systemów OT (na przykład wykorzystanie pracowników wewnętrznych, zlecenie zadań podmiotom zewnętrznym bądź skorzystanie z usług zarządzanych),
- Opisuje architekturę cyberbezpieczeństwa dotyczącą różnych jednostek w ramach programu cyberbezpieczeństwa OT,
- Wskazuje szkolenia i działania uświadamiające w zakresie cyberbezpieczeństwa związanego z systemami OT.

Celem strategii cyberbezpieczeństwa OT jest zwiększanie poziomu tolerowanego ryzyka w organizacji związanego z systemami OT. Założenie to wpływa na priorytety działań związanych z cyberbezpieczeństwem systemów OT. Program ten powinien uwzględniać zagadnienia i wymogi związane z systemami IT oraz OT. Dla przykładu: przedstawiciele działu IT mogą uznać utratę danych lub przerwę w dostępności systemu za wyższy priorytet, jednak pracownicy odpowiedzialni za systemy OT mogą uznawać bezpieczeństwo systemu, wydajność produkcji i szkody wyrządzone środowisku jako ważniejsze kwestie.

Dodatkowe rekomendacje dotyczące opracowywania strategii cyberbezpieczeństwa OT można znaleźć w rozdziałach 5 oraz 6, a także w Załącznikach C i D. Informacje uzupełniające i przykłady strategii cyberbezpieczeństwa systemów OT znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.4. OKREŚLENIE ZASAD ORAZ PROCEDUR DOTYCZĄCYCH SYSTEMÓW OT

Zasady i procedury mają zasadnicze znaczenie dla skutecznej realizacji każdego programu cyberbezpieczeństwa. Tam, gdzie to możliwe, polityki i procedury bezpieczeństwa dotyczące systemów OT powinny opierać się na istniejących zasadach oraz procedurach operacyjnych w zakresie cyberbezpieczeństwa IT i jednostek w celu zapewnienia spójności w całej organizacji.

Jak wspomniano wcześniej, odpowiedzialność za określenie i przekazywanie informacji na temat poziomu tolerowanego ryzyka (poziomu ryzyka, które organizacja jest skłonna zaakceptować) w organizacji spoczywa na jej kierownictwie. Na podstawie tych informacji osoba odpowiedzialna za cyberbezpieczeństwo systemów OT kształtuje strategię zarządzania ryzykiem. Opracowanie zasad i strategii cyberbezpieczeństwa powinno opierać się na ocenie ryzyka uwzględniającej priorytety i cele bezpieczeństwa organizacji. W związku z tym konieczne jest wypracowanie procedur dotyczących realizacji zasad, które umożliwiają ich kompleksowe wdrożenie w systemach OT. Procedury dotyczące cyberbezpieczeństwa winny być dokumentowane, testowane i okresowo aktualizowane w związku ze zmianami dotyczącymi obowiązujących zasad i strategii, dostępnych technologii i zagrożeń.

Dodatkowe rekomendacje dotyczące opracowywania polityk i procedur dotyczących systemów OT znajdują się w rozdziale 6. Informacje uzupełniające wraz z przykładami ilustrującymi proces ustanawiania procedur i zasad dotyczących systemów OT znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.5. USTANOWIENIE PROGRAMU SZKOLENIOWEGO W ZAKRESIE ŚWIADOMOŚCI CYBERBEZPIECZEŃSTWA DLA JEDNOSTEK ZWIĄZANYCH Z SYSTEMAMI OT

Jednym z wymogów wobec organizacji jest zapewnienie, że wszyscy pracownicy, których praca ma związek z systemami OT – w tym pracownicy wewnętrzni, wykonawcy, konsultanci i dostawcy – przejdą stosowne szkolenia dotyczące cyberbezpieczeństwa, które omówią zagadnienia związane ze środowiskiem OT. Edukacja ta powinna stanowić dodatek do szkoleń w zakresie cyberbezpieczeństwa systemów IT. Szkolenie to ma na celu przekazanie pracownikom podstawowych zasad cyberbezpieczeństwa, uświadomienie potencjalnego wpływu tego zagadnienia na bezpieczeństwo oraz wskazanie zasad postępowania, których należy przestrzegać w czasie pracy z systemami OT. Przejście stosownego szkolenia dotyczącego cyberbezpieczeństwa powinno być wymagane w przypadku nowych pracowników

w chwili zatrudnienia. Stosowne szkolenia winny być także przeprowadzane w regularnych odstępach czasu, zgodnie z wymogami prawnymi zasadami obowiązującymi w organizacji.

Dodatkowe rekomendacje dotyczące szkolenia w zakresie cyberbezpieczeństwa systemów OT znajdują się w rozdziale 6 i Załączniku D. Informacje uzupełniające wraz z przykładami szkoleń w zakresie cyberbezpieczeństwa systemów OT znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.6. WDROŻENIE RAM ZARZĄDZANIA RYZYKIEM ZWIĄZANYCH Z SYSTEMAMI OT

Obok ryzyka finansowego, ryzyka w zakresie bezpieczeństwa, ryzyka środowiskowego lub ryzyka związanego z bezpieczeństwem systemów informatycznych, ryzyko związane z systemami OT jest kolejną kategorią ryzyka, którym musi zarządzać organizacja. Przedstawiciele kadry kierowniczej odpowiedzialni za misje lub funkcje biznesowe opracowują i wdrażają program zarządzania ryzykiem we współpracy z kierownictwem wyższego szczebla. Dokument NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji* [NSC 800-39] opisuje ramy programu zarządzania ryzykiem na poziomie organizacji, który został szczegółowo opisany w rozdziale 4 niniejszego dokumentu. Pracownicy odpowiedzialni za systemy OT powinni uczestniczyć w procesie opracowywania programu zarządzania ryzykiem związanym z cyberbezpieczeństwem systemów OT oraz w komunikacji z przedstawicielami kierownictwa wyższego szczebla.

Dokument NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* [NIST SP 800-37] zawiera informacje na temat procesu zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością. Proces ten obejmuje przygotowanie do kompleksowego zarządzania ryzykiem w całej organizacji, kategoryzację systemów, wybór stosownych zabezpieczeń, wdrożenie i ocenę zabezpieczeń, autoryzację zabezpieczeń systemów oraz zabezpieczeń wspólnych, a także ciągłe monitorowanie.

Proces stosowania ram zarządzania ryzykiem w kontekście systemów OT został opisany szczegółowo w rozdziale 4.

3.3.7. USTANOWIENIE MOŻLIWOŚCI W ZAKRESIE DOKUMENTACJI KONSERWACJI

Należy ustanowić procesy i wdrożyć stosowne narzędzia w celu zapewnienia, że zarówno rutynowe, jak i zapobiegawcze konserwacje oraz naprawy systemów OT (zarówno lokalnych, jak i zdalnych) będą realizowane zgodnie z zasadami i procedurami dotyczącymi systemów OT obowiązującymi w organizacji. Narzędzia wykorzystywane w celu dokumentacji i śledzenia prac powinny podlegać odpowiedniemu nadzorowi i zarządzaniu. Należy dołożyć wszelkich starań, by upewnić się, że procesy i narzędzia umożliwiają planowanie, autoryzację, dokumentację, monitorowanie i kontrolowanie prac konserwacyjnych i naprawczych dotyczących komponentów systemów OT. Jeśli wymagana jest możliwość przeprowadzenia zdalnej konserwacji, należy upewnić się, że narzędzie zdalnego dostępu obsługuje funkcje uwierzytelniania pracowników przeprowadzających prace konserwacyjne, nawiązywanie łączności z chwilą rozpoczęcia prac konserwacyjnych i natychmiastowe rozłączanie po zakończeniu prac. Należy zadbać także o to, by stosowne narzędzia dokumentowały czynności wykonywane w ramach zdalnej konserwacji.

Dodatkowe rekomendacje dotyczące dokumentacji konserwacji systemów OT można znaleźć w rozdziale 6. Informacje uzupełniające wraz z konkretnymi przykładami dokumentacji prac konserwacyjnych dotyczących systemów OT znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.8. ROZBUDOWA MOŻLIWOŚCI W ZAKRESIE REAGOWANIA NA INCYDENTY

Jednym z oczekiwań wobec organizacji jest wyznaczenie zespołu odpowiedzialnego za reagowanie na incydenty związane z cyberbezpieczeństwem systemów OT, do którego obowiązków będą należały planowanie działań, wykrywanie i analiza incydentów, a także ograniczanie skutków oraz informowanie na temat działań podejmowanych w przypadku ich wystąpienia. Zbudowanie tego zespołu wymaga

wyznaczenia osób odpowiedzialnych za szereg działań dotyczących cyberbezpieczeństwa, w tym zarządzania incydentami, analizy incydentów, zarządzania podatnościami i komunikacji w ramach incydentu. W ramach tych działań dział odpowiedzialny za cyberbezpieczeństwo systemów OT powinien opracować plan reagowania na incydenty. Celem ustanowienia takiego zespołu jest określenie ryzyka wystąpienia incydentów w zakresie cyberbezpieczeństwa oraz ich potencjalnego zakresu, zapewnienie możliwości reagowania na incydenty, przekazania informacji o incydencie wszystkim zainteresowanym stronom i zmniejszenie jego potencjalnego wpływu. Założenia te dotyczą wszystkich pracowników odpowiedzialnych za systemy OT, a także sieci, systemów i danych OT. Plan reagowania na incydenty stanowi podstawę działań zespołu odpowiedzialnego za cyberbezpieczeństwo i umożliwia reagowanie, komunikację i koordynację działań w przypadku wystąpienia incydentu związanego z cyberbezpieczeństwem. Bez takiego planu organizacja może mieć ogromne trudności z reagowaniem w przypadku wystąpienia incydentu związanego z cyberbezpieczeństwem. Plan winien obejmować role i obowiązki pracowników, działania w zakresie reagowania na incydenty, rodzaje incydentów oraz klasyfikację poziomu dotkliwości, dane kontaktowe kluczowych pracowników, którzy powinni brać udział w procesie reagowania, dane kontaktowe podmiotów zewnętrznych, które mogą stanowić pomoc w reagowaniu na incydenty, zasady udostępniania informacji oraz zasady komunikacji zewnętrznej i wewnętrznej.

Dodatkowe rekomendacje dotyczące reagowania na incydenty związane z cyberbezpieczeństwem systemów OT można znaleźć w rozdziale 6.2.4.5 i Załączniku C do niniejszego dokumentu. Informacje uzupełniające wraz z przykładami reakcji na incydenty związane z systemami OT znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.9. USTANOWIENIE ZDOLNOŚCI W ZAKRESIE PRZYWRACANIA SYSTEMÓW ORAZ ODZYSKIWANIA

Jednym z działań organizacji powinno być zapewnienie możliwości przywrócenia systemów po wystąpieniu incydentów związanych z cyberbezpieczeństwem oraz

odtwarzania zasobów i usług, które ucierpiały w wyniku incydentu, do stanu sprzed jego wystąpienia. Proces ten obejmuje zwykle następujące zadania:

- Określenie celów dotyczących odzyskiwania w przypadku wystąpienia zakłóceń. Oznacza to na przykład stwierdzenie, że przed ponownym uruchomieniem systemu OT, którego działanie zostało przerwane w wyniku zdarzenia związanego z cyberbezpieczeństwem, działania w zakresie odzyskiwania powinny skupiać się przede wszystkim na bezpieczeństwie ludzi i środowiska.
- Opracowanie planu odtworzenia po katastrofie i planu ciągłości działania w celu przygotowania organizacji do podjęcia odpowiednich działań w przypadku wystąpienia znaczących zakłóceń w działaniu systemów OT wynikających z incydentu związanego z cyberbezpieczeństwem.
- Ustanowienie mechanizmów i procesów tworzenia kopii zapasowych w celu zabezpieczenia informacji na temat stanów systemów OT, a także stosownych danych, plików konfiguracyjnych i aplikacji w regularnych odstępach czasu w celu umożliwienia przywrócenia ich do stabilnego działania.
- Opracowanie procesów umożliwiających sprawne przeprowadzenie przywracania stanu systemów OT, danych, plików konfiguracyjnych i aplikacji z kopii zapasowych.
- Ustanowienie procesów i procedur odzyskiwania pozwalających na przywrócenie i odtworzenie zasobów i usług związanych z systemami OT, które ucierpiały w wyniku incydentu związanego z cyberbezpieczeństwem.
- Opracowanie planów komunikacji w celu koordynacji działań związanych z odtwarzaniem z wewnętrznymi i zewnętrznymi interesariuszami oraz przedstawicielami kierownictwa.
- Opracowanie planów komunikacji na potrzeby komunikacji zewnętrznej.
- Uwzględnienie czasu na wyciąganie wniosków w ramach procesu odzyskiwania w celu ciągłego doskonalenia działań w zakresie cyberbezpieczeństwa (obejmujących między innymi zarządzanie podatnościami, działania dotyczące zapewniania cyberbezpieczeństwa, reagowanie na incydenty i odtwarzanie systemów).

- Testowanie opracowanych planów w regularnych odstępach czasu, ustalonych zgodnie z wymogami organizacji.

Dodatkowe rekomendacje dotyczące odtwarzania i przywracania systemów OT zostały przedstawione w rozdziale 6. Informacje uzupełniające wraz z konkretnymi przykładami dotyczącymi odtwarzania i przywracania systemów OT znajdują się również w dokumencie NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.10. SKRÓCONE PRZEDSTAWIENIE ZAŁOŻEŃ PROGRAMU CYBERBEZPIECZEŃSTWA OT

W tym rozdziale zostały opisane elementy programu cyberbezpieczeństwa i różne zagadnienia związane z ustanowieniem takiego programu. Dalsze wytyczne można znaleźć w kolejnych rozdziałach niniejszego dokumentu, których szczegółowa lista znajduje się w **Tabeli 2**.

Tabela 2. Rozdziały zawierające szczegółowe wytyczne dotyczące ustanawiania programu cyberbezpieczeństwa

Element programu cyberbezpieczeństwa	Numer rozdziału zawierającego dodatkowe wytyczne
Ustanowienie systemu zarządzania cyberbezpieczeństwem systemów OT	Rozdział 6
Zbudowanie i przeszkolenie międzywydziałowego zespołu odpowiedzialnego za realizację programu cyberbezpieczeństwa systemów OT	Rozdział 4, Załącznik D
Opracowanie strategii cyberbezpieczeństwa systemów OT	Rozdziały 5 i 6, Załączniki C oraz D
Określenie zasad oraz procedur dotyczących systemów OT	Rozdział 6
Ustanowienie programu szkoleniowego w zakresie świadomości cyberbezpieczeństwa dla jednostek związanych z systemami OT	Rozdział 6, Załącznik D
Wdrożenie ram zarządzania ryzykiem związanych z systemami OT	Rozdziały 4 i 6, Załączniki C oraz D
Ustanowienie możliwości w zakresie dokumentacji konserwacji	Rozdział 6
Rozbudowa możliwości w zakresie reagowania na incydenty	Rozdział 6, Załącznik C
Ustanowienie zdolności w zakresie przywracania systemów oraz odzyskiwania	Rozdział 6

4. ZARZĄDZANIE RYZYKIEM DOTYCZĄCYM SYSTEMÓW OT

Organizacje codziennie zarządzają ryzykiem podczas realizacji swoich celów biznesowych, w tym ryzykiem związanym z możliwością wystąpienia strat finansowych, awarii urządzeń czy zagrożeń dla bezpieczeństwa pracowników. W związku z tym opracowują procesy oceny ryzyka związanego z ich działalnością i decydują, jak zarządzać tym ryzykiem w oparciu o priorytety, poziom tolerowanego ryzyka oraz ograniczenia wewnętrzne i zewnętrzne. Zarządzanie ryzykiem jest dynamicznym i ciągłym procesem, który stanowi element normalnej działalności organizacji. W przeszłości podmioty wykorzystujące w swojej działalności systemy OT zarządzały ryzykiem poprzez stosowanie dobrych praktyk w zakresie bezpieczeństwa i inżynierii. Także przeprowadzanie ocen bezpieczeństwa stanowi element działalności wielu sektorów i często jest ujęte w wymogach regulacyjnych. Zarządzanie ryzykiem związanym z bezpieczeństwem informacji to dodatkowy wymiar tego procesu, który może mieć charakter uzupełniający wobec podstawowych zagadnień. Proces zarządzania ryzykiem i ramy przedstawione w niniejszym rozdziale można zastosować do zarządzania bezpieczeństwem fizycznym, bezpieczeństwem informacji i ryzykiem związanym z łańcuchem dostaw. W przypadku niektórych systemów OT czynnikiem ryzyka może być także prywatność. Dodatkowe wytyczne dotyczące zarządzania ryzykiem związanym z prywatnością znajdują się w ramach zarządzania ryzykiem stanowiących element NIST Risk Management Framework and the Privacy Framework.

Proces zarządzania ryzykiem winien być realizowany w całej organizacji przy użyciu podejścia do ryzyka obejmującego trzy główne poziomy – (I) poziom organizacji, (II) poziom misji i procesów biznesowych oraz (III) poziom systemów – w tym wypadku systemów IT oraz OT. Proces zarządzania ryzykiem jest realizowany na każdym z trzech poziomów, a jego ogólnym celem jest ciągłe doskonalenie działań organizacji związanych z ryzykiem oraz skuteczna komunikacja międzypoziomowa i wewnątrzpoziomowa wśród interesariuszy zainteresowanych działaniami w tym zakresie oraz w sukcesie biznesowym organizacji.

Niniejszy rozdział koncentruje się przede wszystkim na zagadnieniach związanych z systemami OT, a opisane działania skupiają się głównie na poziomie systemów, choć

działania związane z zarządzaniem ryzykiem, informacje i artefakty realizowane na poszczególnych poziomach wpływają na działania podejmowane na pozostałych poziomach. W rozdziale 6 został opracowany przykład zastosowania ram cyberbezpieczeństwa w kontekście systemów OT, z kolei Załącznik F zawiera zalecenia dotyczące rozwiązań OT, które rozszerzają zakres kategorii zabezpieczeń opisanych w dokumencie NSC 800-53 [NSC 800-53]. W tym rozdziale omówione zostały także zagadnienia dotyczące systemów OT oraz ich wpływ na proces zarządzania ryzykiem.

Więcej informacji na temat zarządzania ryzykiem na wielu poziomach oraz procesu zarządzania ryzykiem można znaleźć w dokumentach: NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji* [NSC 800-39] oraz NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* [NSC 800-37].

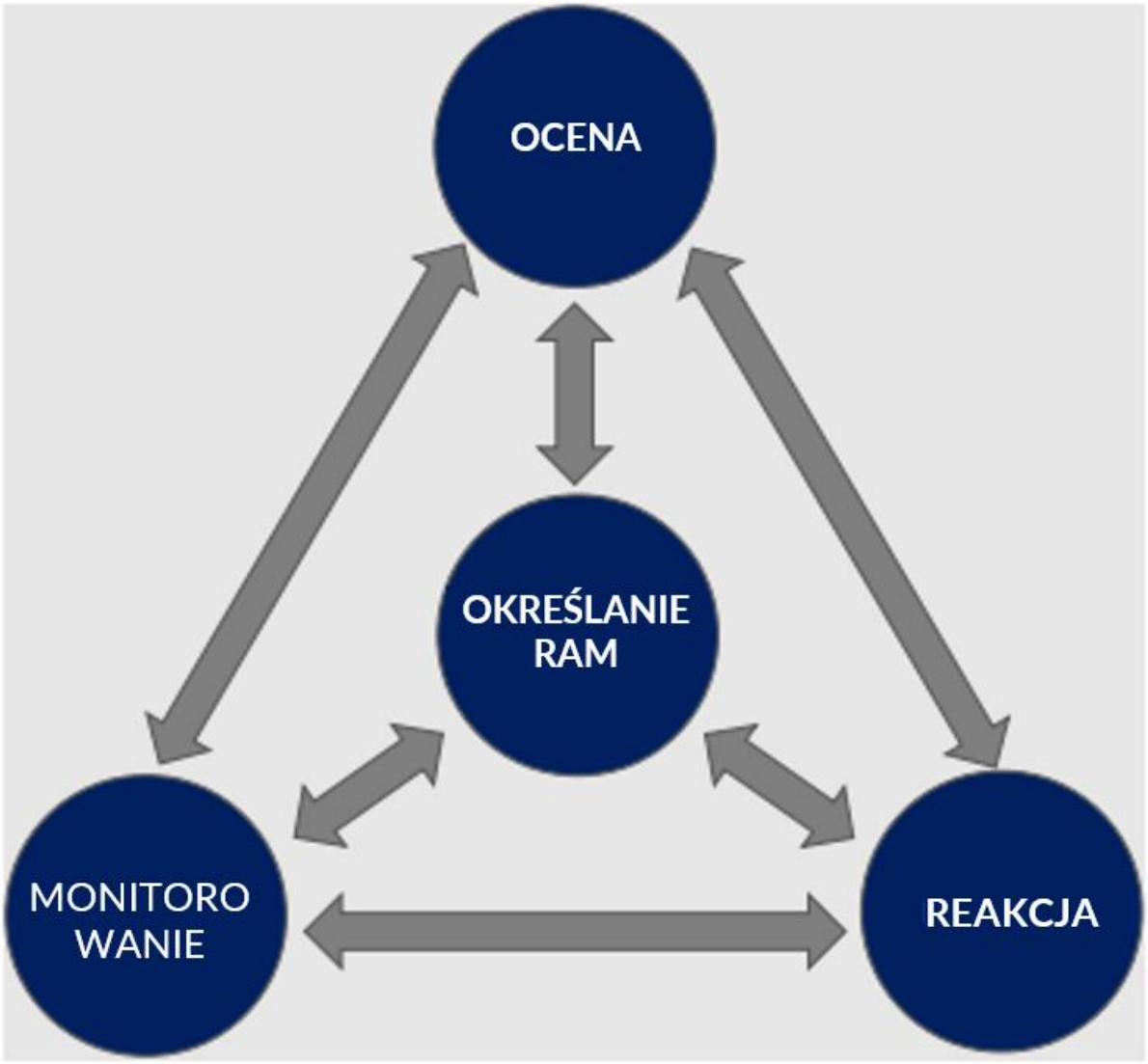
Dokument [NSC 800-37] zawiera wytyczne dotyczące stosowania ram zarządzania ryzykiem w rządowych systemach informatycznych, w tym prowadzenia działań związanych z kategoryzacją bezpieczeństwa[9], wyborem i wdrażaniem środków bezpieczeństwa, oceną środków bezpieczeństwa, autoryzacją systemu informacyjnego[10] oraz monitorowania środków bezpieczeństwa. Dokument NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* [NSC 800-30] opisuje proces (I) przygotowania organizacji do przeprowadzenia szacowania ryzyka, (II) przeprowadzenia szacowania ryzyka, (III) przekazania wyników szacowania ryzyka kluczowym pracownikom w organizacji oraz (IV) aktualizowania szacowania ryzyka w czasie.

[9] Dokument NSC 199 – *Standardy kategoryzacji bezpieczeństwa* [NSC 199] określa wytyczne w zakresie kategoryzacji bezpieczeństwa dla systemów, które nie wpływają na bezpieczeństwo narodowe. Z kolei instrukcja nr 1253 wydana przez Komisję krajowych systemów bezpieczeństwa (CNSS) zawiera zbliżone wytyczne dotyczące systemów wpływających na bezpieczeństwo narodowe.

[10] Autoryzacja bezpieczeństwa to oficjalna decyzja wydana przez przedstawicieli wyższego szczebla organizacji, zezwalająca na działanie systemu informacyjnego i jednoznacznie akceptująca ryzyko dla działalności jednostki organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacji, osób, innych organizacji i narodu na podstawie wdrożenia uzgodnionego zestawu środków bezpieczeństwa i prywatności.

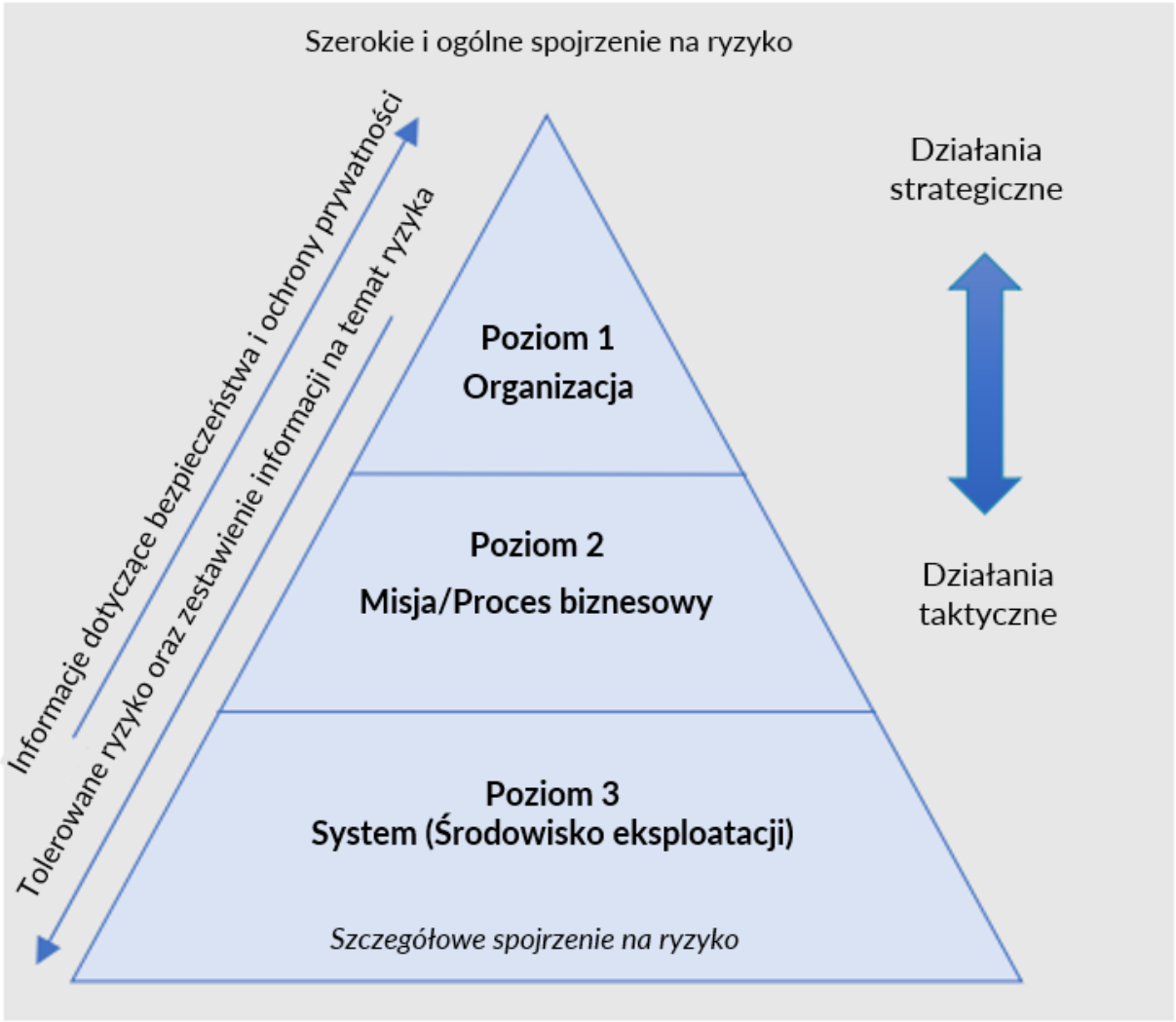
4.1. ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA ZWIĄZANYM Z SYSTEMAMI OT

Choć proces zarządzania ryzykiem opisany w treści dokumentu NSC 800-39 [NSC 800-39] ma zastosowanie do wszystkich rodzajów systemów, zarządzanie ryzykiem związanym z systemami OT wymaga uwzględnienia szeregu wyjątkowych cech charakteryzujących ich działanie. Jak pokazuje **Rysunek 13**, proces zarządzania ryzykiem składa się z czterech kroków – *określania ram ryzyka* (które stanowią kontekst dla podejmowania decyzji opartych na ryzyku), *oceny ryzyka*, *reagowania na ryzyko* oraz *monitorowania ryzyka*. Poszczególne kroki są współzależne i często są realizowane jednocześnie w organizacjach. Za przykład może posłużyć etap monitorowania ryzyka, który może wpływać na etap określania ram ryzyka. Ze względu na zmienność środowisk, w jakich działają organizacje, zarządzanie ryzykiem musi być procesem ciągłym, co wymaga nieustannej realizacji działań w ramach wszystkich czterech etapów. Należy pamiętać, że proces ten ma zastosowanie do zarządzania każdym rodzajem ryzyka, w tym ryzykiem związanym z cyberbezpieczeństwem, bezpieczeństwem fizycznym czy finansami. Podrozdziały od 4.1.1 do 4.1.4 zawierają szczegółowe opisy poszczególnych etapów procesu zarządzania ryzykiem oraz wytyczne w zakresie stosowania ich w kontekście systemów OT.



Rysunek 13. Proces zarządzania ryzykiem: Określanie ram ryzyka, Ocena ryzyka, Reagowanie na ryzyko oraz Monitorowania ryzyka.

Proces zarządzania ryzykiem w całej organizacji jest realizowany na trzech poziomach, przedstawionych na **Rysunku 14** . Poziom 1 obejmuje zarządzanie ryzykiem na szczeblu całej organizacji oraz zakłada określanie ram ryzyka, które stanowią kontekst dla wszystkich działań związanych z zarządzaniem ryzykiem w organizacji. Poziom 2 obejmuje zarządzanie ryzykiem na szczeblu misji i procesów biznesowych, które opiera się na kontekście, decyzjach oraz działaniach podejmowanych na poziomie 1. Poziom 3 obejmuje zarządzanie ryzykiem na szczeblu poszczególnych systemów. Działania podejmowane na tym poziomie opierają się na działaniach i rezultatach wypracowanych na poziomach 1 i 2.



Rysunek 14. Poziomy zarządzania ryzykiem: Poziom organizacji, Poziom misji i procesów biznesowych oraz Poziom systemów

Każdy z etapów procesu zarządzania ryzykiem (określania ram ryzyka, ocena ryzyka, reagowanie na ryzyko oraz monitorowanie ryzyka) jest realizowany na każdym poziomie, czego skutkiem jest pełna świadomość ryzyka w całej organizacji oraz identyfikowalność i przejrzystość decyzji opartych na ryzyku.

4.1.1. OKREŚLANIE RAM RYZYKA W KONTEKŚCIE SYSTEMÓW OT

Etap określania ram ryzyka obejmuje procesy umożliwiające ustalenie kluczowych założeń, ograniczeń, tolerancji ryzyka i strategii zarządzania ryzykiem dla organizacji w celu podejmowania spójnych decyzji w zakresie zarządzania ryzykiem. Celem tego procesu jest wsparcie opracowania ogólnej strategii zarządzania ryzykiem w oparciu

o zagadnienia dotyczące struktury zarządzania organizacją, otoczenia prawnego i obowiązujących regulacji, a także innych czynników, na podstawie których organizacja będzie oceniać ryzyko dotyczące wszystkich systemów IT i OT, a także reagować na jego wystąpienie i skutecznie je monitorować.

Zalecenia i wytyczne dotyczące systemów OT

W przypadku operatorów systemów OT kwestia bezpieczeństwa ma bezpośredni wpływ na podejmowanie decyzji dotyczących projektowania i obsługi systemów. Bezpieczeństwo oznacza w tym przypadku pewność, że nie wystąpią warunki, które mogą doprowadzić do śmierci, urazów, obrażeń, chorób zawodowych, uszkodzeń lub zniszczenia sprzętu lub mienia, a także zniszczeń środowiskowych[11]. W związku z powyższym, wpływ na bezpieczeństwo ludzi zwykle ocenia się na podstawie zakresu obrażeń, chorób lub śmierci, które mogą wynikać z nieprawidłowego działania systemu OT w wyniku incydentu związanego z cyberbezpieczeństwem, przy uwzględnieniu wszelkich uprzednio przeprowadzonych ocen wpływu na bezpieczeństwo pracowników i społeczeństwa. Znaczenie bezpieczeństwa i rozwoju kultury bezpieczeństwa odgrywa kluczową rolę w określaniu poziomu tolerowanego ryzyka.

Organizacje powinny rozważyć uwzględnienie analizy wpływu cyberbezpieczeństwa na systemy OT, które mają wpływ na bezpieczeństwo pracowników i środowiska, a także wdrożenie stosownych środków bezpieczeństwa. W szczególności organizacje mogą wziąć pod uwagę zastosowanie kompleksowego procesu systematycznego przewidywania lub identyfikowania zachowań operacyjnych występujących w przypadku każdej krytycznej dla bezpieczeństwa awarii, usterki oraz instancji błędu ludzkiego, który może skutkować zagrożeniem dla ludzi.

Organizacje powinny również uwzględnić wpływ starszych systemów i komponentów na ich otoczenie. Szczególnie starsze systemy mogą nie mieć możliwości obsługi rozwiązań w zakresie cyberbezpieczeństwa, co może doprowadzić do przekroczenia poziomów ryzyka tolerowanego przez organizację.

[11] Por. https://csrc.nist.gov/glossary/term/safety

Kolejnym ważnym zagadnieniem dla operatorów systemów OT jest dostępność usług realizowanych przez system OT. System OT może być częścią infrastruktury krytycznej, na przykład systemów wodociągowych lub energetycznych, w przypadku których istnieje potrzeba ciągłego i niezawodnego działania. W rezultacie systemy OT mogą być objęte ścisłymi wymogami dotyczącymi dostępności oraz czasu przywrócenia działania w przypadku awarii. Organizacje muszą być świadome takich wymogów oraz odpowiednio planować nadmiarowość z myślą o zapewnieniu stosownego poziomu odporności swoich środowisk operacyjnych, a także uwzględnić te wymogi w swoich ramach ryzyka. Takie działanie pomaga organizacjom w podejmowaniu decyzji dotyczących ryzyka, które pozwalają uniknąć niezamierzonych skutków dotykających osób zależnych od świadczonych usług. Organizacje powinny przede wszystkim uwzględnić w swoich ocenach współzależne systemy OT, w przypadku których istnieje ryzyko związane z cyberbezpieczeństwem zagrażające dostępności systemu.

Organizacje powinny także wziąć pod uwagę możliwości rozprzestrzeniania się skutków incydentu na połączone systemy oraz ich komponenty. Systemy OT mogą być bowiem połączone z innymi systemami, w związku z czym awarie w jednym systemie lub procesie mogą wpłynąć na inne systemy działające w organizacji lub poza nią. Rozprzestrzenianie się skutków zdarzenia może wynikać zarówno z zależności fizycznych, jak i logicznych. Przekazywanie kompletnych wyników oceny ryzyka operatorom połączonych lub współzależnych systemów i procesów jest jednym ze sposobów ochrony przed takimi rodzajami wpływu.

Skutkiem incydentu w zakresie cyberbezpieczeństwa, który rozprzestrzeni się na połączone systemy OT, może być uszkodzenie logiki takich systemów. Za przykład może posłużyć wirus lub robak rozprzestrzeniający się w połączonych systemach OT oraz wpływający na ich działanie.

Także uszkodzenia fizyczne mogą ulegać rozprzestrzenianiu na inne połączone systemy OT lub domeny fizyczne. Skutkiem może być na przykład zagrożenie fizyczne i pogorszenie stanu środowisk fizycznych, a także awaria wspólnych elementów systemu (na przykład układu zasilania) bądź niedobór materiału potrzebnego na późniejszym etapie procesu przemysłowego.

CISA promuje współpracę między organizacjami rządowymi i przemysłem mającą na celu poprawę zdolności wszystkich podmiotów w zakresie przewidywania, ustalania priorytetów i zarządzania ryzykiem związanym z systemami OT na poziomie krajowym. CISA pomaga także dostawcom systemów OT, ich właścicielom, operatorom i innym dostawcom działającym we wszystkich sektorach infrastruktury krytycznej w identyfikowaniu podatności i opracowywaniu kompleksowych, proaktywnych strategii łagodzenia ich skutków, które prowadzą do zwiększenia cyberbezpieczeństwa systemów OT.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje mogą uwzględnić zasoby takie jak Krajowa baza danych dotyczących podatności na zagrożenia (NVD) oraz ramy MITRE ATT&CK dotyczące systemów sterowania przemysłowego (ICS) [ATTACK-ICS] w swoich procesach oceny ryzyka dotyczącego misji oraz systemów OT.

Co więcej, charakter systemów OT wymaga od organizacji uwzględnienia dodatkowych czynników, które nie muszą być brane pod uwagę podczas oceny ryzyka dotyczącej tradycyjnych systemów IT. Systemy OT charakteryzują się bowiem innymi źródłami zagrożeń, podatnościami oraz zabezpieczeniami kompensacyjnymi. Wpływ incydentu związanego z cyberbezpieczeństwem dotyczącego środowisk OT może obejmować zarówno skutki fizyczne, jak i logiczne, które należy uwzględnić w ocenach ryzyka, w tym:

- W ocenach wpływu na bezpieczeństwo i ocenach bezpieczeństwa.
- W ocenach fizycznych skutków incydentu związanego z cyberbezpieczeństwem w środowiskach OT, w tym ocenach wpływu na środowisko fizyczne i kontrolowany proces.
- W ocenach wpływu na oceny ryzyka związanego z fizycznymi elementami systemu sterowania w systemach OT.

W czasie etapu określania ram ryzyka organizacje powinny wybrać odpowiednie metodyki oceny ryzyka, które obejmują systemy OT. Oceniając potencjalne skutki fizyczne incydentu związanego z cyberbezpieczeństwem, organizacje wykorzystujące

systemy OT powinny uwzględnić między innymi następujące kwestie: I) w jaki sposób incydent może wpłynąć na działanie systemów, co spowoduje skutki wpływające na środowisko fizyczne; II) jakie elementy systemu OT mogą pozwolić na ograniczenie lub załagodzenie wpływu; III) w jaki sposób powyższa sytuacja może doprowadzić do wystąpienia incydentu fizycznego.

Zalecenia i wytyczne dotyczące systemów OT

Określając ramy ryzyka dotyczącego środowiska OT, organizacje mogą odkryć, że zagrożenia związane z cyberbezpieczeństwem nie zawsze są przewidywalne oraz ujęte tak precyzyjnie, jak zagrożenia dotyczące samych systemów OT. W związku z tym organizacje mogą uwzględnić scenariusze cyberataków i awarii systemów IT w swoich procesach analizy zagrożeń procesowych (*ang. process hazard analysis – PHA*) lub analizy trybu i skutków awarii (*ang. failure mode and effects analysis – FMEA*). Uwzględniając w tych procesach ryzyko związane z cyberatakami i metody zarządzania tym ryzykiem, organizacje mogą lepiej zrozumieć zagrożenia dla środowiska operacyjnego OT związane z cyberbezpieczeństwem.

W ramach określania ram ryzyka organizacje mogą również uwzględnić:

- Założenia, które wpływają na sposób oceny, reagowania i monitorowania ryzyka w organizacji.
- Poziom tolerowanego ryzyka w organizacji, poziom akceptowalnego ryzyka związanego z realizacją celów strategicznych oraz priorytety i kompromisy uwzględniane w ramach zarządzania ryzykiem.

W kontekście systemów OT, organizacje muszą uwzględnić ryzyko uszkodzenia sprzętu, wystąpienia zagrożeń dla bezpieczeństwa ludzi, środowiska naturalnego i innej infrastruktury krytycznej w ramach tych analiz. Organizacje muszą także uwzględnić ocenę potencjalnych skutków fizycznych dotyczących wszystkich części systemu OT.

Proces określania ram ryzyka może również obejmować określenie, w jaki sposób systemy OT są połączone lub zależne od systemów IT. Wszystkie te procesy mogą wymagać od organizacji określenia wspólnych ram oceny wpływu, które uwzględniają

kwestie systemów OT. Jedno z podejść opiera się na dokumencie NSC 199 [NSC 199], który kategoryzuje systemy przez pryzmat potencjalnego wpływu na realizację celów bezpieczeństwa w zakresie poufności, integralności oraz dostępności, określając go mianem niskiego, umiarkowanego lub wysokiego. Inne podejście oparte na dokumencie ISA 62443-3-2 [ISA62443] obejmuje przykładowe definicje pozwalające na przyporządkowanie systemów do poszczególnych kategorii na podstawie wpływu dotyczącego systemów OT.

Tabela 3 obejmuje przykładowe kategorie i poziomy wpływu, które organizacje mogą dostosować do swoich wymagań wynikających z obszaru działalności lub wymagań biznesowych. Przykładowo, dla wybranych organizacji awaria trwająca do 24 godzin może stanowić przykład wysokiego wpływu, nie zaś umiarkowanego, który wynika z tabeli.

Tabela 3. Przykładowa klasyfikacja poziomów wpływu systemów OT na podstawie wytwarzanych produktów, sektora działalności oraz kwestii bezpieczeństwa

Kategoria	Wysoki wpływ	Umiarkowany wpływ	Niski wpływ
Awaria obejmująca wiele zakładów	Poważne przerwy i zakłócenia działalności wielu zakładów, których naprawa może potrwać jeden dzień lub dłużej	Zakłócenia działalności wielu zakładów, których naprawa może potrwać godzinę lub dłużej	Częściowe zakłócenia działalności wielu zakładów, których naprawa jest możliwa w czasie krótszym niż jedna godzina
Infrastruktura i usługi państwa	Wpływ na wiele sektorów lub znaczące ograniczenie dostępności usług wykorzystywanych przez społeczność	Możliwość wpływu na sektor w stopniu wykraczającym poza pojedyncze przedsiębiorstwo	Znikomy wpływ na sektor lub brak wpływu na sektor w stopniu wykraczającym poza pojedyncze przedsiębiorstwo oraz na społeczność
Koszt (% przychodów)	> 25 %	> 5 %	< 5 %
Skutki prawne	Przestępstwo kryminalne lub naruszenie przepisów, które powoduje uniemożliwienie prowadzenia działalności	Wykroczenie lub naruszenie zgodności, które skutkuje grzywną	Brak
Zaufanie publiczne	Naruszenie wizerunku marki	Naruszenie zaufania klientów	Brak

Kategoria	Wysoki wpływ	Umiarkowany wpływ	Niski wpływ
Pracownicy	Zgon w wyniku zdarzenia	Przestój lub poważny uraz	Zdarzenie wymagające udzielenia pierwszej pomocy lub drobny uraz
Lokalna społeczność	Śmierć lub poważny incydent	Skargi lub wpływ na społeczność lokalną	Brak skarg
Środowisko	Kara nałożona przez odpowiedzialną instytucję lub znaczące szkody na dużym obszarze utrzymujące się przez dłuższy czas	Kara nałożona przez odpowiedzialną instytucję	Niewielkie, ograniczone emisje poniżej limitów podlegających zgłoszeniu

W celu wspomagania procesu oceny ryzyka, organizacje powinny również określić sposób wskazywania prawdopodobieństwa wystąpienia zdarzeń związanych z cyberbezpieczeństwem w celu zachowania spójności podczas oceny ryzyka. Dokument NSC 800-30 [NSC 800-30] zawiera wytyczne dla organizacji dotyczące opracowywania ważonych czynników ryzyka opartych na prawdopodobieństwie. Organizacje powinny uwzględnić możliwość przypisania wag do czynników ryzyka w oparciu o analizę prawdopodobieństwa, że dane zagrożenie będzie w stanie wykorzystać daną podatność (lub zestaw podatności), że zdarzenie powodujące zagrożenie wystąpi oraz że spowoduje niekorzystne skutki.

W przypadku zagrożeń agresywnych ocena prawdopodobieństwa ich wystąpienia opiera się zazwyczaj na zamiarach, możliwościach i celach napastnika. W przypadku zagrożeń innych niż agresywne, prawdopodobieństwo ich wystąpienia jest szacowane na podstawie danych historycznych, danych empirycznych i innych czynników. Jeśli organizacja stwierdzi brak historycznych danych lub dowodów, rozwiązaniem może być rozszerzenie analizy o dane branżowe opisujące zdarzenia związane z cyberbezpieczeństwem zgłaszane przez podobne organizacje.

Określenie prawdopodobieństwa wystąpienia zagrożenia może również opierać się na stanie organizacji (na przykład jej podstawowej misji i procesach biznesowych, architekturze korporacyjnej, architekturze bezpieczeństwa informacji, systemach informatycznych i środowiskach, w których te systemy działają) i uwzględniać warunki predysponujące oraz obecność i skuteczność środków bezpieczeństwa wdrożonych w celu ochrony przed nieautoryzowanym lub niepożądanym zachowaniem,

wykrywania i ograniczania szkód bądź innych czynników odporności w odniesieniu do systemów OT.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje określające prawdopodobieństwa zdarzeń powinny odwołać się do Załącznika G do dokumentu NSC 800-30, gdzie znajdują się bardziej szczegółowe wskazówki i wytyczne. W oparciu o te wytyczne organizacje powinny określić pięć poziomów prawdopodobieństwa, od bardzo niskiego do bardzo wysokiego, zarówno dla zagrożeń agresywnych, wynikających z działalności napastników, jak i innych zagrożeń, takich jak: błędy, wypadki, klęski żywiołowe itp.

Ponadto organizacje powinny określić prawdopodobieństwo, że dane zdarzenie może mieć niekorzystny wpływ. Na podstawie tych dwóch czynników, organizacje mogą opracować wykaz, którego przykład został przedstawiony w tabeli 4, aby na jego podstawie określić prawdopodobieństwo na potrzeby analizy ryzyka.

Tabela 4. Ocena prawdopodobieństwa wystąpienia zdarzenia

Prawdopodobieństwo wystąpienia zdarzenia powodującego zagrożenie negatywnych działań lub zdarzeń	**Prawdopodobieństwo, że zdarzenia powodujące zagrożenie spowodują wystąpienie**				
	Bardzo niskie	Niskie	Umiarkowane	Wysokie	Bardzo wysokie
Bardzo wysokie	Niskie	Umiarkowane	Wysokie	Bardzo wysokie	Bardzo wysokie
Wysokie	Niskie	Umiarkowane	Umiarkowane	Wysokie	Bardzo wysokie
Umiarkowane	Niskie	Niskie	Umiarkowane	Umiarkowane	Wysokie
Niskie	Bardzo niskie	Niskie	Niskie	Umiarkowane	Umiarkowane
Bardzo niskie	Bardzo niskie	Bardzo niskie	Niskie	Niskie	Niskie

4.1.2. SZACOWANIE RYZYKA W ŚRODOWISKU OT

Etap szacowania ryzyka opiera się na wynikach działań mających na celu określenie ram ryzyka (na przykład dopuszczalnych metodach oceny ryzyka, strategiach zarządzania ryzykiem i poziomach tolerowanego ryzyka) i ułatwiają wskazywanie,

szacowanie i ustalanie priorytetów dotyczących ryzyka dotyczącego operacji, zasobów, osób i innych organizacji. Szacowanie ryzyka jest przeprowadzane na wszystkich poziomach zarządzania ryzykiem (organizacji, misji i funkcji biznesowych oraz systemów), a jego wyniki mogą być wykorzystywane na potrzeby szacowania ryzyka na innych poziomach. Niezależnie od tego, na jakim poziomie zarządzania ryzykiem przeprowadzany jest ten proces, każdorazowo wymaga określenia zagrożeń i podatności, a także możliwych szkód i prawdopodobieństwa wystąpienia niepożądanych zdarzeń wynikających z tych zagrożeń i podatności.

Gdy organizacja przeprowadza szacowanie ryzyka obejmujące systemy OT, musi uwzględnić dodatkowe zagadnienia, które nie występują w przypadku szacowania ryzyka związanego z tradycyjnymi systemami IT. Jednym z nich jest fakt, że skutki incydentu związanego z cyberbezpieczeństwem mogą obejmować zarówno skutki fizyczne, jak i cyfrowe.

Zalecenia i wytyczne dotyczące systemów OT

Szacowanie ryzyka zwykle odzwierciedla stan systemu w danym czasie. Z tego powodu organizacje winny dołożyć wszelkich starań, by zawarte w nich informacje były aktualizowane oraz by zapewnić odpowiedni poziom bezpieczeństwa.

Organizacje powinny zapoznać się z informacjami znajdującymi się w alertach i informacjach publikowanych przez CISA, zawartymi w krajowej bazie danych dotyczących podatności na zagrożenia Narodowego Instytutu Standaryzacji i Technologii oraz informacjami dotyczącymi systemów sterowania przemysłowego publikowanymi w bazie danych MITRE ATT&CK, aby określić typowe obszary podatności dotyczące środowisk OT, takie jak:

- Niskie standardy tworzenia oprogramowania, projektowania sieci lub błędne konfiguracje urządzeń.
- Podatne na ataki usługi i protokoły sieciowe.
- Słabe uwierzytelnianie.
- Nadmierne uprawnienia.
- Ujawnianie informacji.

W wielu przypadkach stosowanie systemów OT wiąże się z koniecznością spełnienia określonych wymagań dotyczących środowiska. Przykładowo proces produkcyjny może wymagać precyzyjnego ustawienia temperatury. Tego rodzaju systemy oraz procesy mogą być również powiązane ze środowiskiem fizycznym. Organizacje powinny wziąć pod uwagę możliwość uwzględnienia tych wymagań i ograniczeń w czasie określania ram ryzyka, aby wskazać ryzyko związane z tymi zagadnieniami.

Ponadto organizacje mogą uwzględnić także:

- Wskazanie zasobów fizycznych i zabezpieczeń bezpośrednio związanych z bezpieczeństwem, życiem ludzkim i utrzymaniem ciągłości działania systemu OT.
- Wskazanie zagrożeń związanych z cyberbezpieczeństwem dotyczących zasobów fizycznych, które mogą zagrozić funkcjonowaniu systemu OT.
- Upewnienie się, że pracownicy odpowiedzialni za obszar ochrony fizycznej rozumieją względne ryzyko i środki przeciwdziałania w zakresie bezpieczeństwa fizycznego związane ze środowiskami systemów OT, które chronią.
- Upewnienie się, że pracownicy ochrony fizycznej są świadomi obszarów w środowisku produkcyjnym systemu OT, w których gromadzone są dane i które działają we wrażliwych przestrzeniach.
- Ograniczenie ryzyka związanego z ciągłością działania poprzez określenie planów natychmiastowego reagowania w przypadku zagrożenia bezpieczeństwa fizycznego.

Szacowanie ryzyka wymaga również przeglądu mechanizmów cyfrowych i niecyfrowych wdrażanych w celu zminimalizowania negatywnego wpływu zdarzeń. Systemy OT często obejmują niecyfrowe mechanizmy zapewniające odporność na błędy i zapobiegające przekroczeniu dopuszczalnych zakresów parametrów. Mechanizmy te mogą pomóc w ograniczeniu negatywnego wpływu incydentu cyfrowego na działanie systemów OT i powinny zostać włączone do procesu szacowania ryzyka. Systemy OT są często wyposażone w inne niż cyfrowe zabezpieczenia, które mogą zapobiec przekroczeniu bezpiecznych parametrów granicznych, a tym samym ograniczyć wpływ ataku. Przykładem takiego rozwiązania może być mechaniczny zawór nadmiarowy. Mechanizmy analogowe (na przykład

mierniki, alarmy) mogą być również wykorzystywane jako wskaźniki fizycznego stanu systemu i źródło wiarygodnych danych w przypadku braku lub zakłócenia odczytów cyfrowych. **Tabela 5** określa kategorie zabezpieczeń innych niż cyfrowe, które mogą zmniejszyć wpływ incydentu związanego z systemami OT.

Tabela 5. Kategorie niecyfrowych komponentów zabezpieczeń systemów OT

Rodzaj zabezpieczenia	Opis
Analogowe mierniki lub alarmy	Mechanizmy niecyfrowe umożliwiają dokonywanie pomiarów oraz prezentowanie parametrów systemu fizycznego (na przykład temperatury, ciśnienia, napięcia, prądu) i mogą dostarczyć operatorowi dokładne informacje, gdy wyświetlacze cyfrowe są niedostępne lub uszkodzone. Informacje mogą być przekazywane operatorowi za pośrednictwem mechanizmów innych niż cyfrowe (na przykład termometrów, manometrów) oraz za pośrednictwem alarmów dźwiękowych.
Mechanizmy sterowania ręcznego	Mechanizmy sterowania ręcznego (na przykład ręczne sterowanie zaworami, fizyczne wyłączniki) umożliwiają operatorom ręczne sterowanie siłownikiem bez konieczności polegania na cyfrowym systemie OT. Dzięki temu siłownik może być sterowany nawet wtedy, gdy system OT jest niedostępny lub jego zabezpieczenia zostały naruszone.
Analogowe systemy sterowania	Analogowe systemy sterowania wykorzystują czujniki i siłowniki inne niż cyfrowe w celu monitorowania procesu fizycznego oraz sterowania jego przebiegiem. Mogą one zapobiec wejściu procesu fizycznego w niepożądany stan, gdy cyfrowy system OT jest niedostępny lub uszkodzony. Sterowniki analogowe obejmują takie urządzenia jak regulatory i przekaźniki elektromechaniczne. Za przykład może posłużyć urządzenie zaprojektowane w taki sposób, by uległo otwarciu w sytuacji awaryjnej lub w przypadku, gdy parametry przekroczą ustalone wartości graniczne, aby zapobiec wzrostowi ciśnienia płynu powyżej określonej wartości, a tym samym zapewnić bezpieczny stan procesu. Urządzenie może być również zaprojektowane tak, aby zapobiegać nadmiernemu wzrostowi podciśnienia – może opierać się na przykład na zaworze nadmiarowym, jednorazowym zabezpieczeniu nadmiarowym lub zaworze podciśnienia.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny przeanalizować wszystkie cyfrowe i niecyfrowe mechanizmy sterowania i zabezpieczenia oraz zakres, w jaki mogą złagodzić potencjalny negatywny wpływ zdarzenia na systemy OT. Inne niż cyfrowe mechanizmy sterowania i zabezpieczeń mogą wymagać poświęcenia dodatkowego czasu oraz zaangażowania operatorów, zwłaszcza gdy znajdują się w odległej lokalizacji i wymagają ręcznej

interwencji. Takie mechanizmy mogą również być zależne od czasu reakcji człowieka, który może być wolniejszy niż zautomatyzowane zabezpieczenia i mechanizmy sterujące.

Ponadto organizacje muszą uwzględnić zagadnienie prywatności w ramach szacowania ryzyka, co może wymagać zastosowania innego podejścia. Metodologia oceny ryzyka prywatności opracowana przez NIST (PRAM) to narzędzie, które opiera się na modelu ryzyka opisanym w dokumencie NIST IR 8062 [IR8062]. Na jego podstawie organizacje mogą analizować, oceniać i ustalać priorytety zagrożeń dotyczących prywatności w celu określenia sposobu reagowania i wyboru odpowiednich rozwiązań.

4.1.3. REAGOWANIE NA RYZYKO W ŚRODOWISKU OT

Etap reagowania na ryzyko pozwala organizacji podjąć działania w odpowiedzi na ryzyko wskazane na etapie określania ram ryzyka, oparte na określonych możliwych kierunkach działań, które pozwolą skutecznie przeciwdziałać ryzyku. Możliwości te należy następnie ocenić przy uwzględnieniu poziomu tolerowanego ryzyka oraz innych aspektów określonych na etapie określania ram ryzyka, aby dokonać wyboru najlepszego działania. Etap reagowania na ryzyko obejmuje realizację wybranego sposobu działania w celu przeciwdziałania zidentyfikowanemu ryzyku – są to akceptacja ryzyka, unikanie, łagodzenie, dzielenie się lub przekazywanie, a także dowolne połączenia tych opcji[12].

Zalecenia i wytyczne dotyczące systemów OT

W przypadku systemów OT możliwe reakcje na ryzyko mogą być ograniczone przez wymagania systemowe, potencjalny niekorzystny wpływ na działalność, a nawet konieczność zapewnienia zgodności z przepisami. Przykładem dzielenia się ryzykiem jest sytuacja, w której organizacji z sektora usług komunalnych zawierają umowy dotyczące wypożyczania pracowników w sytuacjach awaryjnych, aby skrócić czas trwania incydentu do akceptowalnego poziomu.

[12] Dodatkowe informacje na temat tych opcji można znaleźć w dokumencie NSC 800-39 [NSC 800-39].

4.1.4. MONITOROWANIE RYZYKA W ŚRODOWISKU OT

Monitorowanie ryzyka jest czwartym etapem działań związanych z zarządzaniem ryzykiem. Organizacje winny na bieżąco monitorować ryzyko, w tym proces wdrażania wybranych strategii zarządzania ryzykiem, zmiany w otoczeniu, które mogą mieć wpływ na kalkulację ryzyka, a także skuteczność i efektywność działań ograniczających ryzyko. Działania realizowane w ramach monitorowania mają wpływ na wszystkie pozostałe etapy.

Zalecenia i wytyczne dotyczące systemów OT

Wiele funkcji monitorowania systemów OT wykorzystuje pasywne techniki monitorowania w celu wykrywania zmian w systemie. Nie zawsze są w stanie wykazać jednak wszelkie modyfikacje i zmiany. Nowoczesne platformy monitorujące, które wykorzystują natywne protokoły komunikacyjne w celu uzyskania dostępu do większej ilości informacji systemowych, mogą zwiększyć świadomość sytuacyjną, mimo to należy uwzględnić ograniczenia systemów OT. Wiele wdrożeń systemów OT nie zakłada regularnego monitorowania działań związanych z cyberbezpieczeństwem. Z tego powodu użytkownicy końcowi powinni przeprowadzać monitorowanie z częstotliwością zgodną z przyjętym profilem ryzyka.

Informacje o zagrożeniach związane ze środowiskiem OT stale się zmieniają, a ich dostępność i dokładność nadal może pozostawiać wiele do życzenia. Co więcej, ze względu na ich charakter, przewidywanie zagrożeń może być utrudnione, nawet pomimo użycia danych historycznych. Organizacje powinny kategoryzować zagrożenia w oparciu o prawdopodobieństwo ich wystąpienia i ich potencjalne skutki.

Zagrożenie skanowaniem systemu podłączonego do Internetu charakteryzuje się wysokim prawdopodobieństwem wystąpienia, lecz niską dotkliwością skutków. Z kolei zagrożenie zakłóceniem łańcucha dostaw przez podmiot działający na rzecz państwa charakteryzuje się niskim prawdopodobieństwem oraz wysoką dotkliwością potencjalnych skutków.

Ze względu na fakt, że środki przeciwdziałania związane z bezpieczeństwem są zwykle opracowywane dla środowisk IT, organizacje powinny przemyśleć, w jaki sposób wdrożenie zabezpieczeń w środowiskach OT może negatywnie wpłynąć na ich działanie lub bezpieczeństwo.

4.2. SZCZEGÓLNE ZAGADNIENIA

Zarządzanie ryzykiem w łańcuchu dostaw i zarządzanie ryzykiem dla bezpieczeństwa to kluczowe aspekty zarządzania ryzykiem związanym z cyberbezpieczeństwem systemów OT.

4.2.1. ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW.

Zagrożenia związane z cyberbezpieczeństwem mogą mieć swoje źródła w produktach lub usługach nabywanych przez organizację w celu zaspokojenia potrzeb dotyczących systemów OT. Ryzyko to może zmaterializować się w dowolnym punkcie łańcucha dostaw i na dowolnym etapie cyklu życia produktu. Niezależnie od tego, czy mowa o złośliwym, naturalnym czy niezamierzonym ryzyku, każde z nich może potencjalnie zagrozić dostępności i integralności krytycznych systemów i komponentów systemów OT, a także dostępności, integralności i poufności danych wykorzystywanych przez systemy OT, powodując tym samym szkody obejmujące zarówno drobne zakłócenia działalności, jak i zagrożenie dla życia i bezpieczeństwa.

Z kilkoma wyjątkami, organizacje odpowiedzialne za systemy OT opierają się na dostawcach oraz usługodawcach zewnętrznych i ich rozszerzonych łańcuchach dostaw w celu zaspokajania wielu zróżnicowanych potrzeb. Organizacje te realizują szereg krytycznych ról i funkcji, między innymi produkują i dostarczają produkty technologiczne, zapewniają aktualizacje i poprawki oprogramowania, świadczą usługi w zakresie integracji systemów lub w inny sposób wspierają codzienne działanie oraz konserwację systemów OT, ich komponentów i środowisk operacyjnych. Z tego powodu organizacje wykorzystujące systemy OT powinny zrozumieć oraz podejmować działania w celu ograniczenia ryzyka związanego z łańcuchem dostaw, którego źródłem mogą być dostawcy i organizacje zewnętrzne, a także produkty i usługi, które dostarczają.

Określanie, szacowanie i skuteczną reakcję reagowanie na zagrożenia dotyczące cyberbezpieczeństwa w łańcuchach dostaw najlepiej osiągnąć poprzez włączenie zagadnienia zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw (*ang. Cybersecurity Supply Chain Risk Management – C-SCRM*) do polityk, planów i praktyk wdrażanych w organizacji. Wymaga to poszerzenia oczekiwań

i wymogów dotyczących cyberbezpieczeństwa w celu objęcia nimi dostawców oraz przeprowadzenia szczegółowych analiz łańcuchów dostaw, które są powiązane z nabywanymi produktami i usługami. Organizacje powinny weryfikować dostawców i usługodawców w celu określenia ich możliwości, wiarygodności, adekwatności ich wewnętrznych praktyk w zakresie bezpieczeństwa, skuteczności stosowanych zabezpieczeń, ich łańcuchów dostaw oraz wszelkich zagrożeń, które mogą być związane z tymi relacjami i zależnościami. Wymagania dotyczące produktów i komponentów oraz ich oceny powinny obejmować swoim zakresem zagadnienia inne niż wyłącznie spełnienie wymagań funkcjonalnych i technicznych. Muszą także uwzględniać stosowne czynniki związane z praktykami C-SCRM, takie jak pochodzenie i skład produktu oraz to, czy produkt nie został zmodyfikowany bądź podrobiony. Ponadto należy zwrócić szczególną uwagę na kwestię trudności w uzyskaniu oryginalnych części zamiennych lub aktualizacji przez cały okres użytkowania produktu oraz zróżnicowanie źródeł dostaw w przyszłości.

Organizacje wykorzystujące systemy OT powinny w związku z tym zapoznać się z treścią dokumentu NIST SP 800-161r1_PL, *Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji* [NIST SP 800-161r1_wer. 1.0_PL] i rozpocząć lub kontynuować wdrażanie kluczowych praktyk, zabezpieczeń oraz działań związanych z zarządzaniem ryzykiem w łańcuchu dostaw opisanych w tej publikacji. Dokument ten zawiera szczegółowe wytyczne dotyczące ustanowienia programu C-SCRM na postawie szeregu etapów, rozpoczynając od wdrożenia podstawowych elementów i rozszerzania ich z upływem czasu, co pozwala na zapewnienie skuteczności oraz umożliwia rozszerzanie zakresu programu. Dokument zawiera także wytyczne dotyczące przeprowadzania ocen ryzyka związanego z łańcuchem dostaw, włączania zagadnień związanych z obszarem C-SCRM do wymagań dotyczących zamówień i zaopatrzenia, konieczności wykorzystania zintegrowanego i interdyscyplinarnego podejścia do zarządzania ryzykiem, a także szereg wytycznych dotyczących zabezpieczeń związanych z obszarem C-SCRM oraz szablonów, które organizacje mogą wykorzystać w ramach własnych wdrożeń.

4.2.2. SYSTEMY BEZPIECZEŃSTWA FIZYCZNEGO

Kultura bezpieczeństwa i ocen bezpieczeństwa to zagadnienia znane wielu użytkownikom systemów OT. Szacowanie ryzyka związanego z bezpieczeństwem informacji powinno stanowić uzupełnienie takich ocen. Proces ten może opierać się na zróżnicowanych podejściach i obejmować różne obszary. Szacowanie bezpieczeństwa dotyczy przede wszystkim zagadnienia bezpieczeństwa fizycznego, z kolei szacowanie ryzyka związanego z bezpieczeństwem informacji uwzględnia także aspekt cyfrowy. Środowiska OT łączą jednak aspekty fizyczne i cyfrowe, co oznacza, że w praktyce może dochodzić do znacznego przenikania się tych obszarów.

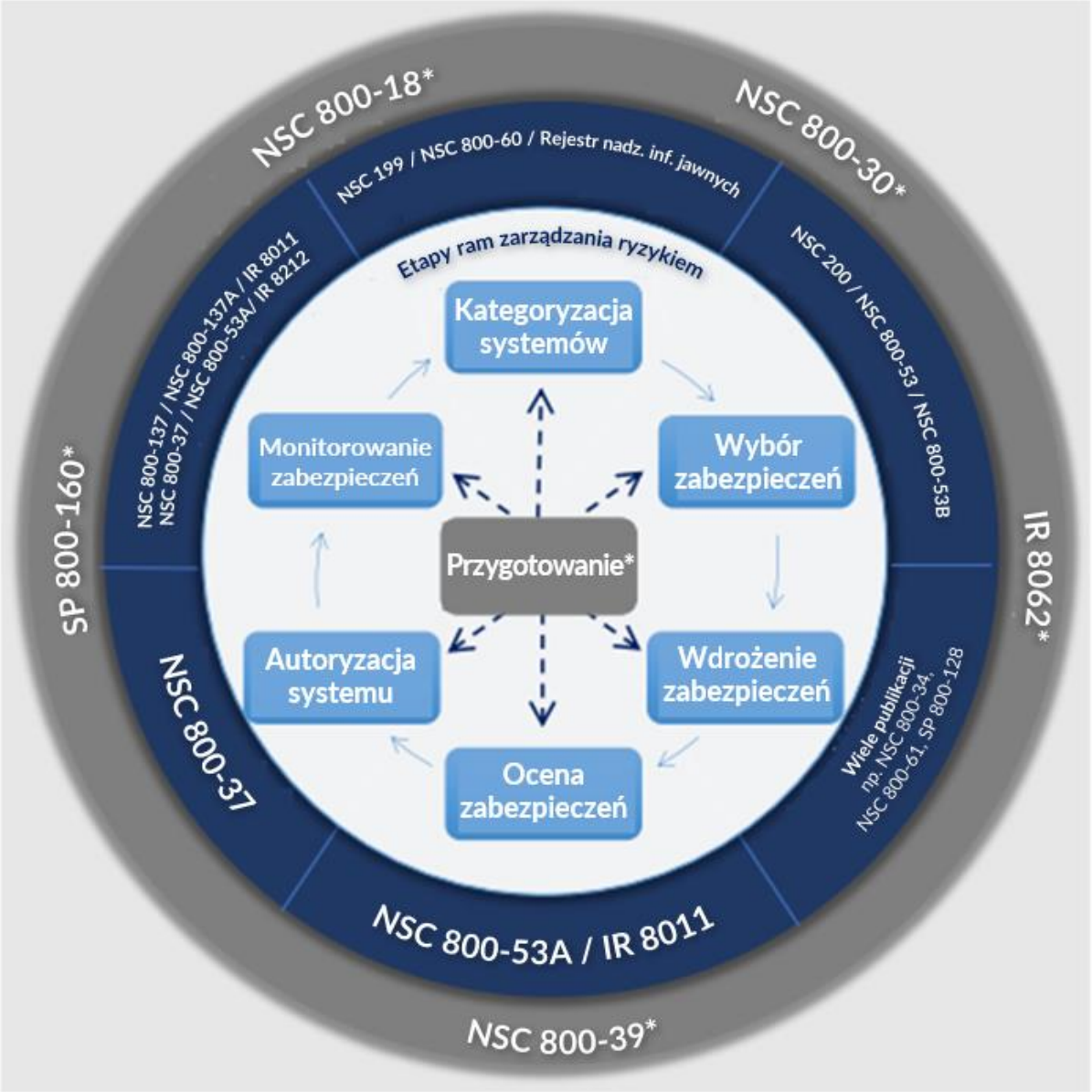
Organizacje powinny zatem uwzględniać wszystkie aspekty zarządzania ryzykiem dla bezpieczeństwa (na przykład określanie ram ryzyka czy poziomu tolerowanego ryzyka), a także wyniki ocen bezpieczeństwa podczas procesu szacowania ryzyka dla bezpieczeństwa informacji. Pracownicy odpowiedzialni za proces szacowania ryzyka związanego z bezpieczeństwem informacji muszą być w stanie określić wykryte zagrożenia, które mogą mieć wpływ na bezpieczeństwo, a następnie przekazać informacje na ich temat. Z kolei pracownicy odpowiedzialni za przeprowadzenie oceny bezpieczeństwa muszą wiedzieć o potencjalnych skutkach fizycznych i prawdopodobieństwie ich wystąpienia.

Systemy bezpieczeństwa mogą zmniejszyć wpływ incydentu związanego z cyberbezpieczeństwem na systemy OT. Ze względu na te możliwości są często wdrażane w celu wykonywania określonych funkcji monitorowania i sterowania w celu zapewnienia bezpieczeństwa ludzi, środowiska, procesów i zasobów. Choć tego rodzaju systemy są zwykle wdrażane ze stosowną nadmiarowością i zapewnia się ich niezależność od głównego systemu OT, niektóre architektury łączą funkcje sterowania i bezpieczeństwa, a także komponenty lub sieci. Połączenie funkcji sterowania oraz zabezpieczeń może umożliwić zaawansowanemu napastnikowi dostęp zarówno do systemów sterowania, jak i systemów zabezpieczeń, w przypadku skutecznego ataku na system OT. Organizacje winny zapewnić odpowiednią separację komponentów zgodnie z oszacowanym ryzykiem naruszenia zasad ochrony i ocenić wpływ wdrożonych zabezpieczeń na system bezpieczeństwa fizycznego w celu ustalenia, czy nie wywierają one negatywnego wpływu na jego działanie.

4.3. ZASTOSOWANIE RAM ZARZĄDZANIA RYZYKIEM W OBSZARZE SYSTEMÓW OT

Ramy zarządzania ryzykiem opracowane przez Narodowy Instytut Standaryzacji i Technologii (*ang. Risk Management Framework – RMF*) opisują proces i koncepcje związane z zarządzaniem ryzykiem (określanie ram ryzyka, szacowanie ryzyka, reagowanie na ryzyko i monitorowanie ryzyka) w odniesieniu do systemów i organizacji. W poniższych podrozdziałach został przedstawiony proces stosowania ram zarządzania ryzykiem w odniesieniu do systemów OT. Każdy z podrozdziałów obejmuje krótkie opisy poszczególnych etapów oraz zadań, zakładanych rezultatów każdego zadania, odniesienia do innych norm i wytycznych dotyczących systemów OT, takich jak ramy cyberbezpieczeństwa czy norma IEC 62443, a także wytyczne na temat procesu wdrożenia dotyczące systemów OT. Warto zauważyć, że wykonanie niektórych zadań nie jest wymagane, ponadto nie wszystkie zadania zawierają uwagi lub wytyczne dotyczące OT.

Poszczególne etapy ram zarządzania ryzykiem przedstawione na **Rysunku 15** zostały zaprezentowane w określonym porządku. Mogą być jednak realizowane w innej kolejności, aby zapewnić ich zgodność z ustalonymi procesami zarządzania i cyklu życia systemu.



Rysunek 15. Etapy ram zarządzania ryzykiem

4.3.1. PRZYGOTOWANIE

Celem etapu *Przygotowanie* jest przeprowadzenie niezbędnych działań na poziomie organizacyjnym, misji i procesu biznesowego oraz systemów, aby umożliwić organizacji skuteczne zarządzanie ryzykiem związanym z bezpieczeństwem i prywatnością dzięki ramom zarządzania ryzykiem. Etap ten opiera się na działaniach realizowanych w ramach programów dotyczących cyberbezpieczeństwa, a ich celem jest zapewnienie istnienia stosownych mechanizmów zarządzania oraz zasobów umożliwiających zarządzanie ryzykiem. **Tabela 6** zawiera szczegółowe informacje na temat realizacji działań związanych z etapem przygotowania w kontekście systemów OT.

Tabela 6. Etap przygotowania ram zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
Poziomy organizacji oraz misji i procesów biznesowych		
ZADANIE P-1 ROLE ZARZĄDZAJĄCE RYZYKIEM	Zidentyfikowanie osób fizycznych i przypisanie im kluczowych ról w realizacji Ram Zarządzania Ryzykiem. [*Ramy Cyberbezpieczeństwa*: **ID.AM-6**; **ID.GV-2**] [IEC 62443-2-1: **ORG 1.3**]	Wskazanie i przypisanie poszczególnych osób do określonych ról związanych z zarządzaniem ryzykiem w zakresie bezpieczeństwa i ochrony prywatności systemów IT oraz OT. W ramach tego zadania należy określić także role i obowiązki podmiotów zewnętrznych w zakresie cyberbezpieczeństwa. Przykładowe stanowiska pracowników odpowiedzialnych za systemy OT obejmują między innymi kierownika procesu/organizacji, inżyniera ds. nadzoru technicznego, operatora, inżyniera ds. bezpieczeństwa funkcjonalnego, pracowników ds. utrzymania ruchu oraz konserwacji, a także kierownika ds. bezpieczeństwa procesu.
ZADANIE P-2 STRATEGIA ZARZĄDZANIA RYZYKIEM	Ustalenie strategii zarządzania ryzykiem dla organizacji, która obejmuje określenie i opisanie tolerancji ryzyka w organizacji. [*Ramy Cyberbezpieczeństwa*: **ID.RM; ID.SC**] [IEC 62443-2-1: **ORG 2.1**]	Strategia zarządzania ryzykiem obejmuje całą organizację. Należy uwzględnić wymogi regulacyjne dotyczące organizacji wykorzystujących systemy OT.
ZADANIE P-3 SZACOWANIE RYZYKA - ORGANIZACJA	Ocena zagrożeń bezpieczeństwa i prywatności w całej organizacji oraz bieżąca aktualizacja wyników szacowania ryzyka. [*Ramy Cyberbezpieczeństwa*: **ID.RA; ID.SC-2**] [IEC 62443-2-1: **Event1.9; ORG 1.3; 2.1**]	

Zadania	**Rezultaty**	**Rekomendacje dotyczące systemów OT**
ZADANIE P-4 DOSTOSOWYWANIE PRZEZ ORGANIZACJĘ PODSTAWOWYCH MECHANIZMÓW ZABEZPIECZEŃ I PROFILI RAM CYBERBEZPIECZEŃSTWA (OPCJONALNIE)	Ustanowienie, udokumentowanie i opublikowanie dostosowanych przez organizację zabezpieczeń bazowych i/lub Profili Ram Cyberbezpieczeństwa. [*Ramy Cyberbezpieczeństwa*: **Profil**]	Opracowanie dostosowanego organizacyjnie zestawu minimalnych zabezpieczeń dotyczących systemów OT w celu zaspokojenia potrzeb związanych z realizacją misji oraz działalności biznesowej, wyjątkowymi środowiskami lub innymi wymogami.
ZADANIE P-5 IDENTYFIKACJA ZABEZPIECZEŃ WSPÓLNYCH	Zidentyfikowanie, udokumentowanie i opublikowanie zabezpieczeń wspólnych, które są dostępne do dziedziczenia przez systemy organizacji.	Zabezpieczenia wspólne dostępne do dziedziczenia mogą mieć negatywny wpływ na działanie systemu OT. Należy sprawdzić, czy zabezpieczenia wspólne mogą być stosowane do systemów OT w sposób skuteczny i bezpieczny bez wywierania negatywnego wpływu na ich działanie.
ZADANIE P-6 PRIORYTETYZACJA NA POZIOMIE WPŁYWU (OPCJONALNIE)	Priorytetyzacja systemów organizacji o tym samym poziomie wpływu. [*Ramy Cyberbezpieczeństwa*: **ID.AM-5**] [IEC 62443-2-1: **DATA 1.1**]	W celu ustalania priorytetów na poziomie wpływu można wykorzystać kryteria takie jak bezpieczeństwo lub świadczenie usług o krytycznym znaczeniu.
ZADANIE P-7 STRATEGIA CIĄGŁEGO MONITOROWANIA – ORGANIZACJA	Opracowanie i wdrożenie w całej organizacji strategii ciągłego monitorowania skuteczności zabezpieczeń. [*Ramy Cyberbezpieczeństwa*: **DE.CM; ID.SC-4**] [IEC 62443-2-1: **EVENT 1.1; COMP 2.2 USER 1.06; EVENT 1.1.; ORG2.2**	
Poziom systemu		
ZADANIE P-8 MISJA LUB PRZEDMIOT DZIAŁANIA	Identyfikowane są misje, funkcje biznesowe i procesy biznesowe, które system ma wspierać. [*Ramy Cyberbezpieczeństwa*: **Profil**; **Poziomy wdrożenia**; **ID.BE**] [IEC 62443-2-1: **ORG1.6; AVAIL 1.2; AVAIL 1.1**]	Podczas przygotowywania opisów procesów OT i IT należy również udokumentować przepływy informacji i protokoły.

Zadania	**Rezultaty**	**Rekomendacje dotyczące systemów OT**
ZADANIE P-9 INTERESARIUSZE SYSTEMU	Identyfikuje się podmioty, które są zainteresowane wykorzystywaniem systemu. [*Ramy Cyberbezpieczeństwa*: **ID.AM**; **ID.BE**]	Przykładowe stanowiska pracowników odpowiedzialnych za systemy OT obejmują między innymi kierownika procesu/organizacji, inżyniera ds. nadzoru technicznego, operatora, inżyniera ds. bezpieczeństwa funkcjonalnego, a także kierownika ds. bezpieczeństwa procesu.
ZADANIE P-10 IDENTYFIKACJA AKTYWÓW	Identyfikowane są aktywa zainteresowanych stron i ustalane są ich priorytety [*Ramy Cyberbezpieczeństwa*: **ID.AM**]	Komponenty systemu OT mogą obejmować programowalne sterowniki logiczne, czujniki, siłowniki, roboty, obrabiarki, oprogramowanie układowe, przełączniki sieciowe, routery, zasilacze i inne komponenty lub urządzenia sieciowe.
ZADANIE P-11 GRANICA AUTORYZACJI	Określona jest granica autoryzacji (tzn. co wchodzi w skład systemu).	
ZADANIE P-12 TYP INFORMACJI	Określane są typy informacji przetwarzanych, magazynowanych i przesyłanych przez system. *[Ramy Cyberbezpieczeństwa:* **ID.AM-5**]	
ZADANIE P-13 CYKL ŻYCIA INFORMACJI	Dla każdego rodzaju informacji przetwarzanej przez system, identyfikowane i interpretowane są wszystkie etapy cyklu życia tych informacji. [*Ramy Cyberbezpieczeństwa*: **ID.AM-3**; **ID.AM-4**]	
ZADANIE P-14 SZACOWANIE RYZYKA – SYSTEM	Szacowanie ryzyka na poziomie systemu jest zakończone lub istniejące szacowanie ryzyka jest aktualizowane. [*Ramy Cyberbezpieczeństwa*: **ID.RA; ID.SC-2**]	Wyniki szacowania ryzyka, w tym testy wydajności/obciążeniowe oraz testy penetracyjne, zostały przeprowadzone na systemach OT z zachowaniem odpowiedniej ostrożności, aby zapewnić, że proces testowania nie wpłynie negatywnie na działanie systemów OT.

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE P-15 DEFINICJA WYMAGAŃ	Zdefiniowane są i uszeregowane pod względem ważności wymagania dotyczące bezpieczeństwa i ochrony prywatności. *[Ramy Cyberbezpieczeństwa:* **ID. GV; PR.IP**]	
ZADANIE P-16 ARCHITEKTURA KORPORACYJNA	Określone jest umiejscowienie systemu w architekturze korporacyjnej.	Należy kategoryzować komponenty systemów OT według funkcji lub poziomu wrażliwości, aby zoptymalizować wdrażanie zabezpieczeń związanych z cyberbezpieczeństwem.
ZADANIE P-17 PRZYDZIAŁ WYMAGAŃ	Wymagania dotyczące bezpieczeństwa i prywatności są przypisane do systemu i środowiska, w którym system działa. [*Ramy Cyberbezpieczeństwa*: **ID.GV**]	Ze względu na to, że wymagania dotyczące bezpieczeństwa i prywatności są przypisywane do systemu OT, należy uwzględniać kwestie takie jak ich wpływ na wydajność i bezpieczeństwo.
ZADANIE P-18 REJESTRACJA SYSTEMU	System jest zarejestrowany zgodnie z celami zarządzania, odpowiedzialności, koordynacji i nadzoru. *[Ramy Cyberbezpieczeństwa:* **ID.GV**]	

4.3.2. KATEGORYZACJA

Na etapie *Kategoryzacja* określane są potencjalne negatywne skutki utraty poufności, integralności i dostępności informacji bądź systemu. W przypadku każdego analizowanego rodzaju informacji i systemu, trzy atrybuty bezpieczeństwa – poufność, integralność i dostępność – są powiązane z jednym z trzech poziomów potencjalnych skutków naruszenia bezpieczeństwa. Spośród trzech atrybutów bezpieczeństwa, dostępność jest najważniejszym czynnikiem w przypadku systemów OT. Normy i wytyczne dotyczące procesu kategoryzacji znajdują się w dokumentach NSC 199 [NSC 199] oraz NSC 800- 60 [NSC 800-60].

Przedstawiony poniżej przykład pochodzi z dokumentu NSC 199:

Zalecenia i wytyczne dotyczące systemów OT

Elektrownia posiada system nadzoru i gromadzenie danych (*ang. Supervisory Control and Data Acquisition – SCADA*) kontrolujący rozdział energii elektrycznej w dużej instalacji wojskowej. System SCADA przetwarza zarówno dane czasu rzeczywistego z czujników, jak i informacje administracyjne. Kierownictwo w elektrowni ustala, że: (I) w przypadku danych z czujników pozyskiwanych przez system SCADA nie występuje potencjalny wpływ utraty poufności, natomiast potencjalny wpływ utraty integralności i dostępności jest wysoki; oraz (II) w przypadku informacji administracyjnych przetwarzanych przez system występuje niewielki potencjalny wpływ utraty poufności, niski potencjalny wpływ utraty integralności oraz niski potencjalny wpływ utraty dostępności. Wynikowe kategorie bezpieczeństwa - KB (*ang. security categories – SC*) tych rodzajów informacji wyrażane są jako:

KB danych z czujników = {(**poufność**, NIE DOTYCZY), (**integralność**, WYSOKI),

(**dostępność**, WYSOKI)} oraz

KB informacji administracyjnej = {(**poufność**, NISKI), (**integralność**, NISKI), (**dostępność**, NISKI)},

Wynikowa kategoria bezpieczeństwa systemu informatycznego wyrażona jest jako:

KB systemu SCADA = {(**poufność**, NISKI), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)},

przedstawiając najwyższy wpływ lub potencjalnie maksymalne wartości wpływu poszczególnych atrybutów bezpieczeństwa dla rodzajów informacji przetwarzanych w systemie SCADA. Zarząd elektrowni wybiera podniesienie potencjalnego wpływu utraty poufności z niskiego do umiarkowanego w celu odzwierciedlenia bardziej realistycznego obrazu potencjalnego wpływu na system informacyjny w sytuacji, w której wystąpiłoby naruszenie bezpieczeństwa związane z nieuprawnionym ujawnieniem informacji na poziomie systemu lub funkcji przetwarzania. Ostateczna kategoria bezpieczeństwa systemu informacyjnego wyrażana jest jako:

KB systemu SCADA = {(**poufność**, UMIARKOWANY), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)}

Tabela 7 zawiera szczegółowe informacje na temat zastosowania etapu kategoryzacji ram zarządzania ryzykiem w kontekście systemów OT.

Tabela 7. Etap kategoryzacji ram zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE C-1 OPIS SYSTEMU	Opisana i udokumentowana charakterystyka systemu. *[Ramy Cyberbezpieczeństwa:* **Profil**]	
ZADANIE C-2 KATEGORYZACJA BEZPIECZEŃSTWA	Zakończona kategoryzacja bezpieczeństwa systemu, w tym informacji przetwarzanych przez system reprezentowany przez zidentyfikowane przez organizację typy informacji. [*Ramy Cyberbezpieczeństwa*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] Wyniki kategoryzacji bezpieczeństwa są dokumentowane w planach dotyczących bezpieczeństwa, prywatności i SCRM. [*Ramy Cyberbezpieczeństwa*: **Profil**] Wyniki kategoryzacji bezpieczeństwa są spójne z architekturą korporacyjną i podejściem do ochrony misji organizacyjnych, funkcji biznesowych i procesów misyjnych/biznesowych. [*Ramy Cyberbezpieczeństwa*: **Profil**] Wyniki kategoryzacji bezpieczeństwa odzwierciedlają strategię zarządzania ryzykiem w organizacji.	Systemy OT i IT mogą charakteryzować się zróżnicowanymi kryteriami kategoryzacji. Podczas kategoryzacji bezpieczeństwa należy uwzględniać informacje na temat systemu oraz procesu realizowanego przez system (na przykład produkcję substancji chemicznych).
ZADANIE C-3 PRZEGLĄD I ZATWIERDZANIE KATEGORII BEZPIECZEŃSTWA	Wyniki kategoryzacji bezpieczeństwa są zweryfikowane, a decyzja o kategoryzacji jest zatwierdzona przez kierownika wyższego szczebla w organizacji.	

4.3.3. WYBÓR

Celem etapu *Wybór* jest wstępne określenie zabezpieczeń w celu ochrony systemu współmiernie do ryzyka. Poziom bazowy zabezpieczeń stanowi punkt wyjścia dla procesu wyboru zabezpieczeń, który odbywa się na podstawie kategorii

bezpieczeństwa oraz poziomu wpływu systemów wskazanych na etapie kategoryzacji. Dokument NSC 800-53B [NSC 800-53B] zawiera opisy zalecanych poziomów bazowych zabezpieczeń stosowanych w odniesieniu do rządowych systemów oraz danych. W celu zaspokojenia potrzeby opracowania ogólnych oraz wyspecjalizowanych zestawów zabezpieczeń dla systemów i organizacji, autorzy publikacji opracowali koncepcję nakładek. *Nakładka* to kompleksowy zestaw zabezpieczeń, zabezpieczeń rozszerzonych oraz dodatkowych wytycznych wynikających z zastosowania zaleceń dotyczących dostosowywania zestawu minimalnych zabezpieczeń opisanych w Załączniku C do dokumentu NSC 800-53B [NSC 800-53B].

Celem nakładek jest ograniczenie potrzeby doraźnego dostosowywania poziomu bazowego zabezpieczeń przez organizacje poprzez wybór zestawu zabezpieczeń i zabezpieczeń rozszerzonych, które są dostosowane do typowych okoliczności, sytuacji bądź warunków. W Załączniku F do niniejszej publikacji znajduje się nakładka obejmująca zabezpieczenia opisane w dokumencie NSC 800-53 [NSC 800-53] dotycząca systemów OT, która zapewnia dostosowane poziomy bazowe zabezpieczeń dla systemów OT o niskim, umiarkowanym i wysokim poziomie wpływu. Opisane poziomy bazowe stanowią punkt wyjścia oraz zbiór zaleceń, które mogą być wdrażane w przypadku określonych systemów OT przez pracowników odpowiedzialnych za ich zabezpieczenie.

W przypadku, gdy wdrożenie wybranych środków bezpieczeństwa okaże się niemożliwe lub niewykonalne, osoby odpowiedzialne za systemy OT mogą dostosować nakładkę zawartą w Załączniku F. Korzystanie z nakładek w żaden sposób nie uniemożliwia organizacjom dalszego dostosowywania zabezpieczeń (w tym nakładek, które mogą również podlegać dostosowaniu) w celu uwzględnienia specyficznych potrzeb, założeń lub ograniczeń danej organizacji. Wszelkie działania prowadzone w celu dostosowania zabezpieczeń powinny skupiać się na realizacji celów podstawowych zabezpieczeń, o ile jest to możliwe oraz wykonalne.
W przykładowej sytuacji, w której dany system OT nie obsługuje wybranych zabezpieczeń lub zabezpieczeń rozszerzonych, bądź organizacja uzna, że objęcie systemów OT wybranymi zabezpieczeniami nie jest wskazane ze względu na

negatywny wpływ na wydajność, bezpieczeństwo lub niezawodność, organizacja powinna przedstawić wybór zabezpieczeń kompensacyjnych wraz z kompleksowym uzasadnieniem wyboru, wyjaśnieniem przyczyn niezastosowania zabezpieczeń bazowych oraz opisem wykorzystanych zabezpieczeń zapewniających zbliżoną zdolność do ochrony. W przypadkach, w których systemy OT nie obsługują zautomatyzowanych mechanizmów, organizacja powinna zastosować niezautomatyzowane mechanizmy lub procedury w roli zabezpieczeń kompensacyjnych zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania zawartymi w rozdziale 3.3 dokumentu NSC 800-53. Stosowanie zabezpieczeń kompensacyjnych nie stanowi wyjątku ani nie zwalnia organizacji ze stosowania zabezpieczeń bazowych. Należy traktować je jako alternatywne zabezpieczenia i środki przeciwdziałania wykorzystywane w kontekście systemów OT realizujące cele zabezpieczeń bazowych, które nie zostały wdrożone. **Decyzje organizacji dotyczące stosowania zabezpieczeń kompensacyjnych winne być udokumentowane w planie bezpieczeństwa dotyczącym systemów OT**.

Tabela 8 zawiera szczegółowe informacje na temat zastosowania etapu wyboru ram zarządzania ryzykiem w kontekście systemów OT.

Tabela 8. Etap wyboru zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE S-1 WYBÓR ZABEZPIECZEŃ	Wybrane zabezpieczenia bazowe niezbędne do ochrony systemu współmiernej do ryzyka. [*Ramy Cyberbezpieczeństwa*: **Profil**]	W przypadku systemów OT można wykorzystać poziomy bazowe zabezpieczeń dla systemów OT opisane w Załączniku F do niniejszego dokumentu jako punkt wyjścia do wyboru zabezpieczeń przez organizację.
ZADANIE S-2 DOSTOSOWYWANIE ZABEZPIECZEŃ	Zabezpieczenia są dostosowane do potrzeb organizacji, co pozwala na stworzenie przystosowanych do jej potrzeb zabezpieczeń bazowych. [*Ramy Cyberbezpieczeństwa*: **Profil**]	Ze względu na ograniczenia operacyjne lub techniczne wdrożenie niektórych zabezpieczeń może okazać się niewykonalne. Organizacje powinny wziąć pod uwagę możliwość zastosowania zabezpieczeń kompensacyjnych w celu ograniczenia ryzyka do akceptowalnego poziomu.

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE S-3 PRZYDZIAŁ ZABEZPIECZEŃ	Zabezpieczenia są oznaczone jako zabezpieczenia specyficzne dla danego systemu, hybrydowe lub wspólne. Zabezpieczenia są przydzielone do poszczególnych elementów systemu (tj. sprzętu, zasobów fizycznych lub ludzkich). *[Ramy Cyberbezpieczeństwa:* **Profil**; **PR.IP**]	
ZADANIE S-4 DOKUMENTACJA WDROŻENIA PLANOWANYCH ZABEZPIECZEŃ	Zabezpieczenia i związane z nimi działania dostosowujące są udokumentowane w planach bezpieczeństwa i ochrony prywatności lub równoważnych dokumentach. *[Ramy Cyberbezpieczeństwa:* **Profil**]	
ZADANIE S-5 STRATEGIA CIĄGŁEGO MONITOROWANIA SYSTEMU	Opracowywana jest strategia ciągłego monitorowania systemu, która odzwierciedla strategię zarządzania ryzykiem organizacyjnym. [*Ramy Cyberbezpieczeństwa*: **ID.GV**; **DE.CM**]	Ze względu na wyjątkowe ograniczenia dotyczące działania, środowiska bądź dostępności konieczne może być zastosowanie strategii ciągłego monitorowania opracowanej z myślą o systemach OT w celu pomiaru skuteczności zabezpieczeń.
ZADANIE S-6 PRZEGLĄD I ZATWIERDZENIE PLANU	Plany bezpieczeństwa i ochrony prywatności odzwierciedlające wybór zabezpieczeń niezbędnych do ochrony systemu i środowiska pracy współmiernych do ryzyka są zweryfikowane i zatwierdzone przez osobę autoryzującą.	Przegląd wszelkich potencjalnych skutków dla skuteczności operacyjnej i bezpieczeństwa systemu OT.

4.3.4. WDROŻENIE

Etap *Wdrożenie* obejmuje działania mające na celu wdrożenie wybranych zabezpieczeń w nowych lub istniejących systemach. Proces wyboru zabezpieczeń opisany w niniejszym rozdziale może odnosić się do systemów OT na dwa sposoby – zarówno do nowych, jak i istniejących systemów.

W przypadku nowych systemów w trakcie rozwoju, proces wyboru zabezpieczeń opiera się na określaniu wymagań – stosowne systemy jeszcze nie powstały, a organizacja przeprowadza wstępne kategoryzacje bezpieczeństwa. Zabezpieczenia uwzględnione w planach bezpieczeństwa systemów pełnią funkcję specyfikacji zabezpieczeń.

Oczekiwane jest uwzględnienie ich na etapach rozwoju i wdrożenia cyklu życia systemu.

Proces wyboru zabezpieczeń dla starszych systemów opiera się z kolei na procesie analizy podatności przeprowadzanym w związku z przewidywanymi zmianami w systemach (na przykład podczas dużych aktualizacji, modyfikacji lub outsourcingu). Ze względu na to, że prace dotyczą istniejących systemów, organizacja prawdopodobnie zakończyła procesy kategoryzacji bezpieczeństwa i wyboru zabezpieczeń, co umożliwia uwzględnienie uzgodnionych zabezpieczeń w odpowiednich planach bezpieczeństwa i wdrożenia ich w systemach.

Tabela 9 zawiera szczegółowe informacje na temat zastosowania etapu wdrożenia ram zarządzania ryzykiem w kontekście systemów OT.

Tabela 9. Etap wdrożenia ram zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE I-1 WDROŻENIE ZABEZPIECZEŃ	Wdrożenie zabezpieczeń w ramach planów bezpieczeństwa i ochrony prywatności. [*Ramy Cyberbezpieczeństwa*: **PR.IP-1**] Metodologie inżynierii bezpieczeństwa i prywatności systemów są wykorzystywane w celu uwzględnienia zabezpieczeń w planach bezpieczeństwa i prywatności systemu. *[Ramy cyberbezpieczeństwa: **PR.IP-2**]*	W przypadku istniejących (działających w organizacji) systemów OT należy zaplanować wdrożenie zabezpieczeń podczas konserwacji systemu. Zalecane jest przeprowadzenie pełnej weryfikacji, aby upewnić się, że zabezpieczenia nie wpływają na wydajność i bezpieczeństwo systemu OT ani nie pogarszają ich działania. W niektórych przypadkach natychmiastowe ograniczenie ryzyka może być niewykonalne ze względu na problemy związane z planowaniem. W takich sytuacjach można jednak wdrożyć tymczasowe zabezpieczenia kompensacyjne.
ZADANIE I-2 AKTUALIZACJA INFORMACJI O REALIZACJI ZABEZPIECZEŃ	Dokumentowanie zmian w planowanych wdrożeniach zabezpieczeń w stosunku do zaimplementowanych dotychczas zabezpieczeń. *[Ramy cyberbezpieczeństwa: **PR.IP-1**]* Plany bezpieczeństwa i prywatności są aktualizowane na podstawie informacji uzyskanych podczas wdrażania zabezpieczeń. *[Ramy Cyberbezpieczeństwa:* **Profil**]	

4.3.5. OCENA

Etap *Ocena* ujęty w ramach zarządzania ryzykiem pozwala na określenie skuteczności stosowania zabezpieczeń oraz stwierdzenie, czy wdrożone zabezpieczenia spełniają oczekiwania. Dokument NSC 800-53A [NSC 800-53A] zawiera wytyczne dotyczące oceny wybranych zabezpieczeń opisanych w dokumencie NSC 800-53 [NSC 800-53] w celu zapewnienia, że są one prawidłowo wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do wymagań bezpieczeństwa systemu.

Tabela 10 zawiera szczegółowe informacje na temat zastosowania etapu oceny ram zarządzania ryzykiem w kontekście systemów OT.

Tabela 10. Etap oceny ram zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE A-1 WYBÓR PODMIOTU OCENIAJĄCEGO	Do przeprowadzenia oceny zabezpieczeń wybierany jest podmiot oceniający lub zespół oceniający. Osiągany jest odpowiedni poziom niezależności wybranego podmiotu oceniającego lub zespołu oceniającego.	Należy włączyć pracowników odpowiedzialnych za system OT oraz operatora systemu do zespołu oceniającego.
ZADANIE A-2 PLAN OCENY	Dokumentacja potrzebna do przeprowadzenia oceny jest dostarczana podmiotowi oceniającemu lub zespołowi oceniającemu. Opracowywane i dokumentowane są plany oceny bezpieczeństwa i ochrony prywatności. Plany oceny bezpieczeństwa i prywatności są poddawane przeglądowi i zatwierdzane w celu ustalenia oczekiwań dotyczących oceny zabezpieczeń i wymaganego poziomu nakładu	
ZADANIE A-3 OCENA ZABEZPIECZEŃ	Ocena zabezpieczeń przeprowadzana jest zgodnie z planami oceny bezpieczeństwa i ochrony prywatności. Rozważane są możliwości ponownego wykorzystania wyników poprzednich ocen w celu zapewnienia terminowości i opłacalności procesu zarządzania ryzykiem. W celu zwiększenia szybkości, skuteczności i wydajności oceny zabezpieczeń wprowadzana jest optymalizacja wykorzystania systemów automatyzacji.	Należy uwzględnić możliwość przeprowadzenia ćwiczeń lub symulacji, aby ograniczyć wpływ oceny na działanie produkcyjnych systemów OT. W celu przeprowadzenia oceny zabezpieczeń należy korzystać ze zautomatyzowanych narzędzi i zachować szczególną ostrożność, aby proces testowania nie miał negatywnego wpływu na system OT i jego działanie.

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE A-4 SPRAWOZDANIA Z OCENY	Sporządzane są sprawozdania z oceny bezpieczeństwa i ochrony prywatności, przedstawiające ustalenia i zalecenia. *[Ramy Cyberbezpieczeństwa:* **ID.RA-1 i ID.RA-3**]	
ZADANIE A-5 DZIAŁANIA NAPRAWCZE	Podejmowane są działania naprawcze mające na celu usunięcie braków w zabezpieczeniach wdrożonych w systemie i środowisku pracy. Plany bezpieczeństwa i ochrony prywatności są aktualizowane w celu odzwierciedlenia zmian w realizacji zabezpieczeń dokonanych w oparciu o oceny i późniejsze działania naprawcze. *[Ramy Cyberbezpieczeństwa:* **Profil**]	Należy upewnić się, że działania naprawcze nie wpłyną negatywnie na wydajność i bezpieczeństwo działania systemów OT. Należy uwzględnić możliwość zastosowania zabezpieczeń kompensacyjnych w roli jednego z działań naprawczych.
ZADANIE A-6 PLAN I ETAPY DZIAŁAŃ	Opracowywany jest plan i etapy działań określające plany naprawcze dotyczące niedopuszczalnych zagrożeń zidentyfikowanych w sprawozdaniach z oceny bezpieczeństwa i ochrony prywatności. [*Ramy Cyberbezpieczeństwa*: **ID.RA-6**]	W ramach opracowywania planów i etapów działań należy uwzględnić ograniczenia dotyczące czasu związane z systemem OT oraz planowaną konserwację lub wyłączenia systemu OT.

4.3.6. AUTORYZACJA

Etap *Autoryzacja* obejmuje podjęcie przez kierownictwo decyzji o autoryzacji działania systemu i oficjalnej akceptacji ryzyka dla działalności, zasobów oraz osób w oparciu o zestaw uzgodnionych i wdrożonych zabezpieczeń. Nowy system nie może być wykorzystywany bądź eksploatowany przed uzyskaniem autoryzacji.

Tabela 11 zawiera szczegółowe informacje na temat zastosowania etapu autoryzacji ram zarządzania ryzykiem w kontekście systemów OT.

Tabela 11. Etap autoryzacji ram zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE R-1 PAKIET AUTORYZACYJNY	Pakiet autoryzacyjny jest opracowywany w celu przedłożenia go osobie autoryzującej.	

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE R-2 ANALIZA I OKREŚLENIE RYZYKA	Ustalenie ryzyka przez osobę autoryzującą, które odzwierciedla strategię zarządzania ryzykiem, w tym tolerancję ryzyka.	
ZADANIE R-3 REAKCJA NA RYZYKO	Zapewnienie reakcji na określone ryzyko. [*Ramy Cyberbezpieczeństwa*: **ID.RA-6**]	Należy opracować i wdrożyć kompleksową strategię zarządzania ryzykiem dotyczącym systemów OT, która obejmuje wykrywanie ryzyka oraz ustalanie priorytetów działań w zakresie reakcji na ryzyko.
ZADANIE R-4 DECYZJA AUTORYZUJĄCA	Zatwierdza się lub odmawia autoryzacji systemu lub zabezpieczeń wspólnych.	Organizacje mogą określić strategie korygujące, gdy po uwzględnieniu zależności związanych z systemami OT ryzyko systemowe wykracza poza akceptowalny zakres. Przykładem takich zależności może być niemożność wyłączenia systemu lub komponentu do czasu naprawy.
ZADANIE R-5 SPRAWOZDANIE Z AUTORYZACJI	Decyzje autoryzacyjne, istotne podatności i ryzyka są zgłaszane kierownictwu organizacji.	Należy upewnić się, że decyzje autoryzacyjne, informacje na temat podatności oraz ryzyka zostaną przekazane pracownikom odpowiedzialnym za systemy OT oraz pracownikom działu operacyjnego.

4.3.7. MONITOROWANIE

Etap *Monitorowanie* pozwala na śledzenie zmian w systemie, które mogą mieć wpływ na zabezpieczenia, a także na kontrolowanie ich skuteczności. Dokument NSC SP 800-37 zawiera wytyczne dotyczące ciągłego monitorowania cyberbezpieczeństwa [NSC 800-37].

Tabela 12 zawiera szczegółowe informacje na temat zastosowania etapu monitorowania ram zarządzania ryzykiem w kontekście systemów OT.

Tabela 12. Etap monitorowania ram zarządzania ryzykiem w kontekście systemów OT

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE M-1 ZMIANY SYSTEMOWE I ŚRODOWISKOWE	System informacyjny i środowisko pracy są monitorowane zgodnie ze strategią ciągłego monitorowania. [*Ramy Cyberbezpieczeństwa*: **DE.CM**; **ID.GV**]	Należy wykorzystać strategię ciągłego monitorowania systemów OT, która uwzględnia wpływ działań na wydajność oraz systemy bezpieczeństwa fizycznego i uznaje te aspekty za kluczowe.
ZADANIE M-2 OCENY BIEŻĄCE	Bieżące oceny skuteczności zabezpieczeń prowadzone są zgodnie ze strategią ciągłego monitorowania. *[Ramy Cyberbezpieczeństwa:* **ID.SC-4**]	Należy przeprowadzać bieżące oceny, które uwzględniają wydajność systemu i wpływ na bezpieczeństwo.
ZADANIE M-3 BIEŻĄCA REAKCJA NA RYZYKO	Wyniki działań z zakresu ciągłego monitorowania są analizowane i podejmowane są stosowne działania korygujące. [Ramy Cyberbezpieczeństwa: RS.AN]	Należy zestawiać informacje o wykrytych zdarzeniach z wynikami szacowania ryzyka w celu określenia wpływu incydentów na systemy OT.
ZADANIE M-4 AKTUALIZACJE PAKIETÓW AUTORYZACYJNYCH	Dokumenty dotyczące zarządzania ryzykiem są aktualizowane w oparciu o ciągłe działania monitorujące. *[Ramy Cyberbezpieczeństwa:* **RS.IM**]	
ZADANIE M-5 SPRAWOZDAWCZOŚĆ W ZAKRESIE BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	Wprowadzenie procesu zgłaszania stanu bezpieczeństwa i prywatności osobie autoryzującej oraz wyższemu personelowi i kierownictwu.	
ZADANIE M-6 BIEŻĄCA AUTORYZACJA	Osoba autoryzująca na bieżąco dokonuje autoryzacji, wykorzystując wyniki ciągłych działań monitorujących oraz informuje o zmianach w określaniu ryzyka i decyzjach akceptacyjnych.	

Zadania	Rezultaty	Rekomendacje dotyczące systemów OT
ZADANIE M-7 UTYLIZACJA SYSTEMU	W razie potrzeby opracowywana i wdrażana jest strategia utylizacji (likwidacji) systemu.	Zjawisko planowanego postarzania, które bywa obserwowane w środowiskach IT, może nie dotyczyć komponentów systemów OT. Należy uwzględnić możliwość utrzymania, konserwacji oraz naprawy komponentów systemów OT, których dostępność jest wymagana znacznie dłużej niż w przypadku komponentów IT.

5. ARCHITEKTURA CYBERBEZPIECZEŃSTWA SYSTEMÓW OT

Zgodnie z zaleceniami, projekt architektury bezpieczeństwa dla środowiska OT wymaga oddzielenia sieci OT od sieci organizacji ze względu na fakt, że charakter i rodzaj ruchu sieciowego w obu tych sieciach jest zupełnie różny. Na przykład dostęp do Internetu, poczty elektronicznej oraz zdalny dostęp są zazwyczaj dozwolone w sieci organizacji, ale niedozwolone w sieciach OT. Mogą również występować różnice dotyczące stopnia ograniczeń oraz ich przestrzegania związanego z procedurami kontroli zmian w środowisku organizacji i OT. Ponadto korzystanie z sieci organizacji na potrzeby protokołów komunikacyjnych OT może narazić komponenty OT na cyberataki (np. atak odmowy świadczenia usługi - DoS, ataki typu “man-in-the-middle” lub inne ataki sieciowe). Wykorzystanie oddzielnych sieci zapewnia większą elastyczność w zakresie ustalania wymagań dotyczących bezpieczeństwa i wydajności dla obu środowisk.

Względy praktyczne takie jak transformacja cyfrowa, koszt instalacji OT lub chęć utrzymania jednolitej infrastruktury sieciowej często oznaczają, że wymagane jest połączenie OT z sieciami organizacji lub innymi sieciami IT. To połączenie stanowi dodatkowe ryzyko, w związku z czym organizacje powinny minimalizować liczbę takich połączeń oraz uwzględnić dodatkowe zabezpieczenia. Niniejszy rozdział opisuje strategie bezpieczeństwa, które organizacje powinny wziąć pod uwagę podczas projektowania środowisk OT w celu realizacji celów cyberbezpieczeństwa.

5.1. STRATEGIA CYBERBEZPIECZEŃSTWA

Wdrożenie strategii cyberbezpieczeństwa może skutkować bardziej systematycznym podejmowaniem decyzji dotyczących ryzyka w procesach rozwoju oraz działania systemu. Kompleksowa i powszechnie akceptowana strategia cyberbezpieczeństwa może pomóc organizacji w konsekwentnym utrzymywaniu procesu zarządzania akceptowalnym ryzykiem przez cały cykl życia systemu OT.

Bezpieczeństwo systemu jest zoptymalizowane dzięki projektowi inżynieryjnemu opartemu na proaktywnej strategii zapobiegania stratom. Taka strategia obejmuje zaplanowane działania zaprojektowane w taki sposób, by rozwiązać problemy, które

mogą się wydarzyć, a nie problemy, które *prawdopodobnie* się wydarzą, aby proaktywnie identyfikować oraz usuwać słabości i wady systemu prowadzące do powstawania podatności w zabezpieczeniach, aby zrozumieć charakter zagrożeń agresywnych i losowych oraz wprowadzić nowe metody ochrony przed niekorzystnymi konsekwencjami. Proaktywna inżynieria bezpieczeństwa systemów obejmuje również planowanie z uwzględnieniem skutków awarii niezależnie od tego, czy awaria jest skutkiem zagrożeń agresywnych, czy też zdarzeń losowych, a także zapewnienie odporności systemu na takie zdarzenia.

Zalecenia i wytyczne dotyczące systemów OT

Planując strategię bezpieczeństwa, organizacje mogą być zmuszone do uwzględnienia standardów dotyczących infrastruktury krytycznej i wymogów regulacyjnych z nimi związanych. Opierając się na wytycznych CISA, organizacje mogą uznać, że zarówno środowiska IT, jak i OT stanowią część infrastruktury krytycznej. Normy i wymagania są zwykle zaprojektowane w celu ochrony krytycznych zasobów cyfrowych w celu zapewnienia niezawodności i mogą wiązać się z dodatkowymi zobowiązaniami prawnymi dla organizacji.

5.1.1. SKUTKI WYBORU STRATEGII CYBERBEZPIECZEŃSTWA

Świadomie decydując się na opracowanie i wdrożenie strategii cyberbezpieczeństwa, organizacja ustanawia zdyscyplinowane podejście, które uwzględnia wszystkie aspekty cyklu życia systemu – od zakupu po wycofanie z eksploatacji – z myślą o cyberbezpieczeństwie. W rezultacie organizacja może zapewnić realizację celów cyberbezpieczeństwa w swoich systemach.

Decyzje dotyczące strategii cyberbezpieczeństwa powinny wynikać z wysokiego poziomu zrozumienia operacji, celów i oczekiwań organizacji w zakresie cyberbezpieczeństwa. Na przykład organizacja może chcieć, aby jej systemy charakteryzowały się pewnymi cechami, takimi jak odporność lub wiarygodność. Celem strategii jest włączenie tych cech do systemów. Strategia może również obejmować dodatkowe zagadnienia, takie jak elastyczność w zakresie integracji nowych technologii (takich jak: kryptowaluty, sztuczna inteligencja [SI] czy

technologia uczenia maszynowego [ML], cyfrowe bliźniaki[13] - *ang. digital twins*). Co więcej, strategia może określać potrzebę wdrożenia sprawdzonych praktyk w zakresie cyberbezpieczeństwa, takich jak instalowanie poprawek lub monitorowanie.

Strategia cyberbezpieczeństwa powinna bezpośrednio wpływać na decyzje dotyczące architektury podejmowane w odniesieniu do systemów. Wdrożenie architektury opartej na strategii cyberbezpieczeństwa zwiększa prawdopodobieństwo, że wysokopoziomowe cele w zakresie cyberbezpieczeństwa zostaną uwzględnione w sposobie realizacji poszczególnych systemów. Strategia stanowi dokument dokumentujący te cele na potrzeby procesów podejmowania decyzji na poziomie poszczególnych systemów.

Zalecenia i wytyczne dotyczące systemów OT

Systemy OT zwykle charakteryzują się długim czasem eksploatacji oraz wiążą się z dużymi inwestycjami w testy operacyjne, niezawodności i bezpieczeństwa. Zastąpienie istniejących urządzeń oraz aplikacji nowszymi rozwiązaniami w perspektywie krótko- lub średnioterminowej bywa nieekonomicznie lub niewykonalne techniczne. W związku z tym takie rozwiązania są narażone na ataki w większym stopniu niż rozwiązania wyposażone w najnowsze wersje zabezpieczeń i poprawki zabezpieczeń. Wdrożenie strategii cyberbezpieczeństwa może pomóc organizacji w zrozumieniu cyklu życia systemów OT i dostosowaniu podejścia w celu zapewnienia stałego bezpieczeństwa.

5.1.2. STRATEGIA OBRONY W GŁĄB

Obrona w głąb (*ang. Defense-in-Depth*) to wieloaspektowa strategia, która łączy zasoby ludzkie, technologię i możliwości operacyjne w celu ustanowienia zmiennych barier na wielu poziomach oraz w wielu wymiarach organizacji. Wiele architektur cyberbezpieczeństwa obejmuje zasady obrony w głąb. Taka strategia jest uważana za najlepszą praktykę i wpisuje się w wiele istniejących norm oraz regulacji.

[13] Cyfrowy bliźniak to cyfrowy model zamierzonego lub rzeczywistego fizycznego produktu, systemu lub procesu (fizycznego bliźniaka), który służy jako skutecznie nieodróżnialny cyfrowy odpowiednik do celów praktycznych, takich jak symulacja, integracja, testowanie, monitorowanie i konserwacja.

Podstawowe koncepcje zakładają zapobieganie powstawaniu pojedynczych punktów awarii w zabezpieczeniach związanych z cyberbezpieczeństwem i uznanie, że nie istnieje jedno źródło zagrożeń. Na tej podstawie organizowane są zabezpieczenia stanowiące warstwy ochrony wokół krytycznego systemu i jego komponentów.

Zalecenia i wytyczne dotyczące systemów OT

Strategia obrony w głąb jest szczególnie istotna dla środowisk OT, ponieważ pozwala na skupienie uwagi oraz zorganizowanie mechanizmów ochronnych wokół krytycznych funkcji. Ponadto zasady obrony w głąb są elastyczne i mogą być stosowane w szerokim zakresie środowisk OT, obejmujących zarówno systemy sterowania przemysłowego, systemy SCADA, Internetu rzeczy (*ang. Internet of Things – IoT*), przemysłowego Internetu rzeczy (IIoT), jak i środowiska hybrydowe.

Skuteczność obrony w głąb wymaga połączenia zasobów ludzkich, procesów i technologii. Co więcej, zabezpieczenia związane z cyberbezpieczeństwem nie są statyczne i wymagają zmian i aktualizacji w miarę zmian ryzyka w środowisku. Aby pomóc w ustanowieniu i zapewnianiu skuteczności architektury obrony w głąb, organizacje powinny rozważyć:

- Szkolenie pracowników dotyczące utrzymywania środowiska bezpieczeństwa i ograniczania ryzykownych zachowań;
- Wdrożenie odpowiedniej i zrównoważonej technologii cyberbezpieczeństwa;
- Wdrożenie procedur monitorowania, reagowania i dostosowywania zabezpieczeń w zakresie cyberbezpieczeństwa do zmieniających się warunków.

5.1.3. INNE ZAGADNIENIA ZWIĄZANE ZE STRATEGIĄ CYBERBEZPIECZEŃSTWA

Tradycyjne systemy OT zostały zaprojektowane z myślą o bezpiecznej i niezawodnej obsłudze procesów przemysłowych bez połączeń z sieciami zewnętrznymi. Ze względu na potrzebę elastyczności biznesowej i redukcji kosztów infrastruktury OT, systemy i sieci OT stają się w coraz większym stopniu powiązanie z sieciami przedsiębiorstw i infrastrukturą w chmurze. Co więcej, wprowadzenie systemów przemysłowego internetu rzeczy (IIoT) do środowisk OT może mieć niezamierzone konsekwencje dla ich cyberbezpieczeństwa.

Także możliwości przetwarzania w chmurze (w tym rozwiązania typu infrastruktura jako usługa, platforma jako usługa, oprogramowanie jako usługa i bezpieczeństwo jako usługa) są coraz częściej wykorzystywane przez organizacje. Choć wykorzystanie tych rozwiązań w związku z obsługą usług IT jest stosunkowo dobrze rozumiane, wykorzystywanie ich do obsługi środowisk OT może wiązać się z dodatkowymi wyzwaniami związanymi z dostępnością, które wynikają ze zwiększonej wrażliwości na wydajność systemu lub problemy z połączeniem. Z tego powodu wdrożenie strategii opartej na architekturze bezpieczeństwa musi uwzględniać stan istniejących środowisk OT. W oparciu o tę strategię organizacja może podejmować decyzje zakupowe dostosowane w celu uwzględnienia migracji określonych komponentów w celu realizacji nowej strategii. Organizacje mogą również dostrzec, że istniejące systemy obsługują wybrane lub niemal wszystkie elementy strategii architektury bezpieczeństwa, zatem ich wykorzystanie może przyspieszyć wdrażanie ogólnej strategii. Ponadto budowa nowych środowisk OT zapewnia możliwość przeprowadzenia oceny ryzyka związanego z cyberbezpieczeństwem na wcześniejszym etapie oraz uwzględnienia cyberbezpieczeństwa na etapie projektowania.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny dołożyć wszelkich starań, by strategia architektury bezpieczeństwa zapewniała wymaganą elastyczność pozwalającą na rozwój i rozbudowę środowiska, jednocześnie starannie uwzględniając jej wpływ na operacje i cyberbezpieczeństwo.

5.2. MOŻLIWOŚCI ARCHITEKTURY OPARTEJ NA STRATEGII OBRONY W GŁĄB

Wiele organizacji podejmuje inicjatywy transformacji cyfrowej, które wymagają wprowadzenia zmian w środowiskach OT i opracowania strategii, na których opiera się wielopoziomowa architektura informacji wspierająca realizację celów organizacji, takich jak:

- Konserwacja urządzeń terenowych, gromadzenie danych telemetrycznych lub wdrażanie systemów odpowiedzialnych za procesy przemysłowe.

- Ulepszone gromadzenie i rozpowszechnianie danych.
- Zdalny dostęp.

Obecnie obserwuje się coraz większe powiązania między środowiskami IT i OT, ponieważ organizacje dostosowują się do zmieniających się lokalnych i globalnych potrzeb i wymagań. Wykorzystanie zasad architektury obrony w głąb do systematycznego wdrażania kolejnych warstw zabezpieczeń dotyczących pracowników, procesów i technologii może pomóc organizacjom wzmocnić ich ogólną obronę i poprawić stan cyberbezpieczeństwa. W rezultacie przeciwnikom może być coraz trudniej przeniknąć do środowiska bez wykrycia. W poniższych podrozdziałach znajduje się omówienie kolejnych warstw strategii obrony w głąb, a także zagadnień oraz koncepcji, które organizacje powinny wziąć pod uwagę podczas opracowywania i wdrażania swojej architektury cyberbezpieczeństwa. Strategia zakłada istnienie następujących warstw:

- Warstwa 1 – Zarządzanie bezpieczeństwem
- Warstwa 2 – Bezpieczeństwo fizyczne
- Warstwa 3 – Bezpieczeństwo sieci
- Warstwa 4 – Bezpieczeństwo sprzętowe
- Warstwa 5 – Bezpieczeństwo oprogramowania

5.2.1. WARSTWA 1 – ZARZĄDZANIE BEZPIECZEŃSTWEM

Warstwa zarządzania bezpieczeństwem stanowi nadrzędny program cyberbezpieczeństwa, który obejmuje środowisko OT. Rozdziały 3 i 4 omawiają program i zagadnienia dotyczące zarządzania ryzykiem w organizacji w kontekście ustanowienia programów cyberbezpieczeństwa. Decyzje dotyczące programu oraz organizacji wpływają na decyzje podejmowane w odniesieniu do innych warstw architektury obrony w głąb. W związku z tym każda organizacja powinna zakończyć pracę nad tą warstwą przed rozpoczęciem prac mających na celu wdrożenie innych warstw.

5.2.2. WARSTWA 2 – BEZPIECZEŃSTWO FIZYCZNE

Środki bezpieczeństwa fizycznego mają na celu zmniejszenie ryzyka przypadkowego lub celowego zniszczenia bądź uszkodzenia zasobów i otaczającego środowiska. Chronione zasoby mogą obejmować systemy sterowania, narzędzia, sprzęt, środowisko, otaczającą społeczność i własność intelektualną, w tym dane wrażliwe, na przykład ustawienia procesów i informacje o klientach. Organizacje muszą również uwzględnić dodatkowe wymogi dotyczące środowiska i bezpieczeństwa, a także wymogi prawne oraz inne wytyczne w procesie wdrażania rozwiązań w zakresie bezpieczeństwa fizycznego.

Komponent bezpieczeństwa fizycznego architektury obrony w głąb powinien uwzględniać następujące atrybuty:

- **Ochrona lokalizacji fizycznych.** Tradycyjne założenia bezpieczeństwa fizycznego zwykle obejmują zabezpieczenia tworzące szereg fizycznych barier wokół budynków, obiektów, pomieszczeń, urządzeń i zasobów informacyjnych. Zabezpieczenia fizyczne powinny być wdrożone w celu ochrony fizycznych lokalizacji i mogą obejmować ogrodzenia, rowy zabezpieczające przed pojazdami, nasypy ziemne, ściany, wzmocnione bariery, bramy, zamki do drzwi i szafek, osłony lub inne środki.
- **Kontrola dostępu fizycznego.** Szafki ze sprzętem powinny być zamykane na klucz, jeśli ich otwarcie nie jest wymagane w celu ich obsługi lub zapewnienia bezpieczeństwa, a okablowanie powinno być uporządkowane i umieszczone w szafkach lub pod podłogą. Ponadto należy zadbać o przechowywanie całego sprzętu komputerowego i sieciowego w zabezpieczonych obszarach. Klucze do elementy systemów OT, w tym programowalnych sterowników logicznych (PLC) i systemów bezpieczeństwa, powinny być zawsze w pozycji: „Włączony”, z wyjątkiem sytuacji, w której są programowane.
- **Systemy monitorowania dostępu.** Systemy monitorowania dostępu realizują funkcje nadzoru elektronicznego. To między innymi aparaty fotograficzne, fotokomórki i kamery, a także czujniki i systemy identyfikacji, w tym czytniki identyfikatorów, skanery biometryczne oraz elektroniczne klawiatury. Takie

urządzenia zazwyczaj nie uniemożliwiają dostępu do określonej lokalizacji. Dokumentują i rejestrują jedynie fizyczną obecność lub brak fizycznej obecności osób, pojazdów, zwierząt lub innych obiektów fizycznych. Należy zapewnić odpowiednie oświetlenie dla wykorzystywanego wdrożonego urządzenia monitorującego dostęp. Systemy te mogą również ostrzegać lub inicjować działania po wykryciu nieautoryzowanego dostępu.

- **Lokalizacja osób i zasobów.** Lokalizacja osób i pojazdów w obiekcie może być istotna zarówno ze względów bezpieczeństwa, jak i ochrony. Technologie lokalizacji zasobów mogą być wykorzystywane do śledzenia ruchu osób i pojazdów w celu zapewnienia, że pozostają one w autoryzowanych obszarach, do identyfikacji osób, które mogą potrzebować pomocy, oraz do wspierania reakcji w sytuacjach awaryjnych.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny zastanowić się, czy bezpieczeństwo fizyczne zdalnych zasobów jest realizowane na różnych poziomach oraz czy różnice w zabezpieczeniach mogą być źródłem zagrożeń związanych z cyberbezpieczeństwem. Przykładowo, w jednej zdalnej lokalizacji zabezpieczenia mogą opierać się wyłącznie na kłódce i minimalnym nadzorze elektronicznym zabezpieczających dostęp do urządzeń sieciowych. Ominięcie tych zabezpieczeń może umożliwić napastnikowi uzyskanie dostępu do segmentu sieci OT z lokalizacji zdalnej.

Organizacje powinny również rozważyć, czy usługi dodatkowe, takie jak systemy komunikacji i zasilania, które obsługują fizyczne urządzenia zabezpieczające (na przykład kamery, czujniki i inne), wymagają nadmiarowości, izolacji, ochrony i monitorowania.

5.2.3. WARSTWA 3 – BEZPIECZEŃSTWO SIECI

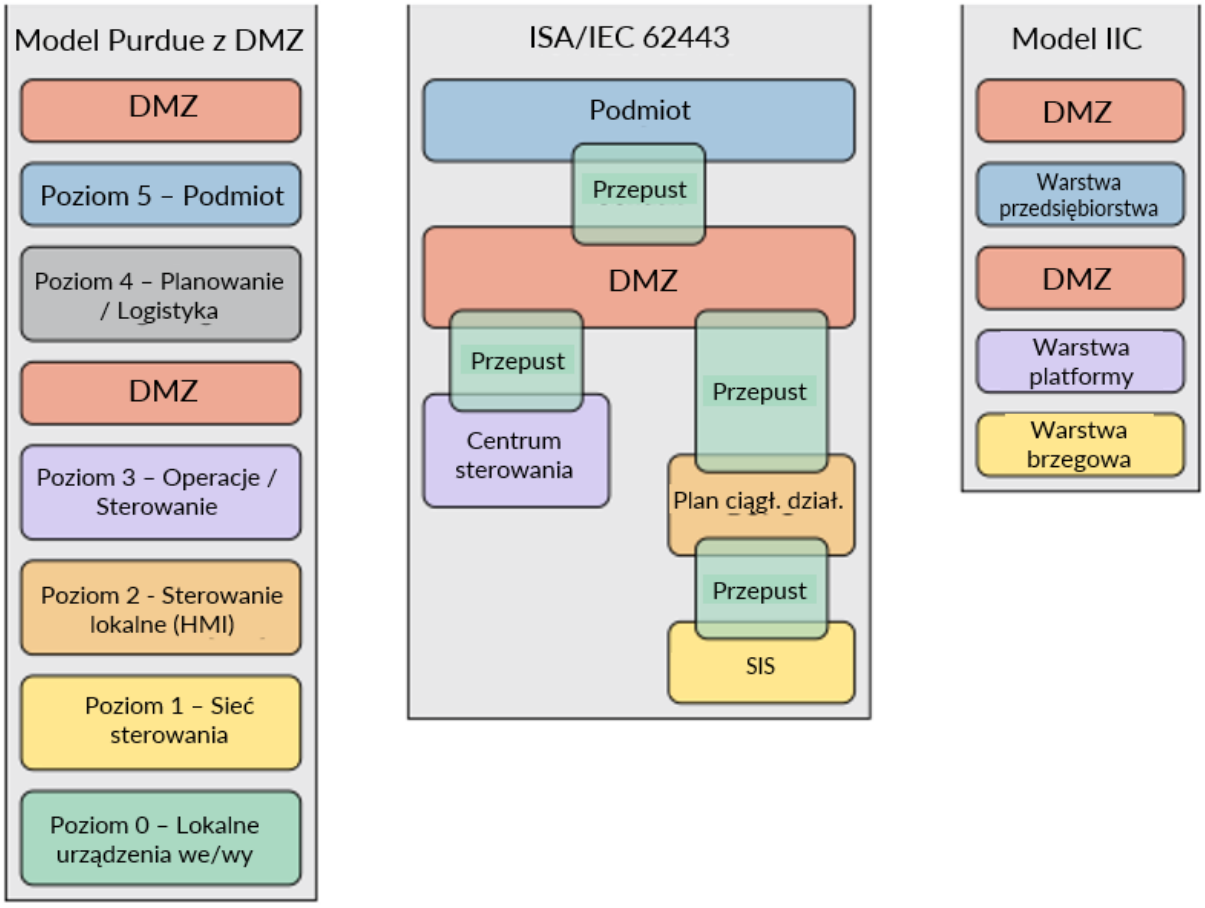
Opierając się na bezpieczeństwie fizycznym, organizacje powinny przeanalizować komunikację sieciową oraz sposoby ochrony danych i urządzeń wykorzystywanych do obsługi środowiska OT. Niniejszy podrozdział koncentruje się na kilku podstawowych zagadnieniach, które pomogą organizacjom w planowaniu i wdrażaniu rozwiązań w zakresie bezpieczeństwa sieci. Obejmują one stosowanie zasad architektury

sieciowej w zakresie segmentacji i izolacji, centralizacji rejestrowania, monitorowania sieci i ochrony przed złośliwym kodem. Dodatkowo poniższy rozdział zawiera omówienie architektury „zerowego zaufania" (*ang. zero trust architecture – ZTA*) i rozważania dotyczące zastosowania tych ulepszeń architektury w środowisku OT.

5.2.3.1. ARCHITEKTURA SIECI

Dobrą praktyką w zakresie architektury sieci jest charakteryzowanie, segmentowanie i izolowanie urządzeń IT oraz OT. Urządzenia mogą być podzielone na segmenty na podstawie uprawnień, poziomu zaufania, krytyczności, przepływu danych, lokalizacji lub innych cech. Organizacje mogą wykorzystać w tym celu uznane modele pozwalające na organizację segmentacji sieci OT, na przykład model Purdue [Williams], poziomy ISA-95 [IEC62264] oraz trójwarstwową architekturę systemu IIoT [IIRA19] lub połączenie tych modeli.

Organizacje mogą ponadto rozważyć włączenie DMZ jako granicy między segmentami sieci, co zostało zaprezentowane na **Rysunku 16**. Wdrożenie segmentacji sieci opartej na poziomach, warstwach lub strefach pozwala organizacjom kontrolować dostęp do informacji wrażliwych i komponentów, jednocześnie uwzględniając wydajność i bezpieczeństwo.



Rysunek 16. Wysokopoziomowy przykład modelu Purdue i modelu IIoT wykorzystanych w celu segmentacji sieci z segmentami DMZ

Zalecenia i wytyczne dotyczące systemów OT

Niezależnie od tego, czy organizacja stosuje podejście oparte na ryzyku, model funkcjonalny czy inny model organizacyjny, grupowanie komponentów w poziomy, warstwy lub strefy jest działaniem podstawowym, które powinno nastąpić przed rozważeniem zastosowania urządzeń izolujących w celu ochrony i monitorowania komunikacji między poziomami, warstwami lub strefami. Organizując zasoby, organizacje powinny rozważyć, w jaki sposób strefy i konfiguracja izolacji wpływają na ich działalność, bezpieczeństwo i możliwości reagowania.

Odpowiednio skonfigurowane architektury sieciowe umożliwiają realizację segmentacji i izolacji poprzez egzekwowanie zasad bezpieczeństwa i kontrolowanie komunikacji sieciowej. Organizacje zazwyczaj wykorzystują opisane przepływy danych w celu identyfikacji wymaganej komunikacji. Wymagania te są następnie włączane do

architektury sieci i konfigurowane na poziomie urządzeń sieciowych w celu monitorowania komunikacji między segmentami i zezwalania tylko na autoryzowaną komunikację. Urządzenia sieciowe, które obsługują funkcje kontroli ruchu (przełączniki, routery, zapory ogniowe i jednokierunkowe bramy lub diody danych) mogą być używane w celu realizacji segmentacji i izolacji sieci.

Zapory sieciowe są powszechnie używane w celu izolacji segmentów sieci oraz ochrony brzegu sieci, a także zabezpieczania połączeń i przepływów informacji między segmentami sieci. Zapory sieciowe mogą być wdrażane jako urządzenia sieciowe lub uruchamiane bezpośrednio na niektórych hostach. Zapory sieciowe są bardzo elastycznymi urządzeniami izolującymi i zwykle stanowią podstawowy mechanizm ochrony urządzeń OT.

Zalecenia i wytyczne dotyczące systemów OT

Odpowiednia konfiguracja zapory sieciowej jest nieodzowna dla prawidłowego zabezpieczenia segmentów sieci. Zestawy reguł zapory sieciowej powinny być tworzone w taki sposób, aby zezwalać tylko na połączenia między sąsiadującymi poziomami, warstwami lub strefami. Na przykład organizacje wykorzystujące architekturę modelu Purdue powinny wdrożyć reguły zapory i ścieżki połączeń, które uniemożliwiają urządzeniom poziomu 4 bezpośrednią komunikację z urządzeniami poziomów 2, 1 lub 0. Podobną koncepcję można zastosować w przypadku architektur opartych na modelach ISA/IEC 62443 i IIC.

Jednym z obszarów, w przypadku których występują znaczące różnice dotyczące reguł zapór sieciowych są zabezpieczenia ruchu wychodzącego z sieci sterowania.

Zezwalanie na połączenia wychodzące z niższych poziomów, warstw lub stref może stanowić znaczące ryzyko, jeśli nie zostaną podjęte odpowiednie działania. Organizacje powinny rozważyć ustanowienie reguł dla połączeń wychodzących zbliżonych poziomem szczegółowości do reguł dla połączeń przychodzących, aby ograniczyć to ryzyko.

Alternatywą dla zapór sieciowych jest jednokierunkowa brama lub dioda danych, która zezwala na autoryzowaną komunikację tylko w jednym kierunku. Korzystanie z jednokierunkowych bram może zapewnić dodatkową ochronę w przypadku

naruszenia zasad ochrony systemów na wyższych poziomach lub warstwach środowiska. Na przykład, jednokierunkowa brama zastosowana między warstwami 2 i 3 może chronić urządzenia warstw 0, 1 i 2 przed zdarzeniem związanym z cyberbezpieczeństwem, które wystąpi w warstwach 3, 4 lub 5.

5.2.3.2. SCENTRALIZOWANE GROMADZENIE PLIKÓW DZIENNIKA

Urządzenia sieciowe i komputerowe (routery, bramy, przełączniki, zapory sieciowe, serwery i stacje robocze) powinny być skonfigurowane w taki sposób, by rejestrowały zdarzenia na potrzeby monitorowania, ostrzegania i analizy reakcji na incydenty. Funkcje rejestrowania umożliwiające rejestrowanie zdarzeń są zwykle dostępne w aplikacjach, systemach operacyjnych i rozwiązaniach sieciowych. Scentralizowana platforma zarządzania plikami dziennika może pomóc organizacjom w realizacji działań związanych z przechowywaniem, monitorowaniem i analizą takich plików.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny zapoznać się z dostępnymi możliwościami rejestrowania zdarzeń i skonfigurować je w taki sposób, by rejestrowały zdarzenia operacyjne i związane z cyberbezpieczeństwem, które dotyczą danego środowiska.

Organizacje powinny ustalić, jak długo dzienniki zdarzeń powinny być przechowywane i upewnić się, że dostępna jest odpowiednia pamięć masowa spełniająca wymogi dotyczące ich magazynowania.

5.2.3.3. MONITOROWANIE SIECI

Monitorowanie sieci obejmuje przeglądanie alertów oraz plików dzienników, a także analizy pod kątem występowania oznak możliwych incydentów związanych z cyberbezpieczeństwem. Narzędzia oraz rozwiązania pozwalające na wykrywanie anomalii w zakresie zachowań (*ang. behavior anomaly detection – BAD*), zarządzanie bezpieczeństwem informacji i zdarzeniami (*ang. security information and event management – SIEM*), systemy wykrywania włamań (*ang. intrusion detection systems – IDS*) i systemy prewencji włamań (*ang. intrusion prevention systems – IPS*) mogą pomóc organizacjom w monitorowaniu ruchu w całej sieci i generowaniu alarmów, gdy zidentyfikują nietypowy lub podejrzany ruch. Inne rozwiązania, które należy uwzględnić w kontekście monitorowania sieci obejmują:

- Zarządzanie zasobami, w tym wykrywanie i inwentaryzacja urządzeń podłączonych do sieci informatycznej
- Ustalenie poziomu bazowego typowego ruchu sieciowego, przepływów danych i komunikacji między urządzeniami.
- Diagnostykę problemów z wydajnością sieci.
- Identyfikację błędów w konfiguracji lub nieprawidłowego działania urządzeń sieciowych;

Organizacje mogą również rozważyć włączenie dodatkowych usług i funkcji, takich jak monitorowanie zagrożeń, które wspomagają skuteczne monitorowanie sieci.

Zalecenia i wytyczne dotyczące systemów OT

Ruch w systemie OT jest zazwyczaj bardziej deterministyczny (powtarzalny, przewidywalny i schematyczny) niż ruch w sieci IT. Charakterystykę tę można wykorzystać do monitorowania sieci w celu wykrywania anomalii i błędów.

Organizacje powinny ustalić normalny stan sieci OT przed wdrożeniem monitorowania bezpieczeństwa sieci, aby być w stanie odróżnić ataki od przejściowych zmian lub normalnych operacji występujących w środowisku. Wdrożenie monitorowania sieci w trybie pasywnym (nasłuchiwania lub uczenia się) i analizowanie informacji w celu rozróżnienia między znaną i nieznaną komunikacją może być niezbędnym pierwszym krokiem we wdrażaniu monitorowania bezpieczeństwa sieci.

Organizacje powinny uwzględnić wpływ szyfrowanej komunikacji sieciowej na możliwości monitorowania sieci i strategie wdrożeniowe. Na przykład system BAD lub IDS może nie być w stanie określić, czy zaszyfrowana komunikacja sieciowa jest złośliwa i może generować fałszywe alarmy lub ignorować rzeczywiste problemy. Zmiana punktu gromadzenia danych w celu przechwytywania ruchu sieciowego przed lub po szyfrowaniu, na przykład przy użyciu narzędzi do monitorowania sieci opartych na hostach, może pomóc w poprawie możliwości monitorowania, gdy wykorzystywana jest szyfrowana komunikacja.

Produkty IDS i IPS są skuteczne w wykrywaniu i zapobieganiu dobrze znanym atakom internetowym, a niektórzy dostawcy systemów IDS i IPS włączają do swoich

produktów sygnatury ataków dla różnych protokołów OT, takich jak Modbus, Distributed Network Protocol 3 (DNP3) i Inter-Control Center Communications Protocol (ICCP). Skuteczne wdrożenie systemów IDS/IPS zazwyczaj obejmuje zarówno rozwiązania oparte na hostach, jak i rozwiązania sieciowe.

Organizacje powinny przeanalizować wpływ zautomatyzowanych działań systemów IPS na środowisko OT przed ich wdrożeniem.

W niektórych przypadkach organizacje mogą rozważyć wdrożenie systemów IPS na wyższych poziomach środowiska (na przykład w interfejsach DMZ), aby ograniczyć ryzyko wystąpienia problemów w związku z automatycznymi działaniami systemu na ruch w sieci OT.

W środowiskach OT funkcje monitorowania dotyczące sieci są zwykle wdrażane na urządzeniach ochrony brzegowej przy użyciu analizatora ruchu sieciowego (*ang. switched port analyzer – SPAN*) lub pasywnych urządzeń sieciowych. Organizacje mogą również wziąć pod uwagę możliwość wdrożenia funkcji monitorowania opartych na hoście na kompatybilnych urządzeniach OT, takich jak: interfejsy HMI, serwery SCADA i stacje robocze inżynierów w celu zwiększenia możliwości monitorowania, pod warunkiem, że wdrożenie tych narzędzi nie wpłynie negatywnie na wydajność lub bezpieczeństwo systemów.

5.2.3.4. ARCHITEKTURA „ZEROWEGO ZAUFANIA" (ZTA)

Architektura „zerowego zaufania" (*ang. Zero-Trust Architecture - ZTA*) to paradygmat cyberbezpieczeństwa, który koncentruje się na ochronie zasobów (w tym usług informacyjnych, danych) w oparciu o założenie, że decyzje dotyczące autoryzacji są podejmowane bliżej żądanego zasobu i są oceniane ciągle, nie zaś przyznawane odgórnie [NSC 800-207]. Konwencjonalne zabezpieczenia sieci koncentrują się na segmentacji i ochronie brzegów sieci. Po przedostaniu się przez urządzenia brzegowe, użytkownicy są zwykle uważani za zaufanych i często mają szeroki dostęp do dostępnych zasobów. W rezultacie urządzenia zabezpieczające granice między strefami nie ograniczają ryzyka przemieszczania się w obrębie strefy. Co więcej, wraz z rosnącą popularnością rozproszonych systemów obliczeniowych, komunikacji bezprzewodowej i komórkowej oraz środowisk chmurowych i hybrydowych,

tradycyjne granice sieci ulegają stopniowemu zacieraniu. W takich sytuacjach organizacje mogą rozważyć włączenie zasad architektury bezpieczeństwa opartej na zasadzie „zerowego zaufania" do swojej sieci.

Niektóre wyzwania związane z wdrożeniem architektury „zerowego zaufania" obejmują:

- Niemożność znalezienia odpowiedniego pojedynczego rozwiązania i konieczność łączenia różnych technologii o różnych poziomach zaawansowania w danym środowisku.
- Większa czaso- i pracochłonność, a także większe zapotrzebowanie na zasoby i kompetencje techniczne wdrożenia architektury „zerowego zaufania" w istniejącym środowisku.

Zalecenia i wytyczne dotyczące systemów OT

Niektóre komponenty systemów OT (sterowniki PLC, kontrolery, interfejsy człowiek-maszyna) mogą nie obsługiwać technologii lub protokołów wymaganych w celu pełnego wdrożenia architektury „zerowego zaufania". W rezultacie implementacja tego modelu może okazać się niewykonalna w przypadku niektórych urządzeń OT. W takiej sytuacji organizacje mogą zastosować architekturę „zerowego zaufania" w przypadku kompatybilnych urządzeń, w szczególności znajdujących się na funkcjonalnie wyższych poziomach architektury OT (na przykład na poziomach 3-5 modelu Purdue, oraz w strefie zdemilitaryzowanej OT).

Organizacje powinny także wziąć pod uwagę wszelkie możliwe negatywne skutki, które mogą wystąpić w wyniku wdrożenia architektury „zerowego zaufania", wynikające na przykład ze zwiększenia opóźnień odpowiedzi na żądania lub braku dostępności jednego lub kilku komponentów systemu. Na podstawie tej analizy organizacje powinny rozważyć dostosowanie implementacji architektury „zerowego zaufania" w celu zminimalizowania opóźnień i zapewnienia odpowiedniej nadmiarowości, aby zminimalizować ryzyko dla działania systemów OT i ich bezpieczeństwa.

Innym ważnym aspektem implementacji architektury „zerowego zaufania" jest tożsamość osób i podmiotów uzyskujących dostęp do zasobów. W środowiskach OT mogą być wykorzystywane współdzielone dane uwierzytelniające, co może mieć wpływ na możliwość pełnego wdrożenia takich rozwiązań.

5.2.4. WARSTWA 4 – BEZPIECZEŃSTWO SPRZĘTOWE

Sprzętowe mechanizmy zabezpieczeń stanowią podstawę bezpieczeństwa i zaufania względem urządzeń w środowisku. Po ustanowieniu zaufania do urządzenia stan musi być utrzymywany i dokumentowany zgodnie z założeniami modelu systemu i obowiązującymi zasadami. W celu umożliwienia prowadzenia takich działań, wybrani producenci wykorzystują wbudowane technologie, takie jak sprzętowe moduły bezpieczeństwa (*ang. Trusted Platform Module – TPM*), lub sprzętową implementację zaawansowanego standardu szyfrowania (*ang. Advanced Encryption Standard - AES*) i bezpiecznej funkcji skrótu (*ang. Secure Hash Algorithm – SHA*). Sprzętowe mechanizmy bezpieczeństwa zawarte w urządzeniach realizują szereg funkcji oraz wymagań bezpieczeństwa, w tym:

- Monitorowanie i analizę zdarzeń.
- Zabezpieczanie konfiguracji i zarządzania.
- Utwardzanie urządzeń.
- Ochronę integralności.
- Kontrolę dostępu.
- Weryfikację tożsamości urządzenia.
- Źródło zaufania.
- Bezpieczeństwo fizyczne.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny przyjrzeć się dostępnym zabezpieczeniom sprzętowym oraz zautomatyzowanym funkcjom, aby określić ich możliwości w zakresie ochrony środowisk OT bez wpływu na wydajność operacyjną, bezpieczeństwo systemów lub ich możliwości.

5.2.5. WARSTWA 5 – BEZPIECZEŃSTWO OPROGRAMOWANIA

Mechanizmy ochrony bezpieczeństwa oprogramowania zapewniają organizacjom możliwości zapewnienia, że aplikacje i usługi wspierające OT są wykorzystywane

i utrzymywane we właściwy sposób. Funkcje zabezpieczeń oprogramowania mogą zwiększyć bezpieczeństwo urządzeń końcowych, gdy organizacje stosują:

- Listy dozwolonych aplikacji.
- Instalowanie poprawek bezpieczeństwa.
- Praktyki bezpiecznego tworzenia kodu.
- Zarządzanie konfiguracją, w tym utwardzanie aplikacji.

5.2.5.1. LISTY DOZWOLONYCH APLIKACJI

Listy dozwolonych aplikacji stanowią dodatkowy mechanizm ochrony hostów, polegający na ograniczeniu aplikacji, które mogą być uruchamiane na urządzeniu. Po prawidłowym skonfigurowaniu nieautoryzowane aplikacje nie będą uruchamiane w środowisku hosta.

Zalecenia i wytyczne dotyczące systemów OT

Stosunkowo statyczny charakter środowisk OT umożliwia organizacjom uwzględnienie list dozwolonych aplikacji w strategii obrony w głąb, co stanowi najlepszą praktykę zalecaną przez Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych.

Analizując możliwość umieszczenia aplikacji na liście dozwolonych aplikacji w środowisku OT, organizacje powinny pozostawać w kontakcie z dostawcami rozwiązań i zapoznać się z dostępnymi wytycznymi dotyczącymi wdrażania, zawartymi w dokumentach takich jak NIST SP 800-167, *Guide to Application Whitelisting* [SP 800-167]; Guidelines for Application Whitelisting in Industrial Control Systems lub innymi wytycznymi dotyczącymi danego sektora. Wszelkie konfiguracje oraz zasady powinny być dokładnie przetestowane przed wdrożeniem do środowisk produkcyjnych, aby zapewnić, że zastosowane reguły i ustawienia realizują cele bezpieczeństwa organizacji.

5.2.5.2. INSTALOWANIE POPRAWEK BEZPIECZEŃSTWA

Poprawki bezpieczeństwa mają dwa główne zastosowania – usuwanie podatności w zabezpieczeniach i rozszerzanie funkcjonalności rozwiązań. W kontekście

bezpieczeństwa oprogramowania oraz architektury obrony w głąb instalowanie poprawek bezpieczeństwa jest kluczowe z punktu widzenia usuwania podatności w zabezpieczeniach. W związku z tym zarządzanie poprawkami stanowi element obrony w głąb, wpisujący się w zarządzanie podatnościami w ramach strategii zarządzania ryzykiem organizacji.

Wprowadzanie poprawek do systemów OT wymaga podjęcia dodatkowych działań, w tym przeprowadzenia testów poprawek, aby upewnić się, że ich instalacja nie wpływa na możliwości operacyjne bądź bezpieczeństwo. Wymagania operacyjne OT mogą również wpływać na częstotliwość instalowania i wdrażania poprawek bezpieczeństwa. Wybrane niektóre środowiska OT muszą działać niemal nieprzerwanie przez dłuższy czas, a okresy konserwacji pozwalające na instalację poprawek i aktualizacji są stosunkowo krótkie. Co więcej, instalowanie poprawek w przypadku starszych komponentów systemów OT, wykorzystujących wycofane systemy operacyjne, może okazać się niemożliwe. W takich przypadkach organizacje muszą przemyśleć możliwości swoich systemów operacyjnych lub zainwestowanie w dodatkowe zabezpieczenia, które ochronią środowisko przed próbami wykorzystania znanych podatności w zabezpieczeniach. Niektóre narzędzia, takie jak zapory aplikacji internetowych (*ang. web application firewalls – WAF*) i systemy prewencji włamań, można skonfigurować w taki sposób, aby zapewniały dodatkową ochronę w celu wykrywania lub zapobiegania atakom na niezałatane podatności w zabezpieczeniach w czasie oczekiwania na możliwość instalacji stosownej poprawki. W przypadku urządzeń, które nie mogą zostać zaktualizowane oraz urządzeń pracujących pod kontrolą przestarzałych systemów operacyjnych, organizacja może zastosować inne narzędzia, w tym zabezpieczenia instalowane przed urządzeniami.

Zalecenia i wytyczne dotyczące systemów OT

O ile to możliwe, poprawki powinny być testowane w środowisku testowym, aby upewnić się, że nie powodują problemów przed wdrożeniem w systemie produkcyjnym. Organizacje powinny planować instalację poprawek i aktualizacji podczas zaplanowanych przerw na konserwację środowiska, a także opracować plan przywracania komponentów systemów OT oraz całego systemu, w którym są instalowane poprawki.

Organizacje powinny również wziąć pod uwagę, że na rożnych poziomach, w różnych warstwach oraz rożnych strefach mogą obowiązywać inne wymagania dotyczące dostępności i w związku z tym możliwości instalacji poprawek mogą być zróżnicowane. O ile to możliwe, organizacje powinny w pierwszej kolejności instalować poprawki komponentów działających w środowiskach znajdujących się w strefach zdemilitaryzowanych oraz gdy istnieją podatności w zabezpieczeniach, które wpływają na dostępność i integralność bądź umożliwiają nieautoryzowany zdalny dostęp do środowiska OT.

5.2.5.3. PRAKTYKI BEZPIECZNEGO TWORZENIA KODU

Organizacje, które opracowują własne systemy i komponenty, powinny włączyć do swojego programu cyberbezpieczeństwa zasady i procedury, które pozwalają na realizację praktyk bezpiecznego tworzenia kodu. Cykl życia software (*ang. software development life cycle – SDLC*) powinien uwzględniać kwestie związane z bezpieczeństwem na każdym etapie procesu powstawania oprogramowania. Zagadnienia te powinny obejmować analizy pod kątem bezpieczeństwa oraz stosowne techniki kodowania w ramach każdego z poniższych procesów:

- Wykorzystywanie lub opracowywanie narzędzi do kontroli i automatyzacji technik tworzenia bezpiecznego kodu.
- Testowanie i sprawdzanie kodu pod kątem zgodności z praktykami w zakresie bezpieczeństwa.
- Testowanie oprogramowania pod kątem podatności dotyczących bezpieczeństwa w kodzie.

Organizacje, które korzystają z komponentów oraz usług dostarczanych przez podmioty zewnętrzne, powinny uwzględnić dokonanie przeglądu tych praktyk przed zawarciem umów z dostawcami. Organizacje mogą przyczynić się do zwiększenia bezpieczeństwa produktów, oczekując stosowania tych praktyk w swoich umowach o gwarancji świadczenia usług i działaniach związanych z zamówieniami.

5.2.5.4. ZARZĄDZANIE KONFIGURACJĄ

Stosowanie praktyk zarządzania konfiguracją, które wspierają bezpieczne konfiguracje i wzmacnianie aplikacji, jest ważne z punktu widzenia realizacji wymogów bezpieczeństwa wynikających z przepisów oraz strategii organizacji. Konfiguracja ta może obejmować ustawienia kontroli dostępu w celu ograniczenia możliwości dostępu lub włączenie szyfrowania w celu ochrony danych w spoczynku lub w tranzycie. Procedury utwardzania aplikacji mogą obejmować wyłączanie lub blokowanie określonych portów komunikacji sieciowej, funkcji aplikacji lub zbędnych usług działających w systemie.

Szyfrowanie danych przepływających przez sieci (danych w tranzycie) lub danych przechowywanych w pamięci dyskowej i lokalnej pamięci masowej (danych w spoczynku) może być również wykorzystywane w celu ochrony środowisk i systemów OT. Szyfrowanie uniemożliwia napastnikom przeglądanie lub modyfikowanie strumieni danych w postaci otwartego tekstu. Ponieważ szyfrowanie i późniejszy proces deszyfrowania wykorzystują algorytmy szyfrujące, jego stosowanie zwiększa opóźnienia, co oznacza, że stosowanie go dla wszystkich urządzeń OT może być niemożliwe. Świadomość zalet i wad szyfrowania może pomóc organizacjom w podjęciu świadomej decyzji o tym, w jakich obszarach strategii obrony w głąb należy uwzględnić jego stosowanie.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny wziąć pod uwagę możliwość wykorzystania szyfrowania do obsługi bezpiecznych połączeń lub kanałów komunikacji w środowiskach OT, gdy połączenia przechodzą przez segmenty sieci inne niż sieć OT, takie jak sieć organizacji lub Internet. Połączenia oparte na wirtualnej sieci prywatnej (*ang. virtual private network – VPN*) powinny wykorzystywać protokoły szyfrowania, takie jak Transport Layer Security (TLS) lub Internet Protocol Security (IPsec), w celu zabezpieczenia przesyłanych danych.

Szyfrowanie może być również stosowane na dyskach twardych oraz w pamięci lokalnej w celu ochrony danych w spoczynku. Pełne szyfrowanie dysku jest zalecane w przypadku laptopów i urządzeń przenośnych. Organizacje mogą również zastosować szyfrowanie folderów zawierających poufne pliki.

Organizacje muszą również wziąć pod uwagę, że szyfrowanie może negatywnie wpływać na inne zabezpieczenia, na przykład rozwiązania do monitorowania sieci. Przykładem mogą być systemy wykrywania włamań, które nie są w stanie stwierdzić, czy zaszyfrowany pakiet jest złośliwy, co może skutkować fałszywymi alarmami lub ignorowaniem rzeczywistych zagrożeń.

Organizacje powinny również stworzyć procedury zarządzania zmianami w logice sterowania, aby chronić się przed ryzykiem, że niewłaściwie przetestowane lub złośliwe zmiany w logice mogą zakłócić działanie systemu.

5.3. DODATKOWE ZAGADNIENIA DOTYCZĄCE ARCHITEKTURY CYBERBEZPIECZEŃSTWA

Organizacje powinny uwzględniać kwestie dotyczące cyberbezpieczeństwa, dostępności, systemów rozproszonych geograficznie, uwarunkowań środowiskowych i wymogów regulacyjnych w projektach i wdrożeniach architektury bezpieczeństwa dla środowisk OT oraz IIoT. Poniższe podrozdziały zawierają szczegółowe omówienie poszczególnych zagadnień.

5.3.1. ZAGADNIENIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

Systemy OT są zazwyczaj projektowane z myślą o spełnieniu określonych wymogów w zakresie bezpieczeństwa fizycznego, z uwzględnieniem zarówno wymogów biznesowych, jak i wynikających z obowiązujących przepisów. Organizacja powinna zastanowić się, czy istnieje konieczność wprowadzenia dodatkowych wymagań dotyczących komunikacji i cyberbezpieczeństwa związanych z systemami zabezpieczeń (np. segmentacji i izolacji systemów bezpieczeństwa od innych systemów OT). Co więcej, należy pamiętać o tym, że wymogi w zakresie bezpieczeństwa mogą wpływać na wybór mechanizmów zabezpieczeń. Względy bezpieczeństwa mogą wymagać od organizacji stosowania separacji fizycznej zamiast separacji logicznej.

Projekty systemów OT zwykle opierają się na zasadzie powrotu do znanego stanu w przypadku wystąpienia awarii, nieoczekiwanej sytuacji lub usterki komponentu. Takie rozwiązanie zakłada powrót urządzenia lub procesu do bezpiecznego stanu, aby

zapobiec urazom lub zniszczeniu mienia, pozwalając uniknąć zdarzeń kaskadowych lub zagrożeń wtórnych. Zdarzenia związane z cyberbezpieczeństwem, takie jak przerwanie komunikacji sieciowej, mogą spowodować wystąpienie awarii. Aby zminimalizować liczbę wyników fałszywie dodatnich, organizacje powinny określić wartości graniczne dla wybranych warunków i sytuacji, takich jak zanik komunikacji sieciowej, przed przekroczeniem których komponenty systemów OT będą działać z ograniczonymi możliwościami.

5.3.2. ZAGADNIENIA ZWIĄZANE Z DOSTĘPNOŚCIĄ

Zarządzanie ciągłością procesów wymaga uwzględniania dostępności wielu elementów i systemów, w tym danych, aplikacji, infrastruktury IT, zasilania oraz mediów (ogrzewania, wentylacji, klimatyzacji, wody, pary wodnej, sprężonego powietrza itd.) Awaria tych systemów może mieć kaskadowy wpływ na systemy OT i może negatywnie wpłynąć na działanie środowiska OT. W dalszej części zostały opisane zagadnienia związane z dostępnością, które należy uwzględnić w czasie prac.

5.3.2.1. DANE, APLIKACJE I INFRASTRUKTURA

Wymagania i projekty architektury powinny uwzględniać nadmiarowość wymaganą w przypadku systemów OT. Dostępność można zapewnić dzięki zapewnieniu nadmiarowości linii komunikacji, systemów lub komponentów, dzięki czemu pojedyncza awaria będzie wiązała się z mniejszym prawdopodobieństwem ograniczenia możliwości działania lub dostępu do informacji i danych. Architektura cyberbezpieczeństwa powinna uwzględniać nadmiarowe linie komunikacyjne, które powinny być objęte ochroną na tym samym poziomie, co linie podstawowe.

Ponadto należy uwzględnić także proces tworzenia kopii zapasowych i przywracania danych, umożliwiający szybkie przywracanie systemów do działania w przypadkach utraty danych z powodu cyberataków lub w wyniku działania innych czynników. Przykładami ważnych danych i plików są dane operacyjne, pliki programów, pliki konfiguracyjne, obrazy systemu, reguły zapory sieciowej i listy sterowania dostępem (*ang. access control lists – ACL*). Podejście oparte na strategii „kopii zapasowych w głąb" opiera się na sporządzaniu kopii zapasowych w wielu warstwach (np. kopia

lokalna, kopia całej organizacji, kopia awaryjna) i uporządkowanie ich w czasie w taki sposób, by najnowsze lokalne kopie zapasowe były dostępne do natychmiastowego użycia, a bezpieczne kopie zapasowe pozwalały na odtworzenie środowiska w przypadku poważnego incydentu związanego z cyberbezpieczeństwem, na przykład ataku z użyciem oprogramowania ransomware. Zastosowanie takiego podejścia pozwala na zwiększenie dostępności systemu OT. Okresowe testowanie możliwości tworzenia kopii zapasowych i przywracania danych pozwoli upewnić się, że są dostępne i możliwe do wykorzystania w razie potrzeby.

5.3.2.2. PODSTAWOWE I ALTERNATYWNE ŹRÓDŁA ZASILANIA

Podczas opracowywania architektury bezpieczeństwa należy uwzględnić także wpływ przerw w zasilaniu na systemy OT. Jeśli systemy OT wymagają stopniowego lub uporządkowanego wyłączenia, należy uwzględnić wdrożenie systemu zasilania awaryjnego. Ponadto, jeśli plan ciągłości działania organizacji wymaga, aby systemy OT nadal działały w przypadku przedłużającej się utraty podstawowego źródła zasilania, należy wykorzystać alternatywne źródło zasilania dla systemów OT, które będzie niezależne od zewnętrznych źródeł energii. Systemy monitorowania i sterowania związane z systemami zasilania są podatne na cyberataki, dlatego należy wdrożyć w ich przypadku stosowne praktyki w zakresie cyberbezpieczeństwa.

5.3.2.3. INNE MEDIA

Zakłady przemysłowe zazwyczaj wykorzystują systemy monitorowania i sterowania, które zarządzają zasilaczami awaryjnymi (UPS), generatorami, systemami ogrzewania, wentylacji oraz klimatyzacji, systemami przeciwpożarowymi, kotłami, instalacją wody chłodzącej, parą, sprężonym powietrzem i innymi krytycznymi mediami. Tego rodzaju systemy monitorowania i sterowania są także podatne na cyberataki i mogą wpływać na systemy OT, dlatego należy wdrożyć odpowiednie praktyki cyberbezpieczeństwa w celu ich ochrony.

Zalecenia i wytyczne dotyczące systemów OT

Planowanie odtworzenia po katastrofie jest kolejnym ważnym działaniem z punktu widzenia systemów OT, zwłaszcza gdy mogą mieć wpływ na bezpieczeństwo.

Organizacje powinny opracować oraz aktualizować plan odtworzenia po katastrofie, szczegółowo opisujący działania podejmowane przed, w trakcie i po katastrofie naturalnej, środowiskowej lub spowodowanej przez człowieka – zarówno celowo, jak i w wyniku wypadku. Plan ten powinien także obejmować instrukcje dotyczące przywracania i ponownego uruchamiania uszkodzonych komponentów oraz ich ponownego włączenia do systemu. Organizacje powinny uwzględnić możliwość przetestowania tego planu, aby upewnić się, że kluczowe elementy architektury mogą zostać przywrócone do działania w przypadku wystąpienia rzeczywistego zdarzenia. Można także przeprowadzić ćwiczenia i symulacje w celu sprawdzenia planu odtworzenia po katastrofie.

5.3.3. SYSTEMY ROZPROSZONE GEOGRAFICZNIE

Wiele organizacji działających w sektorach odpowiedzialnych za obsługę infrastruktury krytycznej wykorzystuje lokalizacje rozproszone geograficznie. Organizacje powinny rozważyć, czy rozbieżności w poziomach zabezpieczeń fizycznych w zdalnych lokalizacjach stwarzają ryzyko dla zdolności operacyjnych lub bezpieczeństwa OT. W zdalnych lokalizacjach należy zapewnić niezbędną infrastrukturę cyberbezpieczeństwa i komunikacji, aby chronić je przed zagrożeniami i umożliwić przekazywanie danych dotyczących monitorowania cyberbezpieczeństwa.

Zalecenia i wytyczne dotyczące systemów OT

Komunikacja między poszczególnymi lokalizacjami powinna być szyfrowana i uwierzytelniana, niezależnie od tego, czy połączenie odbywa się za pośrednictwem łącza punkt-punkt, łącz satelitarnych czy Internetu. Organizacje powinny również zapewnić odpowiednią przepustowość pozwalającą na gromadzenie danych z procesów monitorowania cyberbezpieczeństwa, a także danych operacyjnych ze zdalnych lokalizacji.

Jeśli organizacja dysponuje wieloma rozproszonymi lokalizacjami, powinna podjąć decyzję, czy za bezpieczeństwo będzie odpowiadało scentralizowane operacyjne centrum bezpieczeństwa (*ang. security operations center – SOC*), czy raczej regionalne rozproszone centra bezpieczeństwa. Wpływ na te decyzje może wywierać dostępność wykwalifikowanych pracowników i ekspertów.

5.3.4. WYMOGI REGULACYJNE I PRAWNE

W sektorach podlegających regulacjom konieczne jest uwzględnienie wymogów prawnych związanych z cyberbezpieczeństwem w procesie projektowania architektury cyberbezpieczeństwa. Przykładowo, norma NERC CIP-005 (omówiona w punkcie 1.9 Załącznika D) obejmuje wymagania dotyczące architektury cyberbezpieczeństwa dla masowych systemów elektrycznych. Podobne wymogi i wytyczne obowiązują w przypadku wielu innych branż i sektorów podlegających regulacjom.

5.3.5. ZAGADNIENIA DOTYCZĄCE ŚRODOWISKA

Organizacje powinny przeprowadzić analizę zagrożeń w celu ustalenia, czy którykolwiek z ich procesów lub urządzeń stanowi zagrożenie dla środowiska. Jeśli zostanie zidentyfikowane potencjalne zagrożenie środowiskowe, które może wystąpić w przypadku incydentu związanego z cyberbezpieczeństwem, należy uwzględnić stosowne środki zapobiegawcze w architekturze.

5.3.6. ZAGADNIENIA DOTYCZĄCE BEZPIECZEŃSTWA ZDALNYCH MODUŁÓW WE/WY (POZIOM 0 MODELU PURDUE)

Wiele urządzeń i protokołów komunikacyjnych wykorzystywanych w zdalnych modułach we/wy (poziom 0 modelu Purdue), w tym czujniki oraz siłowniki, nie uwzględnia możliwości ustalania ich tożsamości oraz uwierzytelnienia. Brak uwierzytelnienia umożliwia odtwarzanie, modyfikowanie lub fałszowanie danych. Organizacje muszą w związku z tym podjąć decyzję opartą na ryzyku dotyczącą umieszczenia w systemie OT (na przykład w najbardziej krytycznym procesie) zabezpieczenia, na przykład bliźniaków cyfrowych (*ang. digital twins*) bądź oddzielnej sieci monitorowania modułów we/wy, w celu wykrycia nieprawidłowych danych.

5.3.7. DODATKOWE ZAGADNIENIA DOTYCZĄCE BEZPIECZEŃSTWA ROZWIĄZAŃ IIOT

Wprowadzenie rozwiązań IIoT do środowisk OT przyczynia się do poprawy łączności i wymiany informacji z systemami organizacji oraz rozwiązaniami opartymi na chmurze, co może wymagać uwzględnienia dodatkowych wymogów na etapie tworzenia architektury bezpieczeństwa. Wprowadzenie urządzeń IIoT do środowisk

OT może wymagać zmiany granic stref lub udostępnienia większej liczby interfejsów i usług. Co więcej, w procesie opracowywania architektury bezpieczeństwa konieczne może być uwzględnienie możliwości zabezpieczania urządzeń IIoT.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje muszą przeanalizować skutki wdrożenia rozwiązań i urządzeń IIoT na zarządzanie zasadami, a także ich egzekwowanie. Włączenie rozwiązań IIoT do środowisk OT może wymagać ściślejszej współpracy między zespołami odpowiedzialnymi za bezpieczeństwo systemów IT i OT w celu zarządzania bezpieczeństwem. Przykładem tej współpracy może być odpowiedzialność za świadomość sytuacyjną i obserwowanie sytuacji w czasie rzeczywistym.

5.3.7.1. OBSZARY ZASTOSOWAŃ I INFRASTRUKTURA

Organizacje powinny przeanalizować dane przesyłane przez systemy i rozwiązania IIoT, w szczególności dane wysyłane poza sieć organizacji, aby stwierdzić, czy konieczne są dodatkowe mechanizmy sterowania dostępem. Organizacje powinny również wziąć pod uwagę, że wektory ataków dotyczących urządzeń IIoT mogą być inne niż w przypadku środowisk OT (ze względu na inne możliwości komunikacji lub wykorzystanie dodatkowych usług, takich jak systemy chmurowe, w celu realizacji funkcji).

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny wziąć pod uwagę następujące zdolności do ochrony urządzeń IIoT wdrażanych w swoich środowiskach:

- Ochrona przed zmianami i sabotażem.
- Źródło zaufania urządzenia.
- Tożsamość urządzenia.
- Kontrola dostępu do urządzenia.
- Ochrona integralności urządzenia.
- Ochrona danych urządzenia.
- Monitorowanie i analiza urządzeń.

- Konfiguracja urządzeń i zarządzanie urządzeniami.
- Zastosowanie technik kryptograficznych;
- Możliwość utwardzania urządzeń.

5.3.7.2. ZAGADNIENIA DOTYCZĄCE MOŻLIWOŚCI W ZAKRESIE CYBERBEZPIECZEŃSTWA

Zasoby urządzeń IIoT – procesory, pamięć operacyjna oraz dostępna pamięć masowa – są mocno zróżnicowane i zależne od urządzenia. Niektóre urządzenia IIoT mogą dysponować ograniczonymi zasobami, z kolei inne mogą nie wykorzystywać pełni swoich możliwości sprzętowych, co może mieć daleko idące skutki dla cyberbezpieczeństwa. Organizacje powinny uwzględnić zasoby i możliwości urządzeń IIoT w architekturze bezpieczeństwa, aby zapewnić możliwość realizacji celów dotyczących cyberbezpieczeństwa. Ponadto organizacje powinny przeanalizować wpływ rozwiązań IIoT na działalność i bezpieczeństwo organizacji i ustalić, czy odbiega on od wpływu systemów OT na te aspekty. Urządzenia IIoT mogą pozwalać na przykład na monitorowanie danych dotyczących środowiska w trybie tylko do odczytu, co wiąże się z minimalnym wpływem na zabezpieczenia operacyjne oraz bezpieczeństwo. To pozwoli organizacji na zabezpieczenie tych urządzeń w inny sposób niż przy pomocy zabezpieczeń ustalonych dla systemów OT.

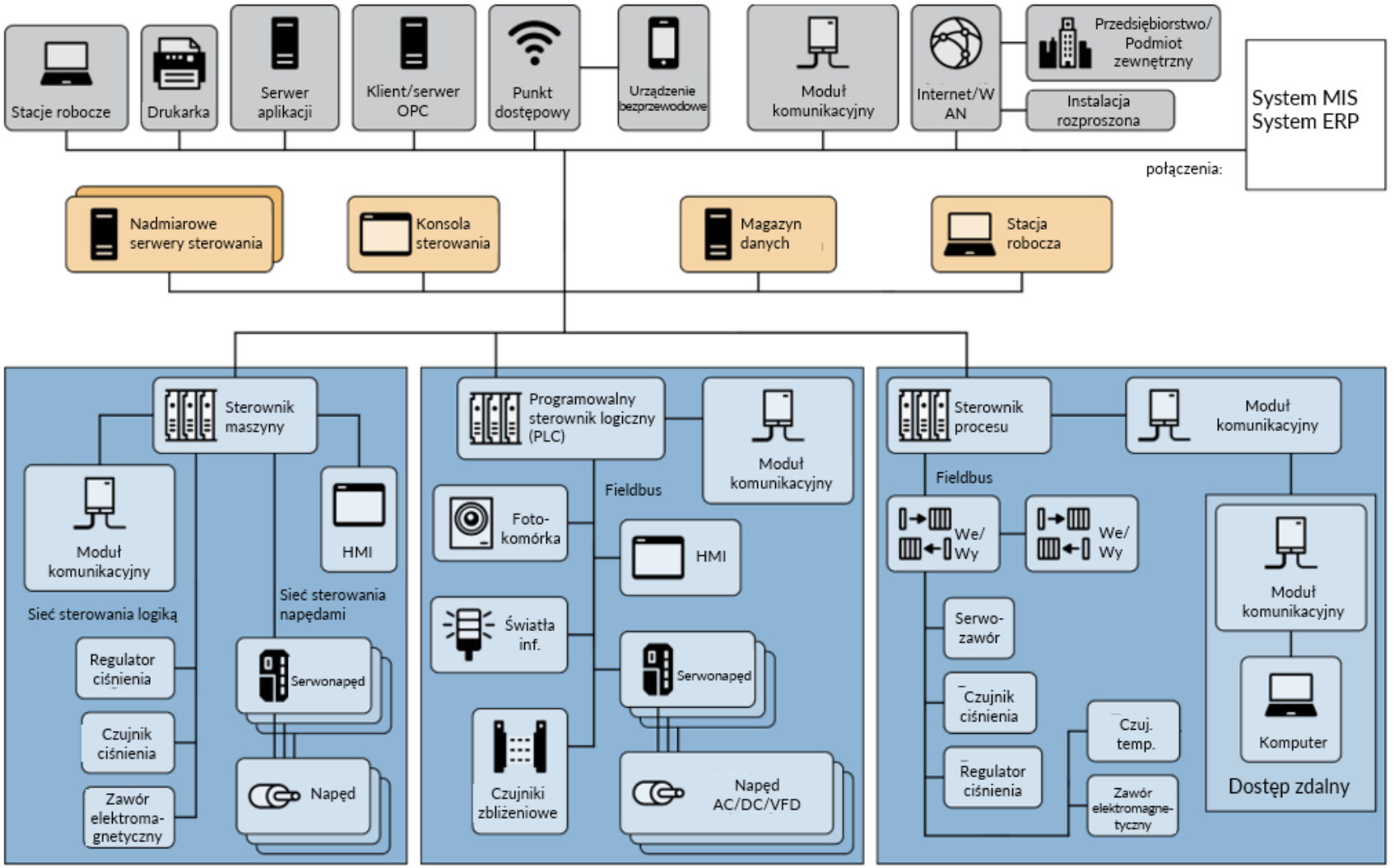
5.4. MODELE ARCHITEKTURY CYBERBEZPIECZEŃSTWA

Na postawie koncepcji oraz wytycznych z rozdziałów 5.1, 5.2 i 5.3 autorzy niniejszej publikacji opracowali przykłady zawarte w następujących podrozdziałach, które ilustrują środowiska OT i IIoT opisane w rozdziale 2 i wskazują, w jaki sposób można dostosować je do potrzeb architektury bezpieczeństwa opartej na zasadzie obrony w głąb.

5.4.1. SYSTEMY OT OPARTE NA ROZPROSZONYCH SYSTEMACH STEROWANIA (DCS)

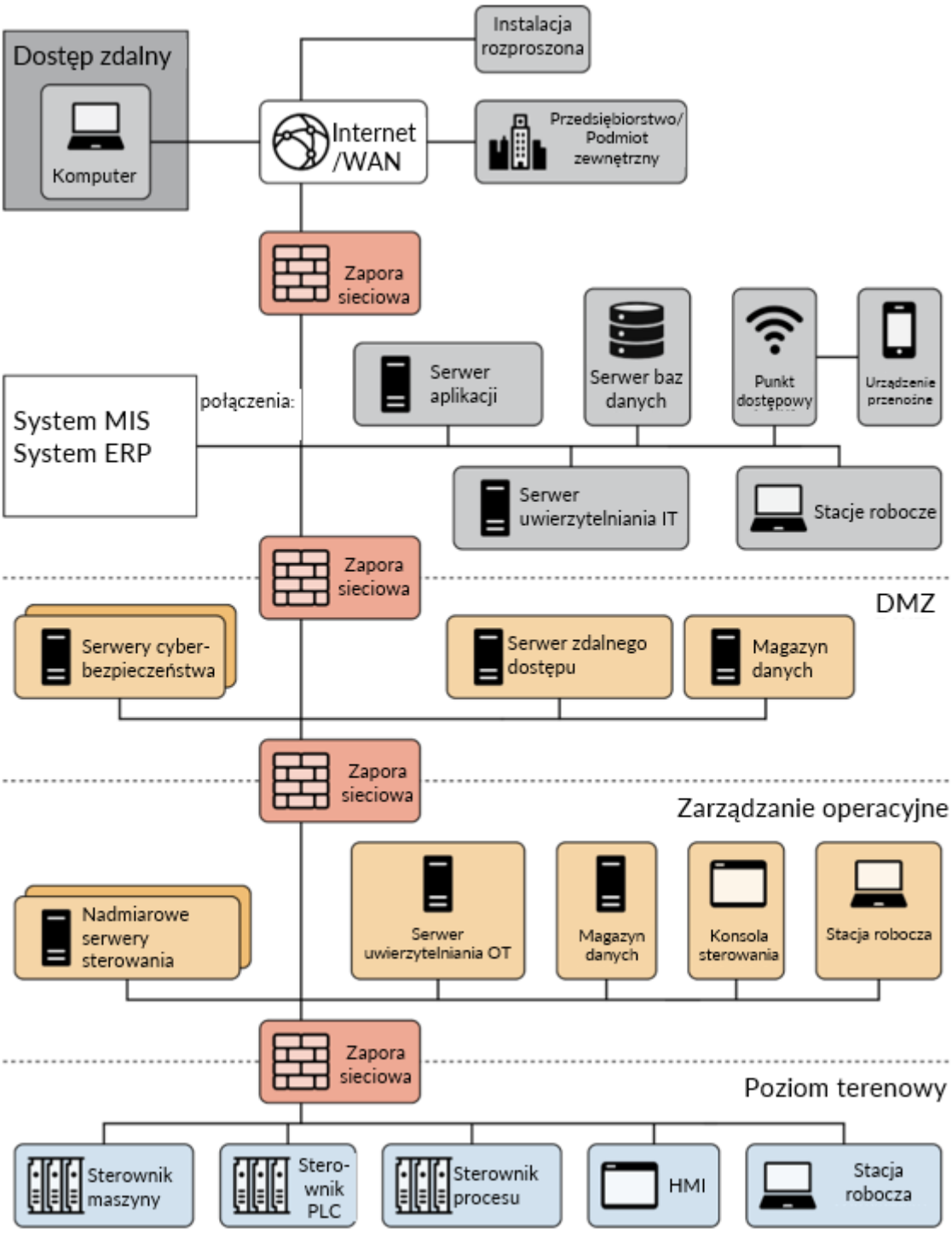
Jak wiemy już z rozdziału 2, rozproszony system sterowania (*ang. distributed control system – DCS*) służy do sterowania przemysłowymi systemami produkcyjnymi znajdującymi się w pojedynczej lokalizacji geograficznej. **Rysunek 17** przedstawia

przykładowe wdrożenie rozproszonego systemu sterowania. **Rysunek 18** przedstawia przykładową architekturę bezpieczeństwa opartą na zasadzie obrony w głąb zastosowaną w rozproszonym systemie sterowania.



Rysunek 17. Przykład wdrożenia rozproszonego systemu sterowania

Tłumaczenie



Rysunek 18. Przykład architektury bezpieczeństwa opartej na zasadzie obrony w głąb zastosowanej w rozproszonym systemie sterowania

Schemat przedstawiony na **Rysunku 18** zakłada, że stosowane rozwiązania dla warstw 1 i 2 zostały już wdrożone w organizacji.

Tłumaczenie

Na poziomie warstwy 3 organizacja powinna uwzględnić włączenie następujących rozwiązań do architektury bezpieczeństwa:

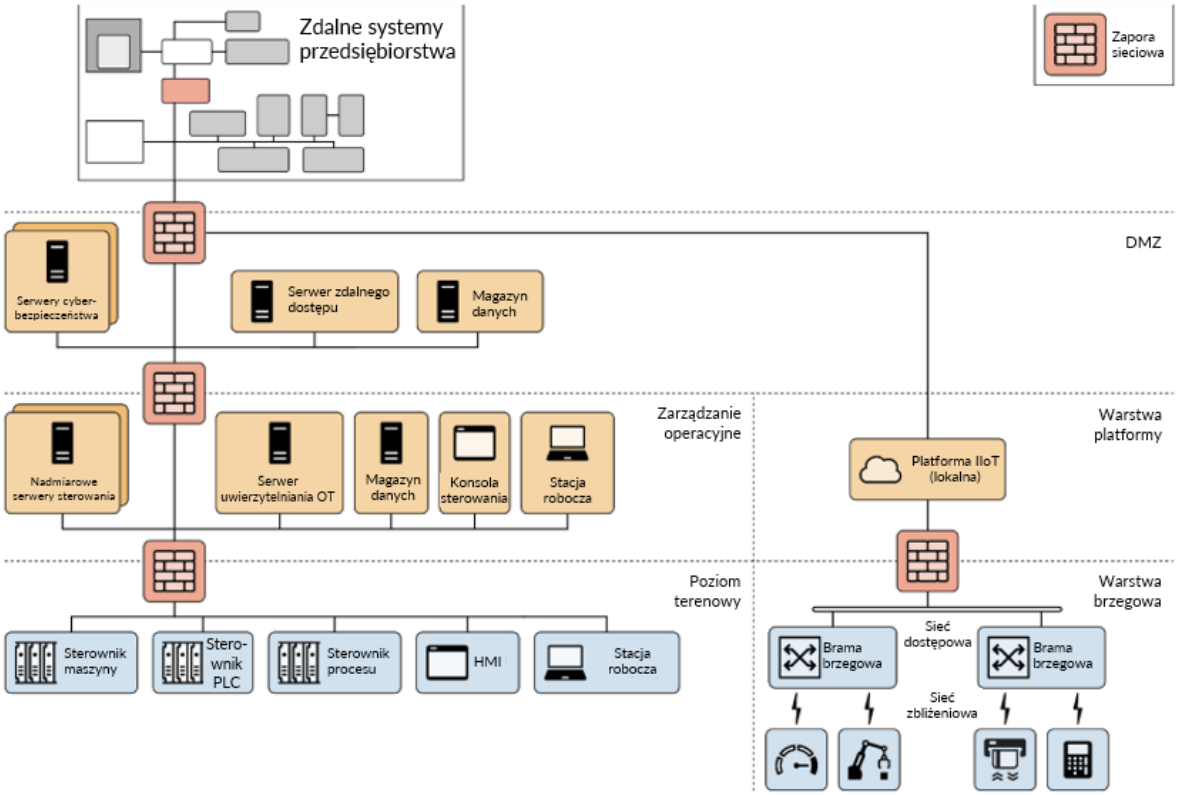
- Podział sieci na różne poziomy lub strefy. W przedstawionym przykładzie urządzenia są podzielone na różne poziomy w zależności od funkcji. Poziom terenowy obejmuje urządzenia uwzględnione zwykle na poziomach 0, 1 i 2 modelu Purdue. Poziom zarządzania obejmuje urządzenia służące do monitorowania urządzeń poziomu terenowego, urządzenia do zarządzania oraz komponenty z poziomu 3 modelu Purdue. Strefa zdemilitaryzowana (DMZ) obejmuje urządzenia, które łączą warstwy zarządzania i organizacji. Organizacje powinny również zastanowić się, czy konieczne jest utworzenie dodatkowych segmentów sieci dla systemów bezpieczeństwa, takich jak: systemy monitoringu obecności, systemy kontroli dostępu, drzwi, bramy, kamery, systemy komunikacji głosowej VoIP, a także czytniki kart dostępu. Segmentacja sieci jest jednym z kluczowych elementów stosowania strategii obrony w głąb.
- Urządzenia brzegowe (na przykład zapory sieciowe) służą do zabezpieczania oraz monitorowania komunikacji między różnymi poziomami. W niektórych przypadkach wykorzystuje się zapory sieciowe klasy przemysłowej między poziomami urządzeń terenowych i zarządzania, aby zapewnić dodatkową ochronę protokołów wykorzystywanych w systemach OT lub umożliwić urządzeniom działanie w trudnych warunkach. Reguły dla komunikacji przychodzącej i wychodzącej powinny być zdefiniowane w taki sposób, aby pomiędzy poziomami przepływały jedynie dozwolone komunikaty.
- Wdrożenie strefy zdemilitaryzowanej (DMZ) w celu oddzielenia środowiska OT od sieci organizacji. Wszelka komunikacja między poziomem organizacji a poziomem zarządzania powinna przechodzić przez usługi umieszczone w strefie zdemilitaryzowanej. Ze względu na fakt, że strefa zdemilitaryzowana jest połączona ze środowiskami zewnętrznymi, usługi działające w tej strefie muszą być monitorowane i chronione. Takie działanie pozwoli na zapobieganie naruszeniom zasad ochrony i przedostaniu się napastników do środowiska OT bez wykrycia.

- Schemat architektury bezpieczeństwa przedstawia serwer uwierzytelniania IT w sieci korporacyjnej, który jest wykorzystywany w celu uwierzytelniania użytkowników, a także oddzielny serwer uwierzytelniania OT w sieci zarządzania, wykorzystywany przez użytkowników systemów OT. Organizacje mogą wykorzystać takie podejście, jeśli pozwoli ono na realizację celów dotyczących bezpieczeństwa opartych na ustalonym ryzyku.

W przypadku warstw 4 oraz 5 organizacje powinny rozważyć zastosowanie zasady minimalnej funkcjonalności do wszystkich urządzeń polowych, zarządzających oraz zlokalizowanych w strefie zdemilitaryzowanej w celu zabezpieczenia i utwardzenia aplikacji i urządzeń. Organizacje powinny określić i wyłączyć wszelkie nieistotne funkcje oraz programy działające na urządzeniach, a także wyłączyć lub zamknąć nieużywane porty. Przykładem mogą być nowoczesne sterowniki PLC oraz interfejsy człowiek-maszyna, które mogą oferować funkcje serwerów WWW lub SSH. Jeśli usługi te nie są używane, należy je wyłączyć, a także zamknąć powiązane z nimi porty TCP/UDP. Funkcje powinny być włączane tylko wtedy, gdy jest to wymagane.

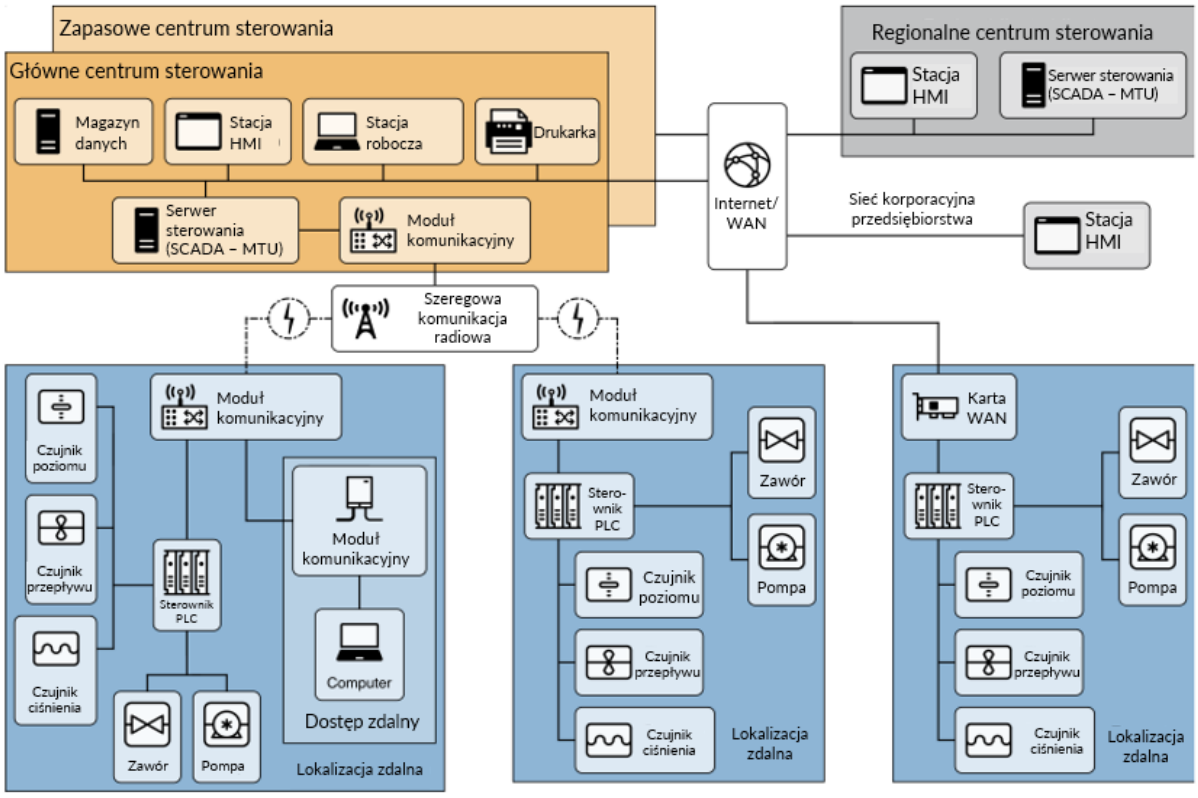
5.4.2. SYSTEMY OT OPARTE NA ROZPROSZONYCH SYSTEMACH STEROWANIA I STEROWNIKACH PLC Z ROZWIĄZANIAMI IIOT

W oparciu o wytyczne dla środowisk OT opartych na rozproszonych systemach sterowania oraz sterownikach PLC opisanych w rozdziale 5.4.1, **Rysunek 19** przedstawia uproszczoną przykładową architekturę bezpieczeństwa dla rozproszonego systemu sterowania z dodatkowymi urządzeniami IIoT skonfigurowanymi w celu korzystania z lokalnej platformy IIoT zapewniającej możliwości przetwarzania. Ze względu na zróżnicowanie komponentów komunikacyjnych oraz architektury, które pozwalają na obsługę urządzeń IIoT, w przykładzie zostały przedstawione oddzielne segmenty sieci obsługujące dodatkowe komponenty IIoT. Komunikacja z warstwy platformy IIoT jest przekierowana przez zaporę graniczną strefy zdemilitaryzowanej, aby umożliwić przesył danych do serwerów w strefie zdemilitaryzowanej lub do sieci organizacji bądź Internetu, zgodnie z wymaganiami operacyjnymi dla rozwiązań IIoT. Takie rozwiązanie pozwala ponadto usługom cyberbezpieczeństwa uruchamianym w DMZ na monitorowanie warstwy platformy IIoT.



Rysunek 19. Przykład architektury bezpieczeństwa dla rozproszonego systemu sterowania z urządzeniami IIoT

Rysunek 20 przedstawia elementy oraz podstawową konfigurację przykładowego systemu kontroli nadzorczej i pozyskiwania danych (SCADA). W typowych przypadkach podstawowe i zapasowe centra sterowania obsługują jedną lub więcej zdalnych lokalizacji, z kolei regionalne centra sterowania są zlokalizowane w taki sposób, by obsługiwać jedno lub więcej podstawowych lub zapasowych centrów sterowania. Ze względu na rozproszony charakter zdalnych lokalizacji i centrów sterowania, komunikacja między lokalizacjami zwykle odbywa się za pośrednictwem połączeń zewnętrznych lub sieci WAN realizowanych za pośrednictwem technologii przewodowych oraz bezprzewodowych.

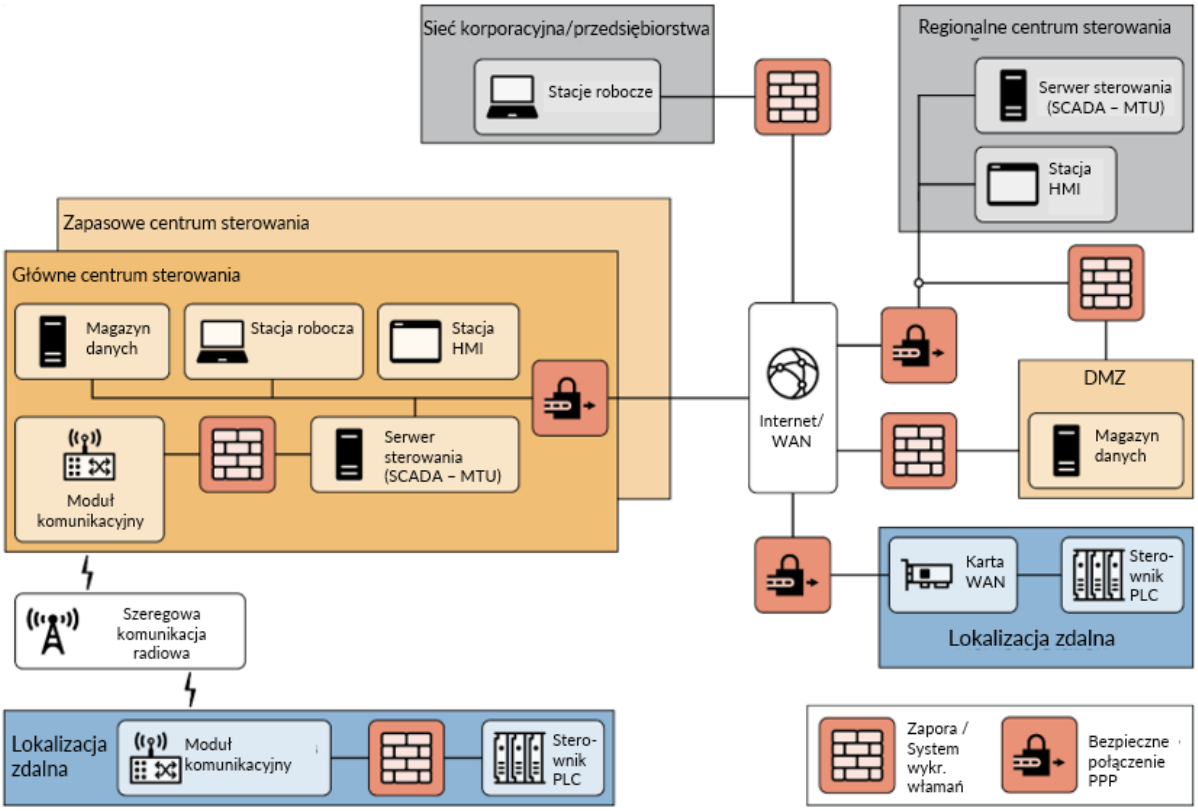


Rysunek 20. Przykładowy system SCADA w środowisku OT

Rysunek 21 przedstawia przykładowe wdrożenie architektury opartej na zasadzie obrony w głąb dla systemu SCADA. Schemat zakłada, że stosowane rozwiązania dla warstw 1 i 2 zostały już wdrożone w organizacji. Na poziomie warstwy 3 organizacja powinna uwzględnić włączenie następujących rozwiązań do architektury bezpieczeństwa:

- Rozdzielenie sieci na różne strefy lub regiony, ważne w przypadku stosowania strategii obrony w głąb w środowisku SCADA. Należy uwzględnić rozdzielenie systemów bezpieczeństwa, takich jak systemy monitoringu obecności, systemy kontroli dostępu, drzwi, bramy, kamery, systemy komunikacji głosowej VoIP, a także czytniki kart dostępu.
- Urządzenia brzegowe (na przykład zapory sieciowe) powinny zostać zastosowane pomiędzy regionami w celu zabezpieczania oraz monitorowania komunikacji między różnymi segmentami sieci. Zapory sieciowe klasy przemysłowej mogą zapewniać lepszą obsługę protokołów wykorzystywanych w systemach OT oraz usprawnić ochronę urządzeń OT, takich jak sterowniki PLC oraz inne sterowniki. Reguły dla komunikacji przychodzącej i wychodzącej powinny być zdefiniowane w taki sposób, aby pomiędzy regionami przepływały jedynie dozwolone komunikaty.

- Należy korzystać z bezpiecznych połączeń (tunelowania VPN, szyfrowanych kanałów, połączeń punkt-punkt) między segmentami sieci, np. między centrum regionalnym a głównymi centrami sterowania oraz między lokalizacjami zdalnymi a centrami sterowania. W przypadku odległych geograficznie lokalizacji, bezpieczne połączenia mogą być realizowane za pośrednictwem sieci Internet/WAN. Urządzenia znajdujące się w poszczególnych segmentach sieci powinny nawiązywać łączność z innymi segmentami tylko za pośrednictwem bezpiecznych połączeń. Powinny mieć także ograniczony dostęp do Internetu.
- Wdrożenie strefy zdemilitaryzowanej (DMZ) w celu oddzielenia centrów sterowania od sieci organizacji. Wszelka komunikacja między siecią organizacji i centrami sterowania powinna przechodzić przez usługi umieszczone w strefie zdemilitaryzowanej. Ze względu na fakt, że strefa zdemilitaryzowana jest połączona ze środowiskami zewnętrznymi, usługi działające w tej strefie muszą być monitorowane i chronione. Takie działanie pozwoli na zapobieganie naruszeniom zasad ochrony w strefie DMZ i przedostaniu się napastników do środowiska OT bez wykrycia.



Rysunek 21. Przykład architektury bezpieczeństwa dla systemu SCADA

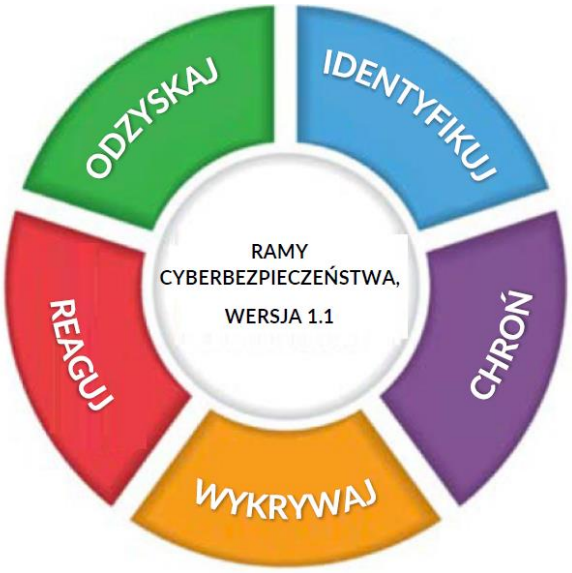
W przypadku warstw 4 oraz 5 organizacje powinny rozważyć zastosowanie zasady minimalnej funkcjonalności do wszystkich komponentów w lokalizacjach zdalnych, komponentów w centrach sterowania oraz urządzeń w strefie zdemilitaryzowanej w celu zabezpieczenia i utwardzenia aplikacji i urządzeń. Organizacje powinny określić i wyłączyć wszelkie nieistotne funkcje oraz programy działające na urządzeniach, a także wyłączyć lub zamknąć nieużywane porty. Przykładem mogą być nowoczesne sterowniki PLC oraz interfejsy człowiek-maszyna, które mogą oferować funkcje serwerów WWW lub SSH. Jeśli usługi te nie są używane, należy je wyłączyć, a także zamknąć powiązane z nimi porty TCP/UDP. Funkcje powinny być włączane tylko wtedy, gdy jest to wymagane.

6. STOSOWANIE RAM CYBERBEZPIECZEŃSTWA W KONTEKŚCIE SYSTEMÓW OT

Wiele organizacji działających w sektorach publicznym i prywatnym wdraża ramy cyberbezpieczeństwa opisane w NIST Cybersecurity Framework (CSF)[CSF], aby zarządzać cyberbezpieczeństwem oraz analizować ryzyko związane z tym obszarem. W skład ram cyberbezpieczeństwa wchodzi pięć funkcji realizowanych w sposób równoległy oraz ciągły – Identyfikacja, Ochrona, Detekcja, Reagowanie oraz Przywracanie. Funkcje te obejmują normy/standardy branżowe, wytyczne oraz praktyki wdrażane w sposób umożliwiający informowanie o działaniach w zakresie cyberbezpieczeństwa oraz ich rezultatach realizowanych w całej organizacji. Celem tych funkcji jest określenie strategii zarządzania ryzykiem związanym z cyberbezpieczeństwem. Ramy określają kluczowe kategorie i podkategorie dla każdej funkcji i dopasowują je do dokumentów referencyjnych, takich jak istniejące normy/standardy i wytyczne, a także praktyki dotyczące każdej podkategorii.

Przedstawione powyżej funkcje obejmują łącznie 23 kategorie rezultatów oraz szereg podkategorii, które umożliwiają podział kategorii na działania techniczne lub zarządcze. W tym rozdziale każdy podrozdział odnosi się do funkcji i kategorii ram cyberbezpieczeństwa oraz wykorzystuje dwuliterowe skróty funkcji ram cyberbezpieczeństwa pozwalające na ich łatwe wyszukanie.

Funkcje ram cyberbezpieczeństwa odpowiadają za realizację następujących działań:



Identyfikacja (*ang. Identify – ID*) – rozwija organizacyjne zrozumienie pozwalające zarządzać zagrożeniami związanymi z cyberbezpieczeństwem systemów, aktywów, danych i możliwości.

Ochrona (*ang. Protect – PR*) – pozwala opracować i wdrożyć odpowiednie środki ochrony zapewniające zrealizowanie najważniejszych usług infrastrukturalnych.

Tłumaczenie

Detekcja (ang. Detect – DE) – opracowanie i wdrożenie odpowiednich czynności w celu zidentyfikowania wystąpienia zdarzenia związanego z cyberbezpieczeństwem.

Reagowanie (*ang. Respond – RS*) – opracowanie i wdrożenie odpowiednich czynności w celu podjęcia działania związanego z cyberbezpieczeństwem.

Przywracanie (*ang. Recover – RC*) – opracowanie i wdrożenie odpowiednich czynności w celu utrzymania planów odporności i przywrócenia możliwości lub usług, na które wpływ miał incydent cyberbezpieczeństwa.

6.1. IDENTYFIKACJA (ANG. IDENTIFY – ID)

Funkcja Identyfikacji określa podstawowe działania umożliwiające skuteczne korzystanie z ram cyberbezpieczeństwa oraz ich wdrożenie. Celem tej funkcji jest rozwój organizacyjnego zrozumienia pozwalającego na zarządzanie zagrożeniami związanymi z cyberbezpieczeństwem systemów, aktywów, danych i możliwości.

6.1.1. ZARZĄDZANIE AKTYWAMI (ANG. ASSET MANAGEMENT – ID.AM)

Zdolność organizacji do prawidłowego i spójnego identyfikowania i zarządzania danymi, pracownikami, urządzeniami, systemami i obiektami w oparciu o ich względne znaczenie zapewnia podstawową zdolność do realizacji organizacyjnego programu cyberbezpieczeństwa. Aktualizacja informacji inwentaryzacyjnych w czasie dodawania, usuwania lub zmian komponentów (np. instalacji poprawek, nowego oprogramowania układowego, wymiany komponentów podczas konserwacji) umożliwia organizacjom zarządzanie ryzykiem związanym ze środowiskiem. Organizacje powinny wziąć pod uwagę uwzględnienie następujących elementów w celu poszerzenia możliwości zarządzania zasobami:

- Wyjątkowych identyfikatorów umożliwiających rozróżnienie i śledzenia zasobów.
- Inwentaryzacji sprzętu w celu śledzenia urządzeń komputerowych i sieciowych w środowisku, w tym informacji na temat urządzeń oraz ich lokalizacji. Szczegółowe informacje mogą obejmować nazwę producenta, model, numer seryjny, informacje dotyczące zakupu oraz informacje dotyczące produkcji lub kompilacji (tj. informacje o pochodzeniu).

- Oprogramowania i oprogramowania układowego w celu śledzenia oprogramowania i oprogramowania układowego zainstalowanego na komponentach systemów OT, w tym numerów wersji, informacji o lokalizacji i specyfikacji materiałowych komponentów oprogramowania.
- Informacji o dostawcach w celu utworzenia repozytorium informacji o dostawcach, punktach kontaktowych, informacjach gwarancyjnych, wycofanych produktach oraz aktualizacjach.
- Dokumentującymi role oraz obowiązki w celu wskazania konkretnych osób, zespołów lub grup organizacyjnych odpowiedzialnych za dane zasoby oraz osób odpowiedzialnych za ich eksploatację, utrzymanie i cyberbezpieczeństwo.

Dodatkowe wytyczne dotyczące praktyk związanych z obszarem ID.AM można znaleźć w następujących dokumentach:

- NIST SP 1800-5, *IT Asset Management*
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny uwzględnić znaczenie kompletnej i dokładnej inwentaryzacji zasobów na potrzeby zarządzania ryzykiem w środowisku OT. Dokładne dane zgromadzone w ramach inwentaryzacji umożliwiają realizację wielu celów programu zarządzania ryzykiem, w tym szacowanie ryzyka, zarządzanie podatnościami oraz identyfikację przestarzałych komponentów.

Choć preferowane jest wykorzystywanie zautomatyzowanych narzędzi wspierających proces zarządzania zasobami, organizacje powinny wziąć pod uwagę sposoby gromadzenia informacji przez tego rodzaju rozwiązania i zweryfikować, czy niektóre metody (np. aktywne skanowanie) nie mają negatywnego wpływu na systemy OT. Przed wdrożeniem takich rozwiązań do środowiska produkcyjnego OT zaleca się przeprowadzenie stosownych testów zautomatyzowanych narzędzi do zarządzania zasobami na osobnych komponentach lub systemach. Jeśli wykorzystanie zautomatyzowanych narzędzi nie jest możliwe ze względu na architekturę sieci lub inne aspekty środowiska OT, organizacja powinna wdrożyć ręczne procesy pozwalające na bieżące inwentaryzowanie zasobów.

6.1.1.1. MAPOWANIE PRZEPŁYWÓW DANYCH I KOMUNIKACJI (ID.AM-3)

Schematy przepływów danych pomagają producentowi zrozumieć przepływ danych między komponentami sieciowymi. Dokumentowanie przepływów danych umożliwia organizacjom określenie oczekiwanego zachowania wykorzystywanych sieci. Rozumienie sposobu komunikacji urządzeń pomaga w rozwiązywaniu problemów, a także w reagowaniu i przywracaniu systemów w przypadku wystąpienia zdarzenia. Informacje te mogą być wykorzystywane podczas dochodzeń oraz analiz mających na celu identyfikację anomalii.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny uwzględnić wpływ wykorzystania zautomatyzowanych narzędzi do mapowania przepływów danych, które wykorzystują aktywne skanowanie lub wymagają narzędzi do monitorowania sieci (np. sond sieciowych) w systemach OT. Wpływ ten może wynikać z charakteru danych, natężenia ruchu sieciowego lub chwilowego odłączenia komponentów systemu produkcyjnego od sieci. Należy rozważyć wdrożenie narzędzi do mapowania przepływów danych, które wykorzystują takie metody, podczas planowanych przestojów konserwacyjnych.

6.1.1.2. DOKUMENTACJA ARCHITEKTURY SIECI (WSPIERAJĄCA REZULTATY REALIZACJI FUNKCJI ID.AM)

Narzędzia do dokumentowania architektury sieci pomagają producentowi identyfikować, dokumentować i tworzyć diagramy połączeń między urządzeniami sieciowymi, sieciami organizacji i połączeniami zewnętrznymi. Pełne zrozumienie wzajemnych powiązań w środowisku ma kluczowe znaczenie dla pomyślnego wdrożenia zabezpieczeń w zakresie cyberbezpieczeństwa. Informacje te są równie cenne z punktu widzenia skutecznego monitorowania sieci.

Zalecenia i wytyczne dotyczące systemów OT

Narzędzia do dokumentowania architektury sieci, które wykorzystują zautomatyzowane technologie wykrywania topologii, mogą gromadzić dane dotyczące wyłącznie urządzeń sieciowych wykorzystujących protokół IP. Wiele środowisk OT obejmuje odizolowane systemy i komponenty, a także systemy podłączone do sieci opartych na protokołach

innych niż IP. Środowisko OT może nie umożliwiać korzystania ze zautomatyzowanych narzędzi do dokumentowania architektury sieci, a do dokumentowania tych komponentów może być wymagane stosowanie procesów ręcznych.

Osoby odpowiedzialne za zasoby muszą również wziąć pod uwagę, w jaki sposób zautomatyzowane czynności skanowania mogą potencjalnie wpłynąć na system OT, testując narzędzia automatyzacji w środowisku testowym. W oparciu o wyniki przeprowadzonych testów należy rozważyć możliwość wykorzystywania zautomatyzowanych narzędzi do dokumentowania architektury sieci OT wyłącznie podczas planowanych przestojów.

Organizacje mogą również wziąć pod uwagę fizyczną weryfikację połączeń sieciowych systemów OT oraz analizy plików dziennika sieci w ramach procesu dokumentowania architektury sieci OT, zwłaszcza jeśli sieć nie jest duża lub złożona. Włączenie monitorowania aktywności w sieci OT może pomóc w skutecznej obserwacji przypadków dodawania lub usuwania urządzeń w ramach środowiska pomiędzy zaplanowanymi skanowaniami.

6.1.2. KIEROWANIE/ŁAD KORPORACYJNY (*ANG. GOVERNANCE – ID.GV*)

Skuteczne kierowanie (ład korporacyjny obejmuje włączenie przez kierownictwo organizacji celów zarządzania ryzykiem do procesu planowania strategii wraz z celami w zakresie odporności, prywatności i cyberbezpieczeństwa, a także zapewnienie zasobów wymaganych do skutecznego wdrożenia i utrzymania programu cyberbezpieczeństwa. Na podstawie tego procesu kierownictwo organizacji opracowuje i rozpowszechnia zasady, które ustanawiają wymagania w zakresie bezpieczeństwa środowisk. Zasady te mogą obejmować identyfikację i przypisanie ról, obowiązków, zaangażowanie kierownictwa oraz zasady dotyczące zgodności z przepisami. Zasady te mogą również odzwierciedlać koordynację między jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty bezpieczeństwa (np. bezpieczeństwo techniczne, fizyczne, pracowników, cyberfizyczne, kontrolę dostępu, ochronę nośników, zarządzanie podatnościami, konserwację, monitorowanie).

W rozdziałach 3 oraz 4 zostały zawarte dodatkowe informacje i wytyczne dotyczące ładu korporacyjnego. Dodatkowe wytyczne dotyczące praktyk związanych z obszarem ID.GV można znaleźć w następujących dokumentach:

- NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji*
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*
- NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)*
- NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny rozważyć:

- Zapewnienie, że realizacja programu cyberbezpieczeństwa wiąże się z przydziałem zasobów pozwalających na skuteczne wdrażanie strategii zarządzania ryzykiem IT i OT organizacji
- Zapewnienie, że zasady uwzględniają cały cykl życia systemów OT
- Zapewnienie, że wymogi prawne i regulacyjne dotyczące cyberbezpieczeństwa, które mają wpływ na operacje OT, są znane oraz uwzględnione w działaniach.
- Ustanowienie co najmniej jednego stanowiska wyższego szczebla, którego zakres odpowiedzialności obejmie zarządzanie ryzykiem związanym z programami cyberbezpieczeństwa IT i OT
- Ustanowienie dróg komunikacji i koordynacji między organizacjami IT i OT.
- Kompleksowe szkolenie pracowników odpowiedzialnych za systemy IT i OT w zakresie realizacji programu cyberbezpieczeństwa.

6.1.3. OCENA RYZYKA (ANG. RISK ASSESSMENT – ID.RA)

Ocena ryzyka związanego z cyberbezpieczeństwem jest przeprowadzana w celu określenia zagrożeń i oszacowania skali szkód dla działalności, zasobów oraz pracowników, które mogą wynikać z incydentów związanych z cyberbezpieczeństwem, takich jak nieautoryzowany dostęp, a także nieautoryzowane wykorzystanie, ujawnienie, zakłócenie działania, wprowadzenie zmian lub zniszczenie systemu informacyjnego bądź danych. Organizacje powinny wziąć pod uwagę częstotliwość aktualizacji ocen ryzyka i testowania zabezpieczeń systemów.

Dodatkowe wytyczne dotyczące praktyk związanych z obszarem ID.RA można znaleźć w następujących dokumentach:

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne*
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*
- NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji*

Zalecenia i wytyczne dotyczące systemów OT

W środowiskach OT pojęcia ryzyka i wpływu nierozerwalnie wiążą się z zagadnieniami bezpieczeństwa, zdrowia oraz środowiska, a także konsekwencjami biznesowymi i finansowymi. W związku z tym niektóre organizacje mogą uznać, że przeprowadzenie analizy kosztów i korzyści dla niektórych rodzajów ryzyka nie jest możliwe. W takich przypadkach organizacje powinny rozważyć przeprowadzenie analizy incydentów związanych z cyberbezpieczeństwem, które wystąpiły w przyszłości i doprowadziły do utraty zasilania, możliwości sterowania, przerwania dostaw surowców, zatrzymania produkcji lub awarii sprzętu. Wstępna ocena ryzyka (*ang. Process Hazard Analysis - PHA*) oraz analiza rodzajów i skutków możliwych błędów (*ang. Failure Mode & Effects Analysis - FMEA*) lub analiza zdarzeń historycznych mogą posłużyć do określenia potencjalnego wpływu incydentu związanego z cyberbezpieczeństwem.

Norma ISA 62443-3-2 zawiera wytyczne dotyczące sposobu oceny ryzyka związanego z cyberbezpieczeństwem w środowisku, w którym awaria może nieść za sobą takie skutki.

Skuteczna ocena ryzyka wymaga również określenia zarówno podatności, jak i zagrożeń dla środowiska OT. Prowadzenie dokładnej inwentaryzacji zasobów IT i OT w środowisku operacyjnym, obejmującej dostawców produktów, numery modeli, wersje oprogramowania układowego, systemy operacyjne i wersje oprogramowania instalowanego na komponentach, ułatwia identyfikację, śledzenie i usuwanie luk w zabezpieczeniach. Informacje dotyczące podatności występujących w systemach OT są dostępne i możliwe do uzyskania na wiele sposobów, obejmujących między innymi:

- Korzystanie z narzędzi opracowanych z myślą o systemach OT w celu zautomatyzowania tworzenia inwentaryzacji zasobów, korelacji list zasobów z listami znanych podatności oraz zagrożeń, a także instalowania regularnych aktualizacji.
- Obserwowanie grup i organizacji zajmujących się bezpieczeństwem, a także stowarzyszeń oraz dostawców i producentów w celu gromadzenia informacji o zagrożeniach oraz porad dotyczących bezpieczeństwa.
- Przeglądanie krajowej bazy danych dotyczących podatności na zagrożenia w celu uzyskiwania szczegółowych informacji na temat znanych podatności sprzętu i oprogramowania.

Informacje o zagrożeniach, które są istotne dla danego środowiska, można uzyskać zarówno z zasobów wewnętrznych, jak i zewnętrznych platform umożliwiających wymianę informacji na temat zagrożeń. Organizacje powinny rozważyć możliwość udostępniania informacji na temat cyberzagrożeń [SP800-150].

6.1.4. STRATEGIA ZARZĄDZANIA RYZYKIEM (ANG. RISK MANAGEMENT STRATEGY – ID.RM)

Strategia zarządzania ryzykiem określa sposób ustalania ram ryzyka, a także jego szacowania, oceny, monitorowania i reagowania na ryzyko, a także zapewnia spójne podejście umożliwiające podejmowanie decyzji opartych na ryzyku w całej organizacji. Strategia określa zagadnienia takie jak tolerowanie ryzyka, założenia, ograniczenia, priorytety i kompromisy na potrzeby podejmowania decyzji inwestycyjnych i dotyczących działalności. Strategia zarządzania ryzykiem określa ponadto dopuszczalne metodyki szacowania ryzyka, potencjalne sposoby reagowania na ryzyko oraz proces ciągłego monitorowania stanu bezpieczeństwa (lub wdrażania środków przeciwdziałania oraz analizy wyników tego procesu) dla organizacji.

Rozdział 3 zawiera ogólny opis procesu zarządzania ryzykiem pozwalającego na skuteczną realizację programu cyberbezpieczeństwa. Poniższe dokumenty zawierają dodatkowe wytyczne dotyczące wdrażania strategii zarządzania ryzykiem:

- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*

- NSC 800-39, *Zarządzanie ryzykiem bezpieczeństwa informacji*
- NIST IR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*

Zalecenia i wytyczne dotyczące systemów OT

Ustanawiając strategię zarządzania ryzykiem OT, organizacje powinny wziąć pod uwagę następujące zagadnienia i działania:

- Upewnienie się, że poziom tolerowanego ryzyka dla środowiska OT jest oparty na znaczeniu organizacji w infrastrukturze krytycznej i analizie ryzyka sektorowego.
- Dokumentowanie scenariuszy awarii obejmujących komponenty IT w środowisku OT oraz ich wpływu na działalność i bezpieczeństwo.
- Ustanowienie procesów okresowej aktualizacji informacji w celu określenia aktualnego stanu ryzyka dla środowiska i koordynowania wprowadzania zmian w strategii zarządzania ryzykiem i zarządzaniu środkami bezpieczeństwa.

Ogólne ryzyko można również ograniczyć poprzez uwzględnienie prawdopodobieństwa wystąpienia zdarzeń oraz ich skutków. W przypadku systemów OT strategia zarządzania ryzykiem powinna uwzględniać zabezpieczenia fizyczne (np. zawory bezpieczeństwa, zawory ręczne), które mogą pomóc w ograniczeniu skutków awarii.

6.1.5. ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW (*ANG. SUPPLY CHAIN RISK MANAGEMENT – ID.SC*)

Łańcuchy dostaw są zróżnicowane oraz opierają się na różnych czynnikach biznesowych, gospodarczych i technologicznych. Organizacje wybierają swoich dostawców, a konsumenci wybierają swoje źródła zaopatrzenia w oparciu o szereg czynników, które mogą obejmować zarówno preferencje organizacji oraz istniejące relacje biznesowe, jak i inne względy, takie jak: ograniczona lista źródeł dostaw lub inne warunki.

Podkategorie (rezultaty) wchodzące w skład kategorii zarządzania ryzykiem w łańcuchu dostaw opisanej w ramach ram cyberbezpieczeństwa stanowią podstawy do opracowania procesów i procedur zarządzania ryzykiem związanym z łańcuchem dostaw. Wśród możliwych zagrożeń można wymienić ryzyko wprowadzenia podróbek do systemu, nieautoryzowaną produkcję, złośliwe działania pracowników organizacji,

sabotaż, kradzieże oraz wprowadzanie złośliwego oprogramowania i złośliwych urządzeń do systemu, a także stosowanie złych praktyk produkcyjnych i rozwojowych w łańcuchu dostaw cyberbezpieczeństwa. Konieczne jest określenie, oszacowanie oraz uwzględnienie tego ryzyka w strategii. Kategoria ta obejmuje także umowy z dostawcami oraz podmiotami zewnętrznymi, oceny, a także planowanie reagowania i przywracania systemów w przypadku awarii.

Organizacje powinny także przeanalizować specyfikacje materiałowe komponentów oprogramowania oraz rozważyć stosowanie technologii rejestrów rozproszonych (np. blockchain) w celu skutecznego zarządzania ryzykiem związanym z łańcuchem dostaw. Informacje zawarte w specyfikacjach materiałowych komponentów oprogramowania mogą określać komponenty oprogramowania i ich relacje lub zależności względem innych komponentów. Wykorzystanie tych informacji może pomóc organizacji w ustaleniu, czy dane urządzenie jest narażone na wykorzystanie zgłoszonej podatności w oprogramowaniu.

Dodatkowe wytyczne dotyczące praktyk związanych z obszarem zarządzania ryzykiem w łańcuchu dostaw można znaleźć w następujących dokumentach:

- NIST SP 800-161, *Supply Chain Risk Management Practices~ for Federal Information Systems and Organizations*
- NIST IR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny rozważyć dokumentowanie i śledzenie numerów seryjnych, sum kontrolnych, cyfrowych certyfikatów/podpisów lub innych cech identyfikacyjnych, które mogą umożliwić weryfikację autentyczności dostarczonego przez dostawcę sprzętu OT, oprogramowania i oprogramowania układowego. Organizacje powinny również uwzględnić to, czy rozwiązania OT są nabywane bezpośrednio od producenta (OEM), czy autoryzowanego dystrybutora lub sprzedawcy.

Dostawcy powinni być poddawani ocenie lub przeglądom, aby zapewnić, że stale stosują najlepsze praktyki.

Wiele komponentów i urządzeń OT wykorzystuje biblioteki otwartoźródłowe w celu realizacji różnych funkcji. Organizacje powinny określić, jakie komponenty otwartoźródłowe są wykorzystywane w komponentach systemów OT oraz monitorować informacje publikowane w witrynach internetowych lub innych kanałach, aby upewnić się, że nie zostały ujawnione żadne znane podatności w zabezpieczeniach lub podróbki. Ponadto organizacje mogą rozważyć wykorzystanie popularnych procesów certyfikacji produktów OT w celu skutecznej realizacji zarządzania ryzykiem związanym z łańcuchem dostaw.

6.2. OCHRONA (*ANG. PROTECT – PR*)

Funkcja Ochrony umożliwia ograniczenie lub zniwelowanie wpływu potencjalnego zdarzenia związanego z cyberbezpieczeństwem. Przykłady kategorii rezultatów w ramach tej funkcji obejmują: zarządzanie tożsamością i kontrolę dostępu; świadomość i szkolenie; bezpieczeństwo danych; procesy i procedury ochrony informacji; konserwację; technologie zabezpieczające.

6.2.1. ZARZĄDZANIE TOŻSAMOŚCIĄ I KONTROLA DOSTĘPU (ANG. IDENTITY MANAGEMENT AND ACCESS CONTROL – PR.AC)

Zarządzanie tożsamością i kontrola dostępu (PR.AC) to kategoria umożliwiająca określanie rezultatów ustanawiania i zarządzania mechanizmami identyfikacji i poświadczeniami użytkowników, urządzeń i usług. Zarządzanie tożsamością umożliwia realizację reguły cyberbezpieczeństwa wymagającej jednoznacznej identyfikacji i autoryzacji osoby, procesu lub urządzenia przed przyznaniem fizycznego lub logicznego dostępu do zasobów, takich jak: chroniony system, informacje lub lokalizacja. Kategoria ochrony dostępu obejmuje zasady, procesy i technologie ograniczające możliwość korzystania z zasobów systemowych tylko do autoryzowanych użytkowników, a także uprawnione programy, procesy lub inne systemy. Zabezpieczenia związane z kategorią PR.AC umożliwiają organizacjom zarządzanie logicznym i fizycznym dostępem do systemów w celu realizacji wymagań w zakresie zarządzania ryzykiem dotyczącym systemów.

Dodatkowe wytyczne dotyczące wdrażania zarządzania tożsamością i kontroli dostępu można znaleźć w następujących dokumentach:

- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-73-4, *Interfaces _ for Personal Identity Verification*
- NIST SP 800-76-2, *Biometric Specifications _ for Personal Identity Verification*
- NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)*

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny przeanalizować cykl zarządzania poświadczeniami OT, w tym wydawanie, unieważnianie i aktualizacje poświadczeń w całym środowisku OT.

Organizacje powinny również uwzględnić możliwość centralizacji funkcji identyfikacji i uwierzytelniania użytkowników, urządzeń i procesów w środowiskach OT, aby usprawnić zarządzanie kontami i możliwości monitorowania. Popularne technologie sieciowe, takie jak Active Directory, Lightweight Directory Access Protocol (LDAP) i podobne rozwiązania, mogą być wykorzystywane w celu realizacji centralizacji zarządzania tożsamością w różnych środowiskach. Organizacje powinny wziąć pod uwagę zwiększone ryzyko związane ze stosowaniem uwierzytelnionych kont związanych ze środowiskami IT w celu dostępu do środowisk OT oraz zestawić je z korzyściami płynącymi z wykorzystywania scentralizowanych kont.

Jeśli systemy OT organizacji nie obsługują uwierzytelniania lub organizacja uzna, że wprowadzenie uwierzytelniania nie jest wskazane ze względu na niekorzystny wpływ na wydajność, bezpieczeństwo lub niezawodność, należy wdrożyć kompensacyjne środki przeciwdziałania, takie jak wdrożenie zabezpieczeń fizycznych (np. zabezpieczenia dostępu do centrum sterowania kartami dostępu wydanymi upoważnionym użytkownikom) w celu zapewnienia równoważnego poziomu bezpieczeństwa systemów OT. Wytyczne te mają również zastosowanie do systemów blokujących oraz kończących sesje w systemach OT.

Szczególnym wyzwaniem w przypadku systemów OT jest potrzeba natychmiastowego dostępu do interfejsów człowiek-maszyna (HMI) w sytuacjach awaryjnych. Czas potrzebny na wprowadzenie danych uwierzytelniających użytkownika może spowolnić reakcję lub interwencję operatora, co będzie skutkowało negatywnym wpływem na bezpieczeństwo, zdrowie lub środowisko.

6.2.1.1. LOGICZNA KONTROLA DOSTĘPU (ANG. LOGICAL ACCESS CONTROLS – PR.AC)

Logiczna kontrola dostępu ogranicza logiczny dostęp do systemów, danych i sieci organizacji. Obsługa logicznej kontroli dostępu opiera się zwykle na listach sterowania dostępem (ACL). Lista sterowania dostępem określa reguły przyznawania dostępu do zasobów oraz zasady minimalnej funkcjonalności i kontroli dostępu do obszarów o ograniczonym dostępie. Listy te są powszechnie używane w połączeniu z technologiami zapewniającymi izolację sieci, takimi jak: zapory sieciowe, w przypadku których określają źródła, miejsca docelowe i protokoły dozwolone w chronionym segmencie sieci. ACL mogą być również używane w celu kontroli fizycznego lub logicznego dostępu do obszarów lub informacji, takich jak: sieciowe udziały plików, bazy danych lub inne repozytoria danych i aplikacje.

Kontrola dostępu oparta na rolach (*ang. attribute-based access control – RBAC*) jest kolejną technologią pozwalającą na logiczną kontrolę dostępu. Technologia ta może zmniejszyć złożoność i koszty administrowania bezpieczeństwem w sieciach z dużą liczbą inteligentnych urządzeń. Metoda ta opiera się na zasadzie, że pracownicy zmieniają stanowiska oraz obowiązki z większą częstotliwością niż obowiązki w ramach ról. Zastosowanie technologii RBAC upraszcza administrację bezpieczeństwem dzięki zastosowaniu ról, hierarchii i ograniczeń do organizowania poziomów dostępu użytkowników.

Kontrola dostępu oparta na atrybutach (*ang. Role-based access control* – ABAC) jest podejściem do kontroli dostępu, w którym dostęp jest określany na podstawie atrybutów powiązanych z podmiotami i obiektami, do których uzyskiwany jest dostęp. Każdy obiekt i podmiot mają zestaw powiązanych atrybutów, takich jak lokalizacja, czas utworzenia i prawa dostępu. Dostęp do obiektu jest autoryzowany lub odmawiany w zależności od tego, czy można dokonać wymaganej (np. zdefiniowanej w zasadach) korelacji między atrybutami tego obiektu a żądającym podmiotem.

W przypadku przedstawicieli organizacji rządowych oraz wykonawców do realizacji kontroli dostępu może być wymagana osobista weryfikacja tożsamości wdrożona zgodnie z założeniami normy FIPS 201. Organizacje mogą również wykorzystać jedną lub wiele technik przy określaniu sposobu obsługi lokalnej kontroli dostępu w swoich

środowiskach. Dodatkowe wskazówki dotyczące praktyk w zakresie kontroli dostępu można znaleźć w następujących dokumentach:

- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-73-4, *Interfaces _ for Personal Identity Verification*
- NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*
- NIST SP 800-78-4, *Cryptographic Algorithms and Key Sizes _ for Personal Identity Verification*
- NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*
- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny rozważyć następujące kwestie:

- Niektóre mechanizmy kontroli dostępu, takie jak RBAC, wspierają zasadę minimalnych uprawnień i rozdziału obowiązków, umożliwiając jednolite zarządzanie dostępem do urządzeń OT przy jednoczesnym zmniejszeniu kosztów utrzymania indywidualnych poziomów dostępu do urządzeń i minimalizacji błędów. Logiczne systemy kontroli dostępu mogą również ograniczać uprawnienia użytkowników systemów OT tylko do tych, które są wymagane do wykonywania ich obowiązków (dzięki konfiguracji każdej roli w oparciu o zasadę minimalnych uprawnień). Poziom uprawnień dostępu może obejmować przeglądanie, używanie i aktualizowane określonych danych w systemach OT lub urządzeniach.
- Rozwiązania realizujące zarządzanie danymi uwierzytelniającymi, uwierzytelnianie, autoryzację i monitorowanie wykorzystania systemu. Technologie te mogą pomóc w zarządzaniu ryzykiem związanym z urządzeniami i protokołami OT, stanowiąc bezpieczną platformę umożliwiającą autoryzowanemu personelowi dostęp do urządzeń OT.

- Systemy kontroli dostępu, które weryfikują tożsamość osoby, procesu lub urządzenia przed przyznaniem dostępu w celu zminimalizowania opóźnień w przetwarzaniu dostępu do systemu OT lub poleceń.
- Wysoce niezawodne systemy, które nie wpływają na rutynowe obowiązki pracowników odpowiedzialnych za systemy OT ani reagowanie na incydenty. Rozwiązania powinny być zaprojektowane w taki sposób, aby ograniczyć wpływ weryfikacji tożsamości i autoryzacji na działanie systemów OT i bezpieczeństwo.

Realizacja kontroli dostępu może obejmować wiele podejść i rozwiązań. W niektórych przypadkach zastosowanie różnych technik kontroli dostępu do różnych stref w oparciu o krytyczność, bezpieczeństwo i wymagania operacyjne jest bardziej wydajne i skuteczne. Na przykład, listy sterowania dostępem na zaporach sieciowych w połączeniu z metodą RBAC na inżynieryjnych stacjach roboczych i serwerach oraz rozwiązanie ABAC zintegrowane z fizycznym zabezpieczeniem wrażliwych obszarów mogą spełnić wymagania organizacji w zakresie kontroli dostępu opartej na ryzyku.

6.2.1.2. FIZYCZNA KONTROLA DOSTĘPU (ANG. PHYSICAL ACCESS CONTROLS – PR.AC-2)

Fizyczne środki bezpieczeństwa to wszelkie środki fizyczne, które ograniczają fizyczny dostęp do zasobów w celu zapobiegania niepożądanym skutkom, w tym nieautoryzowanemu fizycznemu dostępowi do wrażliwych lokalizacji; nieautoryzowanemu wprowadzeniu nowych systemów, infrastruktury, interfejsów komunikacyjnych lub nośników wymiennych do środowiska; oraz nieautoryzowanemu zakłóceniu procesu fizycznego. Fizyczna kontrola dostępu obejmuje zabezpieczenia w zakresie zarządzania i monitorowania dostępu fizycznego, prowadzenie dzienników i opiekę nad gośćmi.

Wdrożenie fizycznych środków bezpieczeństwa często wymaga przestrzegania określonych wymogów środowiskowych, bezpieczeństwa, regulacyjnych, prawnych oraz innych związanych z danym środowiskiem – należy je określić i uwzględnić. Fizyczne środki bezpieczeństwa mogą być stosowane na szeroką skalę lub dotyczyć wyłącznie wybranych zasobów.

Podstawowe warstwy kontroli dostępu fizycznego są często określane na podstawie ryzyka dostępu do całego obiektu, a nie tylko komponentów systemów OT. Niektóre przepisy i regulacje określone w dokumentach NERC CIP-006-5 (ang. *Physical Security of BES Cyber Systems*) oraz wytycznych amerykańskiego urzędu dozoru jądrowego (NRC), mogą również określać zakres oraz liczbę barier stosowanych w celu fizycznej ochrony obiektu.

Zalecenia i wytyczne dotyczące systemów OT

Fizyczna ochrona komponentów i danych związanych z systemami OT musi stanowić element ogólnego bezpieczeństwa środowisk OT. Bezpieczeństwo w wielu organizacjach wykorzystujących systemy OT jest ściśle powiązane z bezpieczeństwem operacyjnym. Głównym założeniem jest ochrona pracowników przed niebezpiecznymi sytuacjami bez uniemożliwiania im wykonywania pracy lub przeprowadzania procedur awaryjnych.

Zabezpieczenia dostępu fizycznego są często stosowane w środowiskach OT w roli zabezpieczeń kompensacyjnych, zwłaszcza w przypadku starszych systemów, które nie obsługują nowoczesnych logicznych rozwiązań kontroli dostępu. Oznacza to, że przykładowe urządzenie może być zamknięte w zabezpieczonej szafie, jeśli ma gniazdo USB lub przycisk zasilania, których wyłączenie logiczne jest niemożliwe. Wdrażając te środki przeciwdziałania, organizacje powinny rozważyć, czy naruszenie zasad ochrony komponentu systemu OT może nastąpić za pośrednictwem połączenia bezprzewodowego lub sieciowego omijającego fizyczne środki bezpieczeństwa.

Komponent bezpieczeństwa fizycznego architektury obrony w głąb powinien uwzględniać następujące atrybuty:

- **Ochrona lokalizacji fizycznych.** Tradycyjne założenia bezpieczeństwa fizycznego zwykle obejmują zabezpieczenia tworzące szereg fizycznych barier wokół budynków, obiektów, pomieszczeń, urządzeń i zasobów informacyjnych. Zabezpieczenia fizyczne powinny być wdrożone w celu ochrony fizycznych lokalizacji i mogą obejmować ogrodzenia, rowy zabezpieczające przed pojazdami, nasypy ziemne, ściany, wzmocnione bariery, bramy, zamki do drzwi i szafek, osłony lub inne środki.

- **Fizyczna kontrola dostępu.** Szafki ze sprzętem powinny być zamykane na klucz, jeśli ich otwarcie nie jest wymagane w celu ich obsługi lub zapewnienia bezpieczeństwa, a okablowanie powinno być uporządkowane i umieszczone w szafkach lub pod podłogą. Ponadto należy zadbać o przechowywanie całego sprzętu komputerowego i sieciowego w zabezpieczonych obszarach. Klucze do elementów systemów OT, w tym programowalnych sterowników logicznych (PLC) i systemów bezpieczeństwa, powinny być zawsze w pozycji włączonej, z wyjątkiem sytuacji, w której są programowane.
- **Systemy monitorowania dostępu.** Systemy monitorowania dostępu realizują funkcje nadzoru elektronicznego. To między innymi aparaty fotograficzne, fotokomórki i kamery, a także czujniki i systemy identyfikacji, w tym czytniki identyfikatorów, skanery biometryczne oraz elektroniczne klawiatury. Takie urządzenia zazwyczaj nie uniemożliwiają dostępu do określonej lokalizacji. Dokumentują i rejestrują jedynie fizyczną obecność lub brak fizycznej obecności osób, pojazdów, zwierząt lub innych obiektów fizycznych. Należy zapewnić odpowiednie oświetlenie dla wykorzystywanego wdrożonego urządzenia monitorującego dostęp. Systemy te mogą również ostrzegać lub inicjować działania po wykryciu nieautoryzowanego dostępu.
- **Lokalizacja osób i zasobów.** Lokalizacja osób i pojazdów w obiekcie może być istotna zarówno ze względów bezpieczeństwa, jak i ochrony. Technologie lokalizacji zasobów mogą być wykorzystywane do śledzenia ruchu osób i pojazdów w celu zapewnienia, że pozostają one w autoryzowanych obszarach, do identyfikacji osób, które mogą potrzebować pomocy, oraz do wspierania reakcji w sytuacjach awaryjnych.

Poniżej opisano dodatkowe zagadnienia związane z bezpieczeństwem fizycznym:

- **Urządzenia przenośne.** Organizacje powinny stosować proces weryfikacji, który obejmuje co najmniej skanowanie urządzeń (np. laptopów, pamięci USB itp.) w poszukiwaniu złośliwego kodu przed zezwoleniem na podłączenie ich do urządzeń lub sieci OT.

- **Kable i przewody.** Choć stosowanie nieekranowanych przewodów typu skrętka jest dopuszczalne w środowisku biurowym, mogą one nie spełniać wymogów niektórych środowisk OT ze względu na ich podatność na zakłócenia powodowane przez pola magnetyczne, fale radiowe, ekstremalne temperatury, wilgoć, kurz i drgania. Organizacje powinny rozważyć zastosowanie alternatywnego okablowania lub ekranowania, które zapewnia odpowiednią ochronę przed zagrożeniami środowiskowymi. Ponadto organizacje powinny rozważyć stosowanie kabli, złącz, kanałów oraz etykiet oraz oznaczeń kolorystycznych w celu wyraźnego odróżnienia segmentów sieci OT i IT oraz ograniczenia ryzyka potencjalnych połączeń krzyżowych.
- **Centra sterowania i sterownie.** Zapewnienie fizycznego bezpieczeństwa centrów sterowania oraz sterowni może zmniejszyć ryzyko związane z wieloma zagrożeniami, w tym nieautoryzowanym dostępem. Dostęp do tych obszarów powinien być ograniczony wyłącznie do upoważnionych pracowników ze względu na zwiększone prawdopodobieństwo odkrycia podatnych serwerów, komponentów sieciowych, systemów sterowania i konsol obsługujących ciągłe monitorowanie i szybkie reagowanie. Uzyskanie fizycznego dostępu do pomieszczenia sterowania lub komponentów systemu OT często wiąże się z uzyskaniem logicznego dostępu do systemu lub jego komponentów. W skrajnych przypadkach organizacje mogą wziąć pod uwagę projektowanie centrów sterowania w taki sposób, by były odporne na wybuchy lub zbudować awaryjne centrum sterowania poza zakładem, by zapewnić ciągłość sterowania nawet w przypadku całkowitej utraty podstawowego centrum sterowania.

6.2.1.3. SEGREGACJA I IZOLACJA SIECI (ANG. NETWORK SEGMENTATION AND ISOLATION - PR.AC-5)

Zgodnie z opisem zawartym w rozdziale 5, typowa architektura sieci oparta na zasadzie obrony w głąb i wynikające z niej podejście do zapewniania cyberbezpieczeństwa obejmuje wykorzystanie segmentacji sieci lub podziału na strefy w celu przypisania urządzeń według lokalizacji lub funkcji. Segmentacja sieci jest zwykle realizowana w warstwie fizycznej dzięki zastosowaniu różnych przełączników sieciowych lub w warstwie logicznej przy użyciu konfiguracji opartej na wirtualnej sieci lokalnej (*ang. virtual local area network – VLAN*). Prawidłowo skonfigurowana segmentacja sieci pomaga w egzekwowaniu zasad bezpieczeństwa i rozdzielaniu ruch w warstwie Ethernet oraz ułatwia izolację sieci.

Organizacje zazwyczaj wykorzystują opisane przepływy danych w celu identyfikacji wymaganej komunikacji na potrzeby izolacji sieci. Urządzenia izolujące, takie jak bramy (w tym bramy jednokierunkowe lub diody danych) i zapory sieciowe, są następnie konfigurowane w celu egzekwowania tych zasad poprzez monitorowanie całego ruchu i zezwalanie tylko na dozwoloną komunikację między segmentami.

Dodatkowe wskazówki dotyczące praktyk w zakresie kontroli dostępu można znaleźć w następujących dokumentach:

- NIST SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*
- NSC 800-207, *Architektura bezpieczeństwa systemów informacyjnych w modelu „Zero zaufania" (wer. 1.0)*
- NIST SP 1800-15, *Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*

Zalecenia i wytyczne dotyczące systemów OT

Korzystanie z segmentacji i izolacji sieci powinno wynikać z architektury cyberbezpieczeństwa systemów OT organizacji, zgodnie z opisem w rozdziale 5.

Choć segmentacja sieci OT przy pomocy sieci VLAN może być przystępnym cenowo rozwiązaniem, organizacje powinny rozważyć wykorzystanie oddzielnych przełączników w celu segmentacji urządzeń o wysokim stopniu krytyczności, takich jak urządzenia obsługujące systemy bezpieczeństwa.

Podczas konfigurowania urządzeń izolujących organizacje mogą mieć trudności z określeniem, który ruch sieciowy jest niezbędny do prawidłowego działania systemów OT. W takich sytuacjach organizacje mogą rozważyć tymczasowe zdjęcie ograniczeń oraz rejestrowanie całej komunikacji między segmentami sieci. Taka decyzja prowadzi do powstania plików dzienników pozwalających na identyfikację i dokumentację komunikacji w celu wdrożenia reguł izolacji sieci.

Działanie to może również doprowadzić do ujawnienia uprzednio nieznanej lub nieudokumentowanej komunikacji, która wymaga weryfikacji przez organizację.

Organizacje powinny również sprawdzić, czy wymogi regulacyjne określają wymagania dotyczące rodzaju urządzeń izolujących w środowiskach OT lub określonych segmentach sieci. Jeśli organizacja podejmie decyzję o wykorzystaniu zapór sieciowych w celu izolacji sieci, powinna rozważyć zastosowanie nowoczesnych zapór sieciowych wyposażonych w funkcję głębokiej inspekcji pakietów oraz urządzenia zaprojektowane z myślą o środowiskach OT. Organizacje powinny wykorzystywać zasady odrzucania wszystkich połączeń i zezwalania na wyjątki w sytuacjach, w których są wymagane. Dodatkowe informacje znajdują się w dokumencie) *Firewall Deployment. for SCADA and Process Control Networks: Good Practice Guide* opracowanym przez Centrum Ochrony Infrastruktury Kraju (*ang. Centre for the Protection of National Infrastructure – CPNI*), który zawiera wytyczne dotyczące wdrażania zapór sieciowych w środowiskach OT.

Urządzenia izolujące mogą nie zapewniać ochrony przed wszystkimi zagrożeniami sieciowymi. Izolacja sieci nie ogranicza między innymi ryzyka związanego z przemieszczaniem się napastników wewnątrz segmentu sieci, nie uniemożliwia też rozprzestrzeniania się złośliwego kodu. Ponadto niektóre protokoły IT i wiele protokołów wykorzystywanych przez urządzenia przemysłowe mają znane podatności, które można wykorzystać pomimo urządzeń izolujących. Organizacje powinny rozważyć ograniczenie ruchu realizowanego za pośrednictwem niebezpiecznych protokołów, ograniczenie kierunków przepływu informacji oraz stosowanie bezpiecznych i uwierzytelnionych protokołów do obsługi wymiany informacji między środowiskiem OT a innymi segmentami sieci.

6.2.1.4. UWIERZYTELNIANIE UŻYTKOWNIKÓW, URZĄDZEŃ I ZASOBÓW (ANG. USER, DEVICE, AND ASSET AUTHENTICATION - PR.AC-7)

W środowiskach OT można wdrożyć różne metody uwierzytelniania, w tym między innymi metody omówione w niniejszym rozdziale.

6.2.1.4.1. UWIERZYTELNIANIE ZA POMOCĄ TOKENA FIZYCZNEGO

Uwierzytelnianie za pomocą fizycznego tokena rozwiązuje przede wszystkim problem łatwego ustalenia kodu dostępu lub udostępniania go innym osobom – na przykład umieszczenia hasła do zabezpieczonego systemu na karteczce samoprzylepnej przyklejonej do ściany obok komputera lub stacji roboczej operatora. W przypadku uwierzytelniania tokenem fizycznym, token zabezpieczający nie może zostać powielony bez dostępu do sprzętu i urządzeń.

Dodatkową zaletą jest fakt, że sekret zawarty w fizycznym tokenie może być bardzo duży, zabezpieczony fizycznie i generowany losowo. Ze względu na zabezpieczenie klucza dostępu w metalu lub krzemie, stosowanie tokenów nie wiąże się z takim samym ryzykiem, jak stosowanie ręcznie wprowadzanych haseł. Tradycyjne hasła mogą zostać zgubione lub skradzione, co umożliwia nieautoryzowane wykorzystanie danych uwierzytelniających. Jeśli token bezpieczeństwa zostanie zgubiony lub skradziony, właściciel tokena będzie świadomy jego zaginięcia i może powiadomić pracowników odpowiedzialnych za ochronę w celu zablokowania dostępu.

Typowe fizyczne urządzenia uwierzytelniające oraz tokeny to między innymi:

- Tradycyjne fizyczne zamki i klucze.
- Karty dostępu (magnetyczne, z inteligentnym chipem, z kodem optycznym).
- Urządzenia wykorzystujące częstotliwości radiowe (*ang. Radio frequency devices – RFID*) w postaci kart, breloczków lub znaczników.
- Klucze sprzętowe z bezpiecznymi kluczami szyfrującymi podłączane do portów USB, szeregowych lub równoległych komputerów.
- Generatory kodów jednorazowego uwierzytelniania (w formie breloków do kluczy).

W przypadku uwierzytelniania jednoskładnikowego za pomocą fizycznego tokena największą słabością jest to, że fizyczne posiadanie tokena zapewnia uzyskanie dostępu do systemu. Na przykład każda osoba, która znajdzie zgubione klucze, może teraz uzyskać dostęp do wszystkich otwieranych przez nie pomieszczeń. Fizyczne uwierzytelnianie za pomocą tokena jest bezpieczniejsze w połączeniu z drugą formą uwierzytelniania, taką jak zapamiętany kod PIN używany wraz z tokenem.

Gdy kontrola dostępu oparta na tokenach wykorzystuje weryfikację kryptograficzną, system kontroli dostępu powinien być zgodny z wymaganiami określonymi w dokumencie NIST SP 800-78-4 [SP800-78-4].

6.2.1.4.2. UWIERZYTELNIANIE BIOMETRYCZNE

Uwierzytelnianie biometryczne uzupełnia rozwiązania oparte wyłącznie na oprogramowaniu, takie jak uwierzytelnianie hasłem, oferując dodatkowy czynnik uwierzytelniania i eliminując potrzebę zapamiętywania złożonych haseł lub kodów. Co więcej, ze względu na fakt, że cechy biometryczne są wyjątkowe dla danej osoby, uwierzytelnianie biometryczne rozwiązuje problemy związane ze zagubionymi lub skradzionymi tokenami fizycznymi i inteligentnymi kartami. Urządzenia biometryczne stanowią wygodne dodatkowe zabezpieczenie, zwłaszcza w zestawieniu z innymi metodami uwierzytelniania, które mogą zostać zgubione lub przekazane innej osobie. Korzystanie z uwierzytelniania biometrycznego w połączeniu z kontrolą dostępu opartą na tokenach lub zegarami czasu pracy odczytującymi identyfikatory pracowników umożliwia zwiększenie bezpieczeństwa.

Znane problemy dotyczące uwierzytelnienia biometrycznego obejmują:

- Trudności z odróżnieniem prawdziwego obiektu od jego podróbki (np. odróżnienie prawdziwego ludzkiego palca od odlewu wykonanego z tworzywa sztucznego lub prawdziwego ludzkiego głosu od nagrania).
- Generowanie błędów typu I i typu II, czyli odrzucenia prawidłowego odczytu biometrycznego i zaakceptowania nieprawidłowego odczytu biometrycznego. Urządzenia uwierzytelniające powinny być skonfigurowane w taki sposób, aby współczynnik wystąpienia obu tych błędów był możliwie najniższy.

- Trudności z działaniem w określonych środowiskach i wrażliwość na parametry środowiskowe, takie jak temperatura czy wysoka wilgotność.
- Trudności z działaniem w zakładach przemysłowych, których pracownicy korzystają z ochrony wzroku, ochrony dłoni lub w których przetwarzane są substancje chemiczne.
- Konieczność kalibracji skanerów biometrycznych po upływie określonego czasu ze względu na zmiany parametrów. Problemem jest także fakt, że ludzkie cechy biometryczne także zmieniają się w czasie, co może wymagać ponownej konfiguracji skanerów.
- Konieczność zapewnienia wsparcia technicznego i weryfikacji w czasie konfiguracji urządzenia, co utrudnia przyznanie dostępu zwłaszcza w porównaniu z hasłem, które można podać przez telefon oraz karty dostępu, którą może wręczyć recepcjonista.
- Problem z odmową dostępu do systemu OT z powodu błędu urządzenia lub braku możliwości potwierdzenia tożsamości autoryzowanego użytkownika.
- Problem z akceptacją społeczną tego rodzaju rozwiązań. Zdaniem użytkowników niektóre urządzenia do uwierzytelniania biometrycznego są bardziej akceptowalne niż inne. Skanery siatkówki oka są powszechnie uważane za nieakceptowalne, z kolei skanery odcisków palców cieszą się większą popularnością. Organizacje wdrażające urządzenia do uwierzytelniania biometrycznego muszą uwzględnić akceptowalność społeczną danego rozwiązania wśród grupy docelowej przy wyborze technologii uwierzytelniania biometrycznego.

Gdy kontrola dostępu oparta na tokenach wykorzystuje weryfikację biometryczną, system kontroli dostępu powinien być zgodny z wymaganiami określonymi w dokumencie NIST SP 800-76-2 [SP800-76-2].

Zalecenia i wytyczne dotyczące systemów OT

Choć uwierzytelnianie biometryczne może stanowić przydatny mechanizm uwierzytelniania, organizacje muszą dokonać starannej analizy technologii pod kątem jej wykorzystania w zastosowaniach przemysłowych. Czynniki fizyczne i środowiskowe związane ze środowiskami OT mogą zmniejszyć niezawodność

uwierzytelniania biometrycznego. W związku z tym konieczny może być kontakt z dostawcami lub producentami systemów w celu omówienia warunków fizycznych i środowiskowych oraz wymagań dotyczących uwierzytelniania biometrycznego.

6.2.1.4.3. UWIERZYTELNIANIE ZA POMOCĄ KART INTELIGENTNYCH

Karty inteligentne są dostępne w różnych formach, od urządzeń USB po układy elektroniczne wbudowane w karty przypominające karty kredytowe, które mogą być wytłaczane i zadrukowane. Karty inteligentne mogą być dostosowywane, personalizowane i wydawane w organizacji lub przez dostawców usług wytwarzających setki lub tysiące sztuk dziennie. Stosowanie kart inteligentnych uzupełnia rozwiązania oparte wyłącznie na oprogramowaniu, takie jak uwierzytelnianie hasłem, oferując dodatkowy czynnik uwierzytelniania i eliminując potrzebę zapamiętywania złożonych haseł lub kodów dzięki:

- Izolacji przetwarzania o krytycznym znaczeniu dla bezpieczeństwa, które obejmują uwierzytelnianie, podpisy cyfrowe i wymianę kluczy od innych części systemu, które nie muszą mieć do nich dostępu.
- Umożliwieniu przenoszenia danych uwierzytelniających i innych prywatnych informacji między systemami komputerowymi.
- Zapewnieniu odpornej na manipulacje pamięci masowej pozwalającej na ochronę kluczy prywatnych i innych form danych osobowych.

Większość problemów związanych z wykorzystaniem kart inteligentnych wiąże się z kwestią logistyki i wydawaniem kart, a w szczególności na wymianie zgubionych lub skradzionych kart.

Zalecenia i wytyczne dotyczące systemów OT

Choć karty inteligentne mogą być przydatnym rozwiązaniem, ich wdrożenie w kontekście systemów OT musi uwzględniać ogólny kontekst bezpieczeństwa środowiska OT.

Konieczność identyfikacji osób, wydawania kart, unieważniania kart w przypadku podejrzenia naruszenia zasad ochrony oraz przypisywanie uprawnień do uwierzytelnionych tożsamości stanowi poważne wyzwanie zarówno na etapie

wdrożenia, jak i eksploatacji tego rozwiązania. W wybranych przypadkach dział IT organizacji lub inni pracownicy mogą udzielić pomocy we wdrożeniu kart inteligentnych i wymaganej infrastruktury klucza publicznego. Organizacje powinny również uwzględnić wpływ takich rozwiązań na działanie systemów OT, jeśli do obsługi technologii kart inteligentnych wymagana jest zależność od systemów i usług IT.

Ponadto w przypadku wdrażania kart inteligentnych w środowisku OT, organizacje powinny wziąć pod uwagę wprowadzenie zasad dotyczących zgubionych oraz uszkodzonych kart, a także uwzględnić koszty opracowania i utrzymania stosownego systemu kontroli dostępu oraz procesu zarządzania dystrybucją i odzyskiwaniem kart.

Procedury te powinny uwzględniać możliwość przyznania tymczasowego dostępu pracownikom odpowiedzialnym za systemy OT, aby zapobiec przerwom w działaniu systemów lub obniżeniu poziomu ich bezpieczeństwa.

Podejście wykorzystywane w jednostkach rządowych opiera się na znormalizowanych kartach inteligentnych, które umożliwiają organizacjom korzystanie z tego samego mechanizmu uwierzytelniania w wielu aplikacjach z jednym do trzech czynników uwierzytelniania (tj. uwierzytelnianie kartą, kartą i numerem PIN, bądź kartą, numerem PIN i czynnikiem biometrycznym) w zależności od poziomu ryzyka chronionego zasobu. W przypadku wykorzystywania takiego rozwiązania, system kontroli dostępu powinien spełniać wymogi opisane w dokumentach FIPS 201 [FIPS201] oraz NIST SP 800-73-4 [SP800-73-4] i wykorzystywać weryfikację kryptograficzną lub biometryczną.

6.2.1.4.4. UWIERZYTELNIANIE WIELOSKŁADNIKOWE

Istnieje kilka możliwych elementów pozwalających na potwierdzenie tożsamości osoby, urządzenia lub systemu. Obejmują składnik oparty na wiedzy (np. numer PIN lub hasło), składnik wykorzystujący posiadane urządzenie (np. klucz, klucz sprzętowy, kartę inteligentną) oraz cechy danego podmiotu (tj. cechy biologiczne, na przykład odcisk palca lub wzór siatkówki oka). Proces wykorzystujący więcej niż jeden element określamy mianem uwierzytelniania wieloskładnikowego (*ang. multi-factor Authentication - MFA*). Im więcej czynników jest wykorzystywanych w procesie uwierzytelniania, tym jest on bardziej niezawodny.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje muszą dokonać analiz w celu ustalenia, czy uwierzytelnianie wieloskładnikowe jest konieczne w celu ochrony środowisk OT w całości lub w części. Uwierzytelnianie wieloskładnikowe jest uznane za najlepszą praktykę w zakresie zabezpieczania zdalnego dostępu do aplikacji OT. Określając miejsca, w których konieczne jest wykorzystanie uwierzytelnienia wieloskładnikowego w środowisku OT, organizacje powinny przeanalizować różne scenariusze uwierzytelniania ze względu na fakt, że niektóre komponenty systemów OT obsługują tylko jeden składnik uwierzytelniający lub nie obsługują funkcji uwierzytelniania. Organizacje mogą rozważyć dostosowanie wymagań dotyczących poświadczeń w oparciu o rodzaj dostępu lub inne czynniki dotyczące danego środowiska. Na przykład zdalny dostęp do środowiska OT może wymagać uwierzytelniania wieloskładnikowego. Z kolei dostęp lokalny może wymagać jedynie podania nazwy użytkownika i hasła ze względu na inne czynniki, takie jak zabezpieczenia dostępu fizycznego uniemożliwiające uzyskanie fizycznego dostępu do obszaru, w którym użytkownik może użyć danych uwierzytelniających.

6.2.1.4.5. UWIERZYTELNIANIE HASŁEM

Choć metody oparte na uwierzytelnianiu przy pomocy haseł są najbardziej powszechną i najprostszą formą uwierzytelniania, liczne podatności w zabezpieczeniach wiążą się z wykorzystywaniem metod uwierzytelniania opartych wyłącznie na hasłach dostępu. Wiele systemów jest dostarczanych z domyślnymi hasłami, które można łatwo odgadnąć, odkryć lub ustalić w inny sposób. Kolejna słabość wiąże się z łatwością pozyskania hasła przez osoby trzecie. Hasła wpisywane na klawiaturze mogą być podejrzane przez inne osoby lub rejestrowane za pomocą rejestratorów naciśnięć klawiszy.

Niektóre usługi i protokoły sieciowe przesyłają hasła otwartym (niezaszyfrowanym) tekstem, umożliwiając wielu narzędziom przechwycenie i ujawnienie haseł. Ponadto hasła mogą być udostępniane innym osobom i nie są zmieniane z wystarczającą częstotliwością. Korzystanie ze współdzielonych danych uwierzytelniających, w tym współdzielonych haseł, ogranicza możliwość identyfikacji konkretnej osoby, a także konkretnego procesu lub urządzenia uzyskujących dostęp do chronionego zasobu.

Celem strategii obrony w głąb jest zapobieganie sytuacji, w której uwierzytelnianie hasłem jest jedynym zabezpieczeniem zapobiegającym dokonaniu nieautoryzowanych modyfikacji i zmian.

Zalecenia i wytyczne dotyczące systemów OT

Wiele systemów OT nie jest wyposażona w funkcje odzyskiwania haseł, w związku z czym bezpieczna i niezawodna obsługa haseł ma kluczowe znaczenie dla zapewnienia ciągłości działania systemów. Organizacje powinny zmienić domyślne hasła do urządzeń OT, aby utrudnić napastnikom ich odgadnięcie. Po zmianie hasło musi zostać udostępnione pracownikom, którzy potrzebują go w związku z wykonywaną pracą. Organizacje mogą wziąć pod uwagę możliwość wdrożenia bezpiecznego menedżera haseł i udostępnienia go osobom, które wymagają dostępu do systemów.

Niektóre systemy operacyjne OT utrudniają konfigurowanie bezpiecznych haseł, jeśli długość hasła jest niższa od wymagań współczesnych standardów, a system zezwala tylko na konfigurowanie haseł grupowych na każdym poziomie dostępu, nie pozwalając na ustawianie haseł indywidualnych. Niektóre protokoły przemysłowe (oraz internetowe) przesyłają hasła w postaci otwartego, niezaszyfrowanego tekstu, dzięki czemu mogą zostać przechwycone. W przypadkach, w których nie można uniknąć stosowania takich protokołów, należy zadbać o to, by użytkownicy korzystali z różnych (i niepowiązanych) haseł w związku z protokołami szyfrowanymi i nieszyfrowanymi.

Ponadto, podczas wdrażania zasad opartych na uwierzytelnianiu na podstawie nazw użytkownika i haseł w środowiskach OT należy wziąć pod uwagę szereg kwestii i zagadnień. W przypadku braku listy wykluczeń opartej na identyfikatorze urządzenia (ID), logowanie osób niebędących operatorami może skutkować zastosowaniem zasad takich jak automatyczne wylogowanie i wymuszenie zmiany hasła administratora, co może wpłynąć negatywnie na działanie systemu OT.

Poniżej przedstawiono ogólne zalecenia i uwagi dotyczące korzystania z haseł:

- Należy zmienić wszystkie domyślne hasła dostępu do komponentów systemów OT.
- Hasła powinny mieć odpowiednią długość, siłę i złożoność zgodnie z wymaganiami w zakresie bezpieczeństwa oraz łatwości dostępu. Powinny także spełniać wymagania oprogramowania i systemu operacyjnego.

- Hasła nie powinny być słowami występującymi w słownikach ani nie powinny zawierać przewidywalnych sekwencji cyfr lub liter.
- Należy zachować rozwagę przy wykorzystywaniu haseł na wyspecjalizowanych urządzeniach OT, takich jak konsole sterowania odpowiedzialne za krytyczne procesy. Korzystanie z haseł na tych konsolach może spowodować problemy związane z bezpieczeństwem w przypadku zablokowania dostępu operatorów lub opóźnienia dostępu w przypadku wystąpienia zdarzenia. Organizacje powinny wziąć pod uwagę możliwość fizycznego lub sieciowego odizolowania urządzeń, których nie można zabezpieczyć hasłem.
- Kopie haseł współdzielonych lub haseł administratora muszą być przechowywane w bezpiecznej lokalizacji, do której dostęp powinien być ograniczony, lecz możliwy w przypadku wystąpienia sytuacji awaryjnej. Organizacje mogą również uwzględnić możliwość wdrożenia procedury okresowej zmiany haseł, a także zmiany haseł w przypadku wycieku lub zakończenia stosunku pracy osoby posiadającej dostęp do haseł.
- Hasła do kont uprzywilejowanych (administracyjnych) wymagają dodatkowej ochrony, na przykład poprzez wymaganie silniejszego hasła, wymuszenie częstszych zmian hasła i dodatkowe zabezpieczenia fizyczne.
- Hasła nie powinny być przesyłane za pośrednictwem żadnej sieci, chyba że są chronione za pomocą jakiejś formy szyfrowania uwzględnionej w standardach FIPS lub solonego skrótu kryptograficznego, aby zapobiec atakom powtórzeniowym.

6.2.2. ŚWIADOMOŚĆ I SZKOLENIA (ANG. AWARENESS AND TRAINING – PR.AT)

Kategoria Świadomość i szkolenia opisuje zasady i procedury zapewniające wszystkim użytkownikom podstawową świadomość i dostęp do szkoleń dotyczących cyberbezpieczeństwa.

Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)*
- NIST SP 800-181, Rev. 1, *Workforce Framework for Cybersecurity (NICE Framework)*

Zalecenia i wytyczne dotyczące systemów OT

Pracownicy powinni być świadomi zagadnień związanych z bezpieczeństwem i przeszkoleni w zakresie zagadnień dotyczących bezpieczeństwa środowiska OT i określonych aplikacji. Ponadto organizacje powinny wskazać, udokumentować i przeszkolić wszystkich pracowników, których zakres obowiązków jest związany ze środowiskami i systemami OT. Działania w zakresie zwiększania świadomości i szkoleń powinny obejmować zarówno proces fizyczny, jak i system OT.

Świadomość zasad bezpieczeństwa jest kluczem do zapobiegania występowaniu incydentów związanych z systemami OT, szczególnie ze względu na ryzyko ataków z wykorzystaniem inżynierii społecznej. Inżynieria społeczna to technika wykorzystywana w celu skłonienia pracowników do ujawnienia napastnikowi prywatnych informacji, takich jak hasła. Informacje te mogą być następnie wykorzystane do naruszenia zasad ochrony systemów.

Programy uświadamiające i szkoleniowe dotyczące bezpieczeństwa systemów OT mogą obejmować podstawową wiedzę na temat technik inżynierii społecznej, identyfikowania anomalii w środowisku OT, łączenia i odłączania środowisk OT od zewnętrznych domen bezpieczeństwa, wymogów w zakresie złożoności haseł i wymagań dotyczących zarządzania oraz praktyk raportowania. Wszyscy pracownicy odpowiedzialni za systemy OT powinni przejść szkolenie, które powinno być dostosowane do ich ról i obowiązków. Role, które należy uwzględnić w programie szkoleń, mogą obejmować kadrę kierowniczą wyższego szczebla, użytkowników kont uprzywilejowanych, dostawców zewnętrznych, pracowników działu ochrony fizycznej, inżynierów ds. nadzoru technicznego, operatorów i pracowników odpowiedzialnych za utrzymanie ruchu.

6.2.3. BEZPIECZEŃSTWO DANYCH (ANG. DATA SECURITY – PR.DS)

Działania mające na celu zapewnienie bezpieczeństwa danych obejmują ochronę poufności, integralności i dostępności danych w spoczynku i w tranzycie, ochronę zasobów po ich usunięciu oraz zapobieganie wyciekom danych.

Metody kryptograficzne są jednym ze sposobów realizacji wymogów w zakresie

bezpieczeństwa danych. Szyfrowanie, podpisy cyfrowe, skróty kryptograficzne oraz inne funkcje pozwalają na zapobieganie nieautoryzowanemu dostępowi lub modyfikacji danych w spoczynku i w tranzycie [RFC4949].Wdrażając rozwiązania kryptograficzne, organizacje powinny korzystać z certyfikowanego systemu kryptograficznego. Organizacje rządowe są zobowiązane do przestrzegania wymogów norm FIPS 140-3 [FIPS140-3] oraz Cryptographic Module Validation Program (CMVP). Urządzenia kryptograficzne powinny być zabezpieczone przed fizyczną ingerencją i możliwością nawiązania połączeń elektronicznych.

Dodatkowe wskazówki dotyczące praktyk w zakresie bezpieczeństwa danych można znaleźć w następujących dokumentach:

- NIST SP 800-47, Rev. 1, *Managing the Security of Information Exchanges*
- NIST SP 800-111, *Guide to Storage Encryption Technologies_ for End User Devices*
- NSC 800-209, *Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych*

Zalecenia i wytyczne dotyczące systemów OT

Należy określić najważniejsze rodzaje plików oraz dane, które wymagają ochrony w stanie spoczynku. Mogą obejmować one informacje umożliwiające identyfikację osób oraz informacje wrażliwe, zastrzeżone lub stanowiące tajemnicę handlową (np. kod programu sterownika PLC, oprogramowanie robotów przemysłowych, pliki projektowe CAD (*ang. computer-aided drafting - CAD*) lub CAM *(ang. aided manufacturing – CAM*), instrukcje obsługi i dokumentację, schematy elektryczne, schematy sieci, historyczne dane produkcyjne) [IR8183A]. Organizacje powinny rozważyć gromadzenie najważniejszych danych w bezpiecznych magazynach danych.

Gdy dane dotyczące systemów OT są przechowywane w chmurze lub na serwerach dostawcy, organizacje powinny rozważyć przeprowadzenie analizy ryzyka w celu ustalenia, w jaki sposób dane są chronione przez dostawcę usług i czy należy wdrożyć dodatkowe zabezpieczenia w celu ograniczenia ryzyka do akceptowalnego poziomu.

Należy monitorować przepływ informacji pomiędzy domeną bezpieczeństwa OT i innymi domenami oraz połączenia między domenami zabezpieczeń. Technologie takie jak diody danych, zapory sieciowe oraz listy sterowania dostępem pozwalają na

ograniczenie przepływu informacji. Przykłady krytycznych interfejsów i połączeń mogą obejmować interfejsy między systemami IT i OT, połączenia między systemami OT i systemami partnerów branżowych oraz połączenia między systemami OT i zewnętrznymi dostawcami usług wsparcia.

Ochrona danych przechowywanych na komponentach systemu po zakończeniu okresu eksploatacji wymaga wdrożenia programu utylizacji zasobów, który obejmuje wymazywanie, usuwanie danych lub niszczenie najważniejszych danych i nośników przed utylizacją komponentu. Program utylizacji zasobów powinien obejmować wszelkie nośniki wymienne, urządzenia przenośne oraz urządzenia OT.

Kryptografia

Najważniejsze dane związane z systemami OT powinny być chronione podczas przesyłania, zwłaszcza gdy odbywa się ono za pośrednictwem segmentów sieci podmiotów zewnętrznych bądź innych niezaufanych lub podatnych na zagrożenia systemów komunikacji, na przykład w sieciach mobilnych, bezprzewodowych, sieciach WAN lub przez Internet. Należy określić zakres krytycznych danych i wykorzystać mechanizmy kryptograficzne (np. szyfrowanie), aby zapobiec nieautoryzowanemu dostępowi lub modyfikacji danych systemowych i dokumentacji audytu.

Szyfrowanie zapewnia poufność i integralność przesyłanych danych.

Aplikacje OT często stawiają na pierwszym miejscu dostępność danych. Przed wdrożeniem szyfrowania w systemach OT należy upewnić się, że celem zastosowania zabezpieczeń jest poufność lub integralność danych. Zastosowanie szyfrowania w środowisku OT może wprowadzić opóźnienia w komunikacji ze względu na dodatkowy czas i zasoby obliczeniowe wymagane do szyfrowania, odszyfrowywania i uwierzytelniania przesyłanych danych. Szyfrowanie może również powodować spadek wydajności urządzenia lub systemu. Przed wdrożeniem szyfrowania w środowisku OT należy przetestować rozwiązania, aby określić, czy powstałe w wyniku wdrożenia opóźnienia są dopuszczalne. Szyfrowanie w warstwie 2 modelu OSI zamiast w warstwie 3 może ograniczyć opóźnienia związane z szyfrowaniem

Co więcej, choć szyfrowanie zapewnia zachowanie poufności pomiędzy urządzeniami szyfrującymi i deszyfrującymi, narzędzia pozwalające na wykrywanie anomalii

w środowiskach OT mogą nie być w stanie odczytać zaszyfrowanych danych. Szyfrowanie powinno być zatem wdrożone po dokładnych analizach, jeśli jest wymagane w celu zarządzania ryzykiem operacyjnym.

Organizacje powinny również wziąć pod uwagę, że stosowanie metod kryptograficznych może skutkować dodatkowymi wymogami w zakresie zarządzania kluczami. Zaawansowane zasady bezpieczeństwa wymagają wdrożenia procesów zarządzania kluczami, które mogą stawać się coraz bardziej złożone wraz ze wzrostem skali środowiska OT. Ze względu na to, że zmiana kluczy lub zarządzanie nimi w odległych lokalizacjach mogą być kosztowne i czasochłonne, organizacje powinny rozważyć, czy ochrona kryptograficzna ze zdalnym zarządzaniem kluczami może stanowić zadowalające rozwiązanie, zwłaszcza w przypadku dużego poziomu rozproszenia geograficznego lub dużej liczby obiektów, uniemożliwiających skuteczne zarządzanie kluczami.

W przypadku środowisk OT szyfrowanie może stanowić część kompleksowych zasad bezpieczeństwa. Klucz kryptograficzny powinien być na tyle długi, aby jego odgadnięcie lub ustalenie za pomocą analizy wymagało od napastnika włożenia ilości wysiłku, poświęcenia czasu oraz zainwestowania kwot przewyższających wartość chronionego zasobu.

6.2.4. PROCESY I PROCEDURY OCHRONY INFORMACJI (ANG. INFORMATION PROTECTION PROCESSES AND PROCEDURES - PR.IP)

Zasady, procesy i procedury powinny być wdrażane i wykorzystywane w celu zarządzania ochroną systemów informacyjnych i zasobów. Należy wdrożyć środki przeciwdziałania i rozwiązania pozwalające na zarządzanie zmianami konfiguracji w całym cyklu życia komponentu i systemu. Należy utrzymywać kopie zapasowe oraz przygotowywać i testować plany reagowania i odtworzenia po katastrofie. Należy opracować i wdrożyć plan zarządzania podatnościami w całym cyklu życia komponentów.

6.2.4.1. ZASADA MINIMALNEJ FUNKCJONALNOŚCI (PR.IP-1)

Zasada minimalnej funkcjonalności opisuje konfigurowanie systemów w taki sposób, aby świadczyły tylko niezbędne funkcje i usługi. Niektóre domyślne funkcje i usługi

mogą nie być konieczne do realizacji podstawowych misji, funkcji lub działań organizacji. Funkcje te obejmują porty i protokoły sieciowe, oprogramowanie i usługi.

Dodatkowe wytyczne znajdują się w następującym dokumencie:

- NIST SP 800-167, *Guide to Application Whitelisting*

Zalecenia i wytyczne dotyczące systemów OT

Systemy i urządzenia działające w środowisku OT udostępniają wiele funkcji i usług, które są zbędne do ich prawidłowego działania, a niektóre z nich mogą być włączone domyślnie bez wiedzy organizacji.

Wszelkie funkcje lub usługi, które nie są wymagane do prawidłowego działania systemu, powinny zostać wyłączone w celu zmniejszenia powierzchni ataku.

Należy zachować ostrożność podczas wyłączania funkcji i usług, ponieważ przypadkowe wyłączenie krytycznej usługi lub funkcji może spowodować nieprzewidziane konsekwencje – na przykład wyłączenie komunikacji zewnętrznej ze sterownikiem PLC może również uniemożliwić komunikację z powiązanymi interfejsami człowiek-maszyna.

Urządzenia powinny zostać poddane szeroko zakrojonym testom przed ich podłączeniem do sieci OT.

6.2.4.2. KONTROLA ZMIAN W KONFIGURACJI (ZARZĄDZANIE KONFIGURACJĄ) (PR.IP-3)

Zarządzanie konfiguracją pomaga zapewnić, że systemy są wdrażane i utrzymywane w bezpiecznym i niezmiennym stanie, co pozwala na ograniczenie ryzyka wystąpienia przestojów z powodu problemów z konfiguracją i naruszeń zasad ochrony dzięki poprawie widoczności oraz śledzeniu zmian w systemie. Zarządzanie konfiguracją pozwala także na wykrywanie błędnych i niewłaściwych zmian w konfiguracji, zanim wpłyną negatywnie na wydajność, bezpieczeństwo lub ochronę systemów. Narzędzia do zarządzania konfiguracją umożliwiają organizacji zapewnienie integralności komponentów sprzętowych i programowych systemu poprzez kontrolowanie procesów wstępnej konfiguracji, a także dokonywanych zmian, monitorowania i kontroli konfiguracji komponentów w całym cyklu życia systemu.

Dodatkowe wskazówki dotyczące praktyk w zakresie zarządzania konfiguracją można znaleźć w następujących dokumentach:

- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 1800-5, *IT Asset Management*

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny udokumentować zatwierdzone konfiguracje podstawowe wykorzystywanych urządzeń i systemów OT, a następnie opracować podejście oparte na cyklu życia systemu (SDLC) w celu dokumentowania, testowania i zatwierdzania zmian przed wdrożeniem w środowisku OT.

Niektóre organizacje mogą wykorzystywać dzienniki lub zbliżone metody dokumentowania zmian dotyczących komponentów OT. Organizacje powinny rozważyć centralizację śledzenia i dokumentowania zmian w środowisku OT, aby poprawić widoczność i zapewnić odpowiednie testowanie i zatwierdzanie zmian w systemie. Taki proces może pomóc organizacjom w zapobieganiu przypadkowym zmianom konfiguracji oraz wykrywaniu celowych zmian konfiguracji komponentów.

Jeśli użycie zautomatyzowanych narzędzi do zarządzania konfiguracją zostanie uznane za stosowne, należy wdrożyć procesy weryfikacji konfiguracji przed jej wprowadzeniem. Wiele zmian konfiguracji systemów OT można wprowadzić tylko podczas zaplanowanych przestojów konserwacyjnych, aby ograniczyć wpływ zmian na ich działanie. Rozważając zastosowanie zautomatyzowanych narzędzi do zarządzania konfiguracją, organizacje powinny również wziąć pod uwagę ich potencjalny wpływ na system OT. W niektórych przypadkach narzędzia te przesyłają duże ilości zróżnicowanych danych za pośrednictwem sieci systemu produkcyjnego. Niektóre narzędzia mogą również wpływać na działanie systemu OT poprzez próby zmiany konfiguracji urządzeń lub wprowadzanie zmian w aktywnych plikach.

6.2.4.3. KOPIE ZAPASOWE (PR.IP-4)

Wykonywanie, utrzymywanie i testowanie kopii zapasowych mają kluczowe znaczenie dla procesu odzyskiwania danych w przypadku wystąpienia incydentu związanego

z cyberbezpieczeństwem lub awarii systemu.

Dodatkowe wytyczne dotyczące ustalania priorytetów oraz opracowywania strategii tworzenia kopii zapasowych można znaleźć w następujących dokumentach:

- NSC 800-34, *Poradnik Planowania Awaryjnego*
- NSC 800-209, *Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych*

Zalecenia i wytyczne dotyczące systemów OT

Należy opracować listę wszystkich kopii zapasowych, w tym nośników instalacyjnych, kluczy licencyjnych i informacji dotyczących konfiguracji.

Należy podjąć dodatkowe działania w celu zapewnienia, że kopie zapasowe będą dostępne w razie wystąpienia zdarzenia, w tym między innymi:

- Weryfikację kopii zapasowych pod kątem niezawodności i integralności (jeśli jest to technicznie możliwe).
- Utworzenie lokalizacji dla kopii zapasowych, która będzie dostępna dla wszystkich pracowników, którzy mogą potrzebować dostępu podczas przywracania systemu.
- Utworzenie alternatywnej lokalizacji przechowywania dodatkowych kopii zapasowych, aby zagwarantować, że zdarzenie wpływające na podstawową kopię danych nie wpłynie na kopię zapasową ani nie doprowadzi do jej zniszczenia. Oznacza to na przykład przechowywanie danych na temat logiki sterowników PLC oraz plików konfiguracyjnych poza organizacją, w innej lokalizacji, która nie ulegnie zniszczeniu w wyniku zdarzenia, które doprowadziło do zniszczenia sterownika PLC.
- Przetestowanie procesu przywracania danych z kopii zapasowej w ramach testowania planu odzyskiwania danych po katastrofie.
- Upewnienie się, że procedury tworzenia kopii zapasowych są uwzględnione w procesach zarządzania konfiguracją lub zmianami.
- Zabezpieczanie kopii zapasowych zgodnie z wymogami w zakresie kontroli dostępu.
- Monitorowanie warunków środowiskowych w miejscach, w których przechowywane są nośniki kopii zapasowych.

6.2.4.4. FIZYCZNE ŚRODOWISKO ROBOCZE (PR.IP-5)

Zarządzanie fizycznym środowiskiem roboczym obejmuje zabezpieczenia awaryjne, w tym awaryjny wyłącznik systemu, oświetlenie awaryjne, zasilanie awaryjne, zapewnienie odpowiedniej temperatury i wilgotności oraz ochronę przed pożarem i zalaniem. Organizacje powinny opracować zasady i procedury w celu zapewnienia stosownych warunków środowiska roboczego dla zasobów.

Zalecenia i wytyczne dotyczące systemów OT

Organizacje powinny wziąć pod uwagę następujące czynniki w procesie określania środków przeciwdziałania i ochrony środowiska roboczego:

- **Czynniki środowiskowe.** Czynniki środowiskowe mogą mieć znaczący wpływ na środowisko robocze. Na przykład, jeśli obszar jest zapylony, systemy powinny być umieszczone w filtrowanym miejscu, zwłaszcza jeśli pył może przewodzić prąd (pył węglowy) lub mieć właściwości magnetyczne (pył żelazny). Jeśli problem mogą stanowić drgania, systemy powinny być montowane na gumowych tulejach, aby zapobiec awariom dysków twardych i problemom z połączeniami kablowymi. Ponadto środowiska, w których znajdują się systemy i nośniki (np. taśmy z kopiami zapasowymi, dyskietki) powinny charakteryzować się stabilną temperaturą i wilgotnością. W przypadku przekroczenia norm środowiskowych, takich jak temperatura lub wilgotność, powinien być uruchamiany alarm.
- **Systemy zapewniające warunki środowiskowe.** Systemy ogrzewania, wentylacji i klimatyzacji (systemy HVAC) w pomieszczeniach sterowania powinny umożliwiać normalną pracę pracowników odpowiedzialnych za systemy OT oraz reagowanie w sytuacjach awaryjnych, które mogą wiązać się z uwolnieniem substancji toksycznych. Oceny ryzyka powinny uwzględniać ryzyko związane z korzystaniem z systemu ogrzewania, wentylacji i klimatyzacji (np. wlotów powietrza) w przypadku uwolnienia toksycznych substancji, a także podtrzymania pracy systemu podczas przerwy w dostawie prądu (np. dzięki wykorzystaniu zasilacza awaryjnego w przypadku krytycznych procesów). Systemy przeciwpożarowe powinny być zaprojektowane w taki sposób, by nie spowodować nieprzewidzianych zniszczeń, na przykład w wyniku kontaktu produktów z wodą.

Systemy ogrzewania, wentylacji i klimatyzacji oraz systemy przeciwpożarowe odgrywają istotną rolę ze względu na współzależność sterowania procesem i bezpieczeństwa. Na przykład systemy przeciwpożarowe oraz systemy ogrzewania, wentylacji i klimatyzacji, które obsługują przemysłowe komputery sterujące, muszą być chronione przed incydentami związanymi z cyberbezpieczeństwem.

- **Systemy zasilania.** Niezawodne zasilanie systemów OT jest jednym z najważniejszych wymogów, dlatego kluczowe systemy powinny być podłączone do zasilania bezprzerwowego (UPS). Jeśli w obiekcie znajduje się generator awaryjny, czas pracy zasilacza bezprzerwowego może wynosić zaledwie kilkanaście sekund. W przypadku, gdy zakład wykorzystuje zasilanie zewnętrzne, czas pracy zasilacza bezprzerwowego powinien wynosić wiele godzin. Zasilacz powinien być dobrany w taki sposób, by umożliwić co najmniej bezpieczne wyłączenie systemu.

6.2.4.5. PLANY REAGOWANIA I PRZYWRACANIA SYSTEMU (PR.IP-9) ORAZ TESTOWANIE PLANÓW REAGOWANIA I PRZYWRACANIA SYSTEMU (PR.IP-10)

Organizacje powinny opracować i aktualizować plany reagowania, w tym plany dotyczące reagowania na incydenty i utrzymanie ciągłości prowadzenia działalności. Plany reagowania powinny być dostosowane do świadczonych usług, nie zaś wyłącznie do systemu, którego zasady ochrony zostały naruszone. Organizacje powinny wdrożyć systematyczne podejście do opracowywania planów reagowania, na przykład oparte na procesie opisanym w dokumencie CISA Cybersecurity Incident and Vulnerability Response Playbooks [CISA-CIVR].Typowe etapy planowania obejmują przygotowanie, wykrywanie i analizę, ograniczenie skutków, przywracanie, działania po wystąpieniu incydentu, komunikację i koordynację. Organizacje powinny również regularnie dokonywać przeglądów i aktualizować swoje plany reagowania.

Plany reagowania powinny być udokumentowane w formie papierowej lub w systemie odłączonym od sieci, który jest chroniony przed skutkami cyberataku. Poszczególne osoby powinny zostać przeszkolone w zakresie tego, gdzie znaleźć plan reagowania i jakie

działania należy podjąć w ramach reagowania na incydenty. Ponadto podczas przygotowywania planu reagowania na incydenty należy uzyskać informacje od różnych zainteresowanych stron, w tym od operatorów, inżynierów, pracowników działu IT, dostawców usług wsparcia, przedstawicieli kierownictwa, organizacji pracowników, działu prawnego oraz pracowników odpowiedzialnych za bezpieczeństwo. Interesariusze ci powinni również przejrzeć i zatwierdzić plan reagowania.

Planowanie ciągłości działania dotyczy utrzymania lub przywrócenia produkcji w przypadku jej przerwania. Przywrócenie systemu po katastrofie może zająć wiele dni, tygodni lub miesięcy, natomiast w przypadku infekcji złośliwym oprogramowaniem, awarii mechanicznej lub elektrycznej odtwarzanie może potrwać kilka minut lub godzin. Plany ciągłości działania (*ang. Business continuity plans – BCPs*) często zakładają wystąpienie wielu rodzajów incydentów obejmujących szereg różnych obszarów. Plan ciągłości działania dotyczący incydentów związanych z cyberbezpieczeństwem powinien obejmować długotrwałe awarie, w tym konieczność odtworzenia po katastrofie, a także krótkotrwałe awarie, które wymagają przywrócenia środowiska pracy. Konieczna jest współpraca z pracownikami odpowiedzialnymi za ochronę fizyczną przy opracowywaniu planu ciągłości działania związanego z incydentami dotyczącymi cyberbezpieczeństwa. Współpraca ta powinna obejmować opracowanie listy krytycznych urządzeń oraz powiązanych środków przeciwdziałania związanych z zapobieganiem incydentom.

Przed utworzeniem planu ważne jest określenie czasu odzyskiwania dla różnych systemów i podsystemów w oparciu o typowe potrzeby biznesowe. Istnieją dwa różne rodzaje celów – cele dotyczące odtworzenia systemu oraz odzyskania danych. Odtwarzanie systemu obejmuje odtwarzanie połączeń komunikacyjnych i możliwości przetwarzania. Zwykle cele te określa się w kategoriach czasu odzyskiwania (RTO). Przedstawiciele kierownictwa powinni określić akceptowalny czas odzyskiwania, a pracownicy techniczni powinni podjąć działania w celu osiągnięcia tego celu. Odzyskiwanie danych obejmuje proces odzyskiwania danych opisujących warunki produkcji lub produktu. Zwykle cele te określa się w kategoriach punktu odtworzenia danych (*ang. recovery point objective – RPO*). Cel ten określa przedział czasu, w którym brak dostępu do danych jest dopuszczalny. Oba te parametry mogą uzasadniać

inwestycje w zapasowe urządzenia, jeśli osiągnięcie ustalonych celów jest niemożliwe w inny sposób.

Po określeniu celów należy utworzyć listę potencjalnych czynników powodujących zakłócenia oraz opracować i opisać procedurę odtwarzania. Następnie należy opracować plany awaryjne obejmujące możliwe zakłócenia. Plan awaryjny powinien zostać zweryfikowany we współpracy z przedstawicielami kierownictwa, którzy powinni zatwierdzić koszty jego realizacji. W przypadku wielu awarii i problemów na mniejszą skalę, zapas kluczowych części zamiennych prawdopodobnie okaże się wystarczający do osiągnięcia celów w zakresie czasu odzyskiwania. W przypadku wystąpienia incydentu na większą skalę konieczne może być wykorzystanie relacji z dostawcami. Niezależnie od rodzaju procesu odtwarzania, kluczowe znaczenie mają kopie zapasowe danych.

Plan odtworzenia po katastrofie stanowi udokumentowany proces lub zestaw procedur, które obejmują kompleksowy program działań naprawczych, które należy podjąć zarówno przed katastrofą, jak i w trakcie katastrofy oraz po jej wystąpieniu. Plan ten jest zwykle utrwalany zarówno w formie elektronicznej, jak i papierowej, aby zapewnić jego dostępność niezależnie od rodzaju zdarzenia (katastrofy naturalnej, katastrofy środowiskowej lub wypadku spowodowanego umyślnie lub nieumyślnie przez człowieka). Organizacje powinny opracowywać, utrzymywać i weryfikować plany odtwarzania swoich środowisk po katastrofie, aby zminimalizować wpływ zdarzeń przez skrócenie czasu wymaganego do przywrócenia pełnej funkcjonalności systemów.

Niektóre organizacje mogą dysponować planami reagowania kryzysowego i powinny rozważyć wykorzystanie istniejących planów podczas opracowywania planu reagowania na zdarzenia związane z cyberbezpieczeństwem. Dodatkowe wskazówki dotyczące praktyk w zakresie opracowywania planów reagowania można znaleźć w następujących dokumentach:

- NSC 800-34, *Poradnik Planowania Awaryjnego*
- NSC 800-61 *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego*
- NIST SP 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling_ for Desktops and Laptops*

- NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)*
- CISA, *Handling Destructive Malware*
- Federal Emergency Management Agency (FEMA) National Incident Management System (NIMS)
- FEMA National Preparedness Goal

Zalecenia i wytyczne dotyczące systemów OT

Planowanie reagowania na incydenty może obejmować następujące elementy:

- **Identyfikacja i klasyfikacja incydentów.** Różne rodzaje incydentów dotyczących systemów OT powinny zostać zidentyfikowane i sklasyfikowane w oparciu o ich potencjalny wpływ w celu ustalenia odpowiedniego sposobu reagowania na każdy potencjalny incydent.
- **Reagowanie.** Reakcja na incydent może obejmować zarówno niepodejmowanie żadnych działań, jak i pełne wyłączenie systemu, co może spowodować zatrzymanie fizycznego procesu. Wybór sposobu reagowania jest uzależniony od rodzaju incydentu i jego wpływu na system OT oraz proces fizyczny. Należy przygotować pisemny plan reakcji na każdy rodzaj incydentu. Plan ten stanowi źródło wytycznych oraz informacji na temat postępowania w czasie wystąpienia incydentu oraz ogranicza zamieszanie i panikę spowodowaną sytuacją. Plan ten powinien zawierać opisy kolejnych działań podejmowanych przez poszczególnych interesariuszy. W planie powinny znaleźć się wymagania dotyczące raportowania wraz z informacjami kontaktowymi i formatem przekazywanych informacji, aby ograniczyć ryzyko wystąpienia nieporozumienia. Działania powinny obejmować wykrywanie, analizę, ograniczenie skutków, usunięcie zagrożenia, odtwarzanie oraz działania po incydencie. Niektóre zagadnienia dotyczące systemów OT mogą obejmować:
  - Określenie priorytetu działań – na przykład najszybszego przywrócenia normalnego działania lub przeprowadzenie dochodzenia i zabezpieczenie danych na potrzeby organów ścigania.
  - Komunikację z zespołem odpowiedzialnym za reagowanie na incydenty.

- Odłączenie zainfekowanych systemów od sieci.
- Fizyczne odizolowanie niezależnych sieci (np. sieci organizacji od sieci sterowania bądź sieci sterowania od sieci środków bezpieczeństwa).
- Przełączenie systemu na sterowanie ręczne.
- Zapewnienie dodatkowego wsparcia w celu ręcznej weryfikacji danych.
- Powiadomienie zarządu, działu komunikacji lub zewnętrznych podmiotów i jednostek zgodnie z wymaganiami.

W przypadku wykrycia incydentu organizacje powinny przeprowadzić ukierunkowaną ocenę ryzyka dla środowiska OT, aby ocenić skutki ataku i możliwości reagowania. Jedną z możliwych opcji jest fizyczne odizolowanie atakowanego systemu. Może to jednak mieć negatywny wpływ na środowisko OT, a przeprowadzenie takiego działania może nie być możliwe ze względu na wpływ na wydajność lub bezpieczeństwo systemu. Należy wykorzystać w takiej sytuacji szacowanie ryzyka w celu określenia działań, które należy podjąć.

Plan powinien również określać wymagania dotyczące wymiany komponentów w przypadku awarii. Jeśli to możliwe, zamienniki trudnych do pozyskania komponentów powinny być dostępne w magazynie organizacji.

Organizacja powinna skutecznie ustalać priorytety działań związanych z odtwarzaniem systemu. Proces ten może opierać się na istniejącej dokumentacji, na przykład na ocenach ryzyka lub procedurach uruchamiania systemu. Proces może koncentrować się na odtwarzaniu systemów obsługujących krytyczne narzędzia przed odtworzeniem systemów obsługujących produkcję w oparciu o kolejność rozruchu.

Testowanie procedur planu odtwarzania w przypadku komponentów OT może być trudne ze względu na wymogi dotyczące dostępności i bezpieczeństwa. Organizacje mogą być zmuszone do ustalenia, czy możliwe jest przeprowadzenie testów na sucho lub symulacji w celu weryfikacji procedur odtwarzania systemów OT. Organizacje powinny zweryfikować integralność kopii zapasowych w przypadku braku możliwości wykonania pełnego testu odtwarzania.

6.2.5. UTRZYMANIE (ANG. MAINTENANCE – PR.MA)

Rezultaty wchodzące w skład kategorii Utrzymanie ram cyberbezpieczeństwa określają wytyczne dotyczące przeprowadzania rutynowej i zapobiegawczej konserwacji komponentów systemu informacyjnego. Działania te obejmują korzystanie z lokalnych i zdalnych narzędzi oraz zarządzanie pracownikami odpowiedzialnymi za utrzymanie.

Zalecenia i wytyczne dotyczące systemów OT

Rozwiązania do planowania konserwacji umożliwiają organizacji planowanie, śledzenie, autoryzację, monitorowanie i kontrolowanie działań konserwacyjnych i naprawczych w systemach OT oraz zapewnienie, że działania oraz zmiany są odpowiednio udokumentowane.

Dokumentowanie tych zdarzeń prowadzi do powstania ścieżki audytu, co może pomóc w rozwiązywaniu problemów związanych z cyberbezpieczeństwem, reagowaniu na incydenty oraz realizacją działań związanych z odtwarzaniem systemów.

Dokumentacja konserwacji zapewnia także wgląd w zaplanowaną obsługę urządzeń OT i może pomóc w podejmowaniu decyzji o zakończeniu ich eksploatacji.

Oprogramowanie używane do przeprowadzania czynności konserwacyjnych w systemach OT powinno być zatwierdzone i weryfikowane przez organizację. Zatwierdzone oprogramowanie należy uzyskać bezpośrednio od dostawców i zweryfikować jego autentyczność (np. poprzez sprawdzenie certyfikatów lub porównanie skrótów kryptograficznych plików instalatora).

Każda konserwacja dotycząca urządzeń OT może doprowadzić do przypadkowej zmiany konfiguracji i spowodować zwiększenie powierzchni ataku. Należy dbać o utwardzanie urządzeń OT niezależnie od przeprowadzanych konserwacji. Konfigurację urządzenia należy zweryfikować po zakończeniu konserwacji i aktualizacji oprogramowania – niektóre funkcje mogą zostać przypadkowo włączone lub zainstalowane wraz z poprawkami. Należy skorzystać z najlepszych praktyk oraz dokumentacji przekazanej przez producenta urządzenia w celu przeprowadzenia konserwacji.

Ograniczenie korzystania z niektórych urządzeń wyłącznie w celu przeprowadzania czynności konserwacyjnych może pomóc w ograniczeniu ryzyka naruszenia zasad

ochrony urządzenia w wyniku przypadkowego podłączenia go do sieci zewnętrznej, udostępnienia nieautoryzowanym użytkownikom lub kradzieży. Korzystanie w celu konserwacji z urządzeń znajdujących się w bezpiecznym środowisku OT zmniejsza poziom ryzyka. Należy ograniczyć do minimum wykorzystywanie takich urządzeń poza środowiskiem OT oraz przypadki podłączania urządzeń do sieci innych niż sieć OT.

Każde urządzenie podłączone do systemu OT powinno zostać odłączone po zakończeniu czynności konserwacyjnych, a wszelkie tymczasowe połączenia powinny zostać usunięte.

Działanie, możliwości i funkcje urządzeń wykorzystywanych w ramach czynności konserwacyjnych powinny być znane i udokumentowane. Urządzenia mogą zawierać mechanizmy łączności bezprzewodowej oraz być wyposażone w inne urządzenia komunikacyjne, które mogą być podatne na ataki typu *side-channel* lub mogą umożliwiać jednoczesne połączenia do wielu sieci. Aby poznać te funkcje, należy zapoznać się z dokumentacją producenta.

6.2.6. TECHNOLOGIA ZABEZPIECZAJĄCA (ANG. PROTECTIVE TECHNOLOGY – PR.PT)

Technologie i rozwiązania techniczne pomagają organizacjom chronić urządzenia i dane znajdujące się w ich środowiskach. Zastosowanie technologii może samo w sobie nie wystarczyć do utrzymania zdolności do ochrony przed nowymi zagrożeniami. W związku z tym organizacje powinny wdrażać rozwiązania techniczne zabezpieczające ich zasoby zgodnie z zasadami, procedurami i umowami.

6.2.6.1. DOKUMENTACJA I REJESTROWANIE (PR.PT-1)

Dokumentacja i rejestrowanie zdarzeń umożliwiają organizacji gromadzenie danych na temat zdarzeń występujących w jej systemach i sieciach. Zdarzenia mogą być generowane przez wiele różnych systemów, w tym systemy operacyjne, stacje robocze, serwery, urządzenia sieciowe, oprogramowanie zapewniające cyberbezpieczeństwo i aplikacje.

Dodatkowe wytyczne znajdują się w następującym dokumencie:

- NIST SP 800-92, *Guide to Computer Security Log Management*

Zalecenia i wytyczne dotyczące systemów OT

Gromadzenie danych na temat zdarzeń w plikach dziennika ma kluczowe znaczenie dla zapewnienia dostępu do informacji na temat działania systemu OT. Typowe zdarzenia obejmują funkcje utrzymania (tj. kontrola dostępu, zmiany konfiguracji, tworzenie kopii zapasowych i ich przywracanie), funkcje systemu operacyjnego i zdarzenia aplikacji (tj. procesów). Rodzaje rejestrowanych zdarzeń mogą być różne w zależności od urządzenia OT i powinny być wybierane w oparciu o możliwości urządzenia, a także potrzeby w zakresie rejestrowania.

Każdy wpis w pliku dziennika powinien jednoznacznie wskazywać urządzenie, które wygenerowało zdarzenie, znacznik czasu zdarzenia oraz konto użytkownika lub systemu, które wygenerowało zdarzenie. Każdy wpis powinien również obejmować miejsce wystąpienia zdarzenia, rodzaj zdarzenia, czas wystąpienia zdarzenia, źródło zdarzenia, tożsamość wszystkich użytkowników lub kont systemowych związanych ze zdarzeniem oraz rezultat zdarzenia.

Zestawienie zdarzeń zarejestrowanych przez wiele urządzeń OT może być trudne, jeśli znaczniki czasu zdarzeń generowane przez urządzenia nie są oparte na wspólnym źródle czasu. Wewnętrzne zegary każdego urządzenia powinny być zsynchronizowane z zegarem głównym, aby umożliwić korelację zdarzeń udokumentowanych na wielu urządzeniach. Wpisy w pliku dziennika powinny zawierać znaczniki czasu w jednolitym formacie (np. formacie strefy czasowej, ciągu znaków, czasu letniego).

Funkcje gromadzenia i przekazywania informacji na temat zdarzeń mogą wpływać na wydajność urządzeń OT. W zależności od częstotliwości rejestrowanych zdarzeń, rozmiar pliku dziennika może szybko rosnąć i zajmować coraz większą ilość dostępnej przestrzeni w pamięci urządzenia. Większość urządzeń OT charakteryzuje się ograniczoną przestrzenią dyskową oraz pamięcią operacyjną, w związku z czym należy zapewnić dostęp do pamięci masowej (lokalnej lub zdalnej), aby zmniejszyć prawdopodobieństwo zapełnienia pamięci urządzenia, co może spowodować utratę możliwości rejestrowania zdarzeń. Należy przemyśleć możliwość przeniesienia plików dziennika z urządzeń OT do innej pamięci masowej.

6.2.7. OCHRONA NOŚNIKÓW (ANG. MEDIA PROTECTION - PR.PT-2)

Nośniki wymienne powinny być chronione, a korzystanie z nich winno być ograniczone zgodnie z obowiązującymi zasadami. Zasady te obejmują opisywanie nośników w celu określenia wymogów w zakresie dystrybucji oraz zasad postępowania, a także wymogów dotyczących przechowywania, transportu, sanityzacji, niszczenia oraz utylizacji nośników.

Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NIST SP 800-88, Rev. 1, *Guidelines for Media Sanitation*
- NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)*
- NSC 800-209, *Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych*

Zalecenia i wytyczne dotyczące systemów OT

Należy opracować i wdrożyć procesy oraz procedury dotyczące nośników oraz ich obsługi. Kategoria nośników danych obejmuje nośniki wymienne oraz inne urządzenia, w tym dyskietki, płyty CD, DVD, karty SD i pamięci USB, a także drukowane sprawozdania i dokumenty. Fizyczne środki bezpieczeństwa powinny uwzględniać konkretne wymagania dotyczące bezpiecznego przechowywania tych nośników. Należy także opracować wytyczne dotyczące transportu nośników, odpowiedniego postępowania z nośnikami, a także usuwania ich zawartości oraz fizycznego niszczenia nośników. Wymogi dotyczące bezpieczeństwa mogą obejmować przechowywanie nośników w sposób chroniący je przed zgubieniem, pożarem, kradzieżą, niezamierzonym ujawnieniem lub szkodami środowiskowymi.

Urządzenia OT powinny być chronione przed niewłaściwym użyciem nośników. Używanie jakichkolwiek nieautoryzowanych nośników wymiennych lub urządzeń na urządzeniu podłączonym do systemu OT powinno być zabronione. Stosowne zabezpieczenia mogą obejmować procedury oraz zabezpieczenia techniczne, których celem jest przeciwdziałanie wprowadzeniu złośliwego oprogramowania lub spowodowaniu nieumyślnego zniszczenia lub kradzieży danych.

Fizyczna ochrona nośników lub szyfrowanie danych na nośnikach ma kluczowe znaczenie dla ochrony środowiska OT przed zagrożeniami. Uzyskanie dostępu do nośników zawierających dane dotyczące systemu OT może dostarczyć napastnikowi cennych informacji umożliwiających przeprowadzenie skutecznego ataku.

6.2.8. BEZPIECZEŃSTWO PRACOWNIKÓW (*ANG. PERSONNEL SECURITY*)

Kwestia cyberbezpieczeństwa powinna być uwzględniona także w procedurach dotyczących pracowników, aby zmniejszyć ryzyko wystąpienia błędu ludzkiego, kradzieży, oszustwa lub innego celowego lub niezamierzonego wykorzystania systemów informacyjnych.

Dodatkowe wskazówki dotyczące praktyk w zakresie bezpieczeństwa pracowników można znaleźć w następujących dokumentach:

- NIST SP 800-35, *Guide to Information Technology Security Services*
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification*
- NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*
- NSC 800-100, *Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających (wer. 1.0)*

Zalecenia i wytyczne dotyczące systemów OT

Ogólny program bezpieczeństwa pracowników powinien obejmować opracowanie zasad, określenie ryzyka związanego z poszczególnymi stanowiskami, weryfikację pracowników, stworzenie procedur dotyczących zakończenia stosunku pracy, przeniesienia pracownika, umów dotyczących dostępu, a także ról i obowiązków podmiotów zewnętrznych. Pracownicy odpowiedzialni za systemy OT powinni komunikować się z działami kadr, IT i bezpieczeństwa fizycznego, aby upewnić się, że wymogi zostaną spełnione.

Organizacja powinna uwzględnić zawieranie umów dotyczących dostępu oraz wdrożenie formularzy próśb o uzyskanie dostępu fizycznego lub logicznego do urządzeń i systemów OT. Organizacje powinny również weryfikować pracowników na kluczowych stanowiskach odpowiedzialnych za nadzorowanie oraz utrzymanie systemów OT.

Ponadto każdy pracownik powinien przejść szkolenie uwzględniające wszystkie zagadnienia związane z pełnionymi obowiązkami. Fizyczny i logiczny dostęp do systemów OT powinien przysługiwać wyłącznie pracownikom wykazującym się stosownymi kompetencjami. Organizacje powinny rozważyć wdrożenie systemu takiego jak National Initiative for Cybersecurity Education (NICE) Framework w celu stosownego przeszkolenia pracowników odpowiedzialnych za systemy OT.

6.2.9. ŁĄCZNOŚĆ BEZPRZEWODOWA (ANG. WIRELESS COMMUNICATIONS)

Systemy łączności bezprzewodowej wykorzystują częstotliwości fal radiowych w celu transmisji danych. Systemy te obejmują zarówno sieci lokalne Wi-Fi działające w oparciu o protokoły IEEE 802.11, jak i łączność za pośrednictwem sieci komórkowych oraz inne metody komunikacji radiowej. Rozwiązania bezprzewodowe zapewniają większą elastyczność w porównaniu z tradycyjnymi rozwiązaniami w zakresie łączności przewodowej. Takie rozwiązania są jednak bardziej podatne na zakłócenia i mogą umożliwiać podsłuchiwanie transmisji przez nieautoryzowane osoby.

Dodatkowe wskazówki dotyczące praktyk w zakresie komunikacji bezprzewodowej można znaleźć w następujących dokumentach:

- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11*
- NIST SP 800-121, Rev. 2, *Guide to Bluetooth Security*
- NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*
- NIST SP 800-187, *Guide to LTE Security*

Zalecenia i wytyczne dotyczące systemów OT

Decyzja o tymczasowym lub stałym korzystaniu z systemów łączności bezprzewodowej w ramach środowisk OT stanowi jedną z decyzji opartych na ryzyku określonym przez organizację. Urządzenia wykorzystujące metody łączności bezprzewodowej powinny zostać umieszczone w oddzielnym segmencie sieci i wykorzystywane tylko w sytuacjach, w których ryzyko szczątkowe dla zdrowia, bezpieczeństwa, środowiska i finansów zostanie uznane za niskie.

Przed wdrożeniem takich urządzeń należy przeprowadzić badanie sieci bezprzewodowej w celu określenia lokalizacji anten i siły sygnału, aby zapewnić

odpowiedni zasięg i zminimalizować narażenie sieci bezprzewodowej na zakłócenia spowodowane czynnikami związanymi ze środowiskiem OT oraz możliwość podsłuchania komunikacji. Napastnicy mogą używać anten kierunkowych, aby zwiększyć efektywny zasięg sieci bezprzewodowej.

Organizacje mogą zdecydować się na wykorzystanie bezprzewodowej sieci typu *mesh* w celu zwiększenia odporności na takie ataki lub ograniczenia występowania obszarów charakteryzujących się słabą siłą sygnału. Sieci typu *mesh* zapewniają większą odporność na awarie, ponieważ umożliwiają wybór alternatywnych tras oraz przełączanie urządzeń w przypadku awarii sieci. Organizacje powinny wziąć pod uwagę możliwy wpływ wdrożenia sieci typu *mesh* na wydajność i bezpieczeństwo systemów. Przykładem zagadnień, jakie należy wziąć pod uwagę, jest na przykład tymczasowa utrata łączności podczas przełączania sieci. Zastosowanie funkcji przełączania może wymagać wdrożenia innych zabezpieczeń w celu skrócenia czasu. Organizacje wdrażające systemy łączności bezprzewodowej muszą równoważyć dodatkowe możliwości i ryzyko związane z cyberbezpieczeństwem, aby ograniczyć poziom ryzyka do dopuszczalnej wartości.

Bezprzewodowe sieci lokalne

- Komunikacja urządzeń bezprzewodowych powinna być szyfrowana. Jednocześnie korzystanie z funkcji szyfrowania nie może wpływać na wydajność operacyjną urządzeń. Zmniejszenie opóźnień związanych z szyfrowaniem może wymagać włączenia funkcji szyfrowania w warstwie 2 modelu OSI zamiast w warstwie 3. Należy również przeanalizować możliwość wykorzystania akceleratorów sprzętowych w celu realizacji funkcji kryptograficznych.
- Bezprzewodowe punkty dostępowe powinny stanowić niezależne segmenty sieci – nie powinny stanowić rozszerzenia istniejących segmentów. Powinny także być wykorzystywane w połączeniu z urządzeniami zabezpieczającymi dostęp do sieci w celu ograniczenia komunikacji oraz jej ochrony.
- Bezprzewodowe punkty dostępowe powinny być skonfigurowane w taki sposób, by rozgłaszały wyjątkowy identyfikator sieci (SSID) i umożliwiały co najmniej filtrowanie sprzętowych adresów kart sieciowych (MAC).

- Wykorzystanie urządzeń bezprzewodowych może wymagać wdrożenia dodatkowych zabezpieczeń i wprowadzenia stosownego podziału na strefy.
- Należy także rozważyć możliwość wykorzystania adaptacyjnego protokołu trasowania (routingu), jeśli urządzenia bezprzewodowe są wykorzystywane w roli urządzeń mobilnych. Czas konwergencji sieci powinien być tak krótki, jak to możliwe, aby umożliwić szybkie przywrócenie sieci w przypadku awarii lub utraty zasilania.

Bezprzewodowe sieci terenowe

Podczas wdrażania bezprzewodowej sieci terenowej należy wziąć pod uwagę następujące funkcje bezpieczeństwa:

- Wybór standardowego, niezastrzeżonego protokołu (np. IEEE 802.15.x)
- Zapewnienie szyfrowania między urządzeniami polowymi a bezprzewodowymi punktami dostępowymi.
- Dopisanie urządzeń do menedżera urządzeń bezprzewodowych, aby uniemożliwić połączenie niepożądanych urządzeń z siecią.
- Konfiguracja odpowiednio złożonych haseł i kluczy dostępu.

Większość bezprzewodowych sieci terenowych jest z natury mniej niezawodna niż ich przewodowe odpowiedniki ze względu na ich podatność na zagłuszanie sygnału, ograniczenia odległości i wymagania dotyczące widoczności anten. Należy nawiązać współpracę z producentem systemu, aby zaprojektować sieć bezprzewodową odpowiednią dla danego zastosowania.

6.2.10. ZDALNY DOSTĘP (ANG. REMOTE ACCESS)

Należy wdrożyć zabezpieczenia, aby zapobiec nieautoryzowanemu zdalnemu dostępowi do sieci, systemów i danych organizacji. Wirtualna sieć prywatna (VPN) to zestaw protokołów zaprojektowanych do obsługi bezpiecznego zdalnego dostępu do środowisk sieciowych. VPN może zapewnić zarówno silne uwierzytelnianie, jak i szyfrowanie w celu zabezpieczenia danych komunikacyjnych poprzez ustanowienie sieci prywatnej, która pełni rolę nakładki działającej w oparciu o infrastrukturę publiczną. Najpopularniejsze typy technologii VPN to:

- **Internet Protocol Security (IPsec).** IPsec obsługuje dwa tryby szyfrowania – transportowy i tunelowy. Tryb transportowy szyfruje tylko część danych (tj. zawartość) każdego pakietu, pozostawiając nagłówek pakietu niezaszyfrowany. Bardziej bezpieczny tryb tunelowania dodaje nowy nagłówek do każdego pakietu i szyfruje zarówno oryginalny nagłówek, jak i zawartość pakietu. Po stronie odbiorczej urządzenie zgodne z protokołem IPsec odszyfrowuje każdy pakiet.
- **Transport Layer Security (TLS).** Protokół określany także starszą nazwą – Secure Sockets Layer (SSL). Umożliwia stworzenie bezpiecznego kanału połączenia między dwoma urządzeniami i szyfruje zawartość każdego pakietu. Protokół TLS jest zwykle wykorzystywany w celu zabezpieczenia ruchu HTTP w ramach bezpiecznego rozszerzenia HTTPS. Stosowanie protokołu TLS nie jest jednak ograniczone do ruchu HTTP i może być używane do zabezpieczania wielu programów warstwy aplikacji. W każdym wypadku należy wykorzystywać protokół TLS w wersji 1.2 lub nowszej.
- **Secure Shell (SSH).** SSH to interfejs poleceń i protokół służący do bezpiecznego uzyskiwania dostępu do zdalnego komputera. Jest on powszechnie używany przez administratorów sieci do zdalnego kontrolowania serwerów pracujących pod kontrolą systemu operacyjnego Linux. SSH jest bezpieczną alternatywą dla aplikacji telnet, jest zawarty w większości dystrybucji systemów z rodziny UNIX, możliwa jest też jego instalacja na innych platformach dzięki dodatkowym pakietom.

Dodatkowe wskazówki dotyczące praktyk w zakresie kontroli dostępu można znaleźć w następujących dokumentach:

- NIST SP 800-52, Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*[14]
- NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*
- NIST SP 800-77, Rev. 1, *Guide to IPsec VPNs*
- NIST SP 800-113, *Guide to SSL VPNs*

[14] Polska wersja – NSC 800-52, *Wskazówki dotyczące wyboru, konfigurowania i wykorzystania implementacji TLS (ang. Transport Layer Security)*

Zalecenia i wytyczne dotyczące systemów OT

Wiele architektur bezpieczeństwa systemów OT obejmuje wiele poziomów, które ilustruje między innymi model Purdue. Takie rozwiązanie ogranicza możliwości dostępu, co ogranicza ryzyko przypadkowego lub celowego zakłócenia działania tych systemów. W związku z tym należy opracować oraz wdrożyć w organizacji proces składania wniosków oraz przyznawania uprawnień do zdalnego dostępu. Zdalny dostęp powinien być możliwy tylko w uzasadnionych sytuacjach, a jego zakres ograniczony do możliwości wymaganych ze względów biznesowych. Przyznanie zdalnego dostępu nie może wiązać się z ominięciem lub wyłączeniem zabezpieczeń. Należy rozważyć wdrożenie uwierzytelniania wieloskładnikowego MFA na potrzeby zdalnego dostępu do systemów OT.

W sytuacjach krytycznych lub gdy potrzebne jest wsparcie producenta, konieczne może być udzielenie tymczasowego dostępu zdalnego w celu przeprowadzenia konserwacji. W takich przypadkach nadal należy postępować zgodnie z procedurami gwarantującymi korzystanie z bezpiecznych połączeń.

Istnieje kilka różnych technik wdrażania tymczasowego dostępu zdalnego, w tym:

- Wykorzystywanie kont użytkowników oraz protokołów (np. RDP, SSH) dopuszczonych przez zaporę sieciową wykorzystywaną w sieci OT lub w sieci organizacji.
- Wykorzystywanie programów do udostępniania ekranu.
- Wykorzystywanie modemów.
- Wykorzystywanie sieci VPN.

Niezależnie od technologii, organizacje powinny uwzględnić następujące zagadnienia:

- Wykorzystywanie wyjątkowych nazw użytkowników i złożonych haseł.
- Usuwanie, wyłączanie lub modyfikowanie domyślnych poświadczeń.
- Aktualizowanie oprogramowania i oprogramowania układowego do najnowszych wersji.
- Wyłączenie dostępu zdalnego, gdy nie jest już potrzebny. Należy uwzględnić możliwość wyłączania dostępu zdalnego po upływie zadanego czasu lub wdrożenie procesu zarządzania zmianą w celu potwierdzenia wyłączenia dostępu.

- Monitorowanie zdalnych działań w systemie.
- Należy upewnić się, że pracownicy odpowiedzialni za systemy OT są świadomi prac i działań zdalnych planowanych w środowisku OT.
- Połączenie powinno zostać zainicjowane ze środowiska OT.
- Należy oznaczyć urządzenia wykorzystywane do dostępu zdalnego, aby umożliwić ich szybkie odłączenie w przypadku nieautoryzowanego użycia.

Modemy Dial-Up

Jeśli modemy dial-up (modemy wdzwaniane) są używane w środowiskach OT, należy zastanowić się nad wdrożeniem systemów oddzwaniania. Dzięki temu można zapewnić, że osoba wykonująca połączenie jest autoryzowanym użytkownikiem – modem ustanawia połączenie robocze na podstawie posiadanych informacji oraz numeru przechowywanego na liście autoryzowanych użytkowników.

Jeśli jest to możliwe, modemy powinny zostać odłączone, gdy nie są używane. W innym wypadku należy rozważyć automatyzację procesu odłączania poprzez wyłączanie połączeń po określonym czasie. W niektórych przypadkach ustanawianie połączeń za pośrednictwem modemów stanowi element umowy o świadczenie usług wsparcia z producentem (zapewniającej na przykład wsparcie techniczne dostępne 24 godziny na dobę, 7 dni w tygodniu i gwarantujące 15-minutowy czas reakcji). Pracownicy organizacji powinni być świadomi, że odłączenie lub usunięcie modemów może wymagać renegocjacji umów.

Wykorzystywanie sieci VPN

Urządzenia VPN używane do ochrony systemów OT powinny być dokładnie przetestowane w celu sprawdzenia, czy technologia VPN jest kompatybilna z danym rozwiązaniem i czy wdrożenie urządzeń VPN nie wpływa negatywnie na działanie ruchu sieciowego.

Technologia VPN może być również stosowana pomiędzy różnymi segmentami sieci. Przykładowo, w zdalnej lokalizacji może znajdować się urządzenie do ochrony brzegu sieci, które wykorzystuje technologię VPN do ustanowienia bezpiecznego tunelu przez niezaufaną sieć (np. Internet) do urządzenia obsługującego sieć VPN w głównym centrum sterowania w innej lokalizacji.

6.2.11. KORYGOWANIE BŁĘDÓW I ZARZĄDZANIE POPRAWKAMI

Poprawki to fragmenty kodu, które zostały opracowane w celu rozwiązania określonych problemów lub błędów w istniejącym oprogramowaniu. Systematyczne podejście do zarządzania poprawkami oraz ich instalowania może pomóc organizacji w zwiększeniu ogólnego bezpieczeństwa ich systemów w przystępny cenowo sposób. Organizacje wdrażające proaktywne metody zarządzania poprawkami oraz ich instalacją ograniczają możliwości wykorzystania podatności w swoich systemach, a także oszczędzają czas i pieniądze przeznaczone na reagowanie na incydenty związane z podatnościami.

Dokument NIST SP 800-40, Rev. 4 [SP800-40r4] zawiera wytyczne dla CIO, CISO i innych osób odpowiedzialnych za zarządzanie ryzykiem w organizacji związanym z korzystaniem z oprogramowania. Dokument ten uwzględnia instalowanie poprawek jako kluczowy element konserwacji zapobiegawczej technologii informacyjnych, jeden z kosztów prowadzenia działalności oraz działanie niezbędne dla realizacji misji organizacji. Autorzy publikacji omawiają także czynniki wpływające na zarządzanie poprawkami w organizacji oraz zalecają opracowanie strategii mającej na celu usprawnienie oraz wdrożenie procedur instalowania poprawek w sposób ograniczający ryzyko. Wytyczne te mogą być również przydatne dla osób odpowiedzialnych za misje i procesy biznesowe, a także inżynierów i architektów bezpieczeństwa, administratorów systemów i pracowników odpowiedzialnych za zapewnienie bezpieczeństwa systemów.

Dodatkowe wskazówki dotyczące praktyk w zakresie korygowania błędów i zarządzania poprawkami można znaleźć w dokumencie:

- NIST SP 800-40, Rev. 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*

Zalecenia i wytyczne dotyczące systemów OT

Podczas instalowania poprawek komponentów systemu operacyjnego należy zachować szczególną ostrożność. Poprawki powinny być odpowiednio przetestowane (na przykład na osobnym systemie testowym) w celu sprawdzenia, czy ewentualny wpływ na wydajność oraz działanie systemu jest dopuszczalny.

Zalecane jest również przeprowadzenie testów regresji. W wielu przypadkach zainstalowane poprawki mogą mieć negatywny wpływ na inne oprogramowanie. Oznacza to, że pomimo tego, że poprawka usuwa podatność lub lukę w zabezpieczeniach, jej instalacja może skutkować zwiększonym ryzykiem z punktu widzenia produkcji lub bezpieczeństwa. Instalacja poprawki może również zmienić sposób, w jaki system operacyjny lub aplikacja współpracuje z aplikacjami sterującymi, w związku z czym aplikacja sterująca może utracić część swoich funkcji. Wiele systemów OT działa pod kontrolą starszych wersji systemów operacyjnych, które nie są już obsługiwane przez producenta. W związku z tym odpowiednie poprawki mogą nie być już dostępne.

Organizacja powinna wdrożyć systematyczny, rozliczalny oraz udokumentowany proces zarządzania poprawkami w środowiskach OT w celu zarządzania ryzykiem związanym z podatnościami. Proces zarządzania poprawkami powinien uwzględniać wytyczne dotyczące sposobu monitorowania publikacji poprawek, określania czasu instalacji, sposobu testowania poprawek (np. we współpracy z producentami lub w osobnych systemach testowych) oraz sposobu wybierania zabezpieczeń kompensacyjnych w celu ograniczenia narażenia podatnego systemu, gdy instalacja poprawki jest niemożliwa.

CISA publikuje informacje na temat wielu podatności dotyczących systemów i komponentów systemów OT. Nie wszyscy producenci zgłaszają jednak znane podatności do CISA. Organizacje mogą otrzymywać informacje o podatnościach śledząc publikacje producentów i dostawców, a także alerty i informacje publikowane przez CISA. Także prywatne spółki zajmujące się cyberbezpieczeństwem oferują usługi w zakresie rozpowszechniania informacji na temat znanych podatności systemów OT. Na organizacji spoczywa odpowiedzialność za pozyskiwanie bieżących informacji oraz ustalanie, w jakich sytuacjach należy zainstalować stosowne poprawki, korzystając w tym celu z udokumentowanego procesu zarządzania poprawkami.

Decyzję na temat instalowania poprawek podejmują pracownicy odpowiedzialni za systemy OT. Należy rozważyć oddzielenie zautomatyzowanego procesu zarządzania poprawkami systemów OT od zautomatyzowanego procesu zarządzania poprawkami dotyczącego innych systemów. Instalowanie poprawek powinno odbywać się podczas planowanych przerw konserwacyjnych.

Niektóre organizacje są objęte specjalnymi wytycznymi branżowymi i sektorowymi dotyczącymi zarządzania poprawkami. W przypadku braku takich wytycznych organizacja może opracować własne procedury zarządzania poprawkami w oparciu o istniejące normy opisane w dokumentach NIST SP 800-40, Rev. 4 [SP800-40r4]; NERC CIP-007 lub ISA 62443-2-3, Patch Management in the IACS Environment.

6.2.12. SYNCHRONIZACJA CZASU (*ANG. TIME SYNCHRONIZATION*)

Rozwiązania do synchronizacji czasu umożliwiają synchronizowanie zegarów wielu urządzeń działających w organizacji. Takie rozwiązanie jest niezwykle ważne z wielu powodów, pośród których można wymienić zestawianie zdarzeń oraz plików dziennika, zapewnienie prawidłowego działania mechanizmów uwierzytelniania, a także systemów kontroli dostępu i jakości usług.

Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST IR 8323, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*

Zalecenia i wytyczne dotyczące systemów OT

Synchronizacja wewnętrznych zegarów systemów i komponentów systemów OT ma kluczowe znaczenie dla korelacji zdarzeń związanych z cyberbezpieczeństwem oraz innych funkcji realizowanych przez systemy OT, w tym między innymi sterowania ruchem.

Jeśli zegar urządzenia lub systemu jest niedokładny, znaczniki czasu generowane we wpisach plików dziennika będą również niedokładne, podobnie jak wszelkie inne funkcje wykorzystujące czas podawany przez zegar.

Wszystkie urządzenia OT powinny wykorzystywać jednolity czas. Wykorzystanie wielu źródeł czasu może wiązać się z szeregiem korzyści, ponieważ pozwala na ograniczenie błędów oraz zapewnienie zapasowych źródeł czasu w przypadku awarii podstawowego źródła lub błędów.

Uwierzytelniony protokół synchronizacji czasu (*ang. Network Time Protocol - NTP*) i bezpieczny protokół Precision Time Protocol (PTP), tj. PTP z uwierzytelnianiem TLV

[typ, długość, wartość] mogą być wykorzystywane, jeśli istnieje ryzyko modyfikacji czasu sieciowego (np. zagłuszanie fal radiowych, fałszowanie pakietów, atak odmowy świadczenia usługi). Nieuwierzytelniony protokół NTP jest podatny na spoofing, a serwery NTP powinny znajdować się za zaporą sieciową.

Źródła czasu działające w środowisku OT powinny być uwzględnione w programach monitorowania systemów i sieci. Jeśli jest to możliwe, pliki dziennika z każdego źródła czasu (np. syslog) powinny być gromadzone w systemie gromadzącym pliki dziennika.

6.3. WYKRYWAJ (ANG. DETECT – DE)

Funkcja Wykrywaj umożliwia opracowanie i wdrożenie odpowiednich działań mających na celu stwierdzenie wystąpienia zdarzenia związanego z cyberbezpieczeństwem.

6.3.1. ANOMALIE I ZDARZENIA (*ANG. ANOMALIES AND EVENTS – DE.AE*)

Zrozumienie przez organizacje różnych zdarzeń, anomalii oraz ich potencjalnego wpływu na systemy i środowisko stanowi skuteczną możliwości ich wykrywania. W każdym środowisku niemal nieprzerwanie występują liczne nieszkodliwe i potencjalnie szkodliwe zdarzenia i anomalie. Niektóre powszechne przykłady zdarzeń obejmują:

Zdarzenia informatyczne

- Wielokrotne nieudane próby logowania
- Zablokowane konta
- Nieautoryzowane tworzenie nowych kont
- Nieoczekiwane zdalne logowania (na przykład logowania pracowników na urlopach, zdalne logowania pracowników przebywających na terenie organizacji, zdalne logowanie na konto konserwacyjne, gdy nie jest wymagana konserwacja)
- Wyczyszczone dzienniki zdarzeń
- Niespodziewanie pełne dzienniki zdarzeń
- Alerty oprogramowania antywirusowego lub wykrywającego włamania
- Wyłączony program antywirusowy lub inne środki bezpieczeństwa

- Prośby o udzielenie informacji na temat systemu lub architektury (na przykład inżynieria społeczna lub próby phishingu)

Zdarzenia operacyjne

- Nieautoryzowane zmiany konfiguracji
- Nieautoryzowana instalacja poprawek bezpieczeństwa
- Nieplanowane wyłączenia i przestoje

Zdarzenia związane z dostępem fizycznym

- Nieautoryzowane wejścia na teren organizacji.

Zdarzenia związane z siecią

- Nieoczekiwane połączenia bądź użycie nowych portów lub protokołów bez przeprowadzenia kompleksowego procesu zarządzania zmianą
- Nieoczekiwany duży ruch sieciowy
- Połączenia ze strony nieautoryzowanych urządzeń łączących się z siecią
- Nieautoryzowana komunikacja z zewnętrznymi adresami IP

Organizacje winny pamiętać o fakcie, że nie wszystkie zdarzenia i anomalie mają złośliwy charakter i wymagają dogłębnej analizy. Z tego powodu konieczne jest określenie progów ostrzeżeń oraz wymogów dotyczących reagowania na zdarzenia i anomalie, które mają wpływ na systemy i środowisko, aby uzyskać możliwość skutecznego wykrywania incydentów.

Z tego powodu należy rozważyć gromadzenie i zestawianie danych o zdarzeniach z wielu źródeł i czujników przy użyciu zautomatyzowanych mechanizmów wszędzie tam, gdzie to możliwe, aby zwiększyć możliwości wykrywania incydentów oraz ostrzegania o ich występowaniu. Przykład może stanowić scentralizowany system wykrywania włamań gromadzący dane i dzienniki z wielu urządzeń i segmentów sieci, aby identyfikować zdarzenia specyficzne dla organizacji lub środowiska i uruchamiać alarm. Narzędzia umożliwiające wykrywanie zdarzeń powinny być również zintegrowane z narzędziami do zarządzania zasobami. Integracja ta może zapewnić dostęp do dodatkowych informacji kontekstowych dotyczących zdarzenia (na przykład

dotyczących lokalizacji fizycznej systemu, wersji oprogramowania układowego czy krytyczności systemu), aby pomóc w ustaleniu stopnia wpływu zdarzenia.

Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems*
- NIST SP 1800-7, *Situational Awareness for Electric Utilities*

Zalecenia i wytyczne dotyczące OT

Organizacje powinny uwzględnić w swoich procesach oraz środowiskach zdarzenia i anomalie dotyczące OT. Należy także pamiętać, że niektóre narzędzia, podobnie jak alerty dotyczące zachowań lub zdarzeń wskazujących na wystąpienie włamania, mogą być typowymi narzędziami, zachowaniami i zdarzeniami w środowisku OT. Aby ograniczyć liczbę fałszywych i powtarzalnych alarmów, należy ustanowić oddzielne progi alarmowe dla systemów OT na podstawie wartości bazowych dla normalnego ruchu sieciowego i przepływów danych, a także normalnego zachowania procesów realizowanych przez pracowników oraz systemy OT. Należy wziąć pod uwagę, że komponenty systemów OT znajdują się w odległych lokalizacjach fizycznych i nie są stale obsługiwane przez pracowników. W związku z tym progi alarmowe muszą uwzględniać czas reakcji związany z alarmem. Za przykład może posłużyć próg alarmu związanego ze zbyt wysoką temperaturą, który może wymagać ustawienia niższego progu uruchomienia alarmu, aby uwzględnić oczekiwany czas reakcji na podjęcie działań w celu zapobieżenia incydentowi.

W systemach OT często wykorzystywane są współdzielone dane poświadczające. Nietypowe zachowania na współdzielonych kontach mogą być trudniejsze do zaobserwowania, dlatego organizacje powinny zastanowić się, czy w tej sytuacji wymagane są dodatkowe środki bezpieczeństwa, takie jak zabezpieczenie korzystania ze współdzielonych danych poświadczających przy pomocy monitorowania dostępu fizycznego.

6.3.2. CIĄGŁE MONITOROWANIE BEZPIECZEŃSTWA (*ANG. SECURITY CONTINUOUS MONITORING – DE.CM*)

Podmioty winny wdrożyć metody ciągłego monitorowania jako jeden z elementów strategii zarządzania ryzykiem organizacyjnym w celu monitorowania skuteczności zabezpieczeń. Działanie to powinno obejmować ustalenie częstotliwości przeprowadzania ocen rezultatów.

Ciągłe monitorowanie może być procesem realizowanym przez pracowników wewnętrznych lub wykonawców zewnętrznych, co pozwoli na identyfikację luk w zabezpieczeniach środowiska. Autorzy dokumentu zachęcają do przeprowadzania wzajemnych ocen przez pracowników różnych oddziałów tego samego podmiotu. W przypadku korzystania z usług firm zewnętrznych w zakresie ciągłego monitorowania bezpieczeństwa ważne jest zrozumienie oraz ocena sposobów ochrony danych przez podmiot zewnętrzny. Podmioty zewnętrzne gromadzące dane z monitorowania wielu podmiotów mogą stać się celem dla napastników. Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NSC 800 53A, *Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych i organizacjach*
- NIST SP 800-55, Rev. 1, *Performance Measurement Guide for Information Security*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) _ for Federal Information Systems and Organizations*
- NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*

Zalecenia i wytyczne dotyczące OT

Organizacje mogą uznać, że automatyzacja w środowiskach OT może nie być możliwa ze względu na wrażliwość systemów lub zapotrzebowanie na zasoby wymagane do jej obsługi. Na przykład niektóre zautomatyzowane systemy mogą wykorzystywać aktywne skanowanie w celu zarządzania podatnościami, poprawkami lub weryfikacji poprawności konfiguracji urządzeń. Rozwiązania, które wykorzystują aktywne

skanowanie lub lokalne zasoby w celu obsługi automatyzacji, powinny zostać przetestowane przed wdrożeniem w systemie OT.

Ciągłe monitorowanie można realizować za pośrednictwem zautomatyzowanych narzędzi, poprzez pasywne skanowanie lub ręczne monitorowanie wykonywane z częstotliwością uznaną za współmierną do ryzyka. Na przykład na podstawie oceny ryzyka można ustalić, że pliki dziennika z izolowanych (odłączonych od sieci), niekrytycznych urządzeń powinny być przeglądane co miesiąc przez osoby odpowiedzialne za systemy OT w celu ustalenia, czy występują anomalie. Zastosowanie pasywnego monitora sieci może pozwolić na wykrycie podatnych na atak usług sieciowych bez konieczności skanowania urządzeń.

Kiedy organizacje wdrażają metodykę opartą na próbkowaniu, należy wziąć pod uwagę krytyczność komponentów. Należy zadbać o to, by proces próbkowania nie omijał urządzeń charakteryzujących się wyższym poziomem ryzyka, takich jak zapory sieciowe warstwy 3 lub 4 modelu OSI.

Korzystając z usług podmiotów zewnętrznych w celu ciągłego monitorowania zabezpieczeń należy upewnić się, że zatrudniony personel posiada odpowiedni zestaw umiejętności pozwalający na przeprowadzanie analiz środowisk OT.

6.3.2.1. MONITOROWANIE SIECI *(ANG. NETWORK MONITORING – DE.CM-1)*

Monitorowanie sieci obejmuje przeglądanie alertów oraz plików dzienników, a także analizy pod kątem występowania oznak możliwych incydentów związanych z cyberbezpieczeństwem. Organizacje powinny rozważyć automatyzację tych czynności, w tym rozwiązania opracowane przez pracowników wewnętrznych, rozwiązania dostępne na rynku lub zestawy narzędzi opracowane w celu wsparcia monitorowania. Narzędzia oraz rozwiązania pozwalające na wykrywanie anomalii w zakresie zachowań (BAD), zarządzanie bezpieczeństwem informacji i zdarzeniami (*ang. security information and event management – SIEM*), systemy wykrywania włamań (ang. *intrusion detection systems – IDS*) i systemy prewencji włamań (*ang. intrusion prevention systems – IPS*) mogą pomóc organizacjom w monitorowaniu ruchu w całej sieci i generowaniu alarmów, gdy zidentyfikują nietypowy lub podejrzany ruch. Inne rozwiązania, które należy uwzględnić w kontekście monitorowania sieci, obejmują:

- Zarządzanie zasobami, w tym wykrywanie i inwentaryzacja urządzeń podłączonych do sieci informatycznej;
- Ustalenie poziomu bazowego typowego ruchu sieciowego, przepływów danych i komunikacji między urządzeniami;
- Diagnostykę problemów z wydajnością sieci;
- Identyfikację błędów w konfiguracji lub nieprawidłowego działania urządzeń sieciowych;

Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST IR 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*

Zalecenia i wytyczne dotyczące OT

Monitorowanie sieci pozwala na znaczące zwiększenie możliwości wykrywania ataków pochodzących z sieci OT lub wymierzonych w sieć OT. Pozwala także na poprawę wydajności sieci dzięki wykrywaniu nieistotnego ruchu. Osoby odpowiedzialne za cyberbezpieczeństwo systemów OT muszą uczestniczyć w procesie diagnostycznym polegającym na interpretowaniu alertów zgłaszanych przez narzędzia do monitorowania sieci. Uważne monitorowanie i zrozumienie normalnego stanu sieci OT może pomóc w skutecznym rozpoznawaniu przejściowych problemów oraz rzeczywistych ataków oraz zrozumieniu anomalii i zdarzeń.

Uzyskanie dostępu do ruchu sieciowego jest zwykle możliwe za pośrednictwem punktów dostępu testowego (*ang. test access points – TAP*) i analizatora portów przełącznika (*ang. switched port analyzer – SPAN*), jednak ich użycie może wpływać na sprawność systemu OT, zwłaszcza w przypadku wykorzystania rozwiązania SPAN.

W celu skutecznego monitorowania sieci OT należy wykorzystywać czujniki i analizatory. W typowych instalacjach czujniki sieciowe znajdują się między siecią sterowania a siecią korporacyjną, choć można je zastosować także w innych lokalizacjach, na przykład na brzegach sieci, w najważniejszych segmentach (na przykład w strefie zdemilitaryzowanej) oraz przy krytycznych urządzeniach OT.

Wszystkie czujniki powinny zostać poddane kompleksowym testom i wdrożone w środowisku testowym przed ich wprowadzeniem do sieci OT. Ustawienie trybu testowego lub nauki po zainstalowaniu czujnika w sieci zapewnia możliwość dostrojenia urządzenia do rzeczywistego ruchu w sieci OT. Wykonanie tej czynności może pomóc w ograniczeniu liczby fałszywych alarmów, informacji związanych z regularnym ruchem sieciowym oraz problemów z wdrożeniem i konfiguracją czujników.

W przypadku wykorzystania czujników należy uwzględnić sposób ich zachowania w przypadku awarii, na przykład czy w przypadku wystąpienia problemu czujnik pozostaje otwarty, czy automatycznie ulega zamknięciu.

6.3.2.2. MONITOROWANIE UŻYTKOWANIA SYSTEMU (ANG. SYSTEM USE MONITORING – DE.CM-1 ORAZ DE-CM-3)

Rozwiązania do monitorowania użytkowania systemu umożliwiają organizacji monitorowanie, zapisywanie oraz audytowanie zdarzeń systemowych (na przykład systemowych plików dziennika, uruchomionych procesów, uzyskiwania dostępu do plików i ich modyfikacji, zmian konfiguracji systemu i aplikacji), które mają miejsce w systemie. Monitorowanie użytkowników i systemów pomaga upewnić się, że zachowują się zgodnie z oczekiwaniami i może pomóc w rozwiązywaniu problemów w przypadku wystąpienia zdarzeń dzięki dostarczeniu informacji na temat użytkowników, którzy pracowali w systemie, gdy doszło do zdarzenia. Pozwala także na wykrycie błędnych konfiguracji systemu i urządzeń.

W porównaniu do rozwiązań w zakresie monitorowania sieci, rozwiązania przeznaczone do monitorowania użytkowania systemu są w stanie analizować aktywności, które nie mają miejsca w sieci. W przypadku rozwiązań uruchamianych na hostach można to osiągnąć poprzez monitorowanie w czasie rzeczywistym komunikacji międzyprocesowej i innych wewnętrznych danych systemu operacyjnego, podczas gdy rozwiązania wykorzystujące aktywne skanowanie zbierają informacje poprzez odpytywanie systemu operacyjnego lub interfejsów programowania aplikacji (API). Dodatkowe wytyczne znajdują się w następujących dokumentach:

- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

Zalecenia i wytyczne dotyczące OT

Świadomość sytuacyjna dotycząca systemu OT jest niezbędna w celu ustalenia aktualnego stanu systemu, sprawdzenia, czy działa on zgodnie z przeznaczeniem i upewnienia się, że żadne naruszenia zasad lub incydenty związane z cyberbezpieczeństwem nie utrudniły jego działania. Dokładne monitorowanie urządzeń, tworzenie dzienników i audyt są niezbędne do gromadzenia, korelowania i analizowania informacji związanych z bezpieczeństwem oraz zapewniania praktycznej komunikacji na temat stanu bezpieczeństwa w całym systemie OT. W przypadku incydentu związanego z cyberbezpieczeństwem, informacje zebrane przez rozwiązania monitorujące wykorzystanie systemu mogą zostać zastosowane do przeprowadzenia analizy systemu OT.

Rozwiązania do monitorowania użycia systemu mogą generować znaczne ilości danych na temat zdarzeń, w związku z czym powinny być używane w połączeniu z systemem zarządzania plikami dzienników, takim jak SIEM, umożliwiającym filtrowanie różnych typów zdarzeń i ograniczenie zmęczenia namiarem alertów. Zakres dostosowywania zdarzeń i alertów zależy od typu systemu OT i liczby urządzeń w systemie.

Rozwiązania do monitorowania użytkowania systemu powinny być poddawane kompleksowym zakrojonym testom i wdrożone w środowisku testowym przed ich wdrożeniem na urządzeniach w systemie OT. Zagadnienia, które należy wziąć pod uwagę, obejmują wpływ wydajności agentów opartych na hostach na urządzenia, wpływ aktywnego skanowania na urządzenia oraz możliwości w zakresie przepustowości infrastruktury sieciowej. Wykorzystanie oddzielnych urządzeń pozwoli na ograniczenie obciążeń związanych z przetwarzaniem. Agenty oparte na hostach mogą wpływać na wydajność urządzenia OT ze względu na zużywane przez nie zasoby.

6.3.2.3. WYKRYWANIE ZŁOŚLIWEGO KODU (ANG. MALICIOUS CODE DETECTION – DE.CM-4)

Podczas przechowywania, przetwarzania i przesyłania pliki i strumienie danych powinny być skanowane przy użyciu specjalistycznych narzędzi wykorzystujących szereg algorytmów heurystycznych i znanych sygnatur złośliwego oprogramowania w celu

wykrywania i blokowania potencjalnie złośliwego kodu. Narzędzia do ochrony przed złośliwym kodem działają skutecznie tylko wtedy, gdy są zainstalowane, skonfigurowane, uruchamiane i nieustannie włączone, a także odpowiednio utrzymywane w celu uwzględnienia informacji na temat znanych metod ataków i ładunków.

Dodatkowe wskazówki dotyczące praktyk w zakresie ochrony przed złośliwym oprogramowaniem można znaleźć w następujących dokumentach:

- NIST SP 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 1058, *Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*

Zalecenia i wytyczne dotyczące OT

Choć narzędzia antywirusowe są powszechnie stosowane w systemach informatycznych, korzystanie z nich w systemach OT może wymagać zastosowania specjalnych praktyk, w tym zapewniania zgodności, zarządzania zmianami i oceny wpływu na wydajność systemu Praktyki te należy wykorzystywać w celu testowania nowych sygnatur i nowych wersji oprogramowania antywirusowego.

Niektórzy dostawcy systemów OT zalecają, a nawet pozwalają na korzystanie z własnych narzędzi antywirusowych. W niektórych przypadkach dostawcy systemów OT przeprowadzają testy regresji w zakresie wszystkich produktów i obsługiwanych wersji określonego narzędzia antywirusowego, a także dostarczają stosowną dokumentację instalacyjną i konfiguracyjną.

Ogólnie rzecz ujmując:

- Systemy operacyjne ogólnego przeznaczenia z rodzin Windows, Unix i Linux, wykorzystywane na stacjach roboczych, a także w roli magazynów danych, systemów operacyjnych na komputerach wykorzystywanych w celu konserwacji, a oraz serwerów kopii zapasowych, mogą korzystać z zabezpieczeń wykorzystywanych w przypadku komercyjnych urządzeń IT, takich jak oprogramowanie antywirusowe z mechanizmem ręcznego lub automatycznego instalowania aktualizacji za pośrednictwem serwera antywirusowego znajdującego

się w sieci sterowania procesem. Należy postępować zgodnie z opracowanymi przez organizację procedurami przesyłania najnowszych aktualizacji z zaufanych witryn dostawców na serwery oprogramowania antywirusowego będące częścią systemów OT oraz inne komputery i serwery należące do tych systemów.

- Należy postępować zgodnie z zaleceniami dostawcy dotyczącymi wszystkich innych serwerów i komponentów (takich jak: rozwiązania DCS, sterowniki PLC oraz inne urządzenia), które wykonują kod w czasie rzeczywistym, działają w oparciu o zmodyfikowane lub rozszerzone systemy operacyjne lub wykorzystują inne rozwiązania, które odróżniają je od standardowego komputera. Jeśli to możliwe, należy przetestować oprogramowanie antywirusowe i aktualizacje w systemie offline (na przykład poprzez instalację na zapasowym urządzeniu HMI w celu weryfikacji, czy wydajność nie uległa pogorszeniu przed instalacją na głównym urządzeniu HMI).

Zgodnie z zaleceniami zawartymi w dokumencie NIST SP 1058 [SP1058], oprogramowanie antywirusowe może wpłynąć negatywnie na procesy sterowania realizowane w czasie rzeczywistym przez systemy sterowania przemysłowego. Autorzy publikacji wskazują także znaczne zużycie zasobów procesora podczas uruchamiania ręcznego skanowania i aktualizacji sygnatur, co może mieć negatywny wpływ na komputery i serwery należące do systemu OT. W związku z powyższym:

- Konfiguracja oprogramowania antywirusowego powinna być przetestowana w systemie offline, jeśli jest to możliwe.
- Ręczne skanowanie i aktualizacje sygnatur powinny być wykonywane, gdy system nie jest kluczowy dla procesu.
- Należy rozważyć zastosowanie nadmiarowości w przypadku krytycznych systemów, które wymagają ciągłych aktualizacji oprogramowania antywirusowego w taki sposób, by aktualizacje sygnatur mogły być wykonywane bez wpływu na ich działanie (dotyczy to na przykład paneli sterowania i interfejsów człowiek-maszyna).
- Podczas konfigurowania list wykluczeń plików należy określić, które pliki aplikacji sterujących nie powinny być skanowane w czasie realizacji procesu z powodu możliwości spowodowania awarii systemu OT lub spadku wydajności.

CISA zapewnia zalecane praktyki aktualizacji oprogramowania antywirusowego w środowiskach OT.

6.3.2.4. SKANOWANIE PODATNOŚCI (ANG. VULNERABILITY SCANNING – DE.CM-8)

Podatności mogą być wykrywane za pomocą kombinacji technik automatycznych i ręcznych. Skanowanie w poszukiwaniu podatności zabezpieczeń powinno być wykonywane na bieżąco, aby dokumentować nowe podatności w miarę ich odkrywania.

Zalecenia i wytyczne dotyczące OT

Niektóre powszechnie stosowane metody wykrywania podatności w środowiskach OT obejmują:

- Ciągłe monitorowanie przy użyciu pasywnych lub aktywnych funkcji skanowania. Organizacje powinny uwzględnić możliwy wpływ narzędzi do skanowania podatności na komponenty systemu OT i komunikację, testując je w środowisku offline przed wdrożeniem ich w środowisku produkcyjnym.
    - Narzędzia do skanowania pasywnego zazwyczaj wykorzystują analizatory ruchu sieciowego do wykrywania zasobów i określania możliwych podatności w zabezpieczeniach wpływających na te zasoby.
    - Narzędzia do skanowania aktywnego zwykle wykorzystują agenty w celu łączenia się z zasobami sieciowymi i wykonywania szczegółowych zapytań i analiz komponentów w celu określenia możliwych podatności w zabezpieczeniach wpływających na zasoby.
- Testy wydajności, obciążeń i penetracyjne winny być przeprowadzane, jeśli nie wpłyną negatywnie na środowisko produkcyjne
- Należy przeprowadzać regularne audyty, oceny i weryfikacje w celu wykrywania podatności zabezpieczeń.

6.3.3. PROCES WYKRYWANIA (*ANG. DETECTION PROCESS – DE.DP*)

Proces wykrywania obejmuje utrzymywanie oraz testowanie procesów, procedur i narzędzi w celu zapewnienia, że anomalie są wykrywane niezwłocznie,

a odpowiedzialne osoby i podmioty są ostrzegane i rozliczane za podjęcie stosownych działań. Aby zapewnić ciągły wgląd w anomalie, należy określić role i obowiązki w zakresie odpowiedzialności; okresowo weryfikować, czy działania związane z wykrywaniem są zgodne z wymaganiami; regularnie testować procesy wykrywania, a także przekazywać informacje na temat wykrytych zdarzeń stosownym osobom w celu umożliwienia podjęcia działań i stałego ulepszania możliwości wykrywania.

6.4. REAGOWANIE (*ANG. RESPOND –RS*)

Reagowanie zwiększa możliwości w zakresie podejmowania stosownych działań i czynności w celu powstrzymania incydentu dotyczącego cyberbezpieczeństwa w momencie jego wystąpienia.

6.4.1. PLANOWANIE REAKCJI (*ANG. RESPONSE PLANNING – RS.RP*)

W przypadku reagowania na zdarzenia, organizacje powinny zadbać o rejestrowanie czynności związanych z realizacją udokumentowanych planów działania. Takie rozwiązanie może pomóc organizacjom zidentyfikować luki lub możliwości poprawy planu reagowania podczas procesu analizy incydentu. Ze względu na konieczność podejmowania natychmiastowych działań w zakresie reagowania, organizacje mogą uwzględnić możliwość zastosowania innych technik, takich jak: analizowanie plików dzienników, przeglądanie nagrań wideo zarejestrowanych w czasie reagowania lub przeprowadzenie rozmów z osobami biorącymi udział w procesie reagowania, jeśli dokumentacja szczegółów może wpływać na bezpieczeństwo lub wydłuża czas potrzebny na realizację planu reagowania.

6.4.2. KOMUNIKACJA W ZAKRESIE REAGOWANIA (*ANG. RESPONSE COMMUNICATIONS – RS.CO*)

Podejmowanie działań w związku z incydentem w zakresie cyberbezpieczeństwa obejmuje koordynację z wewnętrznymi i zewnętrznymi interesariuszami. Należy zebrać zespół reagowania na incydenty. W zależności od złożoności i zakresu skutków incydentu, zespół reagowania na incydenty może składać się z jednej lub wielu osób, które zostały przeszkolone w zakresie reagowania na incydenty. W celu ustanowienia wspólnej terminologii oraz funkcji poszczególnych członków zespołu reagowania na

incydenty można skorzystać z Krajowego Systemu Reagowania na Incydenty (*ang. National Incident Management System – NIMS*) opracowanego przez FEMA.

Przed wystąpieniem incydentu organizacje powinny zastanowić się nad wyborem sposobów komunikacji z osobami odpowiedzialnymi za reagowanie na incydenty oraz podmiotami zewnętrznymi, które mogą obejmować:

- Opracowanie listy dystrybucyjnej poczty elektronicznej związanej z reagowaniem na incydenty.
- Wykorzystanie systemu powiadomień alarmowych.
- Ustanowienie zapasowych planów komunikacji radiowej, telefonicznej lub pocztą elektroniczną w przypadku awarii podstawowych systemów komunikacji.
- Wyznaczenie rzecznika na potrzeby komunikacji z podmiotami zewnętrznymi.
- Wyznaczenie osoby odpowiedzialnej za wewnętrzną komunikację dotyczącą incydentów.

Zalecenia i wytyczne dotyczące OT

Organizacje powinny uwzględnić wytyczne FEMA dotyczące sytuacji kryzysowych i komunikacji w sytuacjach kryzysowych podczas opracowywania planów i strategii komunikacji.

Pracownicy odpowiedzialni za reagowanie na incydenty powinni zostać poinformowani i przeszkoleni w zakresie swoich obowiązków.

Plan reagowania powinien zawierać szczegółową listę organizacji i pracowników, z którymi należy się kontaktować w związku z reagowaniem na incydenty i w celu zgłaszania ich w różnych okolicznościach. Każdej osobie należy przypisać role wymagane na potrzeby reagowania na incydenty. Poszczególne role mogą obejmować osobę odpowiedzialną za dowodzenie, kierownika lub członka działów operacji, planowania, logistyki lub finansów/administracji, a także osoby odpowiedzialne za przekazywanie informacji, bezpieczeństwo oraz łączność.

W celu realizacji działań związanych z reagowaniem na incydenty w środowisku OT, organizacja powinna uwzględnić w planie reagowania następujące osoby:

Pracownicy wewnętrzni

- Osoba odpowiedzialna za kierowanie
- Kierownictwo działu operacji

- Pracownicy działu bezpieczeństwa
- Pracownicy dyżurni odpowiedzialni za systemy OT
- Pracownicy dyżurni działu IT
- Pracownicy działu ochrony fizycznej
- Pracownicy administracyjni
- Pracownicy działu zaopatrzenia
- Pracownicy odpowiedzialni za komunikację zewnętrzną
- Pracownicy działu prawnego

Zewnętrzni partnerzy branżowi

- Wsparcie techniczne systemów OT (na przykład dostawcy, integratorzy systemów)
- Podmioty łańcucha dostaw (na przykład dostawcy, klienci, dystrybutorzy, partnerzy biznesowi)
- Zespół reagowania na incydenty
- Dodatkowi pracownicy wsparcia
- Przedstawiciele społeczności dotkniętej skutkami incydentu (na przykład mieszkańcy w sąsiedztwie organizacji).

Organizacje są zobowiązane do zgłaszania incydentów zgodnie z obowiązującymi przepisami i zarządzeniami wewnętrznymi.

Działy prawne mogą pomóc w opracowaniu umów o zachowaniu poufności lub innych umów, jeśli organizacja planuje wykorzystać zasoby zewnętrzne w zakresie reagowania na incydenty. Warto rozważyć opracowanie tych umów przed wystąpieniem incydentu, aby reakcja na incydent mogła być natychmiastowa. Ponadto organizacje mogą zawierać umowy z prywatnymi spółkami w zakresie reagowania na incydenty związane z systemami OT.

6.4.3. ANALIZA REAKCJI NA INCYDENT (*ANG. RESPONSE ANALYSIS – RS.AN*)

Incydenty dotyczące cyberbezpieczeństwa winny być analizowane w celu przeprowadzenia skutecznego procesu reagowania i stosownych działań naprawczych

zgodnie z procesem wykrywania i planem reagowania. Analiza obejmuje przegląd powiadomień, ustalenie, czy wymagane jest dochodzenie, ustalenie potencjalnego wpływu, przeprowadzenie analiz, kategoryzację incydentu zgodnie z planem reagowania oraz analizę ujawnionych podatności w zabezpieczeniach.

Dodatkowe wskazówki dotyczące praktyk w zakresie analizy reakcji na incydent można znaleźć w następujących dokumentach:

- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*

Zalecenia i wytyczne dotyczące OT

Określając ogólne skutki incydentu dotyczącego cyberbezpieczeństwa, należy wziąć pod uwagę zależności systemów OT i wynikający z nich wpływ na działalność organizacji.

System OT może być na przykład zależny od środowiska informatycznego – przykładowo incydent w sieci IT może spowodować odłączenie lub wyłączenie systemu OT.

Jeśli organizacja nie dysponuje odpowiednimi zasobami lub możliwościami do wykonania analizy systemu OT oraz przeprowadzenia dochodzenia, należy rozważyć zatrudnienie zewnętrznych organizacji do realizacji stosownych czynności.

Organizacje powinny identyfikować i klasyfikować incydenty związane z cyberbezpieczeństwem oraz inne incydenty wpływające na systemy OT zgodnie z planem reagowania na incydenty.

Podczas opracowywania planu reagowania na incydenty związane z systemami OT należy uwzględnić szereg kategorii incydentów, które mogą obejmować między innymi przypadkowe działania podjęte przez upoważnionych pracowników, a także złośliwe ataki wycelowane w określone systemy oraz w samą organizację.

6.4.4. OGRANICZANIE SKUTKÓW INCYDENTU (*ANG. RESPONSE MITIGATION – RS.MI*)

Ograniczanie skutków incydentu ma na celu zapobieganie rozszerzaniu się skutków oraz usunięcie szkód. Wszelkie działania w tym zakresie winny przebiegać zgodnie z planem reagowania.

Zalecenia i wytyczne dotyczące OT

Należy wziąć pod uwagę, że komponenty systemów OT często znajdują się w odległych lokalizacjach fizycznych i nie są stale obsługiwane przez pracowników.

W takich przypadkach należy zastanowić się nad przebiegiem reakcji na incydent w takiej sytuacji oraz uwzględnić dodatkowy czas wymagany do jej skoordynowania. System może wymagać uwzględnienia na etapie projektowania możliwości minimalizowania wpływu do czasu przybycia pracowników na miejsce (takich jak zdalne wyłączenie lub odłączenie).

Łagodzenie skutków incydentów w zakresie cyberbezpieczeństwa może obejmować wyłączenia procesów lub przerwy w komunikacji, które mają wpływ na operacje. Wpływ ten powinien być uwzględniony oraz komunikowany w trakcie ograniczania skutków incydentu.

6.4.5. USPRAWNIENIA W ZAKRESIE REAGOWANIA NA INCYDENTY (*ANG. RESPONSE IMPROVEMENTS – RS.IM*)

Działania organizacji w zakresie reagowania na incydenty winny być usprawniane poprzez uwzględnienie wniosków wyciągniętych z bieżących i poprzednich działań w zakresie wykrywania incydentów i reagowania na ich wystąpienie. Organizacje powinny wyznaczyć osobę lub osoby odpowiedzialne za dokumentowanie działań w zakresie reagowania i przekazywanie informacji zespołowi reagowania na incydenty, które będzie można następnie przeanalizować pod kątem wyciągniętych wniosków.

6.5. PRZYWRACANIE DZIAŁANIA SYSTEMÓW (*ANG. RECOVER – RC*)

Niezwłoczne przywrócenie normalnego działania systemów ma kluczowe znaczenie w procesie reagowania na incydenty związane z cyberbezpieczeństwem. Krok ten obejmuje opracowywanie i wdrażanie działań mających na celu utrzymanie odporności systemu i zapewnienie niezwłocznego przywrócenia systemów i usług objętych zakresem incydentu w zakresie cyberbezpieczeństwa.

6.5.1. PLANOWANIE PRZYWRACANIA DZIAŁANIA (*ANG. RECOVERY PLANNING – RC.RP*)

Podczas przywracania działania po wystąpieniu zdarzenia organizacje powinny podjąć próbę dokumentacji szczegółów dotyczących realizacji udokumentowanych planów przywracania. Dokumentacja realizacji może pomóc organizacji w realizacji procesu analizy incydentu i ustaleniu, czy należy uwzględnić jakiekolwiek podatności lub wprowadzić zmiany do planów. Ze względu na konieczność podejmowania natychmiastowych działań w zakresie przywracania działania systemów, organizacje mogą uwzględnić możliwość zastosowania innych technik, takich jak analizowanie plików dzienników, przeglądanie nagrań wideo zarejestrowanych w czasie reagowania lub przeprowadzenie rozmów z osobami biorącymi udział w procesie przywracania działania systemów, jeśli dokumentacja szczegółów może wpływać na bezpieczeństwo lub wydłuża czas potrzebny na realizację planu przywracania działania.

Dodatkowe wskazówki dotyczące praktyk w zakresie przywracania działania systemów można znaleźć w następujących dokumentach:

- NIST SP 800-184, *Guide_for Cybersecurity Event Recovery*
- NIST SP 800-209, *Security Guidelines_for Storage Infrastructure*

6.5.2. USPRAWNIENIA PLANÓW PRZYWRACANIA (*ANG. RECOVERY IMPROVEMENTS – RC.IM*)

W czasie działań naprawczych należy dokumentować podejmowane działania w celu wyciągnięcia wniosków. Wnioski te można wykorzystać do usprawniania planów i procesów przywracania działania. Dodatkowe wskazówki dotyczące praktyk w zakresie wprowadzania usprawnień do planów przywracania działania systemów można znaleźć w dokumencie:

- NIST SP 800-184, *Guide_ for Cybersecurity Event Recovery* https://doi.org/10.6028/NIST.SP.800-184

6.5.3. KOMUNIKACJA W CZASIE PROCESU PRZYWRACANIA (*ANG. RECOVERY COMMUNICATIONS – RC.CO*)

Działania naprawcze winny być koordynowane z podmiotami wewnętrznymi i zewnętrznymi. Oprócz przywrócenia sprawności operacyjnej, organizacja może wymagać podjęcia działań w zakresie zarządzania komunikacją z zewnętrznymi interesariuszami oraz naprawy reputacji. Dodatkowe wskazówki dotyczące praktyk w zakresie komunikacji w ramach przywracania działania systemów można znaleźć w dokumencie:

- NIST SP 800-184, *Guide for Cybersecurity Event Recovery*

Zalecenia i wytyczne dotyczące OT

W ramach planowania przywracania działania systemów należy opracować listę wewnętrznych i zewnętrznych zasobów i pracowników uczestniczących w tych działaniach. W przypadku wystąpienia zdarzenia lista ta powinna zostać wykorzystana do zebrania całego niezbędnego personelu zgodnie z wymaganiami, aby przeprowadzić proces przywracania systemu do działania.

Pracownicy odpowiedzialni za komunikację wewnętrzną:

Pracownicy wewnętrzni

- Pracownicy odpowiedzialni za systemy OT
- Pracownicy odpowiedzialni za systemy IT
- Pracownicy działu zaopatrzenia
- Przedstawiciele kierownictwa posiadający uprawnienia do zatwierdzania kosztów związanych z przywracaniem działania systemów
- Pracownicy magazynów

Pracownicy odpowiedzialni za komunikację zewnętrzną

- Dostawcy systemów OT
- Przedstawiciele przedsiębiorstw świadczących usługi w zakresie bezpieczeństwa, z których usług można skorzystać w celu skutecznego reagowania na incydenty oraz przywracania systemów

- Pracownicy magazynów
- Dostawcy usług dostępu do Internetu
- Osoby odpowiedzialne za atakowane systemy i potencjalne ofiary

REFERENCJE

STANDARDY I REKOMENDACJE[15]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800 52	Wskazówki dotyczące wyboru, konfigurowania i wykorzystania implementacji TLS (Transport Layer Security) NIST SP 800 52, Rev. 2
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60

[15] Standardy i rekomendacje

Tłumaczenie

STANDARDY I REKOMENDACJE[15]	
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61
NSC 800-100	Podręcznik bezpieczeństwa informacji. Przewodnik dla zarządzających - na podstawie NIST SP 800-100
NSC 800-207	Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania” - na podstawie NIST SP 800-207
NSC 800 209	Rekomendacje w zakresie bezpieczeństwa infrastruktury pamięci masowych- na podstawie NIST SP 800-209
NSC 7298	Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa
NIST SP 800 161r1_wer. 1.0_PL	Praktyki zarządzania ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw dla systemów i organizacji – na podstawie NIST SP 800-161

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[AGA12]	American Gas Association (2006) Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan. AGA Report No. 12.
[ANSI-ISA-5-1]	International Society of Automation (2009) Instrumentation Symbols and Identification, ANSI/ISA-5.1-2009. Available at https://webstore.ansi.org/Standards/ISA/ANSIISA2009
[ANSI-ISA-51-1]	International Society of Automation (1993) Process Instrumentation Terminology, ANSI/ISA-51.1-1979 (R1993). Available at https://www.isa.org/products/isa-51-1-1979-r1993-process-instrumentation-termin
[ANSI-ISA-84]	Instrumentation, Systems, and Automation Society (2004) Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware, and Software Requirements. ANSI/ISA-84.00.01-2004 Part 1. Available at https://webstore.ansi.org/standards/isa/ansiisa8400012004part
[ATTACK-ICS]	The MITRE Corporation (2022) *ATT&CK® for Industrial Control Systems*. Available at https://attack.mitre.org/techniques/ics/
[Bailey]	Bailey D, Wright E (2003) Practical SCADA for Industry. (IDC Technologies, Vancouver, Canada).
[Berge]	Berge J (2002) Fieldbuses for Process Control: Engineering, Operation, and Maintenance. (International Society of Automation, Research Triangle Park, North Carolina).
[Boyer]	Boyer S (2010) SCADA: Supervisory Control and Data Acquisition. 4th ed. (International Society of Automation, Research Triangle Park, North Carolina).
[CISA-CIVR]	Cybersecurity and Infrastructure Security Agency (2021) Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. Available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[16] Publikacje angielskojęzyczne zostały wymienione w celach uzupełniających dla osób zainteresowanych.

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[CNSS1253]	Committee on National Security Systems (2014) Security Categorization and Control Selection for National Security Systems. CNSS Instruction (CNSSI) No. 1253. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSS4009]	Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. CNSS Instruction (CNSSI) No. 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CSF]	National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP6
[EO13636]	Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091
[Erickson]	Erickson K, Hedrick J (1999) Plantwide Process Control. (John Wiley & Sons, Inc., New York, NY).
[FIPS140-2]	National Institute of Standards and Technology (2001) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-2, Change Notice 2 December 03, 2002. https://doi.org/10.6028/NIST.FIPS.140- 2
[FIPS140-3]	National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3
[FIPS180]	National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4
[FIPS186]	National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 186-5. https://doi.org/10.6028/NIST.FIPS.186-5

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[FIPS197]	National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 197-upd1, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1
[FIPS199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199
[FIPS200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200
[FIPS201]	National Institute of Standards and Technology (2022) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3. https://doi.org/10.6028/NIST.FIPS.201-3
[FIPS202]	National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202
[FISMA]	Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283
[IEC61511]	International Electrotechnical Commission (2016) Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements, IEC 61511-1:2016. Available at https://webstore.iec.ch/publication/24241
[IEC62264]	International Electrotechnical Commission (2013) Enterprise-control system integration - Part 1: Models and terminology, IEC 62264-1:2013. Available at https://webstore.iec.ch/publication/6675

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[IIRA19]	Industry IoT Consortium (2019) The Industrial Internet of Things Volume G1: Reference Architecture, Version 1.9. Available at https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf
[IR6859]	Falco J, Stouffer K, Wavering A, Proctor F (2002) IT Security for Industrial Control Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) 6859. Available at https://doi.org/10.6028/NIST.IR.6859
[IR8062]	Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal or Interagency Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062
[IR8183A]	Stouffer KA, Zimmerman T, Tang C, Pease M, Cichonski JA, Shah N, Downard W (2019) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 - General Implementation Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183A, Vol. 1. https://doi.org/10.6028/NIST.IR.8183A-1 Stouffer KA, Zimmerman T, Tang C, Pease M, Cichonski JA, Shah N, Downard W (2019) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 - Process-based Manufacturing System Use Case. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183A, Vol. 2. https://doi.org/10.6028/NIST.IR.8183A-2 Stouffer KA, Zimmerman T, Tang C, Pease M, Cichonski JA, Shah N, Downard W (2019) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 - Discrete-based Manufacturing System Use Case. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183A, Vol. 3. https://doi.org/10.6028/NIST.IR.8183A-3
[ISA62443]	International Society of Automation (2020) Security for industrial automation and control systems (all parts), ISA-62443. Available at https://www.isa.org/standards-and-publications/isa-standards/isa-standards- committees/isa99

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[ISADICT]	International Society of Automation [2002] The Automation, Systems, and Instrumentation Dictionary, 4th Edition. International Society of Automation.
[ISO7498-1]	ISO/IEC 7498-1:1994, Available at https://www.iso.org/standard/20269.html
[Knapp]	Knapp E (2011) Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, (Syngress, Waltham, Massachusetts).
[OMB-A130]	Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A- 130, July 28, 2016. Available at https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource
[OMB-M1917]	Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[Peerenboom]	Peerenboom J (2001) “Infrastructure Interdependencies: Overview of Concepts and Terminology.” (NSF/OSTP Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training, Washington, DC).
[PF]	National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.10
[PPD-21]	Presidential Policy Directive 21 (2013) Critical Infrastructure Security and Resilience. (The White House, Washington, DC), February 12, 2013. Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[PPD-41]	Presidential Policy Directive 41 (2016) United States Cyber Incident Coordination. (The White House, Washington, DC), July 26, 2016. Available at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[RFC4949]	Shirey R (2007) Internet Security Glossary, Version 2. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 4949. https://doi.org/10.17487/RFC4949
[Rinaldi]	Rinaldi SM, Peerenboom JP, Kelly TK (2001) "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, Vol. 21, No. 6, pp. 11-25, December 2001). https://doi.org/10.1109/37.969131
[SP1058]	Falco JA, Hurd S, Teumim D (2006) Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1058. https://doi.org/10.6028/NIST.SP.1058
[SP800-100]	Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100
[SP800-150]	Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150
[SP800-161]	Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1
[SP800-167]	Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[SP800-18r1]	Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1
[SP800-207]	Rose SW, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207
[SP800-28v2]	Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2
[SP800-30r1]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1
[SP800-34r1]	Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1
[SP800-37r2]	Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
[SP800-39]	Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[SP800-40r4]	Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4
[SP800-41r1]	Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1
[SP800-47]	Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47. https://doi.org/10.6028/NIST.SP.800-47
[SP800-53Ar5]	Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5
[SP800-53B]	Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B
[SP800-53r5]	Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5
[SP800-60v1r1]	Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1
[SP800-60v2r1]	Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

PUBLIKACJE ANGLOJĘZYCZNE[16]	
[SP800-61]	Grance T, Kent K, Kim B (2004) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61. https://doi.org/10.6028/NIST.SP.800- 61
[SP800-61r2]	Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2
[SP800-67r2]	Barker EB, Mouha N (2017) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-67, Rev. 2. https://doi.org/10.6028/NIST.SP.800-67r2
[SP800-73-4]	Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016. https://doi.org/10.6028/NIST.SP.800-73-4
[SP800-76-2]	Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2. https://doi.org/10.6028/NIST.SP.800-76-2
[SP800-78-4]	Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4. https://doi.org/10.6028/NIST.SP.800-78-4
[USC44-3552]	"Definitions," Title 44 *U.S. Code*, Sec. 3552. 2018 ed. Available at https://www.govinfo.gov/app/details/USCODE-2020-title44/USCODE-2020-title44-chap35-subchapII-sec3552
[Williams]	Williams TJ (1989) A Reference Model For Computer Integrated Manufacturing (CIM). (Instrument Society of America, Research Triangle Park, NC). Available at http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

ZAŁĄCZNIK A – LISTA SYMBOLI, SKRÓTÓW I AKRONIMÓW

Wybrane akronimy i skróty użyte w treści niniejszego opracowania zostały rozwinięte i zdefiniowane poniżej.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Akronim	Terminologia angielska	Terminologia polska
A3	Association for Advancing Automation	Stowarzyszenie na rzecz Rozwoju Automatyzacji
ABAC	Attribute-Based Access Control	Kontrola dostępu oparta na atrybutach
ACC	American Chemistry Council	Amerykańska Rada Chemii
ACI	Aviation Cyber Initiative	Nazwa własna inicjatywy w zakresie cyberbezpieczeństwa w lotnictwie
ACL	Access Control List	Lista sterowania dostępem
AES	Advanced Encryption Standard	Nazwa symetrycznego szyfru blokowego
AFPM	American Fuel and Petrochemical Manufacturers	Organizacja amerykańskich producentów paliw i produktów petrochemicznych
AGA	American Gas Association	Amerykańskie Towarzystwo Gazownicze
AHA	American Hospital Association	Amerykańskie Stowarzyszenie Szpitali
AI	Artificial Intelligence	Sztuczna inteligencja
AMA	American Medical Association	Amerykańskie Towarzystwo Medyczne
AMWA	Association of Metropolitan Water Agencies	Stowarzyszenie Wodociągów Miejskich
AO	Authorizing Official	Osoba autoryzująca
APCP	American Hospital Association Preferred Cybersecurity Provider	Preferowany dostawca usług w zakresie cyberbezpieczeństwa Amerykańskiego Stowarzyszenia Szpitali

API	American Petroleum Institute; Application Programming Interface	Amerykański Instytut Naftowy; Interfejs programistyczny aplikacji
APPA	American Public Power Association	Amerykańskie Stowarzyszenie Energetyki Publicznej
ASDSO	Association of State Dam Safety Officials	Stowarzyszenie Urzędników Odpowiedzialnych za Bezpieczeństwo Zapór Wodnych
ATO	Air Traffic Organization	Organizacja ruchu lotniczego
AWWA	American Water Works Association	Amerykańskie Stowarzyszenie Wodociągów
BAD	Behavioral Anomaly Detection	Wykrywanie anomalii w zachowaniu
BAS	Building Automation System	System automatyki budynkowej
BCP	Business Continuity Plan	Plan ciągłości działania
BES	Bulk Electric System	Rozległy system elektryczny
BPCS	Basic Process Control System	Podstawowy system sterowania procesem
C-SCRM	Cybersecurity Supply Chain Risk Management	Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w łańcuchu dostaw
CCE	Consequence-Driven Cyber-Informed Engineering	Proces inżynieryjny uwzględniający skutki i cyberbezpieczeństwo
CD	Compact Disc	Płyta kompaktowa
CDC	Cybersecurity Defense Community	Społeczność zajmująca się cyberbezpieczeństwem
CEDS	Cybersecurity for Energy Delivery Systems	Cyberbezpieczeństwo dla systemów energetycznych
CEO	Chief Executive Officer	Dyrektor generalny
CERT	Computer Emergency Response Team	Zespół reagowania na incydenty komputerowe
CESER	Cybersecurity, Energy Security, and Emergency Response	Cyberbezpieczeństwo, bezpieczeństwo energetyczne i reagowanie kryzysowe

CFATS	Chemical Facility Anti-Terrorism Standards	Standardy antyterrorystyczne dla zakładów chemicznych
CI	Critical Infrastructure	Infrastruktura krytyczna
CIE	Cyber-Informed Engineering	Proces inżynieryjny uwzględniający cyberbezpieczeństwo
CIGRE	International Council on Large Electric Systems	Międzynarodowa Rada ds. Dużych Systemów Elektrycznych
CIM	Computer Integrated Manufacturing	Komputerowo Zintegrowane Wytwarzanie
CIO	Chief Information Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne
CIP	Common Industrial Protocol, Critical Infrastructure Protection	Wspólny protokół przemysłowy, ochrona infrastruktury krytycznej
CIPAC	Critical Infrastructure Partnership Advisory Council	Komitet doradczy ds. partnerstwa na rzecz infrastruktury krytycznej
CISA	Cybersecurity and Infrastructure Security Agency	Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury
CISO	Chief Information Security Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo informacji.
CMVP	Cryptographic Module Validation Program	Program weryfikacji modułów kryptograficznych
CNSS	Committee on National Security Systems	Komitet ds. krajowych systemów bezpieczeństwa
CNSSI	Committee on National Security Systems Instruction	Wytyczne Komitetu ds. krajowych systemów bezpieczeństwa
COO	Chief Operating Officer	Dyrektor ds. operacyjnych
COTS	Commercial Off-the-Shelf	Rozwiązania komercyjne
CPNI	Centre for the Protection of National Infrastructure	Centrum Ochrony Infrastruktury Kraju
CPS	Cyber-Physical System	System cyberfizyczny
CPU	Central Processing Unit	Procesor
CRISP	Cybersecurity Risk Information Sharing Program	Program wymiany informacji o zagrożeniach dotyczących cyberbezpieczeństwa

CS3STHLM	Stockholm International Summit on Cyber Security in SCADA and ICS	Międzynarodowy szczyt w Sztokholmie poświęcony cyberbezpieczeństwu w systemach SCADA i ICS
CSET	Cyber Security Evaluation Tool	Narzędzie do oceny cyberbezpieczeństwa
CSF	Cybersecurity Framework	Ramy cyberbezpieczeństwa
CSO	Chief Security Officer	Kluczowa osoba w jednostce organizacyjnej odpowiedzialna za bezpieczeństwo.
CSRC	Computer Security Resource Center	Centrum zasobów dotyczących bezpieczeństwa komputerowego
CSRIC	Communications Security, Reliability, and Interoperability Council	Rada ds. Bezpieczeństwa Łączności, Niezawodności i Interoperacyjności
CVE	Common Vulnerabilities and Exposures	Typowe podatności i zagrożenia
CyOTE	Cybersecurity for the Operational Technology Environment	Cyberbezpieczeństwo w środowiskach technologii operacyjnych
CyTRICS	Cyber Testing for Resilient Industrial Control Systems	Testy cyberbezpieczeństwa na potrzeby budowy odpornych przemysłowych systemów sterowania
DCS	Distributed Control System	Rozproszony system sterowania
DES	Data Encryption Standard	Standard szyfrowania danych
DHCP	Dynamic Host Configuration Protocol	Protokół DHCP, protokół dynamicznego konfigurowania hostów
DHS	Department of Homeland Security	Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych
DICWG	Digital Instrumentation and Control Working Group	Grupa robocza ds. cyfrowego oprzyrządowania i sterowania
DLP	Data Loss Prevention	Zapobieganie utracie danych
DMZ	Demilitarized Zone	Strefa zdemilitaryzowana

DNP3	DNP3 Distributed Network Protocol (published as IEEE 1815)	Protokół sieciowy opublikowany w normie IEEE 1815
DNS	Domain Name System	System DNS, system nazw domen
DOE	Department of Energy	Departament Energetyki Stanów Zjednoczonych
DoS	Denial of Service	Atak odmowy świadczenia usługi
DOT	United States Department of Transportation	Departament Transportu Stanów Zjednoczonych
DRP	Disaster Recovery Plan	Plan odtworzenia po katastrofie
DSS	Digital Signature Standard	Standard podpisu cyfrowego
DVD	Digital Video Disc	Cyfrowy dysk uniwersalny
E-ISAC	Electricity Information Sharing and Analysis Center	Centrum Wymiany Informacji i Analiz dotyczących Energetyki
EM	Electromagnetic	Elektromagnetyczny
EMBS	IEEE Engineering in Medicine and Biology Society	Towarzystwo ds. Inżynierii w Medycynie i Biologii IEEE
EMP	Electromagnetic Pulse	Impuls elektromagnetyczny
EMS	Energy Management System	System zarządzania energią
EPA	United States Environmental Protection Agency	Agencja Ochrony Środowiska Stanów Zjednoczonych
EPRI	Electric Power Research Institute	Instytut Badań nad Energią Elektryczną
ERM	Enterprise Risk Management	Zarządzanie ryzykiem w podmiocie
ESD	Emergency Shutdown	Wyłączenie awaryjne
FAA	Federal Aviation Administration	Federalna Administracja Lotnictwa
FCC	Federal Communications Commission	Federalna Komisja Łączności
FDA	United States Food and Drug Administration	Amerykańska Agencja ds. Żywności i Leków
FEMA	Federal Emergency Management Agency	Federalna Agencja Zarządzania Kryzysowego
FGS	Fire and Gas System	System przeciwpożarowy i gazowy
FHWA	Federal Highway Administration	Federalna Administracja Autostrad

FIPS	Federal Information Processing Standards	Federalne standardy przetwarzania informacji
FISMA	Federal Information Security Modernization Act	Ustawa federalna dotycząca modernizacji standardów bezpieczeństwa informacji
FMCSA	Federal Motor Carrier Safety Administration	Federalna Administracja Bezpieczeństwa Przewoźników Samochodowych
FMEA	Failure Mode and Effects Analysis	Analiza przyczyn i skutków awarii
FRA	Federal Railroad Administration	Federalna Administracja Kolei
FTA	Federal Transit Administration	Federalna Administracja Transportu
FTP	File Transfer Protocol	Protokół transferu plików (nazwa protokołu)
GCC	Government Coordinating Council	Rządowa Rada Koordynacyjna
GCIP	GIAC Critical Infrastructure Protection	Ochrona infrastruktury krytycznej GIAC
GIAC	Global Information Assurance Certification	Globalny certyfikat bezpieczeństwa informacji
GICSP	Global Industrial Cyber Security Professional	Globalny specjalista ds. cyberbezpieczeństwa przemysłowego
GPS	Global Positioning System	Globalny system pozycjonowania
GRID	GIAC Response and Industrial Defense	Reagowanie i obrona środowisk przemysłowych GIAC
HART	Highway Addressable Remote Transducer Protocol	Protokół HART
HC3	Health Sector Cybersecurity Coordination Center	Centrum Koordynacji Cyberbezpieczeństwa w Sektorze Zdrowia
HHS	Health and Human Services	Ochrona zdrowia i opieka społeczna
HMI	Human-Machine Interface	Interfejs człowiek-maszyna
HR	Human Resources	Zasoby ludzkie, także kadry
HSIN	Homeland Security Information Network	Sieć informacyjna dotycząca bezpieczeństwa wewnętrznego

HSIN-CI	Homeland Security Information Network - Critical Infrastructure	Sieć informacyjna dotycząca bezpieczeństwa wewnętrznego w zakresie infrastruktury krytycznej
HTTP	Hypertext Transfer Protocol	Nazwa protokołu
HTTPS	Hypertext Transfer Protocol Secure	Nazwa protokołu
HVAC	Heating, Ventilation, and Air Conditioning	Ogrzewanie, wentylacja, klimatyzacja
I/O	Input/Output	Wejście/wyjście
I3P	Institute for Information Infrastructure Protection	Instytut Ochrony Infrastruktury Informacyjnej
IAARC	International Association for Automation and Robotics in Construction	Międzynarodowe Stowarzyszenie Automatyki i Robotyki w Budownictwie
IACS	Industrial Automation and Control System	Automatyka przemysłowa i system sterowania przemysłowego
IAEA	International Atomic Energy Agency	Międzynarodowa Agencja Energii Atomowej
ICCP	Inter-Control Center Communications Protocol	Protokół komunikacji między centrami sterowania
ICS	Industrial Control System	System sterowania przemysłowego
ICSJWG	Industrial Control Systems Joint Working Group	Wspólna grupa robocza ds. systemów sterowania przemysłowego
ICSS	Integrated Control and Safety Systems	Zintegrowane systemy sterowania i bezpieczeństwa
ID	Identification	Identyfikacja
IDS	Intrusion Detection System	System wykrywania włamań
IEC	International Electrotechnical Commission	Międzynarodowa Komisja Elektrotechniczna
IED	Intelligent Electronic Device	Inteligentne urządzenie elektroniczne
IEEE	Institute of Electrical and Electronics Engineers	Instytut Inżynierów Elektryków i Elektroników
IES	IEEE Industrial Electronics Society	Stowarzyszenie Elektroniki Przemysłowej IEEE

IETF	Internet Engineering Task Force	Grupa Robocza ds. Inżynierii Internetowej
IFIP	International Federation for Information Processing	Międzynarodowa Federacja Przetwarzania Informacji
IIC	Industry IoT Consortium, Industrial Internet of Things Consortium	Konsorcjum Przemysłowego Internetu Rzeczy
IIoT	Industrial Internet of Things	Przemysłowy internet rzeczy
INL	Idaho National Laboratory	Nazwa ośrodka badawczego
IoT	Internet of Things	Internet rzeczy
IP	Internet Protocol	Nazwa protokołu
IPS	Intrusion Prevention System	System prewencji włamań
IPsec	Internet Protocol Security	Bezpieczeństwo protokołu internetowego IP
IR	Incident Response	Reagowanie na incydenty
ISA	International Society of Automation	Międzynarodowe Stowarzyszenie Automatyki
ISAC	International Sharing and Analysis Center	Międzynarodowe Centrum Wymiany Informacji i Analiz
ISCM	Information Security Continuous Monitoring	Ciągłe monitorowanie bezpieczeństwa informacji
ISO	International Organization for Standardization	Międzynarodowa Organizacja Normalizacyjna
IT	Information Technology	Technologia informacyjna/informatyczna
ITL	Information Technology Laboratory	Laboratorium informatyczne
LAN	Local Area Network	Lokalna sieć komputerowa
LDAP	Lightweight Directory Access Protocol	Nazwa protokołu
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity	Stowarzyszenie przemysłów gazowych i naftowych w celu poprawy cyberbezpieczeństwa
MAC	Media Access Control	Kontrola dostępu do nośników

MARAD	Maritime Administration	Administracja morska
MBR	Master Boot Record	Główny rekord rozruchowy
MCAA	Measurement, Control, & Automation Association	Stowarzyszenie Pomiarów, Sterowania i Automatyki
MFA	Multi-Factor Authentication	Uwierzytelnianie wieloskładnikowe
MIB	Management Information Base	Baza danych dotyczących zarządzania
ML	Machine Learning	Uczenie maszynowe
MTU	Master Terminal Unit	Główny terminal
NAM	National Association of Manufacturers	Krajowe Stowarzyszenie Producentów
NAWC	National Association of Water Companies	Krajowe Stowarzyszenie Przedsiębiorstw Wodociągowych
NCC	National Coordinating Center for Communications	Krajowe Centrum koordynacyjne ds. Komunikacji
NEA	Nuclear Energy Agency	Agencja Energii Jądrowej
NEI	Nuclear Energy Institute	Instytut Energii Jądrowej
NERC	North American Electric Reliability Corporation	Nazwa korporacji
NESCOR	National Electric Sector Cybersecurity Resource	Krajowe zasoby w zakresie cyberbezpieczeństwa sektora energetycznego
NFS	Network File System	Nazwa protokołu
NFU	National Farmers Union	Krajowy Związek Rolników
NGFW	Next Generation Firewall	Zapora sieciowa nowej generacji
NHTSA	National Highway Traffic Safety Administration	Krajowa Administracja Bezpieczeństwa Ruchu Drogowego
NICE	National Initiative for Cybersecurity Education	Krajowa inicjatywa dotycząca edukacji w zakresie cyberbezpieczeństwa
NIH	National Institutes of Health	Narodowe Instytuty Zdrowia
NIMS	National Incident Management System	Krajowy system zarządzania incydentami
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii

NIST IR	National Institute of Standards and Technology Internal or Interagency Report	Raport wewnętrzny lub międzyagencyjny Narodowego Instytutu Standaryzacji i Technologii
NITAAC	National Institutes of Health Information Technology Acquisition and Assessment Center	Centrum Pozyskiwania i Oceny Technologii Informacyjnych Narodowych Instytutów Zdrowia
NRC	United States Nuclear Regulatory Commission	Amerykański urząd dozoru jądrowego
NREL	National Renewable Energy Laboratory	Krajowe Laboratorium Energii Odnawialnej
NTP	Network Time Protocol	Nazwa protokołu
NTSB	National Transportation Safety Board	Krajowa Rada Bezpieczeństwa Transportu
NVD	National Vulnerability Database	Krajowa baza danych dotyczących podatności na zagrożenia
OEM	Original Equipment Manufacturer	Producent oryginalnego wyposażenia
OMB	Office of Management and Budget	Agencja ds. zarządzania i budżetu
OPC	Open Platform Communications	Otwarta platforma komunikacyjna
OS	Operating System	System operacyjny
OSI	Open Systems Interconnection	Połączenie systemów otwartych
OT	Operational Technology	Technologia operacyjna
PACS	Physical Access Control System, Picture Archiving and Communications Systems	System kontroli dostępu fizycznego, systemy archiwizacji obrazów i komunikacji
PC	Personal Computer	Komputer osobisty
PERA	Purdue Enterprise Reference Architecture	Referencyjna architektura korporacyjna Purdue
PES	IEEE Power & Energy Society	Towarzystwo ds. Energetyki i Energii IEEE
PHA	Process Hazard Analysis	Analiza zagrożeń procesowych

PHM4SM	Prognostics and Health Management for Reliable Operations in Smart Manufacturing	Diagnostyka i zarządzanie stanem urządzeń dla niezawodności inteligentnej produkcji
PHMSA	Pipeline and Hazardous Materials Safety Administration	Agencja ds. bezpieczeństwa rurociągów i materiałów niebezpiecznych
PID	Proportional-Integral - Derivative	Regulator proporcjonalno – całkująco - różniczkujący
PIN	Personal Identification Number	Osobisty numer identyfikacyjny
PIV	Personal Identity Verification	Weryfikacja tożsamości
PLC	Programmable Logic Controller	Programowalny sterownik logiczny
PNNL	Pacific Northwest National Laboratory	Nazwa laboratorium
PNT	Positioning, Navigation, and Timing	Pozycjonowanie, nawigacja i synchronizacja
PPD	Presidential Policy Directive	Prezydencka dyrektywa polityczna
PRAM	Privacy Risk Assessment Methodology	Oceny ryzyka dla prywatności
PSCCC	IEEE Power System Communications and Cybersecurity	Nazwa jednostki organizacyjnej
PSS	Process Safety Shutdown	Wyłączenie procesu
PT	Pressure Transmitter	Przetwornik ciśnienia
PTP	Precision Time Protocol	Nazwa protokołu
R&D	Research and Development	Badania i rozwój
RAS	IEEE Robotics and Automation Society	Stowarzyszenie Robotyki i Automatyki IEEE
RBAC	Role-Based Access Control	Kontrola dostępu oparta na rolach
RDP	Remote Desktop Protocol	Protokół pulpitu zdalnego; nazwa własna protokołu
RF	Radio Frequency	Częstotliwość radiowa
RFC	Request for Comments	Prośba o komentarz
RFID	Radio Frequency Identification	Zdalna identyfikacja radiowa

RMF	Risk Management Framework	Ramy zarządzania ryzykiem
RPC	Remote Procedure Call	Zdalne wywołanie procedury
RPO	Recovery Point Objective	Punkt odtworzenia danych
RTO	Recovery Time Objective	Czas odzyskiwania
RTOS	Real-Time Operating System	System operacyjny czasu rzeczywistego
RTU	Remote Terminal Unit	Zdalny terminal
S4	SCADA Security Scientific Symposium	Sympozjum naukowe na temat bezpieczeństwa SCADA
SBOM	Software Bill of Materials	Specyfikacja materiałowa komponentów oprogramowania
SBU	Sensitive But Unclassified	Wrażliwe, ale nie klasyfikowane
SC	Security Category	Kategoria bezpieczeństwa
SCADA	Supervisory Control and Data Acquisition	Kontrola nadzorcza i pozyskiwanie danych
SCAI	Safety, Controls, Alarms, and Interlocks	Bezpieczeństwo, elementy sterujące, alarmy i blokady
SCC	Sector Coordinating Council	Sektorowa Rada Koordynacyjna
SD	Secure Digital	Nazwa nośnika
SDLC	Software Development Life Cycle, System Development Life Cycle	Cykl życia oprogramowania, cykl życia rozwoju systemu
SDN	Software-Defined Networking	Sieć definiowana programowo
SEPA	Smart Electric Power Alliance	Nazwa stowarzyszenia zajmującego się inteligentnymi sieciami elektrycznymi
SGCC	Smart Grid Cybersecurity Committee	Komitet ds. cyberbezpieczeństwa inteligentnych sieci elektroenergetycznych
SHA	Secure Hash Algorithm	Nazwa algorytmu
SIEM	Security Information and Event Management	Bezpieczeństwo informacji i zarządzanie zdarzeniami
SIF	Safety Instrumented Function	Przyrządowa funkcja bezpieczeństwa
SIS	Safety Instrumented System	Przyrządowy system bezpieczeństwa

SOC	Security Operations Center	Operacyjne centrum bezpieczeństwa
SOCMA	Society of Chemical Manufacturers and Affiliates	Stowarzyszenie Producentów Chemikaliów i Podmiotów Stowarzyszonych
SP	Special Publication	Publikacja specjalna
SPAN	Switched Port Analyzer	Analizator ruchu sieciowego
SQL	Structured Query Language	Nazwa języka zapytań bazodanowych
SSA	Sector-Specific Agency	Agencja odpowiedzialna za sektor
SSCP	Secure SCADA Communications Protocol	Protokół bezpiecznej komunikacji w systemach SCADA
SSH	Secure Shell	Nazwa rozwiązania
SSID	Service Set Identifier	Identyfikator zestawu usług
SSL	Secure Sockets Layer	Nazwa protokołu
SSPP	Substation Serial Protection Protocol	Nazwa protokołu
TC	Technical Committee	Komitet techniczny
TCP	Transmission Control Protocol	Nazwa protokołu
TCP/IP	Transmission Control Protocol/Internet Protocol	Internet Protocol Nazwa protokołu
TFTP	Trivial File Transfer Protocol	Nazwa protokołu transferu plików
TIP	Technical Information Paper	Dokumentacja techniczna
TLS	Transport Layer Security	Nazwa protokołu
TLV	Type, Length, Value	Rodzaj, długość, wartość
TPM	Trusted Platform Module	Nazwa standardu
TSA	Transportation Security Administration	Administracja ds. Bezpieczeństwa Transportu
TT	Temperature Transmitter	Przetwornik temperatury
UDP	User Datagram Protocol	Protokół pakietów użytkownika
UPS	Uninterruptible Power Supply	Zasilanie bezprzerwowe
U.S.	United States	Stany Zjednoczone

USB	Universal Serial Bus	Uniwersalna magistrala szeregowa
USDA	United States Department of Agriculture	Departament Rolnictwa Stanów Zjednoczonych
VAV	Variable Air Volume	System sterowania zmiennym przepływem powietrza
VDP	Vulnerability Disclosure Policy	Zasady ujawniania podatności
VLAN	Virtual Local Area Network	Wirtualna sieć lokalna
VoIP	Voice over Internet Protocol	Nazwa protokołu komunikacji głosowej
VPN	Virtual Private Network	Wirtualna sieć prywatna
VTS	IEEE Vehicular Technology Society	Towarzystwo ds. Technologii Pojazdów IEEE
WAF	Web Application Firewall	Zapora aplikacji internetowych
WAN	Wide Area Network	Rozległa sieć informatyczna
WG	Working Group	Grupa Robocza
Wi-Fi	Wireless Fidelity	Standard łączności bezprzewodowej
WINS	World Institute of Nuclear Security	Światowy Instytut Bezpieczeństwa Jądrowego
ZTA	Zero Trust Architecture	Architektura „zerowego zaufania”

ZAŁĄCZNIK B – SŁOWNIK

Poniżej zostały przedstawione definicje wybranych terminów użytych w treści niniejszej publikacji. Niektóre definicje zostały opatrzone odnośnikami do źródeł.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Terminologia angielska	Terminologia polska	Definicja
Access control list	Lista sterowania dostępem	Lista specyfikująca podmioty, które mają prawo dostępu do obiektu i ich uprawnienia do wykonywania działań na obiekcie. Zabezpieczenie przed nieuprawnionym dostępem do obiektu w postaci mechanizmu sterowania dostępem. [RFC4949] (termin dostosowany)
Actuator	Siłownik	Urządzenie pozwalające na poruszanie lub sterowanie mechanizmem bądź systemem. Jest połączone ze źródłem energii, zwykle do jego działania wymagany jest prąd elektryczny, ciśnienie płynu hydraulicznego bądź ciśnienie pneumatyczne. Zadaniem siłownika jest przekształcenie energii w ruch. Siłownik to mechanizm, za pomocą którego system sterowania oddziałuje na otoczenie. System sterowania może być prosty (stały system mechaniczny lub elektroniczny), oparty na oprogramowaniu (sterownik drukarki, system sterowania robotem) lub na działaniach człowieka bądź innego podmiotu.
Alarm	Alarm	Urządzenie lub funkcja, która sygnalizuje występowanie stanu lub parametrów wykraczających poza normy przy pomocy słyszalnego lub widocznego sygnału (lub obu jednocześnie) w celu zwrócenia uwagi na ten stan. [ANSI-ISA-5-1]

Terminologia angielska	Terminologia polska	Definicja
Antivirus tools	Narzędzia antywirusowe	Oprogramowanie i technologie służące do wykrywania złośliwego kodu, zapobiegania zainfekowaniu systemu oraz usuwania złośliwego kodu, który doprowadził do zainfekowania systemu.
Attack	Atak	Każdy rodzaj szkodliwej aktywności osób lub procesów, mającej na celu zebranie, zakłócenie, zaprzeczenie, uszkodzenie lub zniszczenie zasobów systemowych lub samych informacji. Próba uzyskania nieautoryzowanego dostępu do usług, zasobów lub informacji systemowych lub próba naruszenia integralności, dostępności lub poufności systemu.
Authentication	Uwierzytelnienie	Proces weryfikacji tożsamości lub innych atrybutów zgłaszanych przez podmiot lub przejętych od podmiotu (użytkownika, procesu lub urządzenia) albo sprawdzenie źródła i integralności danych. [FIPS200]
Authorization	Autoryzacja	Przyznane użytkownikowi, procesowi lub urządzeniu zezwolenie na wykonywanie określonych czynności lub dostęp do zasobu systemowego. [RFC4949] (termin dostosowany)
Backdoor	Tylne drzwi	Mechanizm programowy lub sprzętowy wprowadzony do systemu bez wiedzy i zgody właściciela lub dysponenta tego systemu, stosowany do nieuprawnionego dostępu do systemu. Stanowi potencjalne zagrożenie dla bezpieczeństwa.

Terminologia angielska	Terminologia polska	Definicja
Buffer overflow	Przepełnienie bufora	Zapisanie do bufora programu większej ilości informacji niż przewiduje jego rozmiar. W przypadku braku mechanizmów zabezpieczających przed takim zdarzeniem dochodzi do nadpisania kodu programu znajdującego się poza obszarem pamięci zarezerwowanej na bufor, co może prowadzić do umieszczenia w programie kodu złośliwego i jego wykonania. Napastnicy wykorzystują ten mechanizm w celu spowodowania awarii systemu lub uruchomienia specjalnie przygotowanego kodu, który pozwala im przejąć kontrolę nad systemem. [SP800-28v2]
Cleartext	Otwarty tekst	Informacje, które nie są szyfrowane.
Communications router	Router komunikacyjny	Urządzenie komunikacyjne, które umożliwia przesyłanie danych między dwiema sieciami. Powszechne zastosowania routerów obejmują łączenie sieci LAN z siecią WAN oraz podłączanie urządzeń MTU i RTU do sieci dalekiego zasięgu na potrzeby komunikacji w systemach SCADA.
Confidentiality	Poufność	Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych. [USC44-3552] (termin dostosowany)
Configuration (of a system or device)	Konfiguracja (systemu lub urządzenia)	Etap procesu projektowania systemu, obejmujący na przykład wybór urządzeń funkcjonalnych, ustalenie ich lokalizacji i określenie ich wzajemnych połączeń.

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
Configuration control	Zabezpieczenia konfiguracyjne	Proces modyfikacji sprzętu, oprogramowania układowego i sprzętowego, oprogramowania i jej dokumentowania w celu zabezpieczenia systemu informacyjnego przed niewłaściwymi modyfikacjami przed, w trakcie i po wdrożeniu systemu. [CNSS4009] (termin dostosowany)
Control	Sterowanie	Element systemu OT wykorzystywany w celu monitorowania procesu fizycznego oraz wpływania na jego przebieg. Kategoria ta obejmuje wszystkie serwery sterowania, urządzenia polowe, siłowniki, czujniki i obsługujące je systemy komunikacyjne.
Control algorithm	Algorytm sterowania	Matematyczne przedstawienie działania, które ma zostać wykonane. [ISADICT]
Control center	Centrum sterowania	Urządzenia sprzętowe lub grupa urządzeń sprzętowych odpowiedzialnych za dokonywanie pomiarów związanych z procesem, monitorowanie procesu bądź sterowanie jego przebiegiem. [ANSI-ISA-51-1]
Control loop	Pętla sterowania	Element składający się z czujników pomiarowych, urządzeń sterujących (np. sterowników PLC), siłowników (np. zaworów sterujących, wyłączników, przełączników i silników) oraz systemu umożliwiającego przesyłanie zmiennych. Mierzone zmienne są przesyłane do kontrolera przez czujniki. Sterownik interpretuje sygnały i generuje odpowiednie zmienne manipulowane w oparciu o algorytm sterowania i docelowe wartości zadane, które przekazuje do siłowników. Zmiany w procesie spowodowane zakłóceniami skutkują przesłaniem nowych sygnałów przez czujniki, które określają stan procesu, następnie dane są ponownie przesyłane do sterownika.

Terminologia angielska	Terminologia polska	Definicja
Control network	Sieć sterowania	Sieć organizacji połączona z urządzeniami, które odpowiadają za sterowanie procesami fizycznymi, w przypadku których istotnymi czynnikami są czas bądź bezpieczeństwo. Sieć sterowania może być podzielona na strefy, a w ramach jednej organizacji może współistnieć wiele oddzielnych sieci sterowania.
Control server	Serwer sterowania	Sterownik, który pełni także funkcję serwera obsługującego oprogramowanie sterujące, odpowiedzialnego za komunikację z urządzeniami sterującymi niższego poziomu, takimi jak zdalne urządzenia końcowe (RTU) i programowalne sterowniki logiczne (PLC), za pośrednictwem sieci OT. W systemie SCADA jest on często nazywany serwerem SCADA, MTU lub sterownikiem nadzorczym.
Control system	System sterowania	System wykorzystujący celowe działania lub zmiany w celu osiągnięcia określonej wartości zmiennej. Do kategorii systemów sterowania należą systemy kontroli nadzorczej i pozyskiwania informacji (SCADA), rozproszone systemy sterowania (DCS), programowalne sterowniki logiczne (PLC), systemy automatyki budynkowej (BAS) oraz inne rodzaje systemów pomiaru i sterowania wchodzące w skład technologii operacyjnych.
Controlled variable	Zmienna kontrolowana	Zmienna, którą system sterowania próbuje utrzymać na poziomie wartości zadanej. Wartość zadana może być stała lub zmienna. [ISADICT]
Controller	Sterownik	Urządzenie lub program, który działa automatycznie w celu regulacji zmiennej kontrolowanej. [ANSI-ISA-51-1]

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
Cycle time	Czas cyklu	Czas, zwykle wyrażany w sekundach, w jakim sterownik może zakończyć jedną pętlę sterowania, w ramach której sygnały z czujników są odczytywane do pamięci, wykonywane są algorytmy sterowania, a odpowiednie sygnały sterujące są przesyłane do siłowników, które powodują zmiany w procesie, skutkujące przesłaniem nowych sygnałów przez czujniki. [ISADICT]
Data diode	Dioda danych	Urządzenie sieciowe lub inne urządzenie, które umożliwia przesył danych tylko w jednym kierunku. Określane także mianem *bramy jednokierunkowej*, deterministycznym jednokierunkowym urządzeniem granicznym lub siecią jednokierunkową.
Data historian	Magazyn danych	Scentralizowana baza danych, która umożliwia analizę danych przy użyciu technik statystycznego sterowania procesem.
Database	Baza danych	Repozytorium informacji, które zazwyczaj przechowuje informacje dotyczące całej organizacji, w tym dane procesowe, receptury, dane dotyczące pracowników oraz dane finansowe. [IR6859] (termin dostosowany)
Demilitarized zone	Strefa zdemilitaryzowana	Segment w topologii sieci, który jest logicznie położony między sieciami wewnętrznymi i zewnętrznymi. Celem strefy DMZ jest egzekwowanie zasad ochrony informacji w zakresie wymiany pomiędzy siecią lokalną i zewnętrzną oraz zapewnienie zewnętrznym, niezaufanym źródłom ograniczonego dostępu do informacji podlegających udostępnianiu, przy jednoczesnym zabezpieczeniu sieci wewnętrznych przed atakami z zewnątrz. Ruch sieciowy pomiędzy DMZ a innymi interfejsami po chronionej stronie zapory nadal przechodzi przez zaporę i może podlegać zasadom ochrony. [SP800-41r1]

Terminologia angielska	Terminologia polska	Definicja
Denial of service	Odmowa świadczenia usługi	Nazwa ataku, którego wynikiem jest uniemożliwienie lub znaczne spowolnienie dostępu do zasobów uprawnionym podmiotom. [RFC4949]
Diagnostics	Diagnostyka	Informacje dotyczące znanych trybów awarii i ich charakterystyki. Takie informacje mogą być wykorzystywane w procesach rozwiązywania problemów i analizy awarii w celu wskazania przyczyn awarii oraz określenia odpowiednich działań naprawczych. [ISADICT]
Disaster recovery plan	Plan odtworzenia po katastrofie	Z góry określony plan odzyskiwania jednego lub większej liczby systemów informatycznych w zapasowym obiekcie w odpowiedzi na poważną awarię sprzętu lub oprogramowania lub zniszczenie urządzeń. [SP800-34r1] (termin dostosowany)
Discrete process	Proces dyskretny	Rodzaj procesu, w którym określona ilość materiału przemieszcza się jako jednostka (element lub grupa elementów) między stacjami roboczymi, a każda jednostka zachowuje swoją wyjątkową tożsamość. [ISADICT]
Distributed control system	Rozproszony system sterowania	Rodzaj systemu sterowania, w którym sterowanie odbywa się za pośrednictwem rozproszonych elementów inteligentnych rozmieszczonych wzdłuż procesu, alternatywa dla sterowania przez centralnie zlokalizowaną pojedynczą jednostkę. [ISADICT]
Disturbance	Zakłócenie	Niepożądana zmiana w zmiennej stosowanej w systemie, która może negatywnie wpływać na wartość zmiennej kontrolowanej. [ANSI-ISA-51-1]

Terminologia angielska	Terminologia polska	Definicja
Domain	Domena	Środowisko lub kontekst, który obejmuje zestaw zasobów systemowych i zestaw encji systemowych, które mają prawo dostępu do zasobów określonych przez wspólne zasady bezpieczeństwa, model bezpieczeństwa lub architekturę bezpieczeństwa. [RFC4949] (termin dostosowany)
Encryption	Szyfrowanie	Kryptograficzna transformacja danych („otwartego tekstu”) do postaci zaszyfrowanej, która ukrywa pierwotne znaczenie danych, aby zapobiec ich odczytaniu lub wykorzystaniu. Jeśli transformacja jest odwracalna, odpowiadający jej proces transformacji przywracającej zaszyfrowane dane do ich pierwotnego stanu nazywany jest deszyfrowaniem. [RFC4949] (termin dostosowany)
Enterprise	Podmiot	Także organizacja – wyspecjalizowana jednostka organizacyjna o dowolnej wielkości, złożoności lub pozycjonowaniu w ramach struktury organizacyjnej (np. przedsiębiorstwo, urząd, itp., lub w stosownych przypadkach, którykolwiek z elementów operacyjnych organizacji, urzędu, itp.). W kontekście OT, podmiot bądź organizacja jest jednostką koordynującą działania jednego lub kilku zakładów przetwórczych.
Fault tolerant	Odporność na awarię	Możliwość ciągłego, poprawnego wykonywania funkcji przez system w przypadku awarii sprzętu bądź oprogramowania.

Terminologia angielska	Terminologia polska	Definicja
Field device	Urządzenie terenowe	Urządzenie, które jest przypisane do strefy urządzeń terenowych systemu sterowania przemysłowego. Kategoria ta obejmuje urządzenia zdalne (RTU), sterowniki PLC, siłowniki, czujniki, interfejsy człowiek-maszyna (HMI) oraz powiązane z nimi urządzenia komunikacyjne.
Field site	Jednostka terenowa	Podsystem przypisany do fizycznego, geograficznego lub logicznego segmentu w ramach systemu sterowania przemysłowego. Może obejmować urządzenia zdalne (RTU), sterowniki PLC, siłowniki, czujniki, interfejsy człowiek-maszyna (HMI) oraz powiązane z nimi urządzenia komunikacyjne.
Fieldbus	Fieldbus	Cyfrowa, szeregowa, wielopunktowa, dwukierunkowa magistrala danych, połączenie lub łącze między urządzeniami przemysłowymi niskiego poziomu, takimi jak: czujniki, przetworniki, siłowniki, sterowniki lokalne, a nawet urządzenia w sterowni. Wykorzystanie technologii fieldbus eliminuje konieczność stosowania połączeń punkt-punkt między sterownikiem i poszczególnymi urządzeniami. Komunikaty w sieci Fieldbus są oparte na określonym protokole, a każdy komunikat identyfikuje konkretny czujnik w sieci.
File Transfer Protocol	File Transfer Protocol	Protokół komunikacyjny typu klient - serwer wykorzystujący protokół sterowania transmisją (TCP) według modelu TCP/IP, umożliwiający dwukierunkowy transfer plików w układzie serwer FTP–klient FTP. FTP jest zdefiniowany przez IETF w dokumencie RFC 959. Programy i narzędzia FTP są wykorzystywane w celu przesyłania i pobierania stron internetowych, plików graficznych oraz innych plików między nośnikami lokalnymi a zdalnym serwerem, który umożliwia dostęp do FTP.

Terminologia angielska	Terminologia polska	Definicja
Firewall	Zapora sieciowa	Rozwiązanie sprzętowe lub programowe ograniczające przepływ pakietów pomiędzy segmentami sieci komputerowej zgodnie z określoną polityką bezpieczeństwa. [RFC4949]
Human-machine interface	Interfejs człowiek-maszyna	Sprzęt lub oprogramowanie, za pośrednictwem którego operator obsługuje sterownik. Interfejs człowiek-maszyna może być zarówno fizycznym panelem sterowania z przyciskami i kontrolkami, jak i komputerem przemysłowym z kolorowym wyświetlaczem graficznym, obsługującym oprogramowanie. HMI. [IR6859]
Identification	Identyfikacja	Działanie lub proces, w którym identyfikowany przedstawia się systemowi w taki sposób, że system może go jednoznacznie rozpoznać. [SP800-47]
Incident	Incydent	Zdarzenie, które faktycznie lub potencjalnie zagraża poufności, integralności lub dostępności systemu informacyjnego lub informacji, które system przetwarza, przechowuje lub przesyła, a także zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania. [FIPS200]
Industrial control system	System sterowania przemysłowego	Ogólny termin obejmujący kilka rodzajów systemów sterowania, w tym systemy kontroli nadzorczej i gromadzenia danych (SCADA), rozproszone systemy sterowania (DCS) i inne konfiguracje systemów sterowania wykorzystywane w sektorach przemysłowych i infrastrukturze krytycznej, takie jak programowalne sterowniki logiczne (PLC).

Terminologia angielska	Terminologia polska	Definicja
		System sterowana przemysłowego składa się z szeregu elementów sterujących (elektrycznych, mechanicznych, hydraulicznych, pneumatycznych), które współpracują w celu realizacji określonego celu związanego między innymi z produkcją, transportem materiałów lub wytwarzaniem energii.
Information security program plan	Plan programu bezpieczeństwa informacji	Formalny dokument, który zawiera przegląd wymagań bezpieczeństwa zawartych w programie bezpieczeństwa informacji w organizacji oraz opisuje program zarządzania zabezpieczeniami i zabezpieczeniami wspólnymi istniejącymi lub planowanymi do wdrożenia w celu spełnienia tych wymagań. [OMB-A130]
Input/output	Wejście/wyjście	Ogólny termin określający urządzenia wykorzystywane w celu komunikacji z komputerem, a także dane związane z komunikacją. [ISADICT]
Insider	Pracownik organizacji	Osoba znajdująca się w obwodzie zabezpieczeń, która posiada autoryzację do uzyskiwania dostępu do zasobów systemu, jednak korzysta z nich w sposób wykraczający poza zakres autoryzacji udzielonej przez stosowne podmioty.
Integrity	Integralność	Atrybut bezpieczeństwa informacji oznaczający, że informacja nie uległa nieuprawnionej modyfikacji lub zniszczeniu, w tym świadczący o niezaprzeczalności i autentyczności informacji. [USC44-3552] (termin dostosowany)

Terminologia angielska	Terminologia polska	Definicja
Intelligent electronic device	Inteligentne urządzenie elektroniczne	Dowolne urządzenie zawierające jeden lub więcej procesorów z możliwością odbierania lub wysyłania danych/sygnałów sterowania z lub do zewnętrznego źródła (np. elektroniczne mierniki wielofunkcyjne, przekaźniki cyfrowe, sterowniki). [AGA12]
Internet	Internet	Internet jest globalną siecią komputerową łączącą ze sobą komputery i sieci wewnętrzne różnych podmiotów, w której: standardy protokołów określa IAB (*ang. Internet Architecture Board*), nazwami i adresami zarządza ICANN (*ang. Internet Corporation for Assigned Names and Numbers*). [RFC4949] (termin dostosowany)
Intrusion detection system	System wykrywania włamań	Mechanizm sprzętowy lub programowy pozwalający na pozyskiwanie i analizowanie informacji z różnych obszarów systemu informatycznego w celu wykrycia możliwych naruszeń bezpieczeństwa. [RFC4949] (termin dostosowany)
Intrusion prevention system	System prewencji włamań	System, który wykrywa włamania lub próby włamania, ale jest też zdolny do przeciwdziałania tym próbom, najlepiej zanim osiągną one zamierzony cel.
Jitter	Jitter	Odchylenie w czasie lub fazie między sygnałem danych a idealnym zegarem.
Key logger	Keylogger	Rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika na klawiaturze komputera w celu uzyskania haseł lub kluczy szyfrowania, a tym samym obejścia innych zabezpieczeń.
Local area network	Lokalna sieć komputerowa	Sieć komputerowa łącząca sprzęt informatyczny na określonym obszarze (blok, szkoła, laboratorium, biuro).

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
Machine controller	Sterownik maszyny	Sieć obejmująca system sterowania oraz ruchu, która elektronicznie synchronizuje napędy w systemie maszynowym zamiast polegać na synchronizacji za pomocą mechanicznego połączenia. [IR6859]
Maintenance	Utrzymanie / konserwacja	Każda czynność, która albo zapobiega awarii lub wadliwemu działaniu sprzętu, albo przywraca jego zdolność do działania. [ISADICT]
Malware	Oprogramowanie złośliwe	Oprogramowanie lub oprogramowanie układowe mające na celu wykonanie nieautoryzowanego procesu, który będzie miał niekorzystny wpływ na poufność, integralność lub dostępność systemu informacyjnego. Wirus, robak, koń trojański lub inne oprogramowanie, które infekuje hosta. [NSC 800-53] (termin dostosowany)
Manipulated variable	Manipulowana zmienna	W procesie, który ma na celu regulację pewnych warunków, wartość lub warunek, który wpływa na sterowanie, aby zainicjować zmianę wartości kontrolowanego warunku. [ISADICT]
Master terminal unit	Główne urządzenie końcowe (MTU)	Por. *Serwer sterowania*.
Modem	Modem	Urządzenie służące do przetwarzania szeregowych danych cyfrowych z terminala nadawczego na sygnał możliwy do transmisji przez kanał telefoniczny w celu ponownego przetworzenia transmitowanego sygnału na szeregowe dane cyfrowe dla terminala odbiorczego. [IR6859]

Terminologia angielska	Terminologia polska	Definicja
Operating system	System operacyjny	Główna aplikacja sterująca, którą uruchamia komputer. Jest to pierwszy program ładowany po włączeniu komputera, a jego główny komponent, jądro, cały czas znajduje się w pamięci. System operacyjny wyznacza standardy dla wszystkich programów aplikacyjnych (np. serwera WWW), które działają w komputerze. Aplikacje komunikują się z systemem operacyjnym dla większości operacji interfejsu użytkownika i zarządzania plikami. System operacyjny może wykonywać funkcje sterowania urządzeniami wejścia/wyjścia, planowania zasobów i zarządzania danymi. Zapewnia programom użytkowym dostęp do podstawowych poleceń umożliwiających sterowanie komputerem. [ISADICT]
Operational controls	Zabezpieczenia operacyjne	Środki bezpieczeństwa (tj. zabezpieczenia lub środki zaradcze) systemu informacyjnego, który jest przede wszystkim wdrażany i wykonywany przez ludzi (w przeciwieństwie do zabezpieczeń wdrażanych przez system). [FIPS200]
Operational technology	Technologia operacyjna	Programowalne systemy lub urządzenia, które oddziałują na środowisko fizyczne (lub zarządzają urządzeniami, które oddziałują na środowisko fizyczne). Te systemy/urządzenia wykrywają lub powodują bezpośrednie zmiany poprzez monitorowanie i/lub kontrolę urządzeń, procesów i zdarzeń. Przykłady obejmują przemysłowe systemy sterowania, systemy zarządzania budynkiem, systemy kontroli przeciwpożarowej i mechanizmy kontroli dostępu fizycznego.

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
Password	Hasło	Ciąg znaków (liter, cyfr i innych symboli) używany do uwierzytelniania tożsamości lub weryfikacji autoryzacji dostępu. [FIPS140-2]
Phishing	Wyłudzanie informacji	Rodzaj ataku kombinowanego, na który składają się: przygotowanie złośliwej strony WWW oraz działania socjotechniczne mające na celu spowodowanie skorzystania z usług oferowanych na tej stronie przez atakowany podmiot.
Plant	Zakład / linia produkcyjna	Elementy fizyczne niezbędne do obsługi procesu fizycznego. Może obejmować wiele statycznych komponentów, które nie są sterowane przez system sterowania przemysłowego. Działanie systemu sterowania przemysłowego może jednak wpływać na adekwatność, wytrzymałość i trwałość komponentów.
Port	Gniazdo	Łącze wejściowe lub wyjściowe komputera, służące do podłączania urządzeń komunikacyjnych lub peryferyjnych.
Port scanning	Skanowanie portów	Proces łączenia się z portami komputera przez oprogramowanie skanujące (tzw. skaner) w celu określenia, które z nich są aktywne.
Predisposing condition	Stan predyspozycji	Stan istniejący w organizacji, misji lub procesie biznesowym, architekturze korporacyjnej lub systemie informacyjnym, w tym w jego środowisku operacyjnym, który zwiększa lub zmniejsza prawdopodobieństwo, że jedno lub więcej zdarzeń powodujących zagrożenie spowoduje niepożądane konsekwencje lub negatywny wpływ na działalność i zasoby organizacji, pracowników, inne organizacje lub państwo. [NSC 800-30]

Terminologia angielska	Terminologia polska	Definicja
Pressure regulator	Regulator ciśnienia	Urządzenie służące do ustalania ciśnienia gazu lub cieczy. [IR6859]
Pressure sensor	Czujnik ciśnienia	System czujników, który wytwarza sygnał elektryczny na podstawie ciśnienia oddziałującego medium – cieczy lub gazu. Czujniki ciśnienia mogą również wykorzystywać różnicę ciśnień w celu ustalania pomiarów poziomu i przepływu. [IR6859] (termin dostosowany)
Printer	Drukarka	Urządzenie przetwarzające dane cyfrowe na tekst czytelny dla człowieka na nośniku papierowym. [IR6859] (termin dostosowany)
Process controller	Sterownik/kontroler procesu	Rodzaj systemu komputerowego, zwykle montowanego w szafie instalacyjnej, który przetwarza dane wejściowe z czujników, wykonuje algorytmy sterowania i oblicza dane na potrzeby siłowników. [IR6859] (termin dostosowany)
Programmable logic controller	Programowalny sterownik logiczny	System sterowania wyposażony w moduł pamięci programowalnej przez użytkownika, która pozwala na przechowywanie poleceń umożliwiających realizację określonych funkcji, takich jak: sterowanie sygnałami wejściowymi i wyjściowymi, realizację logiki, synchronizację, zliczanie, sterowanie proporcjonalno-całkująco-różniczkujące (PID) w trzech trybach, komunikację, arytmetykę oraz przetwarzanie danych i plików. [ISADICT]
Protocol	Protokół	Zbiór reguł, formatów, zasad semantyki i syntaktyki pozwalający systemom wymieniać informacje. [RFC4949]

Terminologia angielska	Terminologia polska	Definicja
Protocol analyzer	Analizator protokołów	Urządzenie lub aplikacja, która umożliwia użytkownikowi analizę danych sieciowych w celu zapewnienia, że sieć i przyłączone do niej urządzenia oraz programy działają zgodnie ze specyfikacjami. [ISADICT]
Real time	Czas rzeczywisty	Odnosi się do wykonywania obliczeń w czasie, w którym realizowany jest powiązany proces fizyczny, tak aby wyniki obliczeń można było wykorzystać do sterowania procesem fizycznym.
Redundant control server	Nadmiarowy serwer sterowania	Zapasowy serwer sterowania, który zawiera dokładną kopię stanu podstawowego serwera sterowania. [IR6859]
Relay	Przekaźnik	Urządzenie elektromechaniczne, które zamyka lub przerywa obwód elektryczny poprzez fizyczne przesunięcie styków przewodzących. Ruch przekaźnika może być sprzężony z innym mechanizmem, takim jak zawór lub wyłącznik. [ISADICT]
Remote access	Zdalny dostęp	Dostęp do systemów organizacji przez uprawnionego użytkownika, który łączy się z systemem poprzez zewnętrzną sieć komputerową. [NSC 800-53]
Remote diagnostics	Zdalna diagnostyka	Czynności diagnostyczne lub utrzymaniowe w systemie informacyjnym wykonywane przez upoważnione podmioty komunikujące się z tym systemem poprzez sieć publiczną.
Remote maintenance	Zdalna konserwacja	Czynności konserwacyjne prowadzone przez osoby komunikujące się spoza granic systemu informacyjnego. [NSC 800-53]

Terminologia angielska	Terminologia polska	Definicja
Remote terminal unit	Zdalny terminal	Komputer wyposażony w urządzenia do łączności radiowej używany w zdalnych lokalizacjach, w których metody łączności przewodowej są niedostępne. Zwykle używany do komunikacji ze zdalnymi urządzeniami terenowymi. W wybranych sytuacjach rolę zdalnych terminali mogą pełnić sterowniki PLC. [IR6859]
Risk	Ryzyko	Poziom wpływu na działalność organizacji (w tym realizację misji, funkcji, a także wizerunek lub reputację), jej zasoby lub pracowników, wynikający z działania systemu informacyjnego, uwzględniający potencjalny wpływ zagrożenia i prawdopodobieństwo jego wystąpienia. [NSC 200] (termin dostosowany)
Risk assessment	Szacowanie ryzyka	Proces określania zagrożeń dla działalności organizacji (w tym realizacji misji, funkcji, a także wizerunku lub reputacji), jej zasobów lub pracowników poprzez określenie prawdopodobieństwa wystąpienia wynikającego z tego wpływu oraz dodatkowych zabezpieczeń, które mogą ograniczyć wpływ. Element procesu zarządzania ryzykiem, synonim analizy ryzyka. Obejmuje analizy zagrożeń i podatności. [SP800-39] (termin dostosowany)
Risk management	Zarządzanie ryzykiem	Proces zarządzania ryzykiem dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego. Obejmuje: (I) przeprowadzenie szacowania ryzyka; (II)

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
		wdrożenie strategii ograniczania ryzyka; oraz (III) zastosowanie technik i procedur ciągłego monitorowania stanu bezpieczeństwa systemu informacyjnego. [FIPS200] (termin dostosowany)
Router	Router	Komputer, który pełni funkcję bramy między dwiema sieciami w warstwie 3 modelu OSI, odpowiedzialny za przesyłanie oraz kierowanie pakietów danych pomiędzy sieciami. Typowe urządzenia tego rodzaju odpowiadają za obsługę pakietów IP. [RFC4949] (termin dostosowany)
Safety instrumented system	Przyrządowy system bezpieczeństwa	System, w którego skład wchodzą czujniki, elementy logiczne oraz elementy sterujące, których celem jest przywrócenie systemu do bezpiecznego stanu w przypadku przekroczenia wstępnie skonfigurowanych wartości progowych. Inne powszechnie stosowane synonimy to system awaryjnego wyłączania (ESS), system bezpiecznego wyłączania (SSD) i system blokady zabezpieczającej (SIS). [ANSI-ISA-84]
Scada server	Serwer SCADA	Urządzenie pełniące funkcję urządzenia nadrzędnego w systemie SCADA.
Security audit	Audyt bezpieczeństwa	Niezależny przegląd i badanie dokumentacji oraz działań systemu w celu określenia adekwatności zabezpieczeń systemu, zapewnienia zgodności z ustalonymi zasadami bezpieczeństwa i procedurami, wykrycia naruszeń usług bezpieczeństwa i opracowania zaleceń zmian w zabezpieczeniach. [ISO7498-1]

Terminologia angielska	Terminologia polska	Definicja
Security controls	Zabezpieczenia	Środki zarządcze, organizacyjne lub technologiczne stosowane w celu zapewnienia poufności, integralności i dostępności informacji i/lub dostępności systemu informacyjnego. [FIPS199]
Security plan	Plan bezpieczeństwa	Oficjalny dokument, który zawiera przegląd wymagań dotyczących zabezpieczeń dla systemu informacyjnego i opisuje mechanizmy zabezpieczeń wykorzystywanych lub planowanych do spełnienia tych wymagań. [NSC 7298]
Security policy	Zasady/polityki bezpieczeństwa	Dokument opisujący jak organizacja zarządza, zabezpiecza i realizuje kluczowe procesy biznesowe. Także zorganizowane działania mające doprowadzić do osiągnięcia założonego celu lub celów biznesowych. Zasady są opracowywane na kilku poziomach, począwszy od poziomu organizacji lub podmiotu, aż po zasady dotyczące poszczególnych procesów (np. zdalny dostęp). Celem zasad jest ustanowienie celów oraz wyjaśnienie przyczyn ich wprowadzania, nie zaś określenie konkretnych działań prowadzących do ich osiągnięcia. Zasady są zwykle określane w taki sposób, by ich realizacja nie była uzależniona od wyboru konkretnej technologii.
Sensor	Czujnik	Urządzenie wytwarzające napięcie lub prąd wyjściowy, który pozwala na określenie pomiaru danej właściwości fizycznej (np. prędkości, temperatury, przepływu) [ISADICT]

Terminologia angielska	Terminologia polska	Definicja
Set point	Wartość zadana	Zmienna wejściowa, która stanowi żądaną wartość zmiennej kontrolowanej. Zmienna ta może być ustawiana ręcznie, automatycznie lub zaprogramowana. [ISADICT]
Single loop controller	Sterownik pojedynczej pętli	Sterownik sterujący bardzo małym procesem lub procesem krytycznym. [IR6859]
Social engineering	Inżynieria społeczna	Działanie zmierzające do uzyskania pożądanego zachowania jednostek i grup społecznych. [NSC 7298] na podstawie [SP800-61r2]
Supervisory control	Kontrola nadzorcza	Termin używany do wskazania, że dane wyjściowe sterownika lub programu komputerowego są używane jako dane wejściowe dla innych sterowników. Por. *Serwer sterowania*. [ISADICT]
Supervisory control and data acquisition	System kontroli nadzorczej i pozyskiwania danych	Ogólna nazwa skomputeryzowanego systemu, który jest w stanie gromadzić i przetwarzać dane oraz realizować zadania związane z zabezpieczeniami operacyjnymi na duże odległości. Typowe obszary zastosowań tego rodzaju systemów obejmują przesył i dystrybucję energii oraz zarządzanie rurociągami. System SCADA są opracowywane z uwzględnieniem wyjątkowych problemów związanych z komunikacją (np. opóźnień, wyzwań dotyczących integralności danych) związanych z wykorzystaniem różnych sposobów komunikacji, w tym linii telefonicznych, połączeń mikrofalowych oraz satelitarnych. Połączenia wykorzystywane przez systemy SCADA są zwykle współdzielone. [ISADICT]

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
Technical controls	Zabezpieczenia techniczne	Środki bezpieczeństwa (tj. zabezpieczenia lub środki zaradcze) dla systemu informacyjnego, które są wdrażane i wykonywane głównie przez system informacyjny za pomocą mechanizmów zawartych w sprzęcie, oprogramowaniu lub składnikach oprogramowania układowego systemu. [NSC 7298]
Threat	Zagrożenie	Wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na operacje organizacyjne (w tym misję, funkcje, wizerunek lub reputację), zasoby organizacyjne lub osoby fizyczne za pośrednictwem systemu informacyjnego poprzez nieautoryzowany dostęp, zniszczenie, ujawnienie, modyfikację informacji i/lub odmowę usługi. Ponadto, możliwość pomyślnego wykorzystania luki w zabezpieczeniach określonego systemu informacyjnego przez źródło zagrożenia. [NSC 7298] (termin dostosowany na podstawie [FIPS200])
Threat event	Zdarzenie powodujące zagrożenie	Zdarzenie lub sytuacja, które mogą potencjalnie spowodować niepożądane konsekwencje lub wpływ. [SP800-30r1]
Threat source	Źródło zagrożenia	Intencja i metoda ukierunkowane na celowe wykorzystanie podatności w zabezpieczeniach lub sytuacje i metody, które mogą przypadkowo wykorzystać podatność. *Pojęcie jest synonimem czynnika zagrożenia.* [FIPS200]

Tłumaczenie

Terminologia angielska	Terminologia polska	Definicja
Transmission control protocol	Transmission control protocol	Standard określający sposób nawiązywania i prowadzenia komunikacji sieciowej, za pośrednictwem której programy aplikacyjne mogą wymieniać dane. Protokół IP dotyczy wyłącznie pakietów, z kolei protokół TCP umożliwia dwóm hostom nawiązanie połączenia i wymianę strumieni danych. Zastosowanie protokołu TCP gwarantuje dostarczenie danych, a także zapewnienie, że pakiety zostaną dostarczone w tej samej kolejności, w jakiej zostały wysłane.
Trojan horse	Koń trojański	Oprogramowanie wydające się mieć użytkowy charakter jednak mające również ukryte funkcje szkodliwe. [RFC4949]
Unauthorized access	Nieautoryzowany dostęp	Sytuacja, w której osoba uzyskuje logiczny lub fizyczny dostęp do systemu, aplikacji, danych lub innych zasobów bez odpowiednich uprawnień. [SP800-61]
Unidirectional gateway	Bramka jednokierunkowa	Rozwiązanie łączące sprzęt i oprogramowanie. Sprzęt umożliwia przepływ danych z jednej sieci do drugiej, jednocześnie fizycznie uniemożliwia przesył jakichkolwiek informacji do sieci źródłowej. Oprogramowanie odpowiada za replikację baz danych oraz emulację serwerów, protokołów i urządzeń.
Valve	Zawór	Urządzenie liniowe w systemie przepływu płynu, które pozwala na zatrzymanie przepływu, a także regulację szybkości lub przekierowanie przepływu do innej części układu. [ISADICT]

Terminologia angielska	Terminologia polska	Definicja
Virtual private network	Wirtualna sieć prywatna	Sieć zapewniająca bezpieczne połączenie pomiędzy segmentami, wykorzystująca technikę tunelowania. Logiczna sieć komputerowa o ograniczonym użyciu, zbudowana w oparciu o zasoby systemowe publicznej, fizycznej (tj. rzeczywistej) sieci (takiej jak Internet), często przy użyciu szyfrowania (realizowanego za pośrednictwem hostów lub bram) bądź poprzez tunelowanie łączy sieci wirtualnej w sieci rzeczywistej. [RFC4949] (termin dostosowany)
Virus	Wirus	Fragment kodu programu, zwykle dołączony do jakiegoś pliku wykonywalnego lub skryptu bez wiedzy jego użytkownika, zdolny do samodzielnego replikowania się w sieciach komputerowych, zwykle stanowiący oprogramowanie złośliwe. Wirus nie jest w stanie działać samodzielnie; wymaga uruchomienia programu-hosta. [RFC4949] (termin dostosowany)
Vulnerability	Podatność	Słabość systemu informacyjnego, procedur bezpieczeństwa systemu, wewnętrznych zabezpieczeń lub implementacji, która może zostać wykorzystana lub wywołana przez źródło zagrożenia. [FIPS200]
Wide area network	Rozległa sieć informatyczna	Sieć fizyczna lub logiczna, która zapewnia wymianę danych większej liczbie niezależnych użytkowników (zazwyczaj obsługiwanych przez sieć lokalną LAN) i która jest zazwyczaj rozłożona na większym obszarze geograficznym niż sieć LAN.

Terminologia angielska	Terminologia polska	Definicja
Wireless device	Urządzenie bezprzewodowe	Dowolne urządzenie, które może łączyć się z dana siecią za pośrednictwem fal radiowych lub podczerwonych, zwykle w celu gromadzenia lub monitorowania danych, ale w niektórych przypadkach także w celu modyfikacji ustawień sterowników.
Workstation	Stacja robocza	Komputer wykorzystywany w celu realizacji zadań takich jak: programowanie, inżynieria i projektowanie. [IR6859]
Worm	Robak	Program posiadający zdolność samodzielnego rozprzestrzeniania się w sieciach komputerowych, zwykle stanowiący oprogramowanie złośliwe. [RFC4949] (termin dostosowany)

Tłumaczenie

ZAŁĄCZNIK C – ŹRÓDŁA ZAGROŻEŃ, PODATNOŚCI I INCYDENTY

W celu precyzyjnego opisania powiązanych ze sobą pojęć zagrożenia, źródła zagrożenia, zdarzenia powodującego zagrożenie oraz incydentu wykorzystujemy szereg różnych terminów.

Mianem *zagrożenia* określamy wszelkie okoliczności lub zdarzenia mogące mieć negatywny wpływ na działalność organizacji (w tym misję, funkcję, wizerunek lub reputację), jej zasoby, pracowników, inne organizacje lub państwo w wyniku nieautoryzowanego dostępu do systemu informacyjnego, zniszczenia, ujawnienia, modyfikacji informacji lub odmowy świadczenia usługi.

Jedną z cech zagrożeń jest zamiar lub metoda wykorzystania podatności w zabezpieczeniach w sposób zamierzony lub niezamierzony. Zamiar lub metodę określamy mianem *źródła zagrożenia*.

Podatność to termin określający słabość systemu informacyjnego (w tym systemu OT), procedur bezpieczeństwa systemu, zabezpieczeń wewnętrznych lub wdrożenia, która może zostać wykorzystana lub uruchomiona przez źródło zagrożenia.

Zdarzenie powodujące zagrożenie to zdarzenie lub sytuacja, które mogą potencjalnie spowodować niepożądane konsekwencje lub wpływ. Gdy zdarzenie powodujące zagrożenie wystąpi, staje się *incydentem*, czyli zdarzeniem, które stanowi rzeczywiste lub potencjalne zagrożenie poufności, integralności lub dostępności systemu informacyjnego lub informacji przetwarzanych, przechowywanych lub przesyłanych przez system, lub które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania.

Niniejszy załącznik zawiera omówienie źródeł zagrożeń, podatności i incydentów związanych z systemami OT. Obejmuje także przykłady incydentów związanych z systemami OT, aby wskazać ich potencjalny wpływ. Każda organizacja kalkuluje ryzyko na podstawie konkretnych zagrożeń, podatności, wpływów oraz prawdopodobieństwa wystąpienia incydentów w swoim środowisku.

C.1 ŹRÓDŁA ZAGROŻEŃ

Zagrożenia dotyczące systemów OT mogą wychodzić z wielu źródeł, które można określić mianami agresywnych, przypadkowych, strukturalnych oraz środowiskowych. **Tabela 13** zawiera listę oraz opisy znanych źródeł zagrożeń dla systemów OT. Wymienione źródła zagrożeń powinny być uwzględnione w strategii zarządzania ryzykiem. Aby wybrać oraz wdrożyć odpowiednie zabezpieczenia, należy przede wszystkim określić i zrozumieć źródło zagrożenia. Zdarzenia środowiskowe (takie jak powodzie lub trzęsienia ziemi) są znane i dobrze opisane, mimo to charakteryzują się różną magnitudą, zakresem, częstotliwością oraz związkiem z innymi powiązanymi zdarzeniami. Zagrożenia agresywne zależą z kolei od zasobów dostępnych napastnikom oraz informacji o nieznanych wcześniej podatnościach zabezpieczeń zasobów oraz atakach.

Tabela 13. Zagrożenia dotyczące systemów OT

Rodzaj źródła zagrożenia	Opis	Cechy
ZAGROŻENIA AGRESYWNE – Operatorzy sieci botów – Grupy przestępcze – Hakerzy/haktywiści – Pracownicy organizacji – Państwa – Organizacje terrorystyczne	Osoby, grupy, organizacje lub państwa narodowe, które starają się wykorzystać zależność organizacji od cyber zasobów (np. danych w formie elektronicznej, technologii informacyjno-komunikacyjnych oraz komunikacji i przetwarzania informacji realizowanych za pośrednictwem tych technologii)	Możliwości, zamiar, celowość
ZAGROŻENIA PRZYPADKOWE – Użytkownicy – Użytkownicy uprzywilejowani bądź administratorzy	Błędy pracowników w trakcie wykonywania codziennych obowiązków (na przykład wpisanie 100 zamiast 10 jako wartości zadanej przez operatora bądź dokonanie zmiany w środowisku produkcyjnym ze względu na przekonanie o tym, że zmiana dotyczy środowiska testowego)	Zakres skutków
ZAGROŻENIA STRUKTURALNE – Awaria sprzętu lub urządzenia • Procesory, karty we/wy, karty komunikacyjne • Urządzenia sieciowe • Systemy zasilania • Czujniki i elementy wykonawcze	Awarie urządzeń, zabezpieczeń środowiskowych bądź oprogramowania spowodowane wiekiem, wyczerpaniem zasobów lub innymi okolicznościami, które nie mieszczą się w granicach oczekiwanych parametrów operacyjnych, w tym awarie infrastruktury krytycznej pod kontrolą organizacji	Zakres skutków

Rodzaj źródła zagrożenia	Opis	Cechy
• Interfejsy człowiek-maszyna, wyświetlacze – Awarie oprogramowania • System operacyjny • Aplikacje ogólnego przeznaczenia • Aplikacje realizujące misję organizacji – Awaria systemów zapewniających warunki środowiskowe • System sterowania temperaturą • System sterowania wilgotnością – Awaria systemów łączności • Łączność bezprzewodowa • Łączność przewodowa		
ZAGROŻENIA ŚRODOWISKOWE – Katastrofa naturalna lub spowodowana przez człowieka • Pożar • Powódź/tsunami • Orkan/tornado • Huragan • Trzęsienie ziemi • Bombardowanie • Zdarzenie spowodowane przez zwierzęta • Rozbłyski słoneczne, meteoryty – Awaria infrastruktury krytycznej • Sieć telekomunikacyjna • Sieć elektroenergetyczna • Sieć transportu • Sieć wodociągowa lub kanalizacyjna	Klęski żywiołowe i awarie infrastruktury krytycznej, od której zależy organizacja, które nie zostały spowodowane przez organizację. Uwaga: Klęski żywiołowe i katastrofy spowodowane przez człowieka można również scharakteryzować pod względem ich dotkliwości oraz czasu trwania. Ze względu na fakt, że zarówno źródło zagrożenia, jak i zdarzenie powodujące zagrożenie są jasno określone, dotkliwość i czas trwania zdarzenia mogą zostać uwzględnione w opisie zdarzenia powodującego zagrożenie (np. huragan kategorii 5 powoduje rozległe uszkodzenia budynków, które mieszczą kluczowe systemy, co uniemożliwia dostęp do systemów na trzy tygodnie).	Zakres skutków

C.2 PODATNOŚCI I STAN PREDYSPOZYCJI

Mianem *podatności* określamy słabość systemu informacyjnego, procedur dotyczących systemu, wewnętrznych zabezpieczeń lub implementacji, która może zostać wykorzystana lub wywołana przez źródło zagrożenia. *Stan predyspozycji* lub *warunek predysponujący* to cecha organizacji, misji lub procesu biznesowego, architektury bądź systemu informacyjnego, która zwiększa prawdopodobieństwo wystąpienia zdarzenia powodującego zagrożenie. Kolejność opisanych podatności i stanów predyspozycji nie odzwierciedla prawdopodobieństwa wystąpienia zdarzenia lub dotkliwości jego skutków. Co więcej, należy pamiętać, że wykaz podatności i stanów predyspozycji opisanych w niniejszym rozdziale nie stanowi wyczerpującego zbioru, nie należy także zakładać, że występują one w każdym środowisku OT.

Podatności i stany predyspozycji zostały skategoryzowane na podstawie obszarów, w których występują i których dotyczą. Oznacza to podział na podatności i stany predyspozycji dotyczące zasad i procedur organizacji, a także braków w mechanizmach zabezpieczeń dotyczących urządzeń, oprogramowania układowego oraz oprogramowania. Pierwsza kategoria została określona mianem podatności organizacyjnych, druga zaś obejmuje podatności systemowe. Zrozumienie źródła podatności i stanów predyspozycji może pomóc w określeniu optymalnych strategii ograniczania ryzyka. Dogłębna analiza może umożliwić stwierdzenie, że przyczyny i objawy mogą nie odpowiadać sobie bezpośrednio – niektóre przyczyny mogą skutkować występowaniem wielu objawów, z kolei wybrane objawy mogą wynikać z więcej niż jednej przyczyny.

Z założenia każdy system OT posiada pewien zbiór podatności opisanych w niniejszym załączniku, może jednak także zawierać dodatkowe podatności na zagrożenia i stany predyspozycji, które dotyczą wyłącznie wybranych technologii lub sposobów wdrożenia. Szczegółowe i aktualizowane na bieżąco informacje na temat podatności systemów i komponentów systemów OT publikowane są w witrynie internetowej CISA, ponadto wielu producentów urządzeń publikuje powiadomienia i poprawki, które niekoniecznie są publikowane w witrynie CISA. Z tego powodu należy utrzymywać kontakty z producentami urządzeń, by otrzymywać na bieżąco informacje dotyczące znanych podatności.

Niektóre podatności i stany predyspozycji mogą zostać ograniczone lub usunięte. W innym wypadku mogą zostać zaakceptowane oraz zabezpieczone przy pomocy skutecznych środków przeciwdziałania, co powoduje jednak pewne ryzyko szczątkowe dla środowiska OT. Wybrane zasady oraz procedury mogą zostać zmienione, jeśli nakład prac zostanie uznany za akceptowalny dla organizacji, z kolei rozwiązanie innych problemów może wymagać wdrożenia dodatkowych zasad i procedur.

Podatności w produktach i usługach nabytych od podmiotów zewnętrznych zwykle znajdują się poza obszarem odpowiedzialności organizacji. Na zmiany mogą wpłynąć sygnały ze strony rynku, jednak zwykle jest to powolny i długotrwały proces. Organizacja może w związku z tym zmienić stan predyspozycji, aby ograniczyć prawdopodobieństwo wykorzystania podatności systemowej.

C.2.1. PODATNOŚCI DOTYCZĄCE ZASAD I PROCEDUR ORAZ STANY PREDYSPOZYCJI

Podatności i stany predyspozycji są w wielu przypadkach wprowadzane do środowisk OT w związku z niepełnymi, nieadekwatnymi lub nieistniejącymi zasadami bezpieczeństwa. Mogą dotyczyć też braku stosownej dokumentacji, informacji wdrożeniowych (np. procedur) i zasad egzekwowania. Wsparcie wdrażania zasad bezpieczeństwa oraz procedur ze strony kierownictwa stanowi fundament każdego programu bezpieczeństwa. Zasady bezpieczeństwa organizacji mogą ograniczyć podatność na zagrożenia nakazując i wymuszając właściwe postępowanie. Udokumentowane zasady i procedury pozwalają na informowanie pracowników i interesariuszy o decyzjach dotyczących zachowań uznanych za korzystne dla organizacji. Patrząc przez ten pryzmat, zasady są sposobem na ograniczenie podatności na zagrożenia przez edukację. Egzekwowanie zasad stanowi dopełnienie tych działań, którego celem jest skłonienie pracowników do postępowania we właściwy sposób. Różne formy działań naprawczych mogą być konieczne w przypadkach, w których pracownicy nie będą przestrzegali obowiązujących zasad i procedur. Zasady powinny wyraźnie określać konsekwencje dla osób lub organizacji, które zdecydują się na ich nieprzestrzeganie.

Organizacje działają w pewnym otoczeniu prawnym, które obejmuje przepisy prawa oraz regulacje, różne jurysdykcje i strefy wpływów, a także zasady gospodarcze, zwyczaje oraz uwarunkowania historyczne. Większe organizacje są zwykle podzielone na jednostki organizacyjne, które powinny współpracować w celu zmniejszenia podatności na zagrożenia. Zakres oraz zależności hierarchiczne między zasadami i procedurami muszą być opracowane w taki sposób, by zapewnić najwyższą skuteczność.

Tabela 14 przedstawia przykłady zaobserwowanych podatności zasad i procedur oraz stanów predyspozycji w systemach OT.

Tabela 14. Podatności dotyczące zasad i procedur oraz stany predyspozycji

Podatność	Opis
Niedostateczny poziom odpowiedzialności za szacowanie ryzyka w organizacji	Szacowanie ryzyka winno przebiegać za zgodą kierownictwa na odpowiednich szczeblach organizacji. Niezrozumienie ryzyka może prowadzić do podejmowania niedostatecznych działań dotyczących ograniczania ryzyka oraz wyboru niewłaściwych zabezpieczeń.
Nieodpowiednie zasady bezpieczeństwa dotyczące systemów OT	Częstą przyczyną występowania podatności w systemach i środowiskach OT jest brak odpowiednich zasad lub nieodpowiednie zasady bezpieczeństwa dotyczące tego obszaru. Zabezpieczenia i środki przeciwdziałania powinny opierać się na wynikach szacowania ryzyka lub stosownych zasadach, aby zapewnić ich jednolite stosowanie oraz rozliczalność.
Niedostateczny program szkoleń i podnoszenia świadomości w zakresie bezpieczeństwa systemów OT	Udokumentowany formalny program szkoleń i podnoszenia świadomości w zakresie bezpieczeństwa systemów OT ma na celu informowanie pracowników na bieżąco o zasadach i procedurach bezpieczeństwa obowiązujących w organizacji, zagrożeniach, branżowych standardach cyberbezpieczeństwa i zalecanych praktykach. Bez odpowiedniego ciągłego szkolenia w zakresie zasad i procedur OT nie można oczekiwać od pracowników zapewnienia bezpieczeństwa środowiska OT.
Brak zasad inwentaryzacji i zarządzania zasobami	Zasady i procedury inwentaryzacji powinny obejmować procesy instalacji, demontażu oraz zmian dotyczących urządzeń, oprogramowania sprzętowego oraz oprogramowania uruchamianego na urządzeniach. Brak stosownych procedur w tym zakresie może spowodować pojawienie się w środowisku OT nieznanych lub niezabezpieczonych urządzeń.
Brak zasad zarządzania konfiguracją	Brak zasad i procedur zarządzania konfiguracją systemów OT może prowadzić do sytuacji, w której w środowisku działać będzie niezarządzany oraz podatny na zagrożenia zbiór urządzeń, oprogramowania układowego oraz aplikacji.

Podatność	Opis
Niestosowne wytyczne dotyczące wdrażania rozwiązań OT	Rekomendacje dotyczące wdrażania rozwiązań i urządzeń powinny być aktualizowane i łatwo dostępne. Tego rodzaju informacje stanowią integralną część procedur bezpieczeństwa dotyczących sytuacji awaryjnych związanych z systemami OT.
Brak mechanizmów administracyjnych umożliwiających egzekwowanie zasad bezpieczeństwa	Brak rozliczalności egzekwowanie zasad bezpieczeństwa oznacza ograniczone możliwości zapewnienia, że zasady są przestrzegane. Organizacja winna wdrożyć mechanizmy administracyjne zapewniające rozliczalność.
Brak stosownych przeglądów skuteczności zabezpieczeń systemów OT	Organizacja winna wdrożyć procedury i harmonogramy kontroli, które pozwolą na stwierdzenie, czy program bezpieczeństwa i wchodzące w jego skład zabezpieczenia zostały wdrożone, działają zgodnie z przeznaczeniem i przynoszą pożądane rezultaty w odniesieniu do spełnienia wymogów bezpieczeństwa dotyczących systemów OT. Proces ten jest określany mianem *kontroli*, *audytu* lub *przeglądu*. Zasady powinny określać etap cyklu życia, a także cel, wymagane kompetencje techniczne, metodykę oraz poziom niezależności.
Brak planu awaryjnego dotyczącego systemów OT	Plan awaryjny (np. plan ciągłości działania, plan odtworzenia po katastrofie) powinien być przygotowany, sprawdzony i dostępny na wypadek poważnej awarii sprzętu lub oprogramowania, a także zniszczenia obiektów. Brak planu dotyczącego systemów OT może prowadzić do wydłużonych przestojów i strat produkcyjnych.
Brak stosownych zasad kontroli dostępu	Stosowanie kontroli dostępu opiera się na zasadach, które określają role, obowiązki i uprawnienia. Założenia tych zasad muszą wpisywać się w sposób funkcjonowania organizacji.
Brak stosownych zasad uwierzytelniania	Zasady uwierzytelniania określają, jakie mechanizmy uwierzytelniania (np. hasła, karty inteligentne) powinny być wykorzystywane w organizacji, a także ich parametry oraz sposoby utrzymania. Brak stosownych zasad może oznaczać brak odpowiednich mechanizmów uwierzytelniania w poszczególnych systemach, co może zwiększyć prawdopodobieństwo nieautoryzowanego dostępu do systemów. Zasady uwierzytelniania powinny stanowić element ogólnego programu bezpieczeństwa systemów OT oraz uwzględniać zarówno możliwości systemów OT, jak i kompetencje pracowników w zakresie obsługi bardziej złożonych haseł i innych mechanizmów zabezpieczeń.
Nieodpowiednie plany oraz i procedury wykrywania i odpowiedzi na incydenty	Plany, procedury i metody wykrywania oraz odpowiedzi na incydenty są niezbędne do szybkiego wykrywania incydentów, minimalizowania strat i zniszczeń, gromadzenia dowodów na potrzeby dochodzenia, usuwania podatności, które zostały wykorzystane, a także odtwarzania usług. Skuteczne działania w zakresie reagowania na incydenty obejmują ciągłe monitorowanie anomalii, ustalanie priorytetów obsługi incydentów oraz wdrażanie skutecznych metod gromadzenia, analizowania i raportowania danych.

Podatność	Opis
Brak nadmiarowości w przypadku krytycznych komponentów	Brak nadmiarowości w przypadku krytycznych komponentów może stanowić pojedynczy punkt awarii.

C.2.2. PODATNOŚCI SYSTEMOWE I STANY PREDYSPOZYCJI

Zabezpieczenia muszą być powiązane z systemami, do których mają zastosowanie. Poszczególne systemy mogą różnić się wielkością, zakresem i możliwościami. Mniejsze systemy mogą obejmować pojedyncze urządzenia, usługi lub programy. Na drugim końcu spektrum znajdują się duże i złożone systemy, systemy systemów i sieci, które obejmują architektury sprzętowe oraz ramy oprogramowania (w tym aplikacji) odpowiadające za realizację działań i operacji. Organizacja może zdecydować się na określenie stref bezpieczeństwa w taki sposób, by zabezpieczenia mogły być stosowane do wszystkich systemów w strefie bezpieczeństwa.

Podatności zabezpieczeń systemu mogą występować w sprzęcie, oprogramowaniu układowym i oprogramowaniu wykorzystywanym w systemach OT. Źródła tych podatności obejmują błędy projektowe, błędy programistyczne, błędy w konfiguracji, niedostateczną konserwację, błędy w administracji, a także połączenia z innymi systemami i sieciami. Wiele zabezpieczeń opisanych w dokumencie NSC 800-53 [NSC 800-53] oraz nakładce dotyczącej systemów OT stanowiącej Załącznik F do niniejszego dokumentu dotyczy sposobów ograniczania tych podatności w systemach.

Podatności mogą również występować w komponentach pomocniczych, które towarzyszą systemom OT. Niniejszy rozdział opisuje podzbiór tych podatności, które mogą mieć wpływ na proces fizyczny.

Potencjalne podatności i stany predyspozycji występujące powszechnie w systemach OT zostały podzielone na kategorie przedstawione w poniższych tabelach:

- **Tabela 15.** Podatności dotyczące architektury i projektu oraz stany predyspozycji
- **Tabela 16.** Podatności dotyczące utrzymania oraz konfiguracji oraz stany predyspozycji
- **Tabela 17.** Podatności fizyczne i stany predyspozycji
- **Tabela 18.** Podatności dotyczące rozwoju oprogramowania oraz stany predyspozycji

- **Tabela 19.** Podatności dotyczące łączności i konfiguracji sieci oraz stany predyspozycji
- **Tabela 20.** Podatności dotyczące czujników, elementów wykonawczych oraz zarządzania zasobami oraz stany predyspozycji

Tabela 15. Podatności dotyczące architektury i projektu oraz stany predyspozycji

Podatność	Opis
Niedostateczne uwzględnienie kwestii bezpieczeństwa w architekturze i projekcie	Włączenie bezpieczeństwa do architektury i projektu systemów OT musi rozpocząć się od określenia budżetu oraz harmonogramu dotyczących tego obszaru. Architektury muszą uwzględniać procesy identyfikacji i uwierzytelniania użytkowników, mechanizmy sterowania dostępem, topologie sieci oraz konfigurację systemu i mechanizmy zapewniania integralności.
Niedostateczne zarządzanie zmianami, umożliwiające rozwój niezabezpieczonej architektury	Infrastruktura sieciowa w środowiskach OT była często rozwijana i zmieniana w oparciu o wymagania biznesowe i operacyjne, bez szczegółowego uwzględnienia potencjalnego wpływu zmian na bezpieczeństwo. Z biegiem czasu w infrastrukturze mogą pojawić się nieumyślnie wprowadzone podatności i luki w zabezpieczeniach. Bez podjęcia stosownych działań korygujących, podatności te mogą stanowić tylne drzwi do systemów OT. Czujniki i sterowniki, które w przeszłości były prostymi urządzeniami, stanowią obecnie często urządzenia inteligentne. W niektórych przypadkach czujniki i sterowniki mogą zostać zastąpione urządzeniami przemysłowego internetu rzeczy, wyposażonymi w funkcje bezpośredniej łączności internetowej. Należy uwzględnić zagadnienie bezpieczeństwa w procesach zarządzania zmianami dotyczącymi wszystkich urządzeń OT, podobnie jak w przypadku tradycyjnych komponentów IT.
Brak określonego obwodu zabezpieczeń	W przypadkach, gdy obwód zabezpieczeń nie jest określony dla środowiska OT, nie jest możliwe zapewnienie, że niezbędne zabezpieczenia są wdrażane i konfigurowane prawidłowo. Może to prowadzić do nieautoryzowanego dostępu do systemów i danych, a także innych problemów.
Wykorzystywanie sieci sterowania do obsługi innego ruchu	Ruch związany ze sterowaniem procesami charakteryzuje się innymi wymogami dotyczącymi niezawodności oraz sposobu działania niż inny ruch sieciowy. Obsługa obu rodzajów ruchu w jednej sieci może prowadzić do trudności związanych ze spełnieniem wymagań dotyczących ruchu związanego ze sterowaniem. Przykładem może być nadmierne zużywanie zasobów przez inny ruch, co może powodować zakłócenie działania systemów OT.
Usługi sieci sterowania zależne od innej sieci	Usługi IT wykorzystywane w sieciach sterowania, takie jak system nazw domen (*ang. Domain Name System – DNS*) i protokół dynamicznego konfigurowania hostów (*ang. Dynamic Host Configuration Protocol – DHCP*) są często realizowane w ramach sieci IT. Powoduje to, że sieć OT staje się zależna od sieci IT, która może nie spełniać wymogów w zakresie niezawodności i dostępności dotyczących systemów OT.

Podatność	Opis
Niedostateczne gromadzenie danych dotyczących zdarzeń	Dochodzenie oraz ustalanie przyczyn awarii wymaga gromadzenia i przechowywania wystarczającej ilości danych. Bez właściwego i dokładnego gromadzenia danych ustalenie przyczyny incydentu bezpieczeństwa może być niemożliwe. Ponadto incydenty mogą pozostać niezauważone, prowadząc do dodatkowych szkód bądź zakłóceń. Regularne monitorowanie bezpieczeństwa jest wymagane w celu identyfikowania problemów dotyczących zabezpieczeń, takich jak błędne konfiguracje i awarie. Dane dotyczące zdarzeń w środowisku OT mogą obejmować dane procesów fizycznych, dane dotyczące użytkowania systemu i dane sieciowe.

Tabela 16. Podatności dotyczące utrzymania oraz konfiguracji oraz stany predyspozycji

Podatność	Opis
Sprzęt, oprogramowanie układowe i oprogramowanie nieobjęte procesem zarządzania zasobami	Organizacja, która nie ma kompleksowych informacji na temat używanych urządzeń, ich lokalizacji oraz wersji oprogramowania nie jest w stanie zapewnić ich skutecznej i spójnej ochrony. Skuteczne zabezpieczenie systemów OT wymaga przeprowadzenia inwentaryzacji zasobów w środowisku. Należy wdrożyć procedury zarządzania dodawaniem, usuwaniem i modyfikowaniem zasobów, które obejmują zarządzanie ich inwentaryzacją. Procedury te mają kluczowe znaczenie dla realizacji planów ciągłości działania i odtworzenia po katastrofie.
Sprzęt, oprogramowanie układowe i oprogramowanie nieobjęte procesem zarządzania konfiguracją	Gdy organizacja nie zna stanu zarządzania poprawkami, ustawień zabezpieczeń ani wersji konfiguracji, skutkiem jest niespójna i nieskuteczna ochrona systemów. Brak procedur zarządzania zmianami konfiguracji może prowadzić do błędów wpływających na bezpieczeństwo, narażenie i ryzyko. Należy wdrożyć proces modyfikacji sprzętu, oprogramowania układowego, oprogramowania i ich dokumentowania w celu zabezpieczenia systemów OT przed niewłaściwymi modyfikacjami przed, w trakcie i po wdrożeniu systemu. Skuteczne zabezpieczenie systemów OT wymaga stworzenia listy lub repozytorium konfiguracji zasobów wykorzystywanych w środowisku.
Poprawki do systemów operacyjnych i oprogramowania mogą zostać wydane z opóźnieniem względem wykrycia podatności.	Ze względu na ścisłe powiązanie między oprogramowaniem OT i systemami OT, zmiany muszą być poddawane kosztownym i czasochłonnym testom regresji. Czas poświęcony na testy oraz długi czas dystrybucji aktualizacji oznacza, że systemy mogą pozostawać podatne na ataki przez dłuższy czas. Procedury zarządzania podatnościami powinny zapewniać możliwość wdrożenia tymczasowych alternatywnych zabezpieczeń.

Podatność	Opis
Odmowa opracowania poprawki podatności przez producenta	Nieaktualne systemy operacyjne i aplikacje mogą zawierać nowe podatności, które mogą zostać wykorzystane przez napastników. Niektóre starsze systemy mogą nie być obsługiwane przez producentów, w związku z czym procedury zarządzania podatnościami powinny obejmować plany awaryjne pozwalające na ograniczenie potencjalnego wpływu podatności, dla których nie zostaną wydane poprawki, a także plany wymiany komponentów systemu.
Brak programu zarządzania podatnościami	Podatności nieuwzględnione przez organizację mogą zostać wykorzystane przez napastników. Stosowne procedury zarządzania podatnościami powinny określać plany działania w przypadku wykrycia podatności lub jasno wskazywać, że żadne działania nie zostaną podjęte. W przypadku systemów OT konieczne może być uwzględnienie szeregu kwestii, między innymi dostępności stosownych poprawek, konieczności zaplanowania instalacji poprawek w czasie kolejnej konserwacji, a także braku poprawek bezpieczeństwa dla wybranych systemów OT działających pod kontrolą przestarzałych systemów operacyjnych. Ponadto odizolowane systemy mogą nie wymagać natychmiastowej instalacji poprawek, z kolei systemy OT podłączone do Internetu mogą wymagać ich instalacji w pierwszej kolejności.
Niedostateczne testy zmian dotyczących bezpieczeństwa	Zmiany sprzętu, oprogramowania układowego i oprogramowania wdrożone bez przeprowadzenia stosownych testów mogą wpłynąć negatywnie na działanie systemów OT. Należy opracować udokumentowane procedury testowania wszystkich zmian pod kątem wpływu na bezpieczeństwo. Systemy produkcyjne nie powinny być używane do testowania zmian. Testowanie modyfikacji systemu może wymagać koordynacji z producentami oraz integratorami systemów.
Niedostateczne zabezpieczenia zdalnego dostępu	Zdalny dostęp do systemów OT może być wymagany z wielu powodów. Producenci lub integratorzy systemów mogą wymagać go w celu konserwacji systemu, a inżynierowie OT mogą uzyskiwać w ten sposób dostęp do komponentów zainstalowanych w odległych lokalizacjach. Mechanizmy zdalnego dostępu powinny być wdrażane zgodnie z zasadą minimalnych uprawnień. Możliwości zdalnego dostępu muszą być odpowiednio zabezpieczone, aby uniemożliwić nieupoważnionym osobom uzyskanie dostępu do systemów OT, a także by uniemożliwić upoważnionym użytkownikom uzyskanie nadmiernego dostępu.
Niedostatecznie bezpieczne konfiguracje	Nieprawidłowo skonfigurowane systemy mogą oferować otwarte porty i protokoły, które nie są wymagane do ich prawidłowego działania. Tego rodzaju funkcje mogą zawierać podatności, które zwiększają ogólne ryzyko dla systemu. Korzystanie z domyślnych konfiguracji często przekłada się na zwiększenie liczby podatności, które może wykorzystać napastnik. Z tego powodu należy zweryfikować wszystkie konfiguracje i poszczególne ustawienia.

Podatność	Opis
Brak kopii zapasowych i magazynu krytycznych konfiguracji	Organizacja powinna wdrożyć procedury przywracania ustawień konfiguracji systemów OT w przypadku przypadkowych lub wprowadzonych przez napastników zmian konfiguracji, aby utrzymać dostępność systemu i zapobiec utracie danych. Należy opracować i udokumentować procedury utrzymywania ustawień konfiguracyjnych.
Niezabezpieczone dane na urządzeniu przenośnym	Bezpieczeństwo systemu może być zagrożone, jeśli wrażliwe dane (np. hasła, numery dial-up) są przechowywane w postaci niezaszyfrowanej na zgubionych lub skradzionych urządzeniach przenośnych, takich jak laptopy i urządzenia mobilne. W celu ich ochrony konieczne jest wprowadzenie stosownych zasad, procedur i mechanizmów.
Korzystanie z domyślnych haseł producenta	Większość domyślnych haseł ustawianych przez producentów można łatwo znaleźć w instrukcjach obsługi produktów, które są dostępne dla potencjalnych napastników. Korzystanie z domyślnego hasła może drastycznie zwiększyć podatność systemów OT na zagrożenia.
Tworzenie, używanie i ochrona haseł niezgodne z zasadami Stosowanie nieodpowiednich środków kontroli dostępu	Zasady i procedury dotyczące haseł muszą być przestrzegane, aby były skuteczne. Naruszenie zasad i procedur dotyczących haseł może zwiększyć podatność systemów OT na ataki. Rozwiązania w zakresie kontroli dostępu muszą być zgodne z metodą przydzielania obowiązków i uprawnień pracownikom organizacji. Błędnie skonfigurowane rozwiązania w zakresie kontroli dostępu mogą spowodować, że użytkownicy systemów OT mogą mieć wiele lub zbyt mało uprawnień. Poniższe przykłady ilustrują każdy ze wskazanych przypadków: – System skonfigurowany z domyślnymi ustawieniami kontroli dostępu daje operatorowi uprawnienia administratora. – Błędna konfiguracja systemu powoduje, że operator nie jest w stanie podjąć działań naprawczych w sytuacji awaryjnej.
Niewłaściwe łączenie danych	Systemy przechowywania danych związane z systemami OT mogą być połączone ze źródłami danych innymi niż systemy OT. Z taką sytuacją mamy do czynienia na przykład, gdy powiązania między bazami danych umożliwiają automatyczną replikację danych z jednej bazy danych (np. magazynu danych) do innych baz. Takie połączenie może stanowić podatność, jeśli nie jest odpowiednio skonfigurowane i może umożliwić nieautoryzowany dostęp do danych lub ich modyfikację.
Brak rozwiązań chroniących przed złośliwym oprogramowaniem lub nieaktualne rozwiązania	Instalacja złośliwego oprogramowania w systemie stanowi powszechny rodzaj ataku. Rozwiązania chroniące przed złośliwym oprogramowaniem, takie jak oprogramowanie antywirusowe, powinny być aktualizowane,

Podatność	Opis
	w szczególności w dynamicznym środowisku. Nieaktualne rozwiązania chroniące przed złośliwym oprogramowaniem i wykorzystywane przez nie definicje sprawiają, że system jest podatny na zagrożenia ze strony takiego oprogramowania.
Wdrożenie ochrony przed złośliwym oprogramowaniem bez wystarczających testów	Rozwiązania chroniące przed złośliwym oprogramowaniem, które są wdrażane do środowiska bez przeprowadzenia stosownych testów, mogą wpływać negatywnie na normalne działanie systemów OT i uniemożliwiać skuteczne sterowanie procesem.
Odmowa świadczenia usługi (*ang. Denial of service – DoS*)	Oprogramowanie systemów OT może być podatne na ataki odmowy świadczenia usługi (DoS), skutkujące uniemożliwieniem dostępu do zasobów systemowych lub opóźnieniem działania i funkcji systemu.
Oprogramowanie wykrywające włamania i zapobiegające ich występowaniu nie jest zainstalowane	Incydenty mogą skutkować spadkiem dostępności i utratą integralności systemu, kradzieżą, modyfikacją lub usunięciem danych, a także nieprawidłowym wykonywaniem poleceń sterujących. Oprogramowanie IDS/IPS może powstrzymywać różne rodzaje ataków lub skutecznie przeciwdziałać ich wystąpieniu – dotyczy to także ataków DoS. Może także wskazywać zaatakowane hosty oraz urządzenia zainfekowane przez robaki. Oprogramowanie IDS/IPS powinno zostać przetestowane przed wdrożeniem, aby upewnić się, że nie wpłynie ono negatywnie na normalne działanie systemów OT.
Pliki dzienników nie są tworzone	Brak odpowiednich i dokładnych dzienników uniemożliwia ustalenie, jaki czynnik spowodował wystąpienie zdarzenia związanego z bezpieczeństwem i przeprowadzenie dochodzenia.

Tabela 17. Podatności fizyczne i stany predyspozycji

Podatność	Opis
Nieautoryzowani pracownicy mają fizyczny dostęp do urządzeń	Uprawnienia do fizycznego dostępu do urządzeń OT powinny być ograniczone wyłącznie do pracowników, którzy ich wymagają. Jednocześnie należy uwzględnić wymogi bezpieczeństwa, w tym procesy awaryjnego wyłączenia lub ponownego uruchomienia systemów. Stosowanie niewłaściwych uprawnień do urządzeń OT może prowadzić do jednej z poniższych sytuacji: – Fizycznej kradzieży danych i urządzeń. – Uszkodzenia lub zniszczenia danych i urządzeń. – Wprowadzenia zmian w procesie. – Wprowadzenia nieautoryzowanych zmian w środowisku OT (np. konfiguracji połączenia danych, użycia nośników wymiennych, dodania lub usunięcia urządzeń). – Odłączenia fizycznych łączy danych. – Niewykrywalnego gromadzenia danych (np. naciśnięć klawiszy i innych danych wejściowych).

Podatność	Opis
Zakłócenia częstotliwości radiowych, impuls elektromagnetyczny, wyładowania elektrostatyczne, przerwy w dostawie prądu i skoki napięcia	Niektóre urządzenia wykorzystywane w systemach OT są podatne na zakłócenia radiowe, impulsy elektromagnetyczne, wyładowania elektrostatyczne, przerwy w dostawie prądu i skoki napięcia. Takie działania mogą mieć zróżnicowane skutki od tymczasowego zakłócenia sterowania, aż do trwałego uszkodzenia płytek drukowanych. Zalecane jest odpowiednie ekranowanie, zastosowanie uziemienia, kondycjonowanie zasilania oraz tłumienie przepięć.
Brak zasilania awaryjnego	W przypadku braku zasilania awaryjnego krytycznych elementów systemu utrata zasilania spowoduje wyłączenie systemów OT i może doprowadzić do niebezpiecznej sytuacji. Utrata zasilania może również prowadzić do przywrócenia ustawień domyślnych bez odpowiednich zabezpieczeń. Jeśli plik programu lub dane są przechowywane w pamięci ulotnej, ponowne uruchomienie procesu po zaniku zasilania bez odpowiedniego zasilania awaryjnego może być niemożliwe.
Utrata możliwości sterowania parametrami środowiska	Utrata możliwości sterowania parametrami środowiska (np. temperaturą, wilgotnością powietrza) może prowadzić do uszkodzenia sprzętu, na przykład w wyniku przegrzania procesorów. Niektóre procesory wyłączają się automatycznie, aby zapobiec wystąpieniu awarii. Inne mogą nadal działać z ograniczoną wydajnością i generować sporadyczne błędy, samoczynnie uruchomić się ponownie lub ulec nieodwracalnej awarii.
Niezabezpieczone porty fizyczne	Niezabezpieczone porty uniwersalnej magistrali szeregowej (*ang. universal serial bus – USB*) i PS/2 mogą umożliwiać nieautoryzowane podłączanie pamięci przenośnych lub rejestratorów naciśnięć klawiszy.

Tabela 18. Podatności dotyczące rozwoju oprogramowania oraz stany predyspozycji

Podatność	Opis
Nieprawidłowa weryfikacja danych	Oprogramowanie OT może nieprawidłowo weryfikować dane wprowadzane przez użytkownika lub przez sieć w celu zapewnienia ich poprawności. Nieprawidłowe dane mogą skutkować powstaniem licznych podatności, w tym przepełnień bufora, możliwości wykonania nieautoryzowanych poleceń, a także podatności na ataki XSS oraz ataki typu *path traversal*.
Dostępne zdolności do ochrony nie są domyślnie włączone	Zdolności do ochrony, takie jak funkcje zabezpieczeń, które zostały zainstalowane wraz z produktem, są bezużyteczne, jeśli nie są włączone lub zostały nieświadomie wyłączone.
Niedostateczne uwierzytelnianie, uprawnienia i kontrola dostępu w oprogramowaniu	Nieautoryzowany dostęp do oprogramowania konfiguracyjnego i programistycznego może umożliwić uszkodzenie urządzenia.

Tabela 19. Podatności dotyczące łączności i konfiguracji sieci oraz stany predyspozycji

Podatność	Opis
Brak zabezpieczeń przepływów danych	Zabezpieczenia przepływu danych oparte na charakterystyce danych są potrzebne w celu ograniczenia przepływu informacji między systemami. Zabezpieczenia te mogą zapobiec wyciekom danych oraz niedozwolonym działaniom.
Zapory sieciowe nie istnieją lub zostały nieprawidłowo skonfigurowane	Brak odpowiednio skonfigurowanych zapór sieciowych może pozwolić na przesyłanie niepotrzebnych danych między sieciami, na przykład między siecią sterowania i siecią korporacyjną, umożliwiając rozprzestrzenianie się ataków i złośliwego oprogramowania między sieciami, monitorowanie i kradzież danych, a także nieautoryzowany dostęp do systemów.
Brak odpowiednich dzienników zapór sieciowych i routerów	Bez właściwego i dokładnego gromadzenia danych ustalenie przyczyny incydentu bezpieczeństwa może być niemożliwe.
Korzystanie ze standardowych, dobrze udokumentowanych protokołów komunikacyjnych bez szyfrowania	Napastnicy monitorujący aktywność w sieciach OT mogą korzystać z narzędzi do analizowania protokołów w celu dekodowania danych przesyłanych za pośrednictwem protokołów takich jak telnet, protokół transferu plików (*ang. File Transfer Protocol – FTP*), protokół HTTP (*ang. Hypertext Transfer Protocol*) czy NFS (*ang. Network File System*). Korzystanie z takich protokołów ułatwia również napastnikom przeprowadzanie ataków na systemy OT i manipulowanie aktywnością sieci OT.
Nieistniejące lub niespełniające norm uwierzytelnianie użytkowników, danych lub urządzeń	Wiele protokołów OT nie posiada żadnych funkcji uwierzytelniania. Brak uwierzytelniania umożliwia odtwarzanie, modyfikowanie lub fałszowanie danych, w tym informacji z czujników oraz danych dotyczących tożsamości użytkowników.
Korzystanie z niezabezpieczonych protokołów OT	Protokoły OT często nie są wyposażone w żadne funkcje bezpieczeństwa takie jak uwierzytelnianie i szyfrowanie, chroniące dane przed nieautoryzowanym dostępem lub modyfikacją. Istniejące funkcje są z kolei często ograniczone. Także nieprawidłowa implementacja protokołów może przekładać się na dodatkowe podatności.
Brak weryfikacji integralności komunikacji	Weryfikacja integralności komunikacji to funkcja, która nie istnieje w większości protokołów OT, co umożliwia napastnikom modyfikację komunikacji w sposób niezauważony. Aby zapewnić integralność, systemy OT mogą korzystać z protokołów niższej warstwy (np. IPsec), które oferują ochronę integralności danych podczas przesyłania za pośrednictwem niezaufanych łączy fizycznych.
Brak odpowiedniego uwierzytelniania między klientami bezprzewodowymi a punktami dostępowymi	Silne uwierzytelnianie między klientami bezprzewodowymi a punktami dostępowymi jest konieczne w celu zapewnienia, że urządzenia OT nie będą w stanie połączyć się z niezaufanym punktem dostępowym zainstalowanym przez napastnika oraz uniemożliwienia podłączenia urządzeń napastników do sieci bezprzewodowych OT.

Podatność	Opis
Brak odpowiedniej ochrony danych przesyłanych pomiędzy urządzeniami bezprzewodowymi a punktami dostępowymi	Wrażliwe dane przesyłane między urządzeniami i punktami dostępowymi powinny być chronione przy użyciu silnego szyfrowania, aby zapewnić, że napastnicy nie będą w stanie uzyskać nieautoryzowanego dostępu do niezaszyfrowanych danych.

Tabela 20. Podatności dotyczące czujników, elementów wykonawczych oraz zarządzania zasobami oraz stany predyspozycji

Podatność	Opis
Nieautoryzowany dostęp fizyczny do czujników lub urządzeń wykonawczych	Fizyczny dostęp do czujników i urządzeń wykonawczych pozwala na bezpośrednią modyfikację procesów fizycznych. Wiele urządzeń wykorzystujących magistralę Fieldbus jest skonfigurowane w taki sposób, że fizyczny dostęp do sieci czujników pozwala na manipulowanie parametrami sterowania. Należy ograniczyć fizyczny dostęp do całej pętli w celu zapobiegania incydentom.
Nieautoryzowany bezprzewodowy dostęp do czujników lub urządzeń wykonawczych	Bezprzewodowy dostęp do czujników i urządzeń wykonawczych pozwala na bezpośrednią manipulację procesem fizycznym. Wiele inteligentnych urządzeń udostępnia opcje konfiguracji bezprzewodowej (np. przez Bluetooth, Wi-Fi, WirelessHART). Dostęp bezprzewodowy powinien być zabezpieczony lub wyłączony przy użyciu sprzętowej ochrony przed zapisem wszędzie tam, gdzie to możliwe, aby zapobiec nieautoryzowanej modyfikacji czujników i urządzeń wykonawczych, które są podłączone zarówno do procesu fizycznego, jak i środowiska OT.
Niewłaściwa segmentacja systemu zarządzania zasobami	Większość architektur jest zaprojektowana z myślą o tym, by sterowniki PLC, urządzenia RTU, a także systemy DCS i SCADA odpowiadały za sterowanie procesem, z kolei systemy zarządzania zasobami monitorują zasoby podłączone do sterowników. Wiele systemów zarządzania zasobami ma opcje modyfikowania konfiguracji czujników i urządzeń wykonawczych, choć nie stanowi to ich podstawowej funkcji. System zarządzania zasobami powinien być zabezpieczony, jeśli ma funkcje pozwalające na zmianę parametrów procesu.

C.3 ZDARZENIE POWODUJĄCE ZAGROŻENIE I INCYDENTY

Zdarzenie powodujące zagrożenie to zdarzenie lub sytuacja powiązane ze źródłem zagrożenia, które może skutkować niepożądanymi konsekwencjami lub wpływem na działanie systemu. Załącznik E do dokumentu NSC 800-30 [NSC 800-30] określa szeroki zakres zdarzeń powodujących zagrożenie, które mogą wpływać na systemy informacyjne. Unikalne właściwości systemów OT mogą przekładać się na możliwość wystąpienia wyjątkowych zdarzeń powodujących zagrożenie, wiążących się na przykład z możliwością zmian w OT w celu spowodowania szkód fizycznych. **Tabela 21** przedstawia omówienie potencjalnych zdarzeń powodujących zagrożenia dla systemów OT w oparciu o ramy MITRE ATT&CK® dla systemów sterowania przemysłowego [ATTACK-ICS].

Tabela 21. Przykłady potencjalnych zdarzeń powodujące zagrożenie

Zdarzenie powodujące zagrożenie	Opis
Uniemożliwienie sterowania	Tymczasowo uniemożliwia operatorom i inżynierom dostęp do elementów odpowiedzialnych za sterowanie procesem. Proces, którego to dotyczy, może nadal działać pomimo utraty sterowania, jednak jego stan może odbiegać od założeń i oczekiwań.
Wpływ na sterowanie	Nieautoryzowane zmiany zaprogramowanych instrukcji w sterownikach PLC, urządzeniach RTU, systemach DCS lub SCADA, zmiana wartości wywołujących alarmy lub wydawanie nieautoryzowanych poleceń urządzeniom sterującym. Zmiany te mogą potencjalnie skutkować uszkodzeniem sprzętu (w przypadku przekroczenia dopuszczalnych granic), przedwczesnym wyłączeniem procesów (np. linii przesyłowych), incydentem środowiskowym, a nawet uszkodzeniem urządzeń sterujących.
Sfałszowane komunikaty	Sfałszowane informacje wysyłane do operatora systemu OT w celu uniknięcia wykrycia lub zakłócenia sterowania procesem. Napastnik może sprawić, że osoby odpowiedzialne za bezpieczeństwo i operatorzy uznają, że w systemie występują inne błędy, aby odwrócić ich uwagę od rzeczywistego źródła problemu (np. przez wywołanie wielu alarmów).

Zdarzenie powodujące zagrożenie	Opis
Kradzież informacji dotyczących działania systemu	Przeciwnicy mogą wykraść informacje dotyczące działania systemu dla osobistych korzyści lub w celu planowania przyszłych działań.
Utrata bezpieczeństwa	Napastnicy mogą atakować i wyłączać funkcje systemu bezpieczeństwa przed przeprowadzeniem ataku lub w celu uniemożliwienia weryfikacji niebezpiecznych poleceń.
Utrata dostępności	Napastnicy mogą wykorzystywać złośliwe oprogramowanie w celu usunięcia lub zaszyfrowania krytycznych danych w interfejsach człowiek-maszyna, stacjach roboczych lub bazach danych.

Dotychczas zostały zgłoszone i udokumentowane liczne incydenty dotyczące systemów OT. Opisy tych zdarzeń ilustrują wagę zagrożeń i podatności, a także wskazują na wpływ incydentów dotyczących systemów OT. Jak czytamy w Załączniku C.2, wyróżniamy cztery kategorie źródeł zagrożenia – agresywne, przypadkowe, strukturalne oraz środowiskowe. Wystąpienie incydentu może być wynikiem oddziaływania wielu źródeł zagrożeń; na przykład zdarzenie środowiskowe może spowodować awarię systemu, a błąd operatora podczas awarii skutkuje wystąpieniem przypadkowego zdarzenia.

Autorzy niniejszego dokumentu zgromadzili zestawienie wybranych zgłoszonych incydentów, które zostały przypisane do każdej z czterech powyższych kategorii. Incydenty zostały dodatkowo określone mianem złośliwych lub niezłośliwych, a także bezpośrednich lub pośrednich, aby umożliwić dokładniejsze rozróżnienie możliwych przyczyn występowania incydentów dotyczących systemów OT.

Z = Złośliwy. Zdarzenie zostało wywołane celowo przez osobę lub podmiot w celu wywołania szkód. Osoba odpowiedzialna za wywołanie zdarzenia mogła (lecz nie musiała) obrać za cel systemy OT, mogła też być lub nie być świadoma możliwych konsekwencji.

N = Niezłośliwy. Brak jednoznacznych dowodów na to, że zdarzenie miało na celu spowodowanie incydentu.

B = Bezpośredni. Zdarzenie miało na celu odkrycie, zatrzymanie, uszkodzenie lub wpłynięcie w inny sposób na system OT.

P = Pośredni. Brak jednoznacznych dowodów na to, że zdarzenie miało na celu odkrycie, zatrzymanie, uszkodzenie lub wpłynięcie w inny sposób na system OT. System OT wyłączył się lub wpłynął na otoczenie ze względu na wpływ incydentu na infrastrukturę pomocniczą.

C.3.1. ZDARZENIA AGRESYWNE

- **[Z][B] Bezprzewodowy atak na wynalazek Marconiego**[17]. W 1903 roku włoski wynalazca Guglielmo Marconi przygotowywał się do swojej pierwszej publicznej demonstracji bezpiecznej komunikacji bezprzewodowej na duże odległości – przesłania wiadomości z Kornwalii do profesora Fleminga w Royal Institution of London. Wynalazca i magik Nevil Maskelyne uzyskał dostęp do systemu i wysłał komiczną wiadomość zakodowaną alfabetem Morse'a odnoszącą się do szczurów. Następnie Maskelyne opublikował opis swojego wyczynu w czasopiśmie branżowym *The Electrician*.
- **[Z][P] Komunikacja dotycząca ruchu lotniczego w Worcester.**[18]. W marcu 1997 roku nastolatek z Worcester w stanie Massachusetts wyłączył część publicznej sieci telefonicznej za pomocą modemu dial-up podłączonego do systemu. Spowodowało to wyłączenie usług telefonicznych w wieży kontroli lotów, budynku ochrony lotniska, lotniskowej jednostce straży pożarnej, siedzibie służb meteorologicznych i przewoźników korzystających z lotniska. Wyłączony został także główny nadajnik radiowy wieży i inny nadajnik, który aktywował światła pasa startowego, a nawet drukarka, której kontrolerzy używali do monitorowania lotów. Atak spowodował również wyłączenie usług telefonicznych w 600 gospodarstwach domowych i przedsiębiorstwach w pobliskim miasteczku Rutland.

[17] Dodatkowe informacje na temat incydentu można znaleźć na stronie https://www.osti.gov/biblio/1505628.

[18] Dodatkowe informacje na temat incydentu można znaleźć na stronie http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html

- **[Z][B] Wyciek ścieków w Maroochy Shire**[19]. Wiosną 2000 roku były pracownik australijskiej organizacji odpowiedzialnej za oprogramowanie wykorzystywane w produkcji ubiegał się o pracę na stanowisku samorządowym, jednak jego kandydatura została odrzucona. W ciągu dwóch miesięcy zawiedziony kandydat użył nadajnika radiowego aż 46 razy, aby zdalnie włamać się do systemu odpowiedzialnego za sterowanie oczyszczaniem ścieków. W ten sposób był w stanie zmienić ustawienia wybranych przepompowni ścieków i spowodował awarie, czego skutkiem był wyciek miliona litrów nieprzetworzonych ścieków do pobliskich rzek i parków.
- **[Z][P] Night Dragon**[20]. Spółka McAfee poinformowała o serii ataków, które miały na celu kradzież poufnych danych globalnych spółek naftowych, energetycznych i petrochemicznych. Przestępcy zdołali zdobyć poufne dane dotyczące działalności spółek oraz informacje o finansowaniu projektów, a także dane dotyczące ofert i działalności na polach naftowych i gazowych.
- **[Z][B] Wirówki gazowe w Iranie i Stuxnet**[21]. Stuxnet był robakiem komputerowym infekującym komputery pracujące pod kontrolą systemu Microsoft Windows odkrytym w lipcu 2010 roku. Jego celem było oprogramowanie i urządzenia przemysłowe. Robak początkowo rozprzestrzeniał się masowo, jednak zawierał także wysoce wyspecjalizowany złośliwy kod zaprojektowany z myślą o atakowaniu wybranych systemów SCADA, skonfigurowanych do kontrolowania i monitorowania określonych procesów przemysłowych.
- **[Z][B] Atak na niemiecką hutę stali**[22]**.** W 2014 roku hakerzy zakłócili działanie systemów sterowania w znaczącym stopniu, uniemożliwiając prawidłowe wyłączenie wielkiego pieca, co spowodowało nieokreślone, lecz znaczące szkody.

---

[19] Dodatkowe informacje na temat incydentu można znaleźć na stronie http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

[20] Spółka McAfee opublikowała sprawozdanie na temat ataku Night Dragon dostępne pod adresem https://www.heartland.org/_template-_assets/documents/publications/29423 .pdf.

[21] Dodatkowe informacje na temat robaka Stuxnet można znaleźć na stronie https://www.wired.com/2014/11 /countdown-to-zero-day-stuxnet/.

[22] Dodatkowe informacje na temat incydentu w niemieckiej hucie stali można znaleźć na stronie http://www.wired.com/2015/01/german-steel-mill-hack-desiruction/.

- **[Z][P] Shamoon**[23]**.** W 2012 roku spółka Saudi Aramco padła ofiarą ataku wykorzystującego złośliwe oprogramowanie, wymierzonego w rafinerie. Oprogramowanie nadpisało główne rekordy rozruchowe (*ang. master boot records – MBR*) zaatakowanych systemów, tablice partycji i inne pliki danych. W efekcie jego działania systemy uległy awarii.
- **[Z][B] Zapora w Nowym Jorku**[24]**.** W 2013 roku irańska spółka zajmująca się bezpieczeństwem komputerowym uzyskała zdalny dostęp do komputera, który kontrolował system SCADA tamy Bowman w Rye w stanie Nowy Jork. Napastnicy byli w stanie uzyskać dostęp do danych na temat poziomu wody, temperatury i stanu śluzy. Sterowanie wrotami śluzy zostało odłączone w celu przeprowadzenia konserwacji, która miała miejsce w czasie uzyskania dostępu, co uniemożliwiło zdalne sterowanie zaporą.
- **[Z][B] Kampania Dragonfly, Havex**[25]**.** Sektor energetyczny był celem wieloletniej kampanii szpiegowskiej, opartej głównie na złośliwym oprogramowaniu Havex. Havex to koń trojański umożliwiający zdalny dostęp, wykorzystujący standard Open Platform Communications (OPC) do zbierania informacji o podłączonych systemach sterowania przemysłowego w sieci. Kampanie miały charakter rozpoznawczy.
- **[Z][B] Ukraińska sieć energetyczna, BlackEnergy3**[26]**.** W dniu 23 grudnia 2015 roku ukraińskie spółki energetyczne padły ofiarami cyberataku, który spowodował przerwy w dostawie prądu do ponad 225 000 klientów w Ukrainie. Efektem ataku było zadziałanie wyłączników przeszło 50 regionalnych stacji transformatorowych. Złośliwe oprogramowanie KillDisk zostało wykorzystane do usunięcia plików

[23] Dodatkowe informacje na temat ataku Shamoon można znaleźć na stronie https://www.cisa.gov/uscert/ics/monitors/ICS-MM201209.

[24] Akt oskarżenia Departamentu Sprawiedliwości Stanów Zjednoczonych w sprawie ataków na tamę w Nowym Jorku można znaleźć pod adresem https://www.justice.gov/opa/file/834996/download.

[25] Dodatkowe informacje na temat kampanii Dragonfly/Energetic Bear można znaleźć na stronie https://www.osti.gov/servlets/purl/1505628.

[26] Dodatkowe informacje na temat pierwszego ataku na ukraińską sieć energetyczną można znaleźć na stronie https://info.publicintelligence.net/NCCIC- UkrainianPowerAttack.pdf.

z docelowych systemów, w tym co najmniej jednego interfejsu człowiek-maszyna pracującego pod kontrolą systemu Windows. Napastnicy uszkodzili również oprogramowanie układowe urządzeń pozwalających na połączenie urządzeń wykorzystujących interfejsy szeregowe do sieci Ethernet. Był to pierwszy znany cyberatak na sieć energetyczną.

- **[Z][B] Ukraińska sieć energetyczna, Industroyer**[27]**.** W dniu 17 grudnia 2016 roku doszło do cyberataku na stację transformatorową pod Kijowem, co spowodowało przerwę w dostawie prądu przez około godzinę. Atak ten był pierwszym znanym przypadkiem wykorzystania złośliwego oprogramowania zaprojektowanego z myślą o ataku na urządzenia wchodzące w skład sieci energetycznej.
- **[Z][P] Maersk, NotPetya. W** 2017 roku w wyniku działania złośliwego oprogramowania NotPetya dyski twarde komputerów na całym świecie zostały nieodwracalnie zaszyfrowane. Chociaż pierwszym celem oprogramowania były ukraińskie przedsiębiorstwa, wkrótce rozpowszechniło się na całym świecie, w związku z czym ucierpiały spółki takie jak Maersk, FedEx, Merck i Saint-Gobain. Złośliwe oprogramowanie zniszczyło dane i zakłóciło działalność transportową realizowaną przez Maersk, powodując straty finansowe sięgające przeszło 300 milionów dolarów.
- **[Z][B] Saudi Petrochem, TRITON**[28]**.** Zakład petrochemiczny w Arabii Saudyjskiej został zaatakowany przy użyciu złośliwego oprogramowania, którego celem był przemysłowy system bezpieczeństwa. System zainicjował bezpieczne wyłączenie procesu petrochemicznego w 2017 roku po wykryciu niezgodności kodu pomiędzy trzema procesorami.

[27] Dodatkowe informacje na temat złośliwego oprogramowania Industroyer można znaleźć pod adresem https://us-cert.cisa.gov/ncas/alerts/TA17-163A.

[28] Dodatkowe informacje na temat ataku TRITON można znaleźć na stronie https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections.

- **[Z][P] Norsk Hydro, LockerGoga**[29]**.** W marcu 2019 roku spółka Norsk Hydro padła ofiarą cyberataku, w którym wykorzystano oprogramowanie ransomware LockerGoga do szyfrowania plików komputerowych. Spółka zajmująca się produkcją aluminium oraz energetyką odnawialną musiała przełączyć systemy na sterowanie ręczne, jednocześnie otwarcie informując opinię publiczną o postępach w zakresie odtwarzania systemów. Przejrzystość Norsk Hydro w całym procesie odtwarzania systemów stanowiła zdaniem specjalistów zajmujących się bezpieczeństwem wzór do naśladowania.
- **[Z][P] Rurociąg Colonial Pipeline**[30]**.** W maju 2021 roku atak przy użyciu oprogramowania ransomware spowodował wyłączenie rurociągu o długości ponad 8800 kilometrów, transportującego na wschodnie wybrzeże USA przeszło 400 milionów litrów rafinowanych produktów dziennie. Rurociąg Colonial Pipeline padł ofiarą cyberataku, który doprowadził do zaszyfrowania systemów IT w wyniku wykorzystania przestarzałego profilu VPN. Dochodzenie jest w toku, ale w chwili opracowania niniejszego dokumentu nie ma żadnych dowodów potwierdzających, że oprogramowanie ransomware miało bezpośredni wpływ na środowisko OT. Spółka Colonial podjęła decyzję o wyłączeniu rurociągu, aby ograniczyć wszelkie potencjalne szkody. Zapadła także decyzja o wypłaceniu okupu grupie cyberprzestępczej Darkside, aby uzyskać wszystkie możliwe narzędzia, w tym oprogramowanie deszyfrujące, pozwalające na odtworzenie systemów. Władzom USA udało się odzyskać część zapłaconego okupu[31].

[29] Dodatkowe informacje na temat ataku na spółkę Norsk Hydro można znaleźć na stronach https://news.microsoft.com/transform/hackers-hit-norsk-hvdro-ransomware- company-responded-transparency/, https://doublepulsar.com/how-lockergoga-took-down-hvdro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880, oraz https://www.darkreading.com/application-securitv/ransomware/norsk-hvdro-this-is-how-vou-react-to-a-ransomware-breach/a/d-id/750396.

[30] Dodatkowe informacje na temat incydentu można znaleźć na stronach https://www.c-span.org/video/?512247-1/senate-homeland-securitv-hearing-colonial-pipeline-cyber-attack oraz https://www.hsgac.senate.gov/imo/media/doc/Testimonv-Blount-2021-06-08.pdf.

[31] Dodatkowe informacje można znaleźć na stronie nahttps://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

- **[Z][P] Atak ransomware na system ochrony zdrowia**[32]**.** Szereg przypadków wykorzystania złośliwego oprogramowania dystrybuowanego za pośrednictwem ataków phishingowych wymierzonych w sektor opieki zdrowotnej i zdrowia publicznego w celu zakłócenia działalności i kradzieży danych. Jesienią 2020 roku został wydany alert CISA (AA20-302A) ostrzegający organizacje działające w sektorze opieki zdrowotnej i zdrowia publicznego o powszechności tych ataków.

C.3.2. ZDARZENIA STRUKTURALNE

- **[N][B] Awaria rurociągu transportującego benzynę w Bellingham w stanie Waszyngton**[33]**.** W czerwcu 1999 roku awaria rurociągu o przekroju 40 centymetrów doprowadziła do wycieku miliona litrów benzyny, a następnie do wybuchu pożaru zaledwie 1,5 godziny później. Zdarzenie doprowadziło do śmierci trzech osób, osiem osób odniosło obrażenia, dodatkowym skutkiem były duże straty materialne. Zakres awarii spotęgowały systemy sterowania, które nie były w stanie wykonywać funkcji sterowania i monitorowania rurociągu. Bezpośrednio przed wystąpieniem incydentu oraz w jego trakcie system kontroli nadzorczej i pozyskiwania danych (SCADA) działał z niską wydajnością, która uniemożliwiała pracownikom dostrzeżenie problemów oraz podjęcie odpowiednich działań. Kluczowym zaleceniem zawartym w sprawozdaniu NTSB wydanym w październiku 2002 roku było wdrożenie systemu testowego pozwalającego na implementowanie i testowania zmian w bazie danych systemu SCADA.
- **[Z][P] System sygnalizacji kolejowej CSX**[34]**.** W sierpniu 2003 roku wirus komputerowy Sobig został wskazany jako przyczyna awarii systemu sygnalizacji kolejowej na całym wschodnim wybrzeżu USA. Wirus zainfekował system komputerowy w siedzibie spółki CSX Corp. w Jacksonville w stanie Floryda

[32] Dodatkowe informacje na temat złośliwego oprogramowania atakującego organizacje działające w sektorze ochrony zdrowia można znaleźć na stronie Ransomware Activity Targeting the Healthcare and Public Health Sector | CISA.

[33] Dodatkowe informacje na temat awarii rurociągu w Bellingham w stanie Waszyngton można znaleźć pod adresem http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.

[34] Dodatkowe informacje na temat incydentu można znaleźć na stronie http://www.infonnationweek.com/storv/showArticle.jhtmParticleIDM3100807.

i doprowadził do wyłączenia sygnalizacji, stacji dyspozytorów oraz innych systemów. Dan Stessel, rzecznik prasowy spółki Amtrak, poinformował, że atak spowodował awarię 10 pociągów Amtrak. Pociągi między Pittsburghiem w stanie Pensylwania i Florence w stanie Karolina Południowa zostały zatrzymane z powodu awarii sygnalizacji, z kolei jeden z pociągów regionalnych spółki Amtrak z Richmond w stanie Wirginia do Waszyngtonu i Nowego Jorku był opóźniony o ponad dwie godziny. Pociągi dalekobieżne również zanotowały opóźnienia sięgające od czterech do sześciu godzin.

- **[N][B] Awaria sterownika PLC w elektrowni Browns Ferry-3**[35]**.** W sierpniu 2006 roku spółka TVA została zmuszona do ręcznego wyłączenia jednego z dwóch reaktorów elektrowni w wyniku awarii dwóch pomp wody zagrażającej stabilności elektrowni. Awaria pomp była skutkiem wyłączenia sterowników PLC. Pomimo istnienia dwóch oddzielnych sterowników PLC, były one podłączone do tej samej sieci Ethernet. Późniejsze testy uszkodzonych urządzeń wykazały, że ulegały one awarii w wyniku nadmiernego ruchu sieciowego.

C.3.3. ZDARZENIA ŚRODOWISKOWE

- **[N][P] Katastrofa nuklearna w elektrowni Fukushima Daiichi**[36]**.** Trzęsienie ziemi o wysokiej magnitudzie u wybrzeży wschodniej Japonii, które miało miejsce 11 marca 2011 roku, wywołało potężną falę tsunami, która uderzyła w elektrownię jądrową zlokalizowaną przy brzegu. Fala przelała się ponad falochronem elektrowni, zalewając większość terenu, w tym budynek mieszczący generatory awaryjne. Zasilanie awaryjne było wymagane do obsługi pomieszczeń sterowania oraz zasilania obiegu wody chłodzącej reaktory. Utrata czynnika chłodzącego spowodowała przegrzanie rdzeni reaktorów do poziomu, w którym cyrkonowa osłona prętów paliwowych

[35] Dodatkowe informacje na temat awarii sterowników PLC w elektrowni Browns Ferry -3 można znaleźć na stronie http://www.nrc.gov/reading-m/doc-collections/gen-comm/info-notices/2007/in200715.pdf.

[36] Dodatkowe informacje można znaleźć na stronie http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final- Fukushima-Mission_Report.pdf and http://pbadupws.nrc.gov/docs/ML1414/ML14140A185.pdf.

zaczęła reagować z wodą, wytwarzając wodór. Eksplozja gazu nastąpiła w trzech z czterech budynków reaktorów. Skutkiem zdarzenia było duże skażenie radioaktywne, którego skutki odczuli pracownicy elektrowni, mieszkańcy oraz lokalne środowisko. Badanie przyczyn zdarzenia wykazało, że centrum reagowania kryzysowego w elektrowni nie dysponowało wystarczającą liczbą bezpiecznych linii komunikacyjnych, aby zapewnić płynny obieg informacji na temat kluczowych elementów systemów odpowiedzialnych za bezpieczeństwo.

C.3.4. PRZYPADKOWE ZDARZENIA

- **[N][B] Incydenty związane ze skanowaniem podatności**[37]**.** Podczas testów aktywnej sieci SCADA sterującej 9-metrowymi ramionami robota nastąpiła aktywacja jednego z ramion i jego obrót o 180 stopni. Kontroler ramienia znajdował się w trybie czuwania zanim rozpoczęły się testy. W innym przypadku podobny test został przeprowadzony w systemie sterowania przemysłowego w celu zidentyfikowania hostów podłączonych do sieci w celach inwentaryzacyjnych, co spowodowało zawieszenie się systemu kontrolującego proces produkcji układów scalonych w zakładzie produkcyjnym. Test doprowadził do zniszczenia płytek krzemowych o wartości 50 000 dolarów.
- **[N][B] Incydent związany z testami penetracyjnymi**[38]**.** Przedsiębiorstwo gazownicze zatrudniło firmę konsultingową ds. bezpieczeństwa IT do przeprowadzenia testów penetracyjnych swojej firmowej sieci IT. Pracownicy odpowiedzialni za przeprowadzenie testów penetracyjnych przypadkowo dostali się części sieci, która była bezpośrednio połączona z systemem SCADA. Test doprowadził do awarii systemu SCADA, w wyniku której spółka nie była w stanie dostarczać gazu swoimi rurociągami przez cztery godziny.

[37] Dodatkowe informacje na temat incydentów związanych ze skanowaniem podatności można znaleźć na stronie https://energy.sandia.gov/wp-content/gallery/uploads/sand 2005 2846p.pdf.

[38] Dodatkowe informacje na temat incydentów związanych z testami penetracyjnymi można znaleźć na stronie https://energy.sandia.gov/wp-content/gallery/uploads/sand 2005 2846p.pdf.

- **[N][P] Działania NERC**[39]**.** W 2019 roku pewna amerykańska spółka energetyczna została ukarana grzywną w wysokości 10 milionów dolarów przez NERC za naruszenia dotyczące cyberbezpieczeństwa, które zostały stwierdzone w latach 2015-2018. Brak zgodności z obowiązującymi w Stanach Zjednoczonych standardami cyberbezpieczeństwa został uznany za zagrożenie dla bezpieczeństwa i niezawodności całego systemu energetycznego.
- **[N][B] Pożar w NASA**[40]**.** Pracownicy zainstalowali poprawkę bezpieczeństwa elementu systemu OT odpowiedzialnego za sterowanie pracą dużego pieca. Poprawka i ponowne uruchomienie urządzenia spowodowały, że piec przestał działać, co doprowadziło do pożaru, którego skutkiem było zniszczenie elementów statku kosmicznego. Ponowne uruchomienie systemu uniemożliwiło także aktywację alarmu, w związku z czym pożar nie został wykryty przez 3,5 godziny.
- **[N][B] Elektrownia jądrowa Hatch**[41]**.** W 2008 roku elektrownia jądrowa Hatch w stanie Georgia została awaryjnie wyłączona na czterdzieści osiem godzin po instalacji aktualizacji oprogramowania na jednym komputerze działającym pod kontrolą systemu Windows. Po ponownym uruchomieniu zaktualizowany komputer zresetował dane w systemie sterowania. Systemy bezpieczeństwa błędnie zinterpretowały brak danych jako spadek poziomu wody w zbiornikach chłodzących pręty paliwowe w reaktorze. W rezultacie zautomatyzowane systemy bezpieczeństwa spowodowały automatyczne wyłączenie reaktora.

Tłumaczenie

[39] Dodatkowe informacje na temat grzywien nakładanych na przedsiębiorstwa energetyczne można znaleźć na stronie Enforcement Actions 2019 (nerc.com). https://www.nerc.com/pa/comp/CE/Pages/Actions_2019/Enforcement-Actions-2019.aspx

[40] Dodatkowe informacje na temat niezamierzonych konsekwencji wdrażania zabezpieczeń IT w NASA znajdują się w sprawozdaniu agencji: Final Report - IG-17-011 (nasa.gov).

[41] Dodatkowe informacje na temat incydentu znajdują się na stronie https://www.homelandsecuritynewswire.com/cyber-mishap-causes-nuclear-power-plant-shutdown

ZAŁĄCZNIK D – ORGANIZACJE BEZPIECZEŃSTWA, BADANIA I DZIAŁANIA ZWIĄZANE Z BEZPIECZEŃSTWEM SYSTEMÓW OT

Niniejszy załącznik zawiera opisy wybranych działań dotyczących cyberbezpieczeństwa systemów OT. Opisy organizacji i związane z nimi informacje zawarte w niniejszym załączniku pochodzą głównie z witryn internetowych wymienionych organizacji i innych wiarygodnych źródeł publicznych, jednak autorzy niniejszego dokumentu nie podjęli się weryfikacji tych informacji. W związku z powyższym zachęcamy czytelników do bezpośredniego kontaktu z wymienionymi organizacjami w celu uzyskania najbardziej aktualnych informacji.

D.1 KONSORCJA I ORGANIZACJE NORMALIZACYJNE

D.1.1. KOMITET DORADCZY DS. PARTNERSTWA NA RZECZ INFRASTRUKTURY KRYTYCZNEJ (*ANG. CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL – CIPAC*)

Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych powołał Komitet doradczy ds. partnerstwa na rzecz infrastruktury krytycznej (CIPAC) w celu usprawnienia kontaktów między instytucjami państwowymi i właścicielami oraz operatorami infrastruktury krytycznej. CIPAC realizuje założenia Krajowego Planu Ochrony Infrastruktury (*ang. National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*) oraz dyrektywy Prezydenta Stanów Zjednoczonych nr 21 w sprawie bezpieczeństwa i odporności infrastruktury krytycznej (*ang. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*) pełniąc funkcję forum, w ramach którego przedstawiciele rządu oraz podmiotów sektora prywatnego współpracują w ramach komitetów koordynacyjnych w celu realizacji szeroko zakrojonych działań w zakresie bezpieczeństwa i odporności infrastruktury krytycznej.

https://www.cisa.gov/critical-infrastructure-partnership-advisorv-council

D.1.2. INSTYTUT OCHRONY INFRASTRUKTURY INFORMACYJNEJ (ANG. INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION – I3P)

Instytut Ochrony Infrastruktury Informacyjnej (I3P) to konsorcjum czołowych krajowych instytucji zajmujących się cyberbezpieczeństwem, w tym akademickich

ośrodków badawczych, laboratoriów rządowych i organizacji non-profit. Powstał we wrześniu 2001 roku z myślą o realizacji potrzebnych działań badawczo-rozwojowych ukierunkowanych na ochronę infrastruktury informacyjnej kraju przed katastrofalnymi awariami. Główną rolą I3P jest koordynacja krajowego programu badawczo-rozwojowego w zakresie cyberbezpieczeństwa i wspieranie nawiązywania kontaktów między środowiskiem akademickim, przedstawicielami przemysłu oraz jednostkami rządowymi. Zadaniem I3P jest określanie i rozwiązywanie kluczowych problemów badawczych w zakresie ochrony infrastruktury informacyjnej oraz usprawnianie komunikacji między badaczami, decydentami i operatorami infrastruktury krytycznej.

https://www.thei3p.org

D.1.3. MIĘDZYNARODOWA KOMISJA ELEKTROTECHNICZNA (ANG. INTERNATIONAL ELECTROTECHNICAL COMMISSION – IEC)

IEC jest organizacją normalizacyjną, która przygotowuje i publikuje międzynarodowe normy dotyczące rozwiązań elektrycznych, elektronicznych i pokrewnych sektorów. Normy te stanowią podstawę do opracowywania norm krajowych oraz punkt odniesienia wykorzystywany na potrzeby międzynarodowych przetargów i umów. Członkami IEC są producenci, dostawcy, dystrybutorzy, sprzedawcy, konsumenci, użytkownicy rozwiązań, a także przedstawiciele instytucji rządowych na wszystkich szczeblach stowarzyszeń zawodowych, stowarzyszeń handlowych i jednostek normalizacyjnych z przeszło 60 krajów. Poniżej znajduje się lista komitetów technicznych IEC, których prace są związane z dziedziną bezpieczeństwa systemów OT.

https://www.iec.ch

D.1.3.1. Komitet Techniczny 57 (ang. IEC Technical Committee 57)

Zakres prac Komitetu Technicznego 57 (TC 57) obejmuje przygotowanie międzynarodowych norm dotyczących urządzeń i systemów sterowania systemami elektroenergetycznymi, w tym systemów zarządzania energią (*ang. energy management systems – EMS*), systemów SCADA, systemów automatyzacji dystrybucji, systemów zabezpieczeń oraz systemów wymiany informacji w czasie rzeczywistym i innych systemów wykorzystywanych w planowaniu, eksploatacji i konserwacji systemów elektroenergetycznych.

https://www.iec.ch/dyn/www/f?p=103:7:3323052731869::::FSP_ORG_ID,FSP_LANG_ID:1273,25

Lista grup roboczych (*ang. working groups – WG*) działających w ramach TC 57 obejmuje:

- WG 3: Grupa robocza ds. protokołów telesterowania
- WG 10: Grupa robocza ds. łączności inteligentnych urządzeń elektronicznych w systemach elektroenergetycznych i powiązanych modeli danych
- WG 13: Grupa robocza ds. interfejsów oprogramowania do obsługi i planowania sieci elektrycznej
- WG 14: Grupa robocza ds. interfejsów funkcji biznesowych dla przedsiębiorstw z sektora usług komunalnych
- WG 15: Grupa robocza ds. bezpieczeństwa danych i łączności
- WG 16: Grupa robocza ds. komunikacji w ramach zderegulowanego rynku energii
- WG 17: Grupa robocza ds. łączności inteligentnych urządzeń elektronicznych w systemach elektroenergetycznych i powiązanych modeli danych na potrzeby mikrosieci, rozproszonych źródeł energii i automatyzacji dystrybucji
- WG 18: Grupa robocza ds. elektrowni wodnych – łączność na potrzeby monitorowania i sterowania
- WG 19: Grupa robocza ds. interoperacyjności w ramach TC 57 w perspektywie długoterminowej
- WG 20: Grupa robocza ds. systemów komunikacji wykorzystujących linie elektroenergetyczne
- WG 21: Grupa robocza ds. interfejsów i profili protokołów istotnych dla systemów podłączonych do sieci elektrycznej

D.1.3.2. Komitet Techniczny 65 (ang. IEC Technical Committee 65)

Zakres prac Komitetu Technicznego 65 (TC 65) obejmuje opracowywanie międzynarodowych norm dla systemów i urządzeń wykorzystywanych do pomiarów,

sterowania i automatyzacji procesów przemysłowych w celu koordynacji działań normalizacyjnych, które mają wpływ na integrację komponentów i funkcji w takich systemach, w tym aspektów bezpieczeństwa i ochrony. Prace związane z normalizacją dotyczą międzynarodowych sektorów sprzętu i systemów.

https://www.iec.ch/dvn/www/f?p=103:7:3323052731869::::FSP_ORG_ID,FSP_LANG_ID:1250,25

D.1.4. INSTYTUT INŻYNIERÓW ELEKTRYKÓW I ELEKTRONIKÓW (ANG. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS – IEEE)

Celem IEEE jest wspieranie wdrażania innowacji na rzecz lepszego jutra. Organizacja zrzesza ponad 400 000 członków z przeszło 160 krajów oraz wydaje uznane publikacje, organizuje konferencje, publikuje normy technologiczne oraz prowadzi działalność zarobkową i edukacyjną.

https://www.ieee.org/

Poniżej znajduje się lista towarzystw działających w ramach IEEE, których prace są związane z dziedziną bezpieczeństwa systemów OT.

D.1.4.1. Towarzystwo ds. Inżynierii w Medycynie i Biologii (ang. IEEE Engineering in Medicine and Biology Society – EMBS)

EMBS jest największym na świecie międzynarodowym stowarzyszeniem inżynierów biomedycznych projektujących obwody elektroniczne urządzeń medycznych, tworzących oprogramowanie wspomagające diagnostykę chorób i rozwijają technologie bezprzewodowe, które pozwalają pacjentom i lekarzom komunikować się na duże odległości.

https://www.embs.org/

D.1.4.2. Stowarzyszenie Elektroniki Przemysłowej IEEE (*ang. IEEE Industrial Electronics Society – IES*)

Członkowie IES skupiają się na teorii i zastosowaniu elektroniki, systemów sterowania, komunikacji, sprzętu oraz technologii obliczeniowych w systemach i procesach przemysłowych i produkcyjnych.

http://www.ieee-ies.org/

D.1.4.3. Towarzystwo ds. Energetyki i Energii IEEE (*ang. IEEE Power & Energy Society – PES*)

IEEE PES to największe na świecie forum wymiany informacji na temat najnowszych osiągnięć technologicznych w branży elektroenergetycznej, zajmujące się opracowywaniem norm dotyczących rozwoju oraz budowy nowych rozwiązań i systemów oraz edukacją przedstawicieli sektora i społeczeństwa.

https://www.ieee-pes.org/

D.1.4.4. Komitet Techniczny ds. Komunikacji i Cyberbezpieczeństwa Systemów Energetycznych IEEE (*ang. IEEE Technical Committee on Power System Communications and Cybersecurity – PSCCC*)

Podkomisja ds. cyberbezpieczeństwa IEEE PSCCC koordynuje prace licznych grup roboczych zajmujących się utrzymaniem norm dotyczących bezpieczeństwa systemów OT. https://site.ieee.org/pes-pscc/cybersecurity-subcommittee-s0/

- IEEE Std 1686, Standard for Intelligent Electronic Devices Cyber Security Capabilities
- IEEE Std 1711.1, Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links: Substation Serial Protection Protocol (SSPP)
- IEEE Std 2030.102.1-2020, Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems
- IEEE Std 1711.2-2019, Standard for Secure SCADA Communications Protocol (SSCP)
- IEEE Std C37.240, Standard Cybersecurity Requirements for Power System Automation, Protection and Control Systems
- IEEE Std 2808, Standard for Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity
- IEEE Std 2658, Guide for Cybersecurity Testing in Electric Power Systems
- IEEE Std 1547.3, Guide for Cybersecurity of DERs Interface with Electric Power Systems
- IEEE Std 1815-2012, Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)

D.1.4.5. Stowarzyszenie Robotyki i Automatyki IEEE (ang. IEEE Robotics and Automation Society – RAS)

Członkowie RAS skupiają się na rozwoju i wymianie wiedzy naukowej i technologicznej w dziedzinie robotyki i automatyki, która przynosi korzyści zarówno sektorowi, jak i całej ludzkości.

https://www.ieee-ras.org/

D.1.4.6. Towarzystwo ds. Technologii Pojazdów IEEE (*ang. IEEE Vehicular Technology Society – VTS*)

W skład IEEE VTS wchodzą inżynierowie, naukowcy, studenci oraz pracownicy techniczni zainteresowani rozwojem teorii i praktyki inżynierii elektrycznej w zakresie łączności mobilnej, transportu lądowego, kolejowego i masowego, rozwiązań i systemów elektrotechniki samochodowej oraz usług mobilnych na lądzie, w powietrzu i na morzu.

https://vtsociety.org

D.1.5. MIĘDZYNARODOWE STOWARZYSZENIE AUTOMATYKI (ANG. INTERNATIONAL SOCIETY OF AUTOMATION – ISA)

ISA jest zawodowym stowarzyszeniem non-profit założonym w 1945 roku w celu budowy lepszego świata poprzez automatyzację. ISA rozwija kompetencje techniczne, łącząc społeczność automatyków w celu osiągania doskonałości operacyjnej. Jest zaufanym dostawcą opartych na normach zasobów i materiałów wspierających rozwój pracowników oraz całego sektora. ISA opracowuje uznane na świecie normy, odpowiada za akredytację przedstawicieli zawodu, zapewnia edukację i szkolenia, publikuje książki i artykuły techniczne, organizuje konferencje i wystawy oraz realizuje programy nawiązywania kontaktów i rozwoju kariery dla swoich członków i klientów na całym świecie.

https://www.isa.org

D.1.5.1. Komitet ISA95 ds. integracji systemów sterowania w przedsiębiorstwach (*ang. Enterprise-Control System Integration*)

Komitet ISA95 zajmuje się opracowywaniem norm dotyczących funkcji sterowania oraz innych funkcji realizowanych przez przedsiębiorstwa w oparciu o model referencyjny Purdue dla komputerowo zintegrowanego wytwarzania (*ang. Computer Integrated Manufacturing – CIM*). Norma ISA95 opiera się na architekturze referencyjnej Purdue Enterprise Reference Architecture (PERA) wydanej przez ISA w 1992 roku. Od tego czasu stanowi punkt odniesienia na potrzeby opracowywania interfejsów między sieciami przedsiębiorstw i sieciami sterowania we wszystkich sektorach OT.

https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

D.1.5.2. Komitet ISA99 ds. bezpieczeństwa automatyki przemysłowej i systemów sterowania

Komitet ISA99 zrzesza ekspertów zajmujących się cyberbezpieczeństwem w jednostkach przemysłowych z całego świata w celu opracowania norm dotyczących automatyki przemysłowej i bezpieczeństwa systemów sterowania. Prace komitetu ISA99 stanowią podstawę dla norm z serii ISA/IEC 62443 opracowywanych przez Międzynarodową Komisję Elektrotechniczną, które zostały podzielone na cztery kategorie: Normy ogólne, Zasady i procedury, Normy systemowe i Normy dla komponentów.

https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

Normy ogólne

- ISA-62443-1-1, Concepts, and models
- ISA-62443-1-2, Master glossary of terms and abbreviations
- ISA-62443-1-3, Security system conformance metrics
- ISA-62443-1-4, IACS security lifecycle and use cases

Zasady i procedury

- ISA-62443-2-1, Security program requirements for IACS asset owners
- ISA-62443-2-2, IACS Security Protection Ratings (Draft)

- ISA-62443-2-3, Patch management in the IACS environment
- ISA-62443-2-4, Security Program requirements for IACS service providers
- ISA-62443-2-5, Implementation guidance for IACS asset owners

Normy systemowe

- ISA-62443-3-1, Security technologies for IACS
- ISA-62443-3-2, Security risk assessment for system design
- ISA-62443-3-3, System security requirements and security levels

Normy dla komponentów

- ISA-62443-4-1, Product security development life cycle requirements
- ISA-62443-4-2, Technical security requirements for IACS components

D.1.5.3. ISASecure

https://isasecure.org/

Program ISASecure to system certyfikacji gotowych systemów automatyki i sterowania za zgodność z normami z serii ISA/IEC 62443.

D.1.5.4. ISA-TR84.00.09, Cybersecurity Related to the Functional Safety Lifecycle

Dokument zawiera wytyczne dotyczące łączenia cyklu życia cyberbezpieczeństwa z cyklem życia bezpieczeństwa w odniesieniu do zabezpieczeń, alarmów i blokad (*ang. Safety Controls, Alarms, and Interlocks – SCAI*), w tym systemów automatyki zabezpieczeniowej. Jego zakres obejmuje procesy robocze i środki przeciwdziałania stosowane w celu zmniejszenia ryzyka związanego z zagrożeniami cyberbezpieczeństwa dla sieci automatyki przemysłowej i systemów sterowania (*ang. industrial automation and control system – IACS*).

https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f

D.1.6. MIĘDZYNARODOWA ORGANIZACJA NORMALIZACYJNA (ANG. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO)

Międzynarodowa Organizacja Normalizacyjna (ISO) jest niezależną, pozarządową organizacją międzynarodową zrzeszającą 165 krajowych jednostek normalizacyjnych. Organizacja zrzesza ekspertów w celu udostępniania wiedzy i opracowywania dobrowolnych, opartych na wspólnym porozumieniu i istotnych dla rynku norm międzynarodowych, które wspierają innowacje i zapewniają rozwiązania globalnych wyzwań. Choć normy 27001/27002 zostały opracowane z myślą o systemach i środowiskach IT, wiele zawartych w nich wytycznych można odnieść do bezpieczeństwa systemów OT. Najnowsze wersje każdej z norm zostały wydane w 2013 roku.

https://www.iso.org/home.html

D.1.6.1. ISO 27001

Norma ISO/IEC 27001 określa wymagania dotyczące ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w kontekście organizacji. Obejmuje również wymagania dotyczące oceny i postępowania z ryzykiem bezpieczeństwa informacji dostosowane do potrzeb organizacji. Wymagania określone w normie ISO/IEC 27001 są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od ich rodzaju, wielkości lub charakteru.

https://www.iso.org/standard/54534.html

D.1.6.2. ISO 27002:2022

Norma ISO/IEC 27002:2022 zawiera wytyczne dotyczące organizacyjnych standardów bezpieczeństwa informacji i praktyk zarządzania bezpieczeństwem informacji, w tym wyboru i wdrażania zabezpieczeń oraz zarządzania środkami bezpieczeństwa, uwzględniając środowisko ryzyka bezpieczeństwa informacji danej organizacji.

https://www.iso.org/standard/75652.html

D.1.7. KRAJOWA RADA CENTRÓW WYMIANY INFORMACJI I ANALIZ (ANG. NATIONAL COUNCIL OF INFORMATION SHARING AND ANALYSIS CENTERS – ISAC)

Powołana w 2003 roku Krakowa Rada obejmuje 25 organizacji i jest organem koordynującym, którego celem jest usprawnienie przepływu informacji między infrastrukturami krytycznymi sektora prywatnego i rządowego. Centra wymiany informacji i analiz pomagają właścicielom i operatorom infrastruktur krytycznych chronić obiekty, pracowników i klientów przed zagrożeniami dotyczącymi bezpieczeństwa fizycznego i cyberbezpieczeństwa oraz innymi niebezpieczeństwami. Centra gromadzą, analizują i rozpowszechniają informacje na temat zagrożeń wśród członków oraz zapewniają narzędzia do ograniczania ryzyka i zwiększania odporności. Centra wymiany informacji i analiz działają w swoich sektorach, przekazując kluczowe informacje oraz dbając o świadomość sytuacyjną w całym sektorze.

https://www.nationalisacs.org/member-isacs-3

D.1.8. NARODOWY INSTYTUT STANDARYZACJI I TECHNOLOGII (ANG. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST)

NIST wspiera innowacyjność i konkurencyjność przemysłową Stanów Zjednoczonych poprzez rozwój nauki, norm i technologii pomiarowych w sposób, który zwiększa bezpieczeństwo ekonomiczne i poprawia jakość życia mieszkańców. Od inteligentnej sieci energetycznej i elektronicznej dokumentacji medycznej po zegary atomowe, zaawansowane nanomateriały i mikroukłady, niezliczone produkty i usługi opierają się na technologii, pomiarach i normach NIST. Laboratorium Informatyczne NIST (*ang. Information Technology Laboratory – ITL*) opracowuje i utrzymuje obszerną kolekcję norm bezpieczeństwa komputerowego, wytycznych, zaleceń i badań, które są publikowane w ramach publikacji specjalnych oraz innych sprawozdań.

https://csrc.nist.gov/publications/

D.1.8.1. Wytyczne NIST SP 800 dotyczące cyberbezpieczeństwa

Publikacje specjalne NIST oznaczone numerem 800 zawierają sprawozdania dotyczące badań, wytycznych oraz działań NIST w zakresie komunikacji, bezpieczeństwa systemów informacyjnych oraz współpracy z przemysłem,

jednostkami rządowymi oraz organizacjami akademickimi. Tematyka publikacji obejmuje technologie i rozwiązania kryptograficzne, zaawansowane technologie uwierzytelniania, infrastruktury klucza publicznego, bezpieczeństwo sieci internetowych, zabezpieczenia oraz zarządzanie bezpieczeństwem i wsparcie.

https://csrc.nist.gov/publications/sp800

Na podstawie publikacji specjalnych NIST powstały Narodowe Standardy Cyberbezpieczeństwa – poniżej znajduje się skrócona lista wydanych przez NIST dokumentów oznaczonych numerem 800, które dotyczą bezpieczeństwa systemów OT, a także dokumentów wchodzących w skład Narodowych Standardów Cyberbezpieczeństwa opracowanych na ich podstawie:

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* / NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu / NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-40, Rev. 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji* / NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*
- NSC 800 53A, *Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych i organizacjach*/ NIST SP 800-53A, Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NSC 800-53B *Zabezpieczenia bazowe systemów informacyjnych oraz organizacji* / NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*

- NIST SP 800-70, Rev. 4, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
- NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*
- NIST SP 800-116, Rev. 1, *Guidelines for the Use of PIV Credentials in Facility Access*
- NIST SP 800-123, *Guide to General Server Security*
- NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- NIST SP 800-125, *Guide to Security for Full Virtualization Technologies*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*
- NIST SP 800-150, *Guide to Cyber Threat Information Sharing*
- NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
- NIST SP 800-160 Vol. 2, Rev. 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*

D.1.8.2. Wytyczne NIST SP 1800 dotyczące cyberbezpieczeństwa

Seria publikacji specjalnych NIST oznaczona numerem 1800 obejmuje praktyczne i użyteczne podejścia do cyberbezpieczeństwa oparte na standardach oraz najlepsze praktyki stosowane przez organizacje w rzeczywistych warunkach. Wytyczne te mają na celu pomóc organizacjom w sprawniejszym wdrażaniu rozwiązań w zakresie cyberbezpieczeństwa przy ograniczeniu kosztów testów oraz czasu poświęconego na weryfikację koncepcji. Publikacje specjalne z serii 1800 pozwalają na zestawianie poszczególnych zabezpieczeń z założeniami ram cyberbezpieczeństwa oraz określają działania wymagane w celu odtworzenia przykładowego rozwiązania.

https://csrc.nist.gov/publications/sp1800

Poniższe specjalne publikacje oznaczone numerem 1800 mają zastosowanie do społeczności bezpieczeństwa OT:

- NIST SP 1800-2, *Identity and Access Management for Electric Utilities*
- NIST SP 1800-7, *Situational Awareness for Electric Utilities*
- NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*
- NIST SP 1800-10, *Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector*
- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*
- NIST SP 1800-23, *Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry*
- NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector*
- NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*
- NSC 1800-26, *Integralność danych - wykrywanie i reagowanie na oprogramowanie ransomware i inne zdarzenia destrukcyjne* / NIST SP 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*
- NIST SP 1800-27, *Securing Property Management Systems*
- NIST SP 1800-30, *Securing Telehealth Remote Patient Monitoring Ecosystem*
- NIST SP 1800-32, *Securing Distributed Energy Resources: An Example of Industrial Internet of Things*

D.1.8.3. Sprawozdania wewnętrzne lub międzyresortowe NIST

Publikacje NIST z serii IR (*ang. NIST Internal or Interagency Reports – NIST IR*) obejmują sprawozdania dotyczące wyników badań, w tym informacje ogólne dotyczące federalnych standardów przetwarzania informacji (FIPS) oraz informacje kontekstowe związane z publikacjami specjalnymi.

https://csrc.nist.gov/publications/ir

Do zagadnienia bezpieczeństwa systemów OT mogą odnosić się następujące dokumenty z serii NIST IR:

- NIST IR 7628, Rev. 1, *Guidelines for Smart Grid Cybersecurity*
- NIST IR 8011 Vol. 1, *Automation Support for Security Control Assessments: Volume 1: Overview*
- NIST IR 8011 Vol. 2, *Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management*
- NIST IR 8011 Vol. 3, *Automation Support for Security Control Assessments: Software Asset Management*
- NIST IR 8011 Vol. 4, *Automation Support for Security Control Assessments: Software Vulnerability Management*
- NIST IR 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*
- NIST IR 8183, Rev. 1, *Cybersecurity Framework Version 1.1 Manufacturing Profile*
- NIST IR 8183A Vol. 1, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 - General Implementation Guidance*
- NIST IR 8183A Vol. 2, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 - Process-based Manufacturing System Use Case*
- NIST IR 8183A Vol. 3, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 - Discrete-based Manufacturing System Use Case*
- NIST IR 8212, *ISCMA: An Information Security Continuous Monitoring Program Assessment*
- NIST IR 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*

D.1.9. NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)

Misją North American Electric Reliability Corporation (NERC) jest zwiększanie niezawodności i bezpieczeństwa systemu elektroenergetycznego w Ameryce

Północnej. Aby realizować ten cel, NERC opracowuje i egzekwuje normy w zakresie niezawodności; monitoruje sieć elektroenergetyczną, ocenia możliwości, przeprowadza kontrolę przedsiębiorstw, operatorów i użytkowników pod kątem gotowości; oraz kształci i szkoli pracowników sektora. NERC jest organizacją branżową, która opiera się na zróżnicowanej i zbiorowej wiedzy fachowej przedstawicieli sektora. Jako organizacja zajmująca się zagadnieniem niezawodności dostaw energii, NERC podlega audytowi przeprowadzanemu przez amerykańską Federalną Komisję Regulacji Energetyki (*ang. U.S. Federal Energy Regulatory Commission*) i organy rządowe w Kanadzie.

https://www.nerc.com

D.1.9.1. Normy NERC dotyczące ochrony infrastruktury krytycznej (*ang. Normy NERC Critical Infrastructure Protection – CIP*)

NERC publikuje kolekcję norm dotyczących cyberbezpieczeństwa w celu zmniejszenia ryzyka naruszenia instalacji odpowiadających za wytwarzanie energii elektrycznej i systemów przesyłowych wysokiego napięcia powyżej 100 kV, nazywanych także masowymi systemami elektrycznymi. Masowe systemy elektryczne obejmują organy odpowiedzialne za bilansowanie sieci, koordynatorów niezawodności, organy odpowiedzialne za działanie sieci, dostawców usług przesyłowych, właścicieli infrastruktury przesyłowej, operatorów usług przesyłowych, wytwórców energii, operatorów wytwarzających energię oraz odbiorców. Normy w zakresie cyberbezpieczeństwa obejmują kontrole oraz poziomy niezgodności, które mogą prowadzić do nałożenia kar na wybrane podmioty. NERC publikuje i egzekwuje obecnie 12 norm dotyczących ochrony infrastruktury krytycznej (*ang. Critical Infrastructure Protection – CIP*) oraz diwie dodatkowe normy, które zostały zgłoszone i oczekują na zatwierdzenie przez organy regulacyjne.

https://www.nerc.con/pa/Stand/Pages/RehabihtyStandards.aspx

- CIP-002, Cyber Security - BES Cyber System Categorization
- CIP-003, Cyber Security - Security Management Controls
- CIP-004, Cyber Security - Personnel & Training
- CIP-005, Cyber Security - Electronic Security Perimeter(s)

- CIP-006, Cyber Security - Physical Security of BES Cyber Systems
- CIP-007, Cyber Security - System Security Management
- CIP-008, Cyber Security - Incident Reporting and Response Planning
- CIP-009, Cyber Security - Recovery Plans for BES Cyber Systems
- CIP-010, Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-011, Cyber Security - Information Protection
- CIP-013, Cyber Security - Supply Chain Risk Management
- CIP-014, Cyber Security - Physical Security

D.1.10. KOALICJA NA RZECZ CYBERBEZPIECZEŃSTWA TECHNOLOGII OPERACYJNYCH (*ANG. OPERATIONAL TECHNOLOGY CYBERSECURITY COALITION*)

Misją koalicji na rzecz cyberbezpieczeństwa technologii operacyjnych (*ang. Operational Technology Cybersecurity Coalition*) jest promowanie otwartych, neutralnych dla dostawców, interoperacyjnych, opartych na normach rozwiązań cyberbezpieczeństwa dla systemów OT.

https://www.otcybercoalition.org/

D.2 INICJATYWY I PROGRAMY BADAWCZE

D.2.1. INICJATYWA AKCELERATORA W ZAKRESIE CYBERBEZPIECZEŃSTWA SYSTEMÓW CZYSTEJ ENERGII (*ANG. CLEAN ENERGY CYBERSECURITY ACCELERATOR INITIATIVE*)

Inicjatywa prowadzona przez Departament Energii Stanów Zjednoczonych (*ang. Department of Energy – DOE*) i Krajowe Laboratorium Energii Odnawialnej (*ang. National Renewable Energy Laboratory – NREL*) łączy przedstawicieli infrastruktur federalnych oraz ekspertów, operatorów zasobów sektora energetycznego oraz podmioty wprowadzające innowacje w sektorze energetyki i technologii w celu podjęcia wspólnych wysiłków na rzecz rozwoju nowych rozwiązań w zakresie cyberbezpieczeństwa dla nowoczesnej sieci dystrybucji czystej energii.

Program Cybersecurity Accelerator zapewnia dostęp do światowej klasy infrastruktury operatorom różnych infrastruktur i zasobów, umożliwiając im wspólną pracę nad rozwojem i wdrażaniem odnawialnych, nowoczesnych i bezpiecznych technologii sieciowych, które zapewnią konkurencyjne ceny. Te innowacyjne technologie przyczynią się również do wdrażania zabezpieczeń i utwardzania rozwiązań na etapie projektowania, zapewniając tym samym, że cyberbezpieczeństwo będzie stanowiło ważny aspekt technologii i architektur od początku procesu projektowania i rozwoju.

https://www.energy.gov/ceser/department-energy-clean-energy-accelerator-initiative

D.2.2. PROGRAM BADAWCZO-ROZWOJOWY DOTYCZĄCY CYBERBEZPIECZEŃSTWA SYSTEMÓW DOSTARCZANIA ENERGII (*ANG. CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS R&D PROGRAM*)

Biuro Departamentu Energii (DOE) ds. cyberbezpieczeństwa, bezpieczeństwa energetycznego i reagowania kryzysowego (*ang. Cybersecurity, Energy Security, and Emergency Response – CESER*) zapoczątkowało w 2010 roku program badawczo-rozwojowy CEDS mający na celu opracowanie rozwiązań w zakresie cyberbezpieczeństwa systemów dostarczania energii dzięki ukierunkowanym działaniom badawczo-rozwojowym. Od tamtej pory biuro CESER wraz z partnerami branżowymi zainwestowało przeszło 240 milionów dolarów w celu rozwoju rozwiązań

cyberbezpieczeństwa dotyczących systemów dostarczania energii. Te partnerstwa badawcze pozwalają na wykrywanie cyberincydentów, zapobieganie ich występowaniu oraz łagodzenie ich skutków dla obecnych i przyszłych systemów dostarczania energii.

httpsy/www.energygpv/ceser/actiyilies/cybersecuritycritical-energy-infrastructure/cvbersecuritv-research-development-and

D.2.3. CYBERBEZPIECZEŃSTWO W ŚRODOWISKACH TECHNOLOGII OPERACYJNYCH (ANG. CYBERSECURITY FOR THE OPERATIONAL TECHNOLOGY ENVIRONMENT – CYOTE)

Biuro Departamentu Energii (DOE) ds. cyberbezpieczeństwa, bezpieczeństwa energetycznego i reagowania kryzysowego (CESER) nawiązało współpracę z ośrodkiem Idaho National Laboratory i przedsiębiorstwami energetycznymi w ramach inicjatywy badawczej mającej na celu poprawę wykrywania zagrożeń w sektorze energetycznym, skupionej na złośliwej aktywności w sieciach OT.

https://inl.gov/cyote/

D.2.4. PROGRAM WYMIANY INFORMACJI O ZAGROŻENIACH DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA (*ANG. CYBERSECURITY RISK INFORMATION SHARING PROGRAM – CRISP*)

Cybersecurity Risk Information Sharing Program, czyli Program wymiany informacji o zagrożeniach dotyczących cyberbezpieczeństwa (CRISP) to partnerstwo publiczno-prywatne współfinansowane przez Departament Energii Stanów Zjednoczonych i partnerów przemysłowych, działające pod przewodnictwem ośrodka Electricity Information Sharing and Analysis Center (E-ISAC) pod egidą NERC. Celem CRISP jest współpraca z partnerami z sektora energetycznego w celu usprawnienia szybkiej i dwukierunkowej wymiany jawnych i niejawnych informacji o zagrożeniach oraz opracowania narzędzi zwiększających świadomość sytuacyjną oraz poprawiających możliwości sektora w zakresie identyfikowania, ustalania priorytetów i koordynowania ochrony infrastruktury krytycznej i kluczowych zasobów. CRISP opiera się na zaawansowanych czujnikach Departamentu Energii Stanów Zjednoczonych, analizach zagrożeń oraz wiedzy specjalistycznej partnerów, aby

opracowywać wysokopoziomowe informacje o cyberzagrożeniach w sektorze energetycznym. Informacje te są udostępniane uczestnikom inicjatywy – spółkom odpowiedzialnym za dostarczanie przeszło 80% energii elektrycznej w kraju. Kluczową rolę w CRISP odgrywa Pacific Northwest National Laboratory (PNNL).

https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet 508.pdf

D.2.5. TESTY CYBERBEZPIECZEŃSTWA NA POTRZEBY BUDOWY ODPORNYCH PRZEMYSŁOWYCH SYSTEMÓW STEROWANIA (*ANG. CYBER TESTING FOR RESILIENT INDUSTRIAL CONTROL SYSTEMS – CYTRICS*)

Biuro Departamentu Energii (DOE) ds. cyberbezpieczeństwa, bezpieczeństwa energetycznego i reagowania kryzysowego (CESER) współpracuje z ośrodkiem Idaho National Laboratory i innymi interesariuszami w celu identyfikacji priorytetowych urządzeń i komponentów systemów OT, przeprowadzania testów, udostępniania informacji o podatnościach w cyfrowym łańcuchu dostaw oraz wprowadzania usprawnień w zakresie projektowania i produkcji komponentów.

https://inl.gov/cytrics/

D.2.6. SIEĆ INFORMACYJNA DOTYCZĄCA BEZPIECZEŃSTWA WEWNĘTRZNEGO W ZAKRESIE INFRASTRUKTURY KRYTYCZNEJ (*ANG. HOMELAND SECURITY INFORMATION NETWORK - CRITICAL INFRASTRUCTURE – HSIN-CI*)

Sieć informacyjna dotycząca bezpieczeństwa wewnętrznego (HSIN) jest zaufaną siecią umożliwiającą udostępnianie wrażliwych, lecz nieklasyfikowanych informacji dotyczących bezpieczeństwa. Społeczność podmiotów odpowiedzialnych za infrastrukturę krytyczną w ramach sieci HSIN (HSIN-CI) stanowi platformę, za pośrednictwem której właściciele i operatorzy z sektora prywatnego, Departamentu Bezpieczeństwa Wewnętrznego oraz inne federalne, stanowe i lokalne agencje rządowe współpracują w celu ochrony infrastruktury krytycznej kraju. HSIN-CI zapewnia bezpłatne narzędzia umożliwiające współpracę w czasie rzeczywistym, w tym wirtualną przestrzeń spotkań, platformy do udostępniania dokumentów, a także alerty i komunikatory.

https://www.dhs.gov/hsin-critical-infrastructure

D.2.7. ZESPOŁY CYBER-INFORMED ENGINEERING (CIE) I CONSEQUENCE-DRIVEN CIE (CCE) IDAHO NATIONAL LABORATORY

Departament Energii Stanów Zjednoczonych i Idaho National Laboratory opracowały ramy wdrożeniowe zasad cyberbezpieczeństwa w całym cyklu życia projektów inżynieryjnych. Ramy Cyber-Informed Engineering (CIE) zakładają włączenie cyberbezpieczeństwa jako podstawowego elementu zarządzania ryzykiem rozwiązań inżynieryjnych, wspomaganych przez technologię cyfrową. Wytyczne Consequence-Driven Cyber-Informed Engineering (CCE) obejmują rygorystyczny proces stosowania podstawowych zasad ram CIE w danej organizacji, danym obiekcie lub danym procesie na podstawie identyfikacji kluczowych procesów i metod, a także środków, które mogą być wykorzystane przez napastnika do wpływania na procesy oraz środków przeciwdziałania lub zabezpieczeń.

CIE kładzie nacisk na wyeliminowanie potencjalnego ryzyka w kluczowych obszarach oraz zapewnienie odporności i skuteczności reakcji w ramach projektu systemu inżynieryjnego. CCE stanowi program wdrożenia podstawowych elementów CIE w czterech etapach, aby usunąć lub ograniczyć podatności w kluczowych procesach.

https://inl.gov/cie/

D.2.8. STOWARZYSZENIE PRZEMYSŁÓW GAZOWYCH I NAFTOWYCH W CELU POPRAWY CYBERBEZPIECZEŃSTWA (*ANG. LINKING THE OIL AND GAS INDUSTRY TO IMPROVE CYBERSECURITY – LOGIIC*)

Program Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) jest wynikiem współpracy spółek naftowych i gazowych oraz Dyrekcji ds. Nauki i Technologii Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych. LOGIIC realizuje wspólne projekty badawczo-rozwojowe w celu poprawy poziomu cyberbezpieczeństwa w systemach krytycznych dla sektora ropy naftowej i gazu ziemnego. Celem jest zwiększanie cyberbezpieczeństwa sektora przy jednoczesnym zachowaniu bezstronności, niezależności uczestników i neutralności pod względem doboru dostawców rozwiązań.

LOGIIC działa przy Federacji Automatyki, która zawarła umowy ze spółkami członkowskimi LOGIIC i wszystkimi innymi uczestnikami inicjatywy. Dyrekcja ds. Nauki i Technologii Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych zawarła także umowę z organizacją naukowo-badawczą SRI International w celu zapewnienia wytycznych naukowych i technicznych dla LOGIIC.

https://www.logiic.org/

D.2.9. PROGRAM NIST DS. SYSTEMÓW CYBERFIZYCZNYCH I INTERNETU RZECZY (*ANG. NIST CYBER-PHYSICAL SYSTEMS AND INTERNET OF THINGS PROGRAM*)

Definicje systemów cyberfizycznych (*ang. cyber-physical systems – CPS*) i Internetu Rzeczy (IoT) stają się coraz bardziej zbieżne – kładą coraz większy nacisk na interakcję komponentów cyfrowych, analogowych, fizycznych i ludzkich w systemach zaprojektowanych pod kątem funkcjonalności dzięki zintegrowanej fizyce i logice. Systemy te stanowią podstawę innowacyjnych rozwiązań w wielu kluczowych sektorach gospodarki, takich jak inteligentne miasta, energetyka, produkcja, transport i reagowanie kryzysowe. Zadaniem inicjatywy jest rozwój metod pomiarowych oraz opartych na konsensusie podmiotów branżowych norm i protokołów dla zaawansowanych systemów cyberfizycznych i IoT, które są skalowalne, skuteczne, mierzalne, interoperacyjne, godne zaufania i bezpieczne. Biuro Programu Inteligentnych Sieci i Systemów Cyberfizycznych Laboratorium Inżynieryjnego realizuje również działania mające na celu koordynację programu NIST z Laboratorium Informatycznym, Laboratorium Technologii Komunikacyjnych oraz Laboratorium Pomiarów Fizycznych.

https://www.nist.gov/prograns-projects/cyber-physical-systens-and-internet-things-progran

D.2.10. PROJEKT NIST DOTYCZĄCY CYBERBEZPIECZEŃSTWA INTELIGENTNYCH SIECI (*ANG. NIST CYBERSECURITY FOR SMART GRID SYSTEMS PROJECT*)

Cyberbezpieczeństwo inteligentnych sieci musi dotyczyć zarówno niezamierzonych naruszeń zasad ochrony infrastruktury elektrycznej spowodowanych błędami

użytkowników, awariami sprzętu i klęskami żywiołowymi, jak i celowych ataków realizowanych przez niezadowolonych pracowników, terrorystów czy podmioty odpowiedzialne za szpiegostwo przemysłowe. NIST zajmuje się tymi wyzwaniami dzięki badaniom realizowanym w ośrodku badawczym NIST Smart Grid Testbed oraz pracom w ramach Komitetu ds. Cyberbezpieczeństwa Smart Electric Power Alliance (SEPA) (SGCC) w celu oceny zasad i zabezpieczeń w zakresie cyberbezpieczeństwa ujętych w normach branżowych oraz opracowania odpowiednich dokumentów zawierających wytyczne dla społeczności zajmującej się inteligentnymi sieciami elektrycznymi i ich cyberbezpieczeństwem. Głównym celem jest opracowanie strategii zarządzania ryzykiem w zakresie cyberbezpieczeństwa dla inteligentnych sieci, aby zapewnić bezpieczeństwo i interoperacyjność rozwiązań opartych na różnych komponentach i działających w różnych obszarach. Projekt ma na celu zaspokojenie krytycznych potrzeb w zakresie cyberbezpieczeństwa poprzez promowanie transferu technologii, najlepszych praktyk, standardów, wytycznych i badań w obszarach kryptografii stosowanej i cyberbezpieczeństwa dla mikrosieci. W ramach projektu powstaną podstawowe wytyczne dotyczące cyberbezpieczeństwa, przeglądy cyberbezpieczeństwa i zalecenia dotyczące norm i wymogów, a także będą realizowane działania promujące oraz zachęcające do współpracy na rzecz cyberbezpieczeństwa inteligentnych sieci elektrycznych.

https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems

D.2.11. PROJEKT NIST DOTYCZĄCY CYBERBEZPIECZEŃSTWA INTELIGENTNYCH SYSTEMÓW PRODUKCYJNYCH (*ANG. NIST CYBERSECURITY FOR SMART MANUFACTURING SYSTEMS PROJECT*)

W ramach projektu NIST dotyczącego cyberbezpieczeństwa inteligentnych systemów produkcyjnych Instytut opracowuje rozwiązania w zakresie cyberbezpieczeństwa, wskaźniki oraz narzędzia umożliwiające producentom wdrażanie funkcji dotyczących cyberbezpieczeństwa w inteligentnych systemach produkcyjnych bez uszczerbku dla ich wydajności, niezawodności i bezpieczeństwa.

https://www.nist.gov/programs-projects/cybersecurity-smart-manufacturing-systems

D.2.12. PROJEKT „NIEZAWODNE, WYDAJNE SYSTEMY BEZPRZEWODOWE DO AUTOMATYZACJI FABRYK" (*ANG. NIST RELIABLE, HIGH PERFORMANCE WIRELESS SYSTEMS FOR FACTORY AUTOMATION*)

W ramach projektu „Niezawodne, wydajne systemy bezprzewodowe do automatyzacji fabryk" Instytut opracował kompleksowe wymagania, modele systemów, zalecenia w zakresie architektur oraz wytyczne dotyczące integracji zaufanych systemów bezprzewodowych w fabrykach, w których łączność bezprzewodowa jest podstawowym sposobem komunikacji umożliwiającym mobilność robotów i łatwość instalacji urządzeń brzegowych.

https://www.nist.gov/programs-projects/reliable-high-performance-wireless-systems-factory-automation

D.2.13. DIAGNOSTYKA I ZARZĄDZANIE STANEM URZĄDZEŃ DLA NIEZAWODNOŚCI INTELIGENTNEJ PRODUKCJI (ANG. PROGNOSTICS AND HEALTH MANAGEMENT FOR RELIABLE OPERATIONS IN SMART MANUFACTURING – PHM4SM)

Projekt NIST Prognostics and Health Management for Reliable Operations in Smart Manufacturing (Diagnostyka i zarządzanie stanem urządzeń dla niezawodności inteligentnej produkcji – PHM4SM) rozwija i wdraża nowe metody pomiarów w celu promowania wdrażania, weryfikacji i testowania zaawansowanych technologii monitorowania, diagnostyki i prognozowania w celu zwiększenia niezawodności i skrócenia przestojów inteligentnych systemów produkcyjnych.

https://www.nist.gov/programs-projects/prognostics-and-health-management-reliable-operations-smart-manufacturing-phm4sm

D.2.14. PROJEKT NIST „IDENTYFIKOWALNOŚĆ W ŁAŃCUCHU DOSTAW PRODUKCJI ROLNO-SPOŻYWCZEJ" (*ANG. NIST SUPPLY CHAIN TRACEABILITY FOR AGRI-FOOD MANUFACTURING*)

W ramach projektu Supply Chain Traceability for Agri-Food Manufacturing (Identyfikowalność w łańcuchu dostaw produkcji rolno-spożywczej) Instytut opracowuje i wdraża nowe normy, narzędzia i wytyczne dotyczące identyfikowalności

i cyberbezpieczeństwa, które zwiększają zaufanie uczestników i klientów łańcuchów dostaw produkcji rolno-spożywczej.

https://www.nist.gov/programs-projects/supplv-chain-traceabilitv-agri-food-manufacturing

D.3 NARZĘDZIA I SZKOLENIA

D.3.1. NARZĘDZIE DO OCENY CYBERBEZPIECZEŃSTWA CISA (ANG. CISA CYBER SECURITY EVALUATION TOOL – CSET®)

Narzędzie do oceny cyberbezpieczeństwa CISA (CSET®) zapewnia systematyczne, zdyscyplinowane i powtarzalne podejście do oceny stanu bezpieczeństwa organizacji. CSET to oprogramowanie, które przeprowadza właścicieli i operatorów zasobów przez proces oceny praktyk bezpieczeństwa sieci systemu sterowania przemysłowego oraz sieci IT. Narzędzie pozwala na samodzielną ocenę poziomu cyberbezpieczeństwa, korzystając z wielu uznanych rządowych i branżowych norm i zaleceń.

https://github.com/cisagov/cset/releases

D.3.2. REKOMENDACJE DOTYCZĄCE RAM CYBERBEZPIECZEŃSTWA CISA

Wytyczne sektorowe zostały opracowane dla wszystkich sześciu sektorów infrastruktury krytycznej, dla których Biuro Ochrony Infrastruktury Departamentu Bezpieczeństwa Wewnętrznego pełni funkcję agencji odpowiedzialnej za sektor – chemiczny, obiektów komercyjnych, produkcji krytycznej, zapór wodnych, służb ratunkowych oraz energetyki jądrowej. Wytyczne są opracowywane w ścisłej współpracy z Biurem Ochrony wraz z sektorowymi radami koordynacyjnymi (*ang. Sector Coordinating Councils – SCC*) oraz rządowymi radami koordynacyjnymi (*ang. Government Coordinating Councils – GCC*), aby zapewnić dostęp do kompleksowych informacji na temat ryzyka związanego z cyberbezpieczeństwem w danym sektorze.

https://www.cisa.gov/resources-tools/resources/chemical-sector-cybersecurity-framework-implementation-guidance

https://www.cisa.gov/resources-tools/resources/commercial-facilities-sector-cybersecurity-framework-implementation

https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-cybersecurity-framework-implementation

https://www.cisa.gov/resources-tools/resources/dams-sector-cybersecurity-framework-implementation-guidance-2020

https://www.cisa.gov/resources-tools/resources/emergency-services-sector-cybersecurity-framework-implementation-guidance

https://www.cisa.gov/resources-tools/resources/nuclear-sector-cybersecurity-framework-implementation-guidance

D.3.3. ALERTY, POWIADOMIENIA I SPRAWOZDANIA CISA DOTYCZĄCE SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

Alerty CISA stanowią sposób na szybkie informowanie właścicieli i operatorów infrastruktury krytycznej o zagrożeniach lub działaniach, które mogą mieć wpływ na sieci i zasoby komputerowe wchodzące w skład tych infrastruktur.

Powiadomienia stanowią źródło aktualnych informacji na temat bieżących zagadnień związanych z bezpieczeństwem, w tym podatności oraz sposobów na ich wykorzystanie.

CISA prowadzi listę technicznych sprawozdań informacyjnych (*ang. Technical Information Papers – TIP*) dotyczących systemów sterowania przemysłowego, sprawozdań rocznych (*ang. Year in Review*) oraz opracowań innych podmiotów, które uznaje za istotne dla osób odpowiedzialnych za ochronę takich systemów.

https://www.cisa.gov/topics/industrial-control-systems

D.3.4. KURSY SZKOLENIOWE CISA DOTYCZĄCE SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

CISA oferuje zarówno wirtualne kursy szkoleniowe dostępne za pośrednictwem wirtualnego portalu edukacyjnego, jak i zajęcia prowadzone przez instruktorów w różnych lokalizacjach. Wszystkie szkolenia CISA są bezpłatne dla uczestników.

https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA

D.3.5. MITRE ATT&CK FOR ICS

MITRE ATT&CK for ICS to baza wiedzy na temat działań cyberprzestępców związanych z systemami sterowania przemysłowego. Uwzględnia różne etapy ataków oraz zasoby i systemy, których dotyczą. Baza ATT&CK for ICS opiera się na wewnętrznych badaniach prowadzonych przez MITRE, które mają na celu stosowanie metodyki ATT&CK do sektora systemów sterowania przemysłowego.

https://attack.mitre.org/techniques/ics/

D.3.6. RAMY CYBERBEZPIECZEŃSTWA NIST

Uznając, że bezpieczeństwo narodowe i gospodarcze Stanów Zjednoczonych zależy od niezawodnego funkcjonowania infrastruktury krytycznej, w lutym 2013 roku prezydent wydał rozporządzenie wykonawcze nr 13636 w sprawie *poprawy cyberbezpieczeństwa infrastruktury krytycznej* [EO13636]. W rozporządzeniu prezydent nakazał NIST podjęcie współpracy z interesariuszami w celu opracowania dobrowolnych ram ograniczania ryzyka związanego z cyberbezpieczeństwem dotyczącego infrastruktury krytycznej w oparciu o istniejące normy, wytyczne i praktyki.

Instytut opublikował pierwszą wersję dokumentu *Framework for Improving Critical Infrastructure Cybersecurity* 12 lutego 2014 roku. Ramy te powstały dzięki współpracy między przedstawicielami sektora przemysłu oraz instytucji rządowych w oparciu o normy, wytyczne i praktyki w zakresie ochrony infrastruktury krytycznej. Oparte na priorytetach, elastyczne, powtarzalne i tanie w realizacji podejście opisane w dokumencie pomaga właścicielom i operatorom infrastruktury krytycznej zarządzać ryzykiem związanym z cyberbezpieczeństwem.

W kwietniu 2018 roku Instytut wydał wersję 1.1 dokumentu *Framework for Improving Critical Infrastructure Cybersecurity*. Wprowadzone zmiany powstały w wyniku konsultacji obejmujących przeszło 1200 uczestnikami corocznych warsztatów zrealizowanych w latach 2016 i 2017, a także ponad 200 nadesłanych uwag dotyczących wersji roboczych publikacji.

https://www.nist.gov/cyberfranework/franework

D.3.7. KURSY SZKOLENIOWE SANS DOTYCZĄCE SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

SANS oferuje szereg kursów obejmujących praktyczne szkolenia koncentrujące się na cyberbezpieczeństwie środowisk OT. Kursy te stanowią dla specjalistów ds. bezpieczeństwa, jak i inżynierów systemów sterowania źródła wiedzy i umiejętności wymaganych do ochrony infrastruktury krytycznej.

https://www.sans.org/industrial-control-systens-security/

Aktualna oferta kursów i odpowiadające im certyfikaty zostały wymienione poniżej:

- ICS410: ICS/SCADA Security Essentials, Global Industrial Cyber Security Professional
- (GICSP)
- ICS456: Essentials for NERC CIP, GIAC Critical Infrastructure Protection (GCIP)
- ICS515: ICS Visibility Detection, and Response, GIAC Response and Industrial Defense (GRID)

D.4 ZASOBY DOTYCZĄCE POSZCZEGÓLNYCH SEKTORÓW

D.4.1. SEKTOR CHEMICZNY

- Standardy antyterrorystyczne dla zakładów chemicznych (*ang. Chemical Facility Anti-Terrorism Standards – CFATS*) - https://www.cisa.gov/chemical-facility-anti-terrorisn-standards
- ChemLock - https://www.cisa.gov/chemlock
- Amerykańska Rada Chemii (*ang. American Chemistry Council – ACC*) - https://www.anericanchenistry.con
- Amerykański Instytut Naftowy (*ang. American Petroleum Institute – API*) - https://www.api.org
- Amerykańskie Towarzystwo Gazownicze (*ang. American Gas Association – AGA*) - https://www.aga.org
- Organizacja amerykańskich producentów paliw i produktów petrochemicznych (*ang. American Fuel and Petrochemical Manufacturers – AFPM*) - https://www.afpn.org
- Stowarzyszenie Producentów Chemikaliów i Podmiotów Stowarzyszonych (*ang. Society of Chemical Manufacturers and Affiliates – SOCMA*) - https://www.socma.org

D.4.2. KOMUNIKACJA

- Federalna Komisja Łączności (*ang. Federal Communications Commission – FCC*) - https://www.fcc.gov
  - ✓ Cybersecurity and Communications Reliability Division o Communications Security, Reliability, and Interoperability Council (Wydział ds. Cyberbezpieczeństwa i Niezawodności Łączności Rady ds. Bezpieczeństwa Łączności, Niezawodności i Interoperacyjności – CSRIC)

D.4.3. SEKTOR PRODUKCJI KRYTYCZNEJ

- Krajowe Stowarzyszenie Producentów (*ang. National Association of Manufacturers – NAM*) - https://www.nam.org
  - ✓ NAM Cyber Cover

- Stowarzyszenie na rzecz Rozwoju Automatyzacji (*ang. Association for Advancing Automation – A3*) - https://www.automate.org
- Stowarzyszenie Pomiarów, Sterowania i Automatyki (*ang. Measurement, Control & Automation Association – MCAA*) - https://www.themcaa.org
- Międzynarodowe Stowarzyszenie Automatyki i Robotyki w Budownictwie (*ang. International Association for Automation and Robotics in Construction – IAARC*) - https://www.iaarc.org
- ODVA - https://www.odva.org

D.4.4. SEKTOR ZAPÓR WODNYCH

- Stowarzyszenie Urzędników Odpowiedzialnych za Bezpieczeństwo Zapór Wodnych (*ang. Association of State Dam Safety Officials – ASDSO*) - http://www.damsafety.org

D.4.5. SEKTOR ENERGETYKI

- Departament Energetyki Stanów Zjednoczonych (*ang. U.S. Department of Energy – DOE*) - https://www.energy.gov
  - ✓ Biuro Departamentu Energetyki (DOE) ds. cyberbezpieczeństwa, bezpieczeństwa energetycznego i reagowania kryzysowego (*ang. Office of Cybersecurity, Energy Security, and Emergency Response – CESER*)
- Międzynarodowa Rada ds. Dużych Systemów Elektrycznych (*ang. International Council on Large Electric Systems – CIGRE*) - https://www.cigre.org
- Amerykańskie Stowarzyszenie Energetyki Publicznej (*ang. American Public Power Association – APPA*) - https://www.publicpower.org
  - ✓ Cybersecurity Defense Community (CDC)
- Instytut Badań nad Energią Elektryczną (*ang. Electric Power Research Institute – EPRI*) - https://www.epri.com
  - ✓ Krajowe zasoby w zakresie cyberbezpieczeństwa sektora energetycznego (*ang. National Electric Sector Cybersecurity Resource – NESCOR*)

D.4.6. SEKTOR ŻYWNOŚCI I ROLNICTWA

- Departament Rolnictwa Stanów Zjednoczonych (ang. *U.S. Department of Agriculture – USDA*) - https://www.usda.gov
- Amerykańska Agencja ds. Żywności i Leków (*ang. U.S. Food and Drug Administration – FDA*) - https://www.fda.gov
- Krajowy Związek Rolników (*ang. National Farmers Union – NFU*) - https://www.nfu.org
  - ✓ Rolnicze Centrum Kryzysowe (*ang. Farm Crisis Center*)

D.4.7. SEKTOR OPIEKI ZDROWOTNEJ I ZDROWIA PUBLICZNEGO

- Amerykańska Agencja ds. Żywności i Leków (ang. *U.S. Food and Drug Administration – FDA*) - https://www.fda.gov
  - ✓ Cyfrowe Centrum doskonałości w dziedzinie zdrowia (*ang. Digital Health Center of Excellence*)
- Agencja Zdrowia i Opieki Społecznej (*ang. Department of Health and Human Services – HHS*) - https://www.hhs.gov
  - ✓ Centrum Koordynacji Cyberbezpieczeństwa w Sektorze Zdrowia (*ang. Health Sector Cybersecurity Coordination Center – HC3*)
- Amerykańskie Stowarzyszenie Szpitali (*ang. American Hospital Association – AHA*) - https://www.aha.org/
  - ✓ Program preferowanych dostawców usług w zakresie cyberbezpieczeństwa Amerykańskiego Stowarzyszenia Szpitali (*ang. AHA Preferred Cybersecurity Provider (APCP) Program*)
- Narodowe Instytuty Zdrowia (*ang. National Institutes of Health – NIH*) - https://www.nih.gov
  - ✓ Centrum Pozyskiwania i Oceny Technologii Informacyjnych Narodowych Instytutów Zdrowia (*ang. NIH Information Technology Acquisition and Assessment Center – NITAAC*)
- Amerykańskie Towarzystwo Medyczne (*ang. American Medical Association – AMA*) - https://www.ama-assn.org

D.4.8. SEKTOR REAKTORÓW JĄDROWYCH, MATERIAŁÓW I ODPADÓW NUKLEARNYCH

- Amerykański Urząd Dozoru Jądrowego (*ang. U.S. Nuclear Regulatory Commission – NRC*) - https://www.nrc.gov
  - ✓ Biuro Bezpieczeństwa Jądrowego i Reagowania na Incydenty – Oddział Cyberbezpieczeństwa (*ang. Office of Nuclear Security and Incident Response Cyber Security Branch – CSB*)
- Międzynarodowa Agencja Energii Atomowej (*ang. International Atomic Energy Agency – IAEA*) - https://www.iaea.org
- Agencja Energii Jądrowej (*ang. Nuclear Energy Agency – NEA*) - https://www.oecd-nea.org
  - ✓ Grupa robocza ds. cyfrowego oprzyrządowania i sterowania (*ang. Digital Instrumentation and Control Working Group – DICWG*)
- Instytut Energii Jądrowej (*Nuclear Energy Institute – NEI*) - https://www.nei.org
- Światowy Instytut Bezpieczeństwa Jądrowego (*ang. World Institute of Nuclear Security – WINS*) - https://www.wins.org

D.4.9. SEKTOR SYSTEMÓW TRANSPORTOWYCH

- Departament Transportu Stanów Zjednoczonych (*ang. U.S. Department of Transportation – DOT*) - https://www.transportation.gov
  - ✓ Wspólne Biuro Programowe ds. Inteligentnych Systemów Transportowych *(ang. Intelligent Transportation Systems Joint Program Office)*
- Federalna Administracja Lotnictwa (*ang. Federal Aviation Administration – FAA*) - https://www.faa.gov
  - ✓ Inicjatywa w zakresie cyberbezpieczeństwa w lotnictwie grupy ds. cyberbezpieczeństwa organizacji ruchu lotniczego (ATO) (*ang. Aviation Cyber Initiative (ACI) of Air Traffic Organization (ATO) Cybersecurity Group*)
- Federalna Administracja Autostrad (*ang. Federal Highway Administration – FHWA*) - https://highways.dot.gov
  - ✓ Biuro Badań Operacyjnych, Rozwoju i Technologii *(ang. FHWA Office of Operations Research – Development – and Technology)*

- Federalna Administracja Bezpieczeństwa Przewoźników Samochodowych (*ang. Federal Motor Carrier Safety Administration – FMCSA*) - https://www.fmcsa.dot.gov
- Federalna Administracja Kolei (ang. *Federal Railroad Administration – FRA*) - https://railroads.dot.gov
  - ✓ Biuro Badań, Rozwoju i Technologii FRA (*ang. FRA Office of Research – Development – and Technology*)
- Federalna Administracja Transportu (*ang. Federal Transit Administration – FTA*) - https://www.transit.dot.gov
- Administracja Morska (*ang. Maritime Administration – MARAD*) - https://www.maritime.dot.gov
  - ✓ Biuro Bezpieczeństwa Morskiego (*ang. Office of Maritime Security*)
- Agencja ds. bezpieczeństwa rurociągów i materiałów niebezpiecznych (*ang. Pipeline and Hazardous Materials Safety Administration – PHMSA*) - https://www.phmsa.dot.gov
- Krajowa Administracja Bezpieczeństwa Ruchu Drogowego (*ang. National Highway Traffic Safety Administration – NHTSA*) - https://www.nhtsa.gov
- Administracja ds. Bezpieczeństwa Transportu (*ang. Transportation Security Administration – TSA*) - https://www.tsa.gov/for-industry
  - ✓ Zestaw narzędzi dotyczących cyberbezpieczeństwa dla sektora transportu naziemnego (*ang. Surface Transportation Cybersecurity Resource Toolkit*)
- Stowarzyszenie Kolei Amerykańskich (*ang. Association of American Railroads*) - https://www.aar.org

D.4.10. SEKTOR SYSTEMÓW WODNO-KANALIZACYJNYCH

- Amerykańska Agencja Ochrony Środowiska (*ang. U.S. Environmental Protection Agency – EPA*) - https://www.epa.gov
  - ✓ Ochrona wody pitnej i systemów oczyszczania ścieków (*ang. Drinking Water and Wastewater Resilience*)

- Amerykańskie Stowarzyszenie Wodociągów (*ang. American Water Works Association – AWWA*) - https://www.awwa.org
  - ✓ Narzędzie cyberbezpieczeństwa AWWA (*ang. AWWA Cybersecurity Tool*)
- Stowarzyszenie Wodociągów Miejskich (*ang. Association of Metropolitan Water Agencies – AMWA*) - https://www.amwa.net
- Krajowe Stowarzyszenie Przedsiębiorstw Wodociągowych (*ang. National Association of Water Companies – NAWC*) - https://www.nawc.org

D.5 KONFERENCJE I GRUPY ROBOCZE

D.5.1. SYMPOZJUM NAUKOWE DIGITAL BOND NA TEMAT BEZPIECZEŃSTWA SYSTEMÓW SCADA (S4)

Od 2007 roku S4 jest gospodarzem konferencji poświęconej bezpieczeństwu systemów sterowania przemysłowego, która początkowo miała na celu prezentację zaawansowanych i wysoce technicznych treści dla odbiorców związanych z tym sektorem. Od tego czasu zakres konferencji uległ rozszerzeniu i obejmuje więcej zagadnień związanych z bezpieczeństwem systemów sterowania przemysłowego, jednak niezmiennie pozostaje kluczową platformą prezentacji nowinek technicznych dotyczących bezpieczeństwa systemów OT.

https://s4xevents.com/

D.5.2. WSPÓLNA GRUPA ROBOCZA DS. SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO (*ANG. INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP – ICSJWG*)

CISA organizuje dwa razy w roku spotkania grupy roboczej, której celem jest promowanie komunikacji i współpracy między agencjami i departamentami rządu federalnego Stanów Zjednoczonych oraz podmiotami prywatnymi oraz operatorami systemów sterowania przemysłowego działających we wszystkich sektorach infrastruktury krytycznej. Celem ICSJWG jest wspieranie wspólnych wysiłków społeczności interesariuszy związanych z systemami sterowania ukierunkowanych na zabezpieczenie infrastruktur krytycznych poprzez działania w zakresie projektowania, rozwoju i wdrażania bezpiecznych systemów sterowania przemysłowego.

https://www.cisa.gov/resources-tools/groups/industrial-control-systens-joint-working-group-icsjwg

D.5.3. GRUPA ROBOCZA IFIP 11.10 DS. OCHRONY INFRASTRUKTURY KRYTYCZNEJ

Grupa Robocza 11.10 Międzynarodowej Federacji Przetwarzania Informacji (*ang. International Federation for Information Processing – IFIP*) to międzynarodowa społeczność zrzeszająca naukowców, inżynierów i praktyków zajmujących się

rozwojem najnowocześniejszych badań i praktyk w rozwojowej dziedzinie ochrony infrastruktury krytycznej.

http://ifip1110.org/Conferences/

D.5.4. KONFERENCJA SECURITYWEEK NA TEMAT CYBERBEZPIECZEŃSTWA SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

Od 2002 roku SecurityWeek organizuje doroczną konferencję poświęconą cyberbezpieczeństwu w sektorze systemów sterowania przemysłowego, podczas której użytkownicy, sprzedawcy, dostawcy zabezpieczeń i przedstawiciele organizacji rządowych spotykają się, by omówić najnowsze incydenty, przeanalizować ich przyczyny i wspólnie pracować nad rozwiązaniami.

https://www.icscybersecuritvconference.com/

D.5.5. MIĘDZYNARODOWY SZCZYT W SZTOKHOLMIE POŚWIĘCONY CYBERBEZPIECZEŃSTWU W SYSTEMACH SCADA I ICS (*ANG. STOCKHOLM INTERNATIONAL SUMMIT ON CYBER SECURITY IN SCADA AND ICS – CS3STHLM*)

Zorganizowany po raz pierwszy w 2014 roku szczyt CS3STHLM szybko stał się najważniejszym wydarzeniem dotyczącym bezpieczeństwa przemysłowych systemów sterowania w Europie Północnej. CS3STHLM oferuje wiele wykładów, a także okazji do nawiązywania kontaktów oraz dzielenia się wiedzą dotyczącą aktualnych wyzwań związanych z bezpieczeństwem systemów sterowania przemysłowego.

https://cs3sthlm.se/

ZAŁĄCZNIK E – ZDOLNOŚĆ DO OCHRONY ORAZ NARZĘDZIA ZABEZPIECZAJĄCE SYSTEMY OT

Niniejszy załącznik przedstawia najważniejsze technologie zabezpieczające, które są dostępne na rynku lub są opracowywane w celu zaspokajania potrzeb operatorów systemów OT. Na rynku dostępnych jest kilka produktów zabezpieczających opracowanych i oferowanych z myślą o systemach OT. Z kolei inne przedstawione rozwiązania to produkty zabezpieczające rozwiązania i systemy IT, które mogą również zostać wykorzystane w celu zabezpieczania systemów OT. Wiele produktów związanych z cyberbezpieczeństwem dostępnych na rynku to jednolite platformy, które obejmują opisane w tym załączniku funkcje oraz narzędzia. Każda organizacja powinna samodzielnie podjąć decyzję opartą na ryzyku dotyczącą stosowania technologii i narzędzi zabezpieczających przedstawionych w niniejszym załączniku.

E.1 SEGMENTACJA I IZOLACJA SIECI

Technologie segmentacji i izolacji sieci umożliwiają operatorom sieci OT realizowanie strategii cyberbezpieczeństwa opartych na fizycznej i logicznej izolacji ruchu sieciowego i urządzeń. Poniżej zostały przedstawione opisy popularnych narzędzi wykorzystywanych w tych celach.

E.1.1. ZAPORY SIECIOWE (*ANG. FIREWALLS*)

Zapory sieciowe mogą być wykorzystywane w celu egzekwowania określonych przez użytkowników zestawów reguł dla ruchu sieciowego na poziomie logicznym. Urządzenia te są zwykle stosowane jako urządzenia brzegowe w sieci, gdzie mogą ograniczać zarówno ruch przychodzący, jak i wychodzący na podstawie cech i parametrów przesyłanych danych.

Istnieje kilka rodzajów zapór sieciowych stosowanych powszechnie w środowiskach IT. Podstawowe *zapory sieciowe z filtrami pakietów* analizują na bieżąco ruch sieciowy realizowany w warstwach 3 oraz 4 modelu OSI, a następnie podejmują decyzje dotyczące odrzucania bądź przesyłania pakietów do miejsca docelowego. *Zapory sieciowe typu SFI*[42] opierają się z kolei na historii przeszłych oraz wykazie istniejących

[42] Zapory sieciowe z inspekcją stanów (*ang. stateful inspection firewalls – SFI*)

połączeń sieciowych w procesie podejmowania decyzji dotyczących filtrowania. Takie rozwiązanie wymaga wykorzystania większych mocy obliczeniowych, ale jednocześnie zapewnia większe możliwości i dodatkowe funkcje. *Zapory sieciowe nowej generacji (ang. Next generation firewalls – NGFW)* stanowią kolejny etap rozwojowy zapór sieciowych typu SFI – rozszerzają ich możliwości o funkcje takie jak: filtrowanie aplikacji, głęboka inspekcja pakietów, analiza ruchu w sieciach VPN, adaptacyjne reguły oraz wykrywanie zagrożeń.

Na rynku działa szereg producentów oferujących zapory sieciowe wyposażone w wyjątkowe zestawy funkcji opracowane z myślą o systemach OT. Takie produkty obejmują między innymi funkcje przetwarzania i odczytu komunikacji za pośrednictwem typowych protokołów wykorzystywanych w sieciach i systemach OT, takich jak: DNP3, CIP i Modbus, co pozwala na głęboką inspekcję pakietów przesyłanych w sieciach OT.

E.1.2. BRAMKI JEDNOKIERUNKOWE (ANG. UNIDIRECTIONAL GATEWAYS)

Bramki jednokierunkowe, nazywane także diodami danych, to urządzenia zaprojektowane w sposób umożliwiający przesył danych wyłącznie w jednym kierunku. W przeciwieństwie do zapór sieciowych, diody danych nie mogą być zaprogramowane w taki sposób, by umożliwić przepływ danych w obu kierunkach – nie pozwala na to konstrukcja urządzenia. Typowym zastosowaniem diody danych jest umieszczenie jej na granicy między siecią systemu OT i siecią organizacji. Dzięki zastosowaniu diody danych ruch z sieci OT jest w stanie przepływać do sieci organizacji, jednocześnie żadne pakiety nie są w stanie trafić do sieci OT, co zamyka jedną z możliwości przeprowadzenia cyberataku.

E.1.3. WIRTUALNE SIECI LOKALNE (ANG. VIRTUAL LOCAL AREA NETWORKS – VLAN)

Wirtualne sieci lokalne (VLAN) mogą być wykorzystywane w celu logicznej izolacji wybranych obszarów sieci w sytuacjach, gdy fizyczna separacja może nie być możliwa ze względu na koszty lub inne ograniczenia. Współczesne przełączniki sieciowe wykorzystują sieci VLAN w celu logicznego oddzielenia ruchu sieciowego na podstawie wybranych portów. Przykładowo, 8-portowy przełącznik można

skonfigurować w taki sposób, by rozdzielał ruch na dwie sieci VLAN. Jedna z tych sieci będzie obejmowała urządzenia podłączone do portów 1-4, natomiast druga obejmie urządzenia podłączone do portów 5-8. Pomimo tego, że wszystkie porty znajdują się fizycznie w jednym urządzeniu, poszczególne porty są połączone na poziomie logicznym wyłącznie z pozostałymi portami w danej sieci VLAN.

E.1.4. SIECI DEFINIOWANE PROGRAMOWO (ANG. SOFTWARE-DEFINED NETWORKING – SDN)

Konwencjonalne przełączniki sieciowe realizują funkcje przekazywania pakietów (w płaszczyźnie danych) oraz uruchamiania rozproszonych algorytmów odpowiedzialnych za trasowanie (w płaszczyźnie sterowania). Sieci definiowane programowo stanowią rozwinięcie tej koncepcji. W rozwiązaniach opartych na tej technologii funkcje związane z płaszczyzną danych realizuje przełącznik, natomiast algorytmy związane z płaszczyzną sterowania są realizowane przez centralny sterownik. Sterownik ten stanowi warstwę abstrakcji zapewniającą programowalność sieci, dzięki czemu nie jest konieczne konfigurowanie każdego przełącznika w sieci. Technologia sieci definiowanych programowo umożliwia prostą i dynamiczną rekonfigurację płaszczyzny danych, co pozwala na szybką izolację urządzeń lub przekierowanie i duplikowanie ruchu w celu monitorowania i przechwytywania danych. Wykorzystanie technologii sieci definiowanych programowo w środowiskach OT umożliwia bardziej elastyczne projektowanie ich architektur sieciowych oraz zwiększa możliwości ich aktualizacji w przyszłości.

E.2 MONITOROWANIE SIECI – BEZPIECZEŃSTWO INFORMACJI I ZARZĄDZANIE ZDARZENIAMI (*ANG. SECURITY INFORMATION AND EVENT MANAGEMENT – SIEM*)

Technologie monitorowania sieci zapewniają podmiotom odpowiedzialnym za sieci OT wgląd w stan nadzorowanych procesów oraz umożliwiają realizację celów związanych z cyberbezpieczeństwem, takich jak wykrywanie zdarzeń lub anomalii. Producenci urządzeń i systemów OT często wskazują, że oferowane przez nich technologie monitorowania sieci mogą zostać połączone z rozwiązaniami SIEM. Metoda działania tych systemów opiera się na gromadzeniu i zestawianiu danych z plików dziennika oraz

narzędzi skanujących sieci oraz wykrywaniu zagrożeń na podstawie analiz. Niektóre rozwiązania tego rodzaju pozwalają na automatyczne reagowanie na incydenty. Rozwiązania tego rodzaju są nieustannie rozbudowywane o nowe funkcje i możliwości, między innymi algorytmy uczenia maszynowego i sztucznej inteligencji w celu zwiększenia dokładności wykrywania i zmniejszenia liczby niepotrzebnych alarmów. Podmioty wykorzystujące systemy OT muszą jednak zachować szczególną ostrożność w przypadku wdrażania tego rodzaju rozwiązań, ponieważ ich stosowanie może bezpośrednio ograniczać dostępność nadzorowanego procesu.

E.2.1. SCENTRALIZOWANE GROMADZENIE PLIKÓW DZIENNIKA

Pliki dziennika (logi) z systemów oraz urządzeń sieciowych stanowią podstawowe źródło danych wykorzystywanych przez rozwiązania z rodziny SIEM. Pliki dziennika stanowią także podstawowe źródło danych historycznych, na którym opiera się proces reagowania na incydenty. Dzięki zgromadzeniu i zestawieniu danych w centralnej lokacji zawartość plików dziennika może być korelowana i analizowana w celu dokonania kompleksowego przeglądu stanu sieci. Rozwiązania SIEM wykorzystują szereg czujników rozmieszczonych strategicznie w sieci docelowej w celu gromadzenia informacji z urządzeń końcowych oraz danych dotyczących ruchu sieciowego, które są następnie przechowywane w bazie danych w celu przeprowadzania analiz w czasie rzeczywistym. Magazyny danych historycznych dotyczących sieci OT mogą stanowić dodatkowe źródło danych na temat zdarzeń, zapewniających szerszy kontekst i okoliczności wystąpienia incydentu związanego z cyberbezpieczeństwem.

E.2.2. SKANOWANIE PASYWNE

Pasywne skanowanie sieci to forma analizy sieci polegająca na obserwowaniu i analizowaniu odbywającego się w niej ruchu przechodzącego przez przełączniki sieciowe lub inne urządzenia. Rozwiązania realizujące funkcje pasywnego skanowania sieci nie wprowadzają do niej żadnego dodatkowego ruchu, dzięki czemu sprawdzają się dobrze w celu kontrolowania wrażliwych urządzeń działających w sieciach OT, w przypadku których bezpośrednie skanowanie może prowadzić do nieprzewidzianych skutków bądź zachowań. Dzięki zastosowaniu skanowania

pasywnego można wskazać wszystkie urządzenia, które aktywnie komunikują się w monitorowanych segmentach sieci. Dzięki kontroli danych znajdujących się w sieci, systemy skanowania pasywnego mogą gromadzić znaczące ilości informacji o urządzeniach, w tym między innymi określać producentów, numery części i wersje oprogramowania układowego. Skanowanie pasywne nie umożliwia wykrywania urządzeń, które nie prowadzą aktywnej komunikacji w sieci, nie jest też w stanie analizować zaszyfrowanego ruchu (jeśli nie jest skonfigurowane w tym celu). Warto także pamiętać o tym, że pełne skanowanie pasywne sieci często trwa kilka dni ze względu na konieczność analizy istniejącego ruchu sieciowego.

E.2.3. AKTYWNE SKANOWANIE

Aktywne skanowanie sieci to forma analizy sieci polegająca na bezpośrednim wykrywaniu podłączonych do niej urządzeń. Systemy oparte na mechanizmach aktywnego skanowania sieci wprowadzają ruch do sieci i wchodzą w bezpośrednią interakcję z urządzeniami znajdującymi się w zasięgu skanowania. Podmioty wykorzystujące sieci OT powinny zachować szczególną ostrożność, podejmując próbę aktywnego skanowania takich sieci ze względu na wrażliwość podłączonych do niej urządzeń. Próba aktywnego skanowania może negatywnie wpłynąć na stabilność lub działanie urządzenia, wpłynąć na realizowane przez nie funkcje, a nawet mieć wpływ na bezpieczeństwo i integralność procesu. Aktywne skanowanie należy zaplanować w taki sposób, by odbywało się podczas planowanych przestojów, jeśli jest to możliwe.

Wybrane rozwiązania opracowane z myślą o systemach OT łączą skanowanie pasywne i aktywne, aby umożliwić przeprowadzanie skanowania aktywnego w sposób bezpieczniejszy dla sieci. Tego rodzaju systemy najpierw ustalają przy pomocy metod skanowania pasywnego wykaz urządzeń podłączonych do sieci, a następnie wykorzystują aktywne metody dobrane z myślą o konkretnych urządzeniach, aby uzyskać dodatkowe informacje o podłączonym do sieci sprzęcie bez ryzyka dla działania systemu OT.

E.2.4. WYKRYWANIE ZŁOŚLIWEGO OPROGRAMOWANIA

Wykrywanie złośliwego oprogramowania działającego na urządzeniach końcowych umożliwia oprogramowanie antywirusowe, którego zadaniem jest monitorowanie

aktywności na hoście i ostrzeganie użytkownika o możliwych złośliwych działaniach. Starsze techniki wykrywania opierają się na sygnaturach plików, na podstawie których oprogramowanie wskazuje znane zagrożenia. Z biegiem czasu twórcy złośliwego oprogramowania znaleźli sposoby na obejście tego mechanizmu, między innymi za pomocą kodu polimorficznego. Nowoczesne oprogramowanie antywirusowe wykorzystuje analizę behawioralną uruchomionych procesów i zaawansowane techniki analizy plików w celu wykrywania potencjalnie złośliwej aktywności.

Wykrywanie złośliwego oprogramowania na hostach przy użyciu oprogramowania antywirusowego to rozwiązanie, którego stosowanie może być niemożliwe bądź niewskazane w przypadku wybranych urządzeń i komponentów systemów OT ze względu na zastosowane systemy operacyjne, niekompatybilne oprogramowanie bądź wymogi dotyczące czasu działania. Tego rodzaju problemy nie stanowią jednak przeszkody uniemożliwiającej korzystanie z sieciowych rozwiązań w celu wykrywania złośliwego oprogramowania. W przeciwieństwie do oprogramowania antywirusowego uruchamianego bezpośrednio na hoście, rozwiązania wykrywające złośliwe oprogramowanie w sieci są uruchamiane na niezależnym urządzeniu, które analizuje i sprawdza ruch sieciowy pod kątem anomalii. Rozwiązania sieciowe w zakresie wykrywania złośliwego oprogramowania oferują możliwości i funkcje zbliżone do rozwiązań uruchamianych na hostach, jednocześnie nie wykorzystują zasobów i nie ograniczają wydajności chronionych urządzeń i komponentów systemów. Tego rodzaju rozwiązania należą do podstawowych funkcji pakietów SIEM.

E.2.5. SYSTEMY WYKRYWANIA ANOMALII BEHAWIORALNYCH

Działanie systemów wykrywania anomalii behawioralnych (*ang. Behavioral anomaly detection – BAD*) opiera się na porównywaniu bieżącego stanu środowiska z poziomem bazowym w celu wykrywania nietypowych i anomalnych zachowań oraz przeprowadzenia dokładniejszych analiz. Wykrywane zachowania obejmują między innymi nietypowy ruch sieciowy, w tym przesyłanie dużych ilości danych, a także wykorzystanie nowych portów lub protokołów bądź nowe połączenia między urządzeniami. Wykrywane rodzaje nietypowych zachowań urządzeń to między innymi nadmierne wykorzystanie zasobów procesora, logowanie poza godzinami pracy lub

uruchomienie nowych procesów. Wykaz wykrywanych zdarzeń jest uzależniony od zakresu działania czujników danego rozwiązania. Niektóre systemy tego rodzaju wykorzystują algorytmy uczenia maszynowego oraz rozwiązania oparte na sztucznej inteligencji w celu automatycznej aktualizacji poziomu bazowego. Dzięki automatyzacji tego procesu system jest w stanie gromadzić dane na temat typowej aktywności systemu nawet pomimo zmian dokonywanych w środowisku przez jego operatorów z upływem czasu. Zastosowanie takich rozwiązań zmniejsza liczbę wyników fałszywie dodatnich oraz usprawnia reagowanie na incydenty.

E.2.6. ZAPOBIEGANIE UTRACIE DANYCH (ANG. DATA LOSS PREVENTION – DLP)

Rozwiązania w zakresie zapobiegania utracie danych, określane często skrótem DLP, stanowią zbiór narzędzi opracowanych z myślą o zwiększeniu poufności wrażliwych danych w sieci. Rozwiązania DLP często stanowią zestaw funkcji w ramach systemów SIEM, umożliwiających aktywne monitorowanie danych w spoczynku (w składowaniu), zapobiegając w ten sposób nieautoryzowanemu dostępowi, a także przesyłanych danych, co pozwala zapobiegać ich przechwytywaniu. Co więcej, rozwiązania DLP mogą dostarczyć organizacji informacji na temat naruszenia zasad ochrony danych, nawet jeśli nie będą w stanie zapobiec jego wystąpieniu.

E.2.7. ZWODZENIE NAPASTNIKÓW (ANG. DECEPTION TECHNOLOGY)

Rozwiązania wykorzystywane w celu zwodzenia napastników opierają się na przynętach w postaci zbiorów danych oraz urządzeń podłączonych do sieci, których zadaniem jest odwrócenie uwagi od chronionych zasobów. Mogą obejmować zarówno poświadczenia i dane dostępowe, jak i pliki oraz urządzenia. Gdy napastnik wykona jakiekolwiek działania związane z przynętą, uruchamia alarm ostrzegający pracowników organizacji odpowiedzialnych za bezpieczeństwo o ataku, którzy mogą następnie podjąć decyzję o obserwowaniu przeciwnika w celu uzyskania dodatkowych informacji lub eliminacji zagrożenia. Ze względu na to, że tego rodzaju rozwiązania nie wchodzą w interakcje z innymi komponentami sieci, przynęty mogą stanowić cenne wsparcie procesów monitorowania i wykrywania złośliwej aktywności, jednocześnie w żaden sposób nie wpływając na nadzorowany proces.

E.2.8. CYFROWE BLIŹNIAKI (*ANG. DIGITAL TWINS*)

Cyfrowy bliźniak to cyfrowa replika fizycznego systemu lub komponentu, wykorzystywana w wybranych środowiskach OT w roli narzędzia umożliwiającego wykrywanie nietypowych zachowań. Cyfrowy bliźniak przetwarza dane wejściowe z czujników w czasie rzeczywistym i porównuje je za pomocą heurystyki i algorytmów (w tym uczenia maszynowego) z modelem określającym poziom bazowy. Większość anomalii wykrywanych dzięki cyfrowym bliźniakom zwykle wskazuje na konieczność przeprowadzenia prac utrzymaniowych lub wystąpienie awarii, jednak w wybranych przypadkach może być także wskazaniem zaawansowanego cyberataku, którego sprawcom udało się ominąć inne środki bezpieczeństwa, w związku z czym mógłby w innym przypadku pozostać niewykryty.

E.3 BEZPIECZEŃSTWO DANYCH

Różne technologie zapewniające bezpieczeństwo danych pomagają właścicielom informacji w ochronie poufności, integralności i dostępności informacji. Podmioty wykorzystujące w swojej działalności sieci i systemy OT powinny opracować wykazy najważniejszych plików oraz danych przetwarzanych i składowanych w tych sieciach, a także wdrożyć stosowne technologie bezpieczeństwa danych w celu ograniczenia ryzyka.

E.3.1. MAGAZYNY KOPII ZAPASOWYCH

Magazyn kopii zapasowych to zapasowa lokalizacja przechowywania plików, mieszcząca kopie najważniejszych plików i umożliwiająca ich ochronę, aby umożliwić odtworzenie danych w przypadku utraty, naruszenia zasad ochrony lub zniszczenia oryginałów danych. Wdrożenie narzędzi i procedur tworzenia kopii zapasowych ma kluczowe znaczenie dla zapewnienia dostępności krytycznych danych w środowisku sieci OT. Opracowane na podstawie oszacowanego ryzyka plany tworzenia kopii zapasowych powinny wskazywać dane wymagające stworzenia kopii zapasowych, częstotliwość tworzenia kopii, liczbę wykonywanych kopii, lokację kopii zapasowych (na przykład w odłączonych od sieci systemach lub w innej lokalizacji geograficznej) oraz czas przechowywania (retencji) utworzonych kopii zapasowych. Na rynku są dostępne różne rozwiązania automatyzujące regularne tworzenie kopii zapasowych krytycznych danych.

E.3.2. NIEZMIENNA PAMIĘĆ MASOWA

Niezmienna pamięć masowa to specjalny rodzaj pamięci masowej umożliwiający przechowywanie kopii zapasowych w sposób zapewniający integralność danych dzięki uniemożliwieniu wprowadzania zmian i modyfikacji – wszelkie dane są dostępne wyłącznie w formie tylko do odczytu. Niezmienna pamięć masowa może być wykorzystywana w celu przechowywania kopii zapasowych programów lub konfiguracji urządzeń. Może także być używana jako dysk pracujący w trybie tylko do odczytu w stacji roboczej, co stanowi dodatkowy sposób ochrony przed instalacją nowego oprogramowania.

E.3.3. WYLICZANIE SKRÓTÓW KRYPTOGRAFICZNYCH PLIKÓW

Integralność najważniejszych plików w systemie, w tym logiki programów uruchamianych w środowisku, może zostać zweryfikowana dzięki skrótom kryptograficznym (haszom). Rozwiązania pozwalające na wykorzystanie tej funkcji obliczają ciąg znaków o ustalonej długości w oparciu o zawartość pliku. Obliczenie oraz zapisanie skrótu kryptograficznego pliku po jego utworzeniu umożliwia weryfikację integralności pliku oraz sprawdzenie, czy nie zostały w nim dokonane żadne zmiany dzięki ponownemu obliczeniu i porównaniu skrótu. Przykładowo w sytuacji, w której użytkownik końcowy chce przywrócić konfigurację urządzenia do poziomu bazowego poprzez przywrócenie plików, powinien najpierw zweryfikować ich integralność obliczając ich skróty kryptograficzne. W przypadku stwierdzenia, że wykonanie funkcji skrótu doprowadziło do obliczenia innej wartości skrótu, należy założyć, że zasady ochrony plików kopii zapasowej zostały naruszone. Funkcja obliczania skrótów kryptograficznych plików jest rozwiązaniem stosowanym w wielu rozwiązaniach umożliwiających tworzenie kopii zapasowych. Stosowne algorytmy funkcji skrótu dopuszczone do użytkowania przez NIST zostały opisane w dokumentach FIPS 180-4, *Secure Hash Standard* [FIPS180], a także FIPS 202, *SHA-3 Standard* [FIPS202].

E.3.4. PODPISY CYFROWE

Podpisy cyfrowe stanowią dodatkowy czynnik zapewniający integralność danych. Podpis cyfrowy stanowi elektroniczny odpowiednik tradycyjnego podpisu, a jego

celem jest wskazanie, że dany podmiot dokonał podpisu informacji oraz że po dokonaniu podpisu informacje nie uległy zmianie. Dokument FIPS 186-4, *Digital Signature Standard (DSS)* [FIPS186], zawiera opisy trzech algorytmów podpisu cyfrowego wskazanych przez NIST jako dopuszczalne do stosowania w systemach: DSA, RSA oraz ECDSA.

E.3.5. SZYFROWANIE BLOKOWE

Podmioty mogą chronić poufność danych w spoczynku (w składowaniu) za pomocą algorytmów szyfrowania blokowego, które pozwalają na szyfrowanie fragmentów danych określanych mianem bloków, zamiast szyfrować je bit po bicie. Takie rozwiązanie jest szczególnie przydatne w przypadku jednoczesnego szyfrowania dużych ilości danych. Algorytmy szyfrowania blokowego wskazane przez NIST jako stosowne to Advanced Encryption Standard (AES) oraz Triple Data Encryption Standard (DES). Algorytm AES został opisany w dokumencie FIPS 197, *Advanced Encryption Standard* [FIPS197]. Opis algorytmu DES znajduje się w dokumencie NIST SP 800-67, Rev. 2, *Recommendation for the Triple Data Encryption Algorithm Block Cipher* [SP800-67r2].

E.3.6. ZDALNY DOSTĘP

Należy wdrożyć zabezpieczenia, aby zapobiec nieautoryzowanemu zdalnemu dostępowi do sieci, systemów i danych organizacji. Wirtualne sieci prywatne (VPN) wykorzystują zestaw technologii i protokołów zaprojektowanych do obsługi bezpiecznego zdalnego dostępu do środowisk sieciowych. VPN może zapewnić zarówno silne uwierzytelnianie, jak i szyfrowanie w celu zabezpieczenia danych komunikacyjnych poprzez ustanowienie sieci prywatnej, która pełni rolę nakładki działającej w oparciu o infrastrukturę publiczną. Najpopularniejsze typy technologii VPN to:

Internet Protocol Security (IPsec). IPsec obsługuje dwa tryby szyfrowania – transportowy i tunelowy. Tryb transportowy szyfruje tylko część danych (zawartość) każdego pakietu, pozostawiając nagłówek pakietu niezaszyfrowany. Bardziej bezpieczny tryb tunelowania dodaje nowy nagłówek do każdego pakietu i szyfruje zarówno oryginalny nagłówek, jak i zawartość pakietu. Po stronie odbiorczej urządzenie zgodne z protokołem IPsec

odszyfrowuje każdy pakiet. Więcej informacji można znaleźć w dokumencie NIST SP 800-77, Rev. 1, *Guide to IPsec VPNs*.

Transport Layer Security (TLS). Protokół określany także starszą nazwą – Secure Sockets Layer (SSL). Umożliwia stworzenie bezpiecznego kanału połączenia między dwoma urządzeniami i szyfruje zawartość każdego pakietu. Protokół TLS jest zwykle wykorzystywany w celu zabezpieczenia ruchu HTTP w ramach bezpiecznego rozszerzenia HTTPS. Stosowanie protokołu TLS nie jest jednak ograniczone do ruchu HTTP i może być używane do zabezpieczania wielu programów warstwy aplikacji. Więcej informacji można znaleźć w dokumencie NIST SP 800-52, Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*

Secure Shell (SSH). SSH to interfejs poleceń i protokół służący do bezpiecznego uzyskiwania dostępu do zdalnego komputera. Jest on powszechnie używany przez administratorów sieci do zdalnego kontrolowania serwerów pracujących pod kontrolą systemu operacyjnego Linux. SSH jest bezpieczną alternatywą dla aplikacji telnet, jest zawarty w większości dystrybucji systemów z rodziny UNIX, możliwa jest też jego instalacja na innych platformach dzięki dodatkowym pakietom.

Wdrożone z należytą starannością technologie zdalnego dostępu mogą zwiększyć możliwości organizacji. Wśród rozwiązań umożliwiających zdalny dostęp do systemów można wymienić między innymi protokół pulpitu zdalnego (*ang. Remote Desktop Protocol – RDP*), a także ekrany oraz oprogramowanie dodatkowe. Należy jednak pamiętać, że brak stosownych zabezpieczeń związanych z technologiami zdalnego dostępu, w tym brak zarządzania podatnościami i poprawkami, może umożliwić napastnikom wykorzystanie tych rozwiązań w celu naruszenia zasad ochrony systemu.

ZAŁĄCZNIK F – NAKŁADKA DOTYCZĄCA SYSTEMÓW OT

Informacja dla czytelników

Nakładka dotycząca systemów OT stanowi próbę częściowego dostosowania zabezpieczeń oraz zabezpieczeń bazowych opisanych w Narodowym Standardzie Cyberbezpieczeństwa NSC 800-53 [NSC 800-53][43], obejmująca dodatkowe wytyczne opracowane z myślą o systemach OT. Koncepcja nakładek została omówiona w Załączniku C do dokumentu NSC 800-53B [NSC 800-53B][44]. Nakładka dotycząca systemów OT została opracowana z myślą o stosowaniu jej w przypadku wszystkich systemów OT wykorzystywanych we wszystkich sektorach przemysłu. Dodatkowe zmiany mogą pozwolić na dostosowanie zabezpieczeń do wymogów danego sektora (na przykład energetyki lub rurociągów). Nakładka może także zostać opracowana z myślą o określonym systemie (na przykład produkcie spółki XYZ).

Przedstawiona nakładka dotycząca systemów OT obejmuje wytyczne i zmiany dotyczące zabezpieczeń opisanych w dokumencie NSC 800-53 [NSC 800-53]. Ze względu na to, że uwzględnienie w niniejszej publikacji kopii załącznika F do dokumentu NSC 800-53 [NSC 800-53] znacznie zwiększyłoby jej objętość, autorzy podjęli decyzję o jego pominięciu.

Autorzy uznali również, że przedstawiona w niniejszym dokumencie nakładka dotycząca systemów OT może posłużyć jako wzór do opracowania innych nakładek. Prosimy o zgłaszanie informacji zwrotnych na temat struktury niniejszego załącznika, zwłaszcza dotyczących poziomu abstrakcji oraz przykładów zawartych w dodatkowych wytycznych, a także ich kompletności oraz przydatności z punktu widzenia wdrożenia.

Nakładki stanowią uporządkowany sposób na wsparcie organizacji w procesie ustalania poziomu bazowego zabezpieczeń dostosowanego do własnych potrzeb, a także opracowania wyspecjalizowanych planów bezpieczeństwa, które można zastosować do określonych misji i funkcji biznesowych, środowisk operacyjnych bądź

[43] Oryginalna wersja anglojęzyczna – NIST SP 800-53 rev. 5
[44] Oryginalna wersja anglojęzyczna – NIST SP 800-53B, październik 2020 roku

technologii. Zastosowanie takiego podejścia jest ważne, ponieważ liczba zabezpieczeń opartych na zagrożeniach i zabezpieczeń rozszerzonych uwzględnionych w katalogu stale rośnie, z kolei organizacje opracowują strategie zarządzania ryzykiem, aby zaspokoić swoje potrzeby w zakresie ochrony w ramach określonych poziomów tolerowanego ryzyka.

Zbiór nakładek znajduje się pod adresem NIST Risk Management Framework | CSRC. Nazwa dokumentu zawierającego treść niniejszej nakładki w języku angielskim to NIST SP 800-82, Rev. 3 Operational Technology Overlay („NIST SP 800-82 Rev 3 OT Overlay"). Treść nakładki jest oparta na publikacji specjalnej NIST SP 800-53 [NSC 800-53], a jej polska wersja została opracowana na podstawie dokumentu NSC 800-53 – *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji*.

Powodem opracowania niniejszej nakładki przez Narodowy Instytut Standaryzacji i Technologii jest realizacja obowiązków wynikających z przepisów federalnej ustawy o modernizacji standardów bezpieczeństwa informacji (FISMA) z 2014 roku (Public Law 113-283) [FISMA], prezydenckiej dyrektywy politycznej nr 21 (PPD-21) [PPD-21], oraz rozporządzenia wykonawczego nr 13636 [EO13636]. Obszar odpowiedzialności NIST obejmuje opracowywanie norm oraz wytycznych dotyczących bezpieczeństwa informacji dotyczących zróżnicowanych podmiotów oraz zasobów, w tym minimalnych wymagań dotyczących federalnych systemów informacyjnych. Opracowane normy i wytyczne nie mogą być jednak stosowane w odniesieniu do krajowych systemów bezpieczeństwa bez wyraźnej zgody stosownych urzędników federalnych odpowiedzialnych za ustalanie zasad dotyczących tych systemów.

F.1 OPIS NAKŁADKI

Systemy i urządzenia wchodzące w zakres technologii operacyjnych to rozwiązania, które wchodzą w interakcje ze środowiskiem fizycznym lub zarządzają urządzeniami wchodzącymi w interakcje ze środowiskiem fizycznym. Takie systemy oraz urządzenia wykrywają lub wywołują zmiany poprzez monitorowanie lub kontrolowanie urządzeń, procesów i zdarzeń. Przykłady takich rozwiązań obejmują przemysłowe systemy sterowania, systemy automatyki budynków, systemy transportowe, systemy kontroli

dostępu fizycznego, systemy monitorowania i systemy pomiarowe działające w środowiskach fizycznych.

System sterowana przemysłowego składa się z szeregu elementów sterujących (elektrycznych, mechanicznych, hydraulicznych, pneumatycznych), które współpracują w celu realizacji określonego celu związanego między innymi z produkcją, transportem materiałów lub wytwarzaniem energii. Komponenty i części systemu, których celem jest przede wszystkim wytwarzanie produktów końcowych określamy mianem procesu. Komponenty sterujące systemu obejmują specyfikację pożądanego produktu końcowego lub osiągów i wydajności. Sterowanie może być w pełni zautomatyzowane lub może odbywać się z udziałem człowieka.

Rozdział 2 zawiera omówienie różnych systemów OT, w tym systemów kontroli nadzorczej i pozyskiwania danych (SCADA), rozproszonych systemów sterowania (DCS), programowalnych sterowników logicznych (PLC), systemów automatyki budynków (BAS), systemów kontroli dostępu fizycznego (PACS) oraz systemów przemysłowego Internetu rzeczy (IIoT).

F.2 ZAKRES STOSOWANIA NAKŁADKI

Celem niniejszej nakładki jest przedstawienie wytycznych dotyczących stosowania zabezpieczeń w systemach OT. Treść nakładki została opracowana z myślą o korzystaniu z niej przez przedstawicieli organów rządowych. Organizacje pozarządowe oraz przedsiębiorstwa mogą wykorzystywać wytyczne zawarte w niniejszym dokumencie na zasadzie dobrowolności.

W przypadku niektórych systemów OT prywatność może stanowić czynnik ryzyka. Dodatkowe wytyczne dotyczące tego zagadnienia znajdują się dokumencie NIST Privacy Framework [PF]. Zakres prywatności w systemach OT jest uzależniony od ryzyka sektorowego i organizacyjnego, w związku z czym zabezpieczenia związane wyłącznie z prywatnością nie zostały uwzględnione w treści nakładki. Poszczególne organizacje muszą samodzielnie określić zakres stosowania zawartych wytycznych. Wszystkie zabezpieczenia i zabezpieczenia rozszerzone, które zostały uwzględnione w poziomie bazowym zabezpieczeń prywatności nie zostały uwzględnione w treści niniejszej nakładki.

F.3 PODSUMOWANIE NAKŁADKI

Tabela 22 zawiera podsumowanie środków bezpieczeństwa i zabezpieczeń rozszerzonych opisanych w Załączniku F do dokumentu NSC 800-53 [NSC 800-53], przyporządkowanych do poziomów wpływu na system/informacje (Niskiego, Umiarkowanego lub Wysokiego) bazowych zabezpieczeń wraz z omówieniem zabezpieczeń w kontekście systemów OT oraz dostosowania ich do potrzeb tych systemów. W przedstawionej tabeli zastosowano następujące konwencje:

Pogrubienie oznacza środek bezpieczeństwa lub zabezpieczenie rozszerzone obejmujące omówienie zabezpieczenia w kontekście systemów OT.

Podkreślenie wskazuje, że niniejsza nakładka dodaje zabezpieczenie do poziomu bazowego, który stanowi uzupełnienie poziomu bazowego zabezpieczeń przedstawionego w dokumencie NSC 800-53B [NSC 800-53B].

~~Przekreślenie~~ wskazuje, że dany środek bezpieczeństwa lub zabezpieczenie rozszerzone zostały usunięte z zabezpieczeń poziomu bazowego przedstawionych w dokumencie NSC 800-53B [NSC 800-53B].

W przykładzie przedstawionym poniżej omówienie zabezpieczenia w kontekście systemów OT zostało dodane do zabezpieczenie rozszerzonego nr 1 do zabezpieczenia AU-4 (zapisanego pogrubioną czcionką). Ponadto zabezpieczenie rozszerzone nr 1 do zabezpieczenia AU-4 zostało uwzględnione w poziomach bazowych Niskim, Umiarkowanym oraz Wysokim (podkreślone) poziomie wpływu, co stanowi zmianę względem poziomów bazowych opisanych w dokumencie NSC 800-53B [NSC 800-53B], które nie obejmują zabezpieczenia rozszerzonego nr 1 do zabezpieczenia AU-4.

Au-4	Pojemność pamięci zapisów audytu	Au-4 **(1)**	Au-4 **(1)**	Au-4 **(1)**

Niektóre środki bezpieczeństwa i zabezpieczenia rozszerzone mogą znaleźć zastosowanie w wielu środowiskach OT, jednak nie są użyteczne we wszystkich sektorach lub architekturach OT. Tego rodzaju zabezpieczenia mogą być opatrzone dodatkowym omówieniem w kontekście systemów OT. Omówienia te znajdują się w tabelach obok stosownych zabezpieczeń. Środki bezpieczeństwa i zabezpieczenia rozszerzone nie uwzględnione w poziomach bazowych, nie zostały uwzględnione w **tabeli 22**.

Tabela 22. Poziomy bazowe zabezpieczeń

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
AC-1	Polityka i procedury	**AC-1**	**AC-1**	**AC-1**
AC-2	Zarządzanie kontami	**AC-2**	**AC-2** (1) **(2)** (3) (4) **(5) (13)**	**AC-2** (1) **(2)** (3) (4) **(5)** (11) (12) **(13)**
AC-3	Egzekwowanie uprawnień dostępu	**AC-3**	**AC-3**	**AC-3 (11)**
AC-4	Egzekwowanie zasad przepływu informacji		**AC-4**	**AC-4** (4)
AC-5	Rozdział obowiązków		**AC-5**	**AC-5**
AC-6	Zasada minimalnych uprawnień		**AC-6 (1) (2) (5)** (7) **(9) (10)**	**AC-6 (1) (2) (3) (5)** (7) **(9) (10)**
AC-7	Nieudane próby logowania	**AC-7**	**AC-7**	**AC-7**
AC-8	Powiadomienie o zasadach użycia systemu	**AC-8**	**AC-8**	**AC-8**
AC-10	Kontrola liczby jednoczesnych sesji			**AC-10**
AC-11	Blokada urządzenia		**AC-11 (1)**	**AC-11 (1)**
AC-12	Zakończenie sesji		**AC-12**	**AC-12**
AC-14	Działania dozwolone bez identyfikacji lub uwierzytelnienia	AC-14	AC-14	AC-14
AC-17	Dostęp zdalny	**AC-17 (9)**	**AC-17 (1) (2) (3)** (4) **(9)** (10)	**AC-17 (1) (2) (3)** (4) **(9)** (10)
AC-18	Dostęp bezprzewodowy	**AC-18**	**AC-18 (1)** (3)	**AC-18 (1)** (3) (4) **(5)**
AC-19	Kontrola dostępu do urządzeń przenośnych	AC-19	AC-19 (5)	AC-19 (5)

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
AC-20	Wykorzystanie systemów zewnętrznych	**AC-20**	**AC-20** (1) (2)	**AC-20** (1) (2)
AC-21	Udostępnianie informacji		AC-21	AC-21
AC-22	Treści publicznie dostępne	**AC-22**	**AC-22**	**AC-22**
AT-1	Polityka i procedury	**AT-1**	**AT-1**	**AT-1**
AT-2	Szkolenie w zakresie uświadamiania bezpieczeństwa	**AT-2** (2)	**AT-2** (2) (3) **(4)**	**AT-2** (2) (3) **(4)**
AT-3	Szkolenie w zakresie bezpieczeństwa opartego na rolach	**AT-3**	**AT-3**	**AT-3**
AT-4	Dokumentacja szkoleniowa	AT-4	AT-4	AT-4
AU-1	Polityka i procedury	**AU-1**	**AU-1**	**AU-1**
AU-2	Audyt zdarzeń	**AU-2**	**AU-2**	**AU-2**
AU-3	Zawartość rejestrów audytu	AU-3	AU-3 (1)	AU-3 (1)
AU-4	Pojemność pamięci zapisów audytu	AU-4 (1)	AU-4 (1)	AU-4 (1)
AU-5	Reakcja na błędy procesów audytu	AU-5	AU-5	AU-5 (1) (2)
AU-6	Przegląd audytu, analiza i raportowanie	AU-6	AU-6 **(1)** (3)	AU-6 **(1)** (3) (5) (6)
AU-7	Redukcja treści zapisów z audytu i generowanie raportów		AU-7 (1)	AU-7 (1)
AU-8	Znaczniki czasu	**AU-8**	**AU-8**	**AU-8**
AU-9	Ochrona informacji audytowych	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Niezaprzeczalność			**AU-10**
AU-11	Retencja zapisów audytu	AU-11	AU-11	AU-11

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
AU-12	Tworzenie zapisów audytu	AU-12	AU-12	AU-12 **(1) (3)**
CA-1	Polityka i procedury	**CA-1**	**CA-1**	**CA-1**
CA-2	Ocena zabezpieczeń	**CA-2**	**CA-2** (1)	**CA-2** (1) **(2)**
CA-3	Wymiana informacji	**CA-3**	**CA-3**	**CA-3** (6)
CA-5	Plan i etapy działania	**CA-5**	**CA-5**	**CA-5**
CA-6	Autoryzacja	CA-6	CA-6	CA-6
CA-7	Ciągłe monitorowanie	**CA-7** (4)	**CA-7** (1) (4)	**CA-7** (1) (4)
CA-8	Testy penetracyjne			**CA-8** ~~(4)~~
CA-9	Połączenia wewnątrzsystemowe	**CA-9**	**CA-9**	**CA-9**
CM-1	Polityka i procedury	**CM-1**	**CM-1**	**CM-1**
CM-2	Konfiguracja bazowa	CM-2	CM-2 (2) (3) (7)	CM-2 (2) (3) (7)
CM-3	Zabezpieczanie zmian konfiguracji		**CM-3** (2) (4)	**CM-3** (1) (2) (4) (6)
CM-4	Analizy wpływu	**CM-4**	**CM-4** (2)	**CM-4** (1) (2)
CM-5	Ograniczenia możliwości dokonywania zmian	**CM-5**	**CM-5**	**CM-5** (1)
CM-6	Ustawienia konfiguracji	CM-6	CM-6	CM-6 (1) (2)
CM-7	Zasada minimalnej funkcjonalności	**CM-7**	**CM-7** (1) (2) **(5)**	**CM-7** (1) (2) **(5)**
CM-8	Inwentaryzacja komponentów systemu	CM-8	CM-8 (1) (3)	CM-8 (1) (2) (3) (4)
CM-9	Plan zarządzania konfiguracją		**CM-9**	**CM-9**
CM-10	Ograniczenia w użyciu oprogramowania	CM-10	CM-10	CM-10

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
CM-11	Oprogramowanie instalowane przez użytkownika	CM-11	CM-11	CM-11
CM-12	Położenie (lokacja) informacji		**CM-12** (1)	**CM-12** (1)
CP-1	Polityka i procedury	**CP-1**	**CP-1**	**CP-1**
CP-2	Plan ciągłości działania	**CP-2**	**CP-2** (1) (3) (8)	**CP-2** (1) (2) (3) (5) (8)
CP-3	Szkolenie w zakresie planowania ciągłości działania	CP-3	CP-3	CP-3 (1)
CP-4	Testowanie planu ciągłości działania	CP-4	CP-4 (1)	CP-4 (1) **(2)**
CP-6	Zapasowe miejsce przechowywania kopii		CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Zapasowe miejsce przetwarzania		**CP-7** (1) (2) (3)	**CP-7** (1) (2) (3) (4)
CP-8	Usługi telekomunikacyjne		**CP-8** (1) (2)	**CP-8** (1) (2) (3) (4)
CP-9	Kopia zapasowa	CP-9	CP-9 **(1)** (8)	CP-9 **(1) (2)** (3) (5) (8)
CP-10	Odzyskiwanie i odtwarzanie systemu	**CP-10**	**CP-10** (2) **(6)**	**CP-10** (2) (4) **(6)**
CP-12	Tryb bezpieczny	CP-12	CP-12	CP-12
IA-1	Polityka i procedury	**IA-1**	**IA-1**	**IA-1**
IA-2	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)	**IA-2 (1) (2)** (8) **(12)**	**IA-2 (1) (2)** (8) **(12)**	**IA-2 (1) (2) (5)** (8) **(12)**
IA-3	Identyfikacja i uwierzytelnianie urządzenia	IA-3	IA-3	IA-3
IA-4	Zarządzanie identyfikatorem	IA-4	IA-4 **(4)**	IA-4 **(4)**

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
IA-5	Zarządzanie metodami uwierzytelniania	**IA-5** (1)	**IA-5** (1) (2) (6)	**IA-5** (1) (2) (6)
IA-6	Ochrona procesu uwierzytelniania	**IA-6**	**IA-6**	**IA-6**
IA-7	Uwierzytelnianie modułu kryptograficznego	IA-7	IA-7	IA-7
IA-8	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji)	**IA-8 (1) (2) (4)**	**IA-8 (1) (2) (4)**	**IA-8 (1) (2) (4)**
IA-11	Ponowne uwierzytelnienie	IA-11	IA-11	IA-11
IA-12	Potwierdzanie tożsamości		**IA-12 (2) (3) (5)**	**IA-12 (1) (2) (3) (4) (5)**
IR-1	Polityka i procedury	**IR-1**	**IR-1**	**IR-1**
IR-2	Szkolenie w zakresie reagowania na incydenty	IR-2	IR-2	IR-2 (1) (2)
IR-3	Testowanie reagowania na incydenty		IR-3 (2)	IR-3 (2)
IR-4	Obsługa incydentów	**IR-4**	**IR-4** (1)	**IR-4** (1) (4) (11)
IR-5	Monitorowanie incydentów	IR-5	IR-5	IR-5 (1)
IR-6	Zgłaszanie incydentów	**IR-6**	**IR-6 (1)** (3)	**IR-6 (1)** (3)
IR-7	Wsparcie reagowania na incydenty	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Plan reagowania na incydenty	IR-8	IR-8	IR-8
MA-1	Polityka i procedury	**MA-1**	**MA-1**	**MA-1**
MA-2	Nadzór nad utrzymaniem	MA-2	MA-2	MA-2 (2)
MA-3	Narzędzia utrzymaniowe		MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Utrzymanie zdalne	MA-4	MA-4 (1)	MA-4 (1) **(3)**

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
MA-5	Personel utrzymaniowy	MA-5	MA-5	MA-5 (1)
MA-6	Terminowość przeprowadzania konserwacji		MA-6	MA-6
MA-7	Konserwacja w terenie	**MA-7**	**MA-7**	**MA-7**
MP-1	Polityka i procedury	**MP-1**	**MP-1**	**MP-1**
MP-2	Dostęp do nośników danych	MP-2	MP-2	MP-2
MP-3	Oznakowanie nośników danych		MP-3	MP-3
MP-4	Przechowywanie nośników danych		MP-4	MP-4
MP-5	Transport nośników danych		MP-5	MP-5
MP-6	Sanityzacja nośników danych	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Używanie nośników danych	MP-7	MP-7	MP-7
PE-1	Polityka i procedury	**PE-1**	**PE-1**	**PE-1**
PE-2	Zezwolenia na dostęp fizyczny	PE-2	PE-2	PE-2
PE-3	Kontrola dostępu fizycznego	**PE-3**	**PE-3**	**PE-3** (1)
PE-4	Kontrola dostępu do medium transmisyjnego		PE-4	PE-4
PE-5	Kontrola dostępu do urządzeń wejścia - wyjścia		PE-5	PE-5
PE-6	Monitorowanie dostępu fizycznego	PE-6	PE-6 (1) (4)	PE-6 (1) (4)
PE-8	Rejestracja dostępu gości	PE-8	PE-8	PE-8 (1)
PE-9	Wyposażenie energetyczne i okablowanie		PE-9	PE-9
PE-10	Wyłączenie awaryjne		**PE-10**	**PE-10**

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
PE-11	Zasilanie awaryjne		PE-11	PE-11 (1)
PE-12	Oświetlenie awaryjne	PE-12	PE-12	PE-12
PE-13	Ochrona przeciwpożarowa	**PE-13**	**PE-13** (1)	**PE-13** (1) (2)
PE-14	Zabezpieczenia środowiskowe	**PE-14**	**PE-14**	**PE-14**
PE-15	Ochrona przed zalaniem	**PE-15**	**PE-15**	**PE-15** (1)
PE-16	Dostawa i usuwanie	PE-16	PE-16	PE-16
PE-17	Zapasowe miejsce pracy		PE-17	PE-17
PE-18	Lokalizacja komponentów systemu			PE-18
PE-22	Znakowanie komponentów		**PE-22**	**PE-22**
PL-1	Polityka i procedury	**PL-1**	**PL-1**	**PL-1**
PL-2	Plany bezpieczeństwa systemu ii ochrony prywatności	**PL-2**	**PL-2**	**PL-2**
PL-4	Zasady postępowania	PL-4 (1)	PL-4 (1)	PL-4 (1)
PL-8	Architektury bezpieczeństwa i ochrony prywatności		PL-8	PL-8
PL-10	Wybór zabezpieczeń bazowych	PL-10	PL-10	PL-10
PL-11	Dostosowanie zabezpieczeń bazowych	PL-11	PL-11	PL-11
PM-1	Plan programu bezpieczeństwa informacji	PM-1		
PM-2	Role kierownicze programu bezpieczeństwa informacji	PM-2		
PM-3	Zasoby w zakresie bezpieczeństwa informacji i ochrony prywatności	PM-3		

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
PM-4	Plan działania i etapy wprowadzania zabezpieczeń	PM-4		
PM-5	Inwentaryzacja systemu	PM-5		
PM-6	Miary skuteczności	PM-6		
PM-7	Struktura organizacyjna	PM-7		
PM-8	Plan infrastruktury krytycznej	**PM-8**		
PM-9	Strategia zarządzania ryzykiem	PM-9		
PM-10	Proces autoryzacji	PM-10		
PM-11	Definicja misji i procesu biznesowego	PM-11		
PM-12	Zagrożenia wewnętrzne	PM-12		
PM-13	Personel bezpieczeństwa i ochrony prywatności	PM-13		
PM-14	Testowanie, szkolenia i monitorowanie	PM-14		
PM-15	Grupy i stowarzyszenia zajmujące się bezpieczeństwem i ochroną prywatności	**PM-15**		
PM-16	Ostrzeganie o zagrożeniach	**PM-16**		
PM-17	Ochrona nadzorowanych informacji jawnych przetwarzanych w systemach zewnętrznych	**PM-17**		
PM-18	Plan programu ochrony prywatności	PM-18		
PM-19	Role kierownicze programu ochrony prywatności	PM-19		

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
PM-20	Rozpowszechnianie informacji o programie ochrony prywatności	PM-20 (1)		
PM-21	Rejestrowanie ujawnień	PM-21		
PM-22	Zarządzanie jakością danych osobowych	PM-22		
PM-23	Organ zarządzania danymi	PM-23		
PM-24	Rada ds. integralności danych	PM-24		
PM-25	Minimalizacja danych osobowych wykorzystywanych w testach, szkoleniach i badaniach	PM-25		
PM-26	Zarządzanie skargami	PM-26		
PM-27	Sprawozdawczość w zakresie ochrony prywatności	PM-27		
PM-28	Opracowywanie ram ryzyka	PM-28		
PM-29	Role kierownicze programu zarządzania ryzykiem	PM-29		
PM-30	Strategia zarządzania ryzykiem w łańcuchu dostaw	PM-30 (1)		
PM-31	Strategia ciągłego monitorowania	PM-31		
PM-32	Przeznaczenie	PM-32		
PS-1	Polityka i procedury	**PS-1**	**PS-1**	**PS-1**
PS-2	Określanie ryzyka dla stanowiska pracy	**PS-2**	**PS-2**	**PS-2**
PS-3	Dobór personelu	PS-3	PS-3	PS-3
PS-4	Zakończenie zatrudnienia	PS-4	PS-4	PS-4 (2)
PS-5	Obsadzenie lub przeniesienie stanowiska	PS-5	PS-5	PS-5

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
PS-6	Umowy dostępu / współpracy	PS-6	PS-6	PS-6
PS-7	Bezpieczeństwo osobowe stron trzecich	PS-7	PS-7	PS-7
PS-8	Sankcje personalne	PS-8	PS-8	PS-8
PS-9	Opisy stanowisk pracy	PS-9	PS-9	PS-9
RA-1	Polityka i procedury	**RA-1**	**RA-1**	**RA-1**
RA-2	Kategoryzacja bezpieczeństwa	**RA-2**	**RA-2**	**RA-2**
RA-3	Szacowanie ryzyka	RA-3 (1)	RA-3 (1)	RA-3 (1)
RA-5	Monitorowanie i skanowanie podatności	**RA-5** (2) **(11)**	**RA-5** (2) (5) **(11)**	**RA-5** (2) **(4)** (5) **(11)**
RA-7	Reakcja na ryzyko	RA-7	RA-7	RA-7
RA-9	Analiza krytyczności		RA-9	RA-9
SA-1	Polityka i procedury	**SA-1**	**SA-1**	**SA-1**
SA-2	Przydział zasobów	SA-2	SA-2	SA-2
SA-3	Cykl życia systemu	SA-3	SA-3	SA-3
SA-4	Proces nabycia	**SA-4 (10)** (12)	**SA-4 (1) (2) (9) (10)** (12)	**SA-4 (1) (2)** (5) **(9) (10)** (12)
SA-5	Dokumentacja systemu	SA-5	SA-5	SA-5
SA-8	Zasady inżynierii bezpieczeństwa i ochrony prywatności	SA-8	SA-8	SA-8
SA-9	Usługi systemu zewnętrznego	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Zarządzanie konfiguracją dewelopera		**SA-10**	**SA-10**
SA-11	Testowanie i ocena przez dewelopera		SA-11	SA-11

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
SA-15	Proces rozwoju, standardy i narzędzia		SA-15 (3)	SA-15 (3)
SA-16	Szkolenia prowadzone przez dewelopera			SA-16
SA-17	Architektura oraz projekt bezpieczeństwa i ochrony prywatności dewelopera			SA-17
SA-21	Dobór deweloperów			SA-21
SA-22	Komponenty systemu bez wsparcia	**SA-22**	**SA-22**	**SA-22**
SC-1	Polityka i procedury	**SC-1**	**SC-1**	**SC-1**
SC-2	Rozdzielenie funkcjonalności systemu i użytkownika		**SC-2**	**SC-2**
SC-3	Izolacja funkcji bezpieczeństwa			**SC-3**
SC-4	Informacje na współdzielonych zasobach systemowych		**SC-4**	**SC-4**
SC-5	Ochrona przed blokadą usług (DoS)	**SC-5**	**SC-5**	**SC-5**
SC-7	Ochrona połączeń brzegowych	SC-7 **(28) (29)**	SC-7 (3) (4) (5) (7) (8) **(18) (28) (29)**	SC-7 (3) (4) (5) (7) (8) **(18)** (21) **(28) (29)**
SC-8	Poufność i integralność transmisji		SC-8 **(1)**	SC-8 **(1)**
SC-10	Zakończenie połączenia sieciowego		~~SC-11~~	~~SC-11~~
SC-12	Generowanie i zarządzanie kluczami kryptograficznymi	SC-12	SC-12	SC-12 (1)
SC-13	Ochrona kryptograficzna	SC-13	SC-13	SC-13

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
SC-15	Współpracujące urządzenia i aplikacje	SC-15	SC-15	SC-15
SC-17	Certyfikaty infrastruktury klucza publicznego		SC-17	SC-17
SC-18	Kod mobilny		SC-18	SC-18
SC-20	Bezpieczeństwo nazw domen / adresów IP (autentyczność pochodzenia)	**SC-20**	**SC-20**	**SC-20**
SC-21	Bezpieczeństwo nazw domen / usługa ustalania adresu IP	**SC-21**	**SC-21**	**SC-21**
SC-22	Architektura nazw domen / adresów IP / zamawianie usługi DNS	**SC-22**	**SC-22**	**SC-22**
SC-23	Autentyczność sesji		**SC-23**	**SC-23**
SC-24	Przejście do określonego stanu systemu po błędzie		**SC-24**	**SC-24**
SC-28	Ochrona danych w składowaniu / Kopie konfiguracji systemu		**SC-28** (1)	**SC-28** (1)
SC-39	Izolacja procesów	**SC-39**	**SC-39**	**SC-39**
SC-41	Dostęp do portów i urządzeń wejścia / wyjścia	SC-41	SC-41	SC-41
SC-45	Synchronizacja czasu systemowego	**SC-45**	**SC-45**	**SC-45**
SC-47	Alternatywne ścieżki komunikacyjne			**SC-47**
SI-1	Polityka i procedury	**SI-1**	**SI-1**	**SI-1**
SI-2	Usuwanie usterek	**SI-2**	**SI-2** (2)	**SI-2** (2)
SI-3	Zabezpieczenie przed złośliwym kodem	**SI-3**	**SI-3**	**SI-3**

Tłumaczenie

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Niski**	**Niski**
SI-4	Monitorowanie systemu	**SI-4**	**SI-4 (2)** (4) **(5)**	**SI-4 (2)** (4) **(5)** (10) (12) (14) (20) (22)
SI-5	Alerty bezpieczeństwa, porady i dyrektywy	**SI-5**	**SI-5**	**SI-5** (1)
SI-6	Weryfikacja funkcji bezpieczeństwa i ochrony prywatności			**SI-6**
SI-7	Aplikacje, oprogramowanie układowe i integralność informacji		**SI-7 (1) (7)**	**SI-7 (1) (2) (5) (7) (15)**
SI-8	Ochrona przed spamem		**SI-8** ~~(2)~~	**SI-8** ~~(2)~~
SI-10	Weryfikacja wprowadzanych informacji		SI-10	SI-10
SI-11	Obsługa błędów		SI-11	SI-11
SI-12	Zarządzanie i retencja danych	SI-12	SI-12	SI-12
SI-13	Przewidywanie awarii			SI-13
SI-16	Ochrona pamięci		SI-16	SI-16
SI-17	Procedury testowania awaryjnego	**SI-17**	**SI-17**	**SI-17**
SR-1	Polityka i procedury	**SR-1**	**SR-1**	**SR-1**
SR-2	Plan zarządzania ryzykiem w łańcuchu dostaw	SR-2 (1)	SR-2 (1)	SR-2 (1)
SR-3	Zabezpieczenia i procesy w łańcuchu dostaw	SR-3	SR-3	SR-3
SR-5	Strategie, narzędzia i metody nabycia	SR-5	SR-5 **(1)**	SR-5 **(1)**
SR-6	Oceny i przeglądy dostawców		SR-6	SR-6
SR-8	Umowy dotyczące powiadomień	SR-8	SR-8	SR-8

Tłumaczenie

Numer zabezpieczenia	Nazwa zabezpieczenia Nazwa zabezpieczenia rozszerzonego	Zabezpieczenie bazowe Poziom wpływu na system informacyjny		
		Niski	Niski	Niski
SR-9	Odporność na manipulacje i wykrywanie sabotażu			SR-9 (1)
SR-10	Kontrola systemów / komponentów	SR-10	SR-10	SR-10
SR-11	Autentyczność komponentów	SR-11 (1) (2)	SR-11 (1) (2)	SR-11 (1) (2)
SR-12	Usuwanie komponentów	SR-12	SR-12	SR-12

F.4 INFORMACJE DOTYCZĄCE DOSTOSOWYWANIA NAKŁADKI

Nakładka dotycząca systemów OT zawarta w niniejszej publikacji opiera się na zabezpieczeniach bazowych opisanych w dokumencie NSC 800-53B [NSC 800-53B], uwzględniając wyjątkowe cechy oraz wymagania systemów OT, takie jak potrzeba zapewnienia ciągłej dostępności, bezpieczeństwa i odpowiedniego środowiska działania. Co więcej, systemy OT są zróżnicowane pod względem architektury i doboru rozwiązań technologicznych. Zabezpieczenia bazowe zawarte w dokumencie NSC 800-53B zostały dostosowane w celu uwzględnienia tych wymagań, dodano także zabezpieczenia istotne z punktu widzenia środowisk OT. Organizacje mogą wykorzystać tę nakładkę jako punkt wyjścia w celu dalszego dostosowywania uwzględnionych w niej zabezpieczeń do swoich potrzeb i zróżnicowanych systemów.

W procesie dostosowywania środków bezpieczeństwa z myślą o zaspokojeniu wewnętrznych wymagań dotyczących bezpieczeństwa, a także uwzględnieniu ograniczeń (technologicznych, wynikających z działalności lub ze względów środowiskowych) może pojawić się potrzeba wyboru zabezpieczeń kompensacyjnych. Zastosowanie takich zabezpieczeń w środowisku OT może być wymagane w sytuacjach, w których system OT nie jest w stanie obsługiwać wybranych środków bezpieczeństwa lub zabezpieczeń rozszerzonych, a także w sytuacji, gdy zdaniem organizacji wdrażanie środków bezpieczeństwa lub zabezpieczeń rozszerzonych nie jest wskazane ze względu na potencjalny niekorzystny wpływ na wydajność,

bezpieczeństwo lub niezawodność systemu. Zabezpieczenia kompensacyjne stanowią alternatywy dla danego środka bezpieczeństwa lub zabezpieczenia rozszerzonego, które zapewniają równoważną lub porównywalną ochronę. Na przykład, jeśli środki bezpieczeństwa lub zabezpieczenia rozszerzone wymagają zastosowania zautomatyzowanych mechanizmów, które nie są dostępne lub możliwe do wdrożenia w środowiskach OT, zabezpieczenia kompensacyjne wdrożone w oparciu o niezautomatyzowane mechanizmy lub procedury mogą być dopuszczalne, jeśli spełniają założenie danego zabezpieczenia.

Zabezpieczenia kompensacyjne wdrożone zgodnie z założeniami środka bezpieczeństwa PL-11 opisanego w dokumencie NSC 800-53 nie są uważane za wyjątki lub odstępstwa od zabezpieczeń bazowych. Należy traktować je jako alternatywne zabezpieczenia i środki przeciwdziałania wykorzystywane w kontekście systemów i środowiska OT realizujące cele zabezpieczeń bazowych, które nie zostały wdrożone. Więcej informacji znajduje się w podrozdziale 3.3 dokumentu NSC 800-37 – „Dostosowywanie zabezpieczeń” [NSC 800-37].

Korzystanie z zabezpieczeń kompensacyjnych może również obejmować zabezpieczenia rozszerzone, które stanowią uzupełnienie względem poziomu bazowego. Wdrażanie zabezpieczeń kompensacyjnych zazwyczaj wiąże się z koniecznością znalezienia kompromisu między zwiększonym ryzykiem i ograniczeniem funkcjonalności. Każde zastosowanie zabezpieczeń kompensacyjnych powinno wiązać się z podjęciem decyzji dotyczącej poziomu dopuszczalnego ryzyka szczątkowego oraz zakresu ograniczenia funkcjonalności w oparciu o ryzyko. Dodatkowo, gdy stosowane są zabezpieczenia kompensacyjne, organizacje powinny udokumentować uzasadnienie ich zastosowania, uwzględniające następujące informacje:

- Dlaczego nie było możliwe wdrożenie zabezpieczenia bazowego?
- W jaki sposób zabezpieczenia kompensacyjne zapewniają równoważny zakres zabezpieczenia systemów OT?
- Poziom akceptowanego ryzyka szczątkowego wynikającego ze stosowania zabezpieczeń kompensacyjnych zamiast zabezpieczeń bazowych poziomu.

Decyzje organizacji dotyczące stosowania zabezpieczeń kompensacyjnych winne być udokumentowane w planie bezpieczeństwa dotyczącym systemów OT.

Środki bezpieczeństwa obejmujące przypisania (na przykład *przypisanie warunków określonych przez organizację lub wybranych zdarzeń*) mogą zostać wyłączone z zabezpieczeń bazowych. Takie działanie jest równoznaczne z przypisaniem wartości „brak". Przypisanie może przyjmować różne wartości dla różnych bazowych poziomów wpływu.

F.5 PROTOKOŁY KOMUNIKACYJNE WYKORZYSTYWANE W SYSTEMACH OT

Wyjątkowy charakter sieci stosowanych w ramach środowisk i systemów OT może wymagać wprowadzenia zmian w przypadku stosowania wybranych zabezpieczeń. Wiele środków bezpieczeństwa opisanych w dokumencie NSC 800-53 [NSC 800-53] odnoszących się do łączności, urządzeń i interfejsów, domyślnie zakłada możliwość zastosowania routingu lub łączności sieciowej pomiędzy segmentami lub strefami sieci. Niektóre urządzenia lub systemy wykorzystywane w środowiskach OT mogą być skonfigurowane lub zaprojektowane w sposób, który może stanowić wyjątek od tego założenia. W rezultacie środki bezpieczeństwa dotyczące urządzeń wyposażonych w mechanizmy łączności oparte na standardach i protokołach nieadresowalnych sieciowo, zwykle wymagają dostosowania. Interfejs RS-232 (szeregowy) jest przykładem połączenia, które jest nieadresowalne sieciowo i nieroutowalne, powszechnie stosowanego w systemach OT.

F.6 DEFINICJE

Terminy wykorzystywane w niniejszej nakładce zostały opisane w glosariuszu CSRC.

F.7 SZCZEGÓŁOWE SPECYFIKACJE ZABEZPIECZEŃ OPISANYCH W NAKŁADCE

Treść niniejszej nakładki została opracowana na podstawie dokumentu NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji* [NSC 800-53], który stanowi katalog środków bezpieczeństwa i prywatności, a także dokumentu NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji*. [NSC 800-53B] Poszczególne środki bezpieczeństwa są możliwe do

dostosowania oraz wdrożenia w ramach procesu obejmującego całą organizację, który zarządza ryzykiem związanym z bezpieczeństwem i prywatnością. Opisane środki bezpieczeństwa obejmują katalog zróżnicowanych wymogów w zakresie bezpieczeństwa i prywatności dotyczących organizacji rządowych oraz operatorów infrastruktury krytycznej, opartych na przepisach obowiązującego prawa, rozporządzeniach, dyrektywach, normach, wytycznych, a także potrzebach misji oraz procesów biznesowych. Dokumenty te opisują również proces opracowywania zestawów środków bezpieczeństwa stosowanych w szczególnych przypadkach – nakładek, które są dostosowane do określonych rodzajów misji i procesów biznesowych, technologii lub środowisk operacyjnych. Zabezpieczenia wymienione na łamach tych dokumentów odnoszą się do kwestii bezpieczeństwa zarówno z punktu widzenia funkcjonalności (możliwości środków bezpieczeństwa i ochrony prywatności) oraz wiarygodności (zaufania względem możliwości wdrożonych zabezpieczeń). Takie podejście pozwala na zapewnienie, że poszczególne komponenty oraz systemy składające się z tych komponentów opierają się na kompleksowych założeniach projektowych oraz zasadach bezpieczeństwa, dzięki czemu są godne zaufania.

Przygotowując się do wyboru i dopasowania odpowiednich środków bezpieczeństwa dla systemów organizacji i ich odpowiednich środowisk eksploatacji, organizacje muszą określić krytyczność i wrażliwość informacji, które mają być przetwarzane, przechowywane lub przesyłane za pośrednictwem tych systemów. Proces ten określamy mianem kategoryzacji bezpieczeństwa. Na podstawie dokumentu NSC 199 [NSC 199] organizacje rządowe mogą ustalać kategorie bezpieczeństwa zarówno dla informacji, jak i systemów informacyjnych. Inne dokumenty, w tym wytyczne opracowane przez ISA i CNSS, również zawierają wytyczne dotyczące określania niskich, umiarkowanych i wysokich poziomów wpływu na bezpieczeństwo. Kategorie te opierają się na potencjalnym wpływie wystąpienia pewnych zdarzeń, które zagrażają informacjom i systemom wykorzystywanym przez organizację w celu realizacji określonych misji, takich jak: ochrona zasobów, realizacja zobowiązań wynikających z praw i ustaw, bieżąca działalność oraz ochrona bezpieczeństwa, zdrowia i życia osób, na samą organizację lub ludzi (tj. pracowników bądź przedstawicieli społeczeństwa). Kategorie bezpieczeństwa mają być zestawiane z informacjami o podatnościach i zagrożeniach w celu oceny ryzyka dla organizacji.

Niniejsza nakładka obejmuje omówienie zabezpieczeń i zabezpieczeń rozszerzonych w kontekście systemów OT w przypadku, gdy autorzy zalecają ich stosowanie w systemach i organizacjach, których zadaniem jest ochrona poufności, integralności i dostępności jej danych oraz w celu spełnienia określonych wymogów dotyczących bezpieczeństwa. Wraz z omówieniami zabezpieczeń w kontekście systemów OT należy zapoznać się także z omówieniami poszczególnych środków bezpieczeństwa i zabezpieczeń rozszerzonych zawartymi w rozdziale 3 dokumentu NSC 800-53 [NSC 800-53]. Niniejsza nakładka zawiera wytyczne w zakresie dostosowania zabezpieczeń bazowych, a jej specyfikacja może być bardziej rygorystyczna lub mniej rygorystyczna niż specyfikacja zabezpieczeń bazowych zawartych w pierwotnym dokumencie. Wytyczne zawarte w nakładce stanowią wysokopoziomowe opisy, które mogą zostać zastosowane w kontekście wszystkich środowisk OT i zróżnicowanych systemów. Mogą w związku z tym stanowić podstawę do opracowania bardziej szczegółowych nakładek. Stosowne scenariusze zastosowania dotyczące określonych systemów w określonych środowiskach eksploatacji mogą być publikowane oddzielnie (np. w publikacjach z serii NIST IR).

Rysunek 22 zawiera przykład formatu i treści specyfikacji zabezpieczenia zawartego w niniejszej nakładce na przykładzie zabezpieczenia AU-4.

❶ Numer i nazwa zabezpieczenia

❷ Kolumna zawierająca numer środka bezpieczeństwa oraz zabezpieczenia rozszerzonego

❸ Kolumna zawierająca nazwę środka bezpieczeństwa oraz zabezpieczenia rozszerzonego:

❹ Kolumny zawierające poziomy wpływu zabezpieczeń bazowych na bezpieczeństwo. Jeśli poziom wpływu zabezpieczeń bazowych został zmieniony, w tym miejscu pojawi się informacja ZMIENIONE.

❺ Wiersz zawierający środek bezpieczeństwa lub zabezpieczenie rozszerzone

❻ Kolumny zawierające NISKI, UMIARKOWANY oraz WYSOKI poziom wpływu zabezpieczeń bazowych

❼ Informacja „Wybrano” oznacza, że dane zabezpieczenie zostało wybrane z dokumentu NSC 800-53. Informacja „Dodano” oznacza, że dane zabezpieczenie zostało dodane do poziomów bazowych w nakładce OT. Pusta komórka oznacza, że dane zabezpieczenie nie zostało wybrane. Informacja „~~Usunięto~~” oznacza, że dane zabezpieczenie zostało usunięte z poziomu bazowego.

❽ Omówienie zabezpieczenia w kontekście systemów OT: W przypadku braku omówienia, w tym miejscu znajduje się stosowna informacja.

❾ Omówienie zabezpieczenia rozszerzonego w kontekście systemów OT: W przypadku braku omówienia, w tym miejscu znajduje się stosowna informacja.

❿ Uzasadnienie uwzględnienia lub usunięcia środka bezpieczeństwa lub zabezpieczenia rozszerzonego w poziomie bazowym.

❶ AC-3 Egzekwowanie uprawnień dostępu

❷ **Numer zabezpieczenia**	❸ **Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	❹ **Zabezpieczenie bazowe** ❻ **Poziom wpływu na system informacyjny**		
		Niski	**Umiarkowany**	**Wysoki**
❺ **AC-3**	**Egzekwowanie uprawnień dostępu**	**Wybrano**	**Wybrano**	❼ **Wybrano**
AC-3 (11)	*EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI*			**Dodano**

❽ Omówienie zabezpieczenia w kontekście systemów OT: Organizacja musi zapewnić, że mechanizmy egzekwowania uprawnień dostępu nie wpłyną negatywnie na wydajność i działanie systemów OT. Przykładowe zabezpieczenia kompensacyjne obejmują enkapsulację. Należy określić precyzyjne zasady kontroli dostępu logicznego do nieadresowalnych i nieroutowalnych zasobów systemowych oraz związanych z nimi informacji i danych. Mechanizmy kontroli dostępu obejmują sprzęt, oprogramowanie układowe i oprogramowanie, które odpowiadają za sterowanie urządzeniem lub uzyskują dostęp do urządzenia, takie jak sterowniki urządzeń i kontrolery łączności. Kontrola dostępu fizycznego może stanowić zabezpieczenie kompensacyjne stosowane w miejscu kontroli dostępu logicznego. W przypadku jego zastosowania może jednak nie być możliwe osiągnięcie odpowiedniej szczegółowości, zwłaszcza gdy użytkownicy muszą mieć dostęp do różnych funkcji.

❾ Zabezpieczenie rozszerzone: (11) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna określić oraz ograniczyć dostęp do informacji, który może wpływać na środowisko OT. Musi także mieć na uwadze rodzaje informacji, które mogą być wrażliwe, zastrzeżone, zawierają tajemnice handlowe lub mogą mieć wpływ na bezpieczeństwo.

❿ Uzasadnienie uwzględnienia zabezpieczenia AC-3 (11) do WYSOKIEGO poziomu wpływu bazowego: Utrata dostępności, integralności i poufności niektórych rodzajów informacji, przetwarzanych w systemie OT o wysokim poziomie wpływu może spowodować poważne lub katastrofalne skutki dla działalności organizacji, a także jej zasobów oraz pracowników, obejmujące poważne ograniczenie lub utratę zdolności do realizacji swoich misji, utratę zasobów organizacyjnych, a także śmierć lub urazy zagrażające życiu osób.

Rysunek 22. Szczegółowe specyfikacje zabezpieczeń opisanych w nakładce

F.7.1. KONTROLA DOSTĘPU – AC

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Kontrola dostępu”

Przed wdrożeniem zabezpieczeń należących do kategorii AC – Kontrola dostępu organizacja powinna wziąć pod uwagę, że ich stosowanie wiąże się z koniecznością znalezienia kompromisów pomiędzy poziomem bezpieczeństwa i prywatności, a możliwymi opóźnieniami, osiągami, wydajnością i niezawodnością systemu. Organizacja powinna na przykład przeanalizować, czy opóźnienia wynikające z zastosowania mechanizmów zapewniania poufności i integralności opartych na metodach kryptograficznych mogą mieć negatywny wpływ na wydajność systemów OT.

W sytuacjach, gdy systemy OT nie obsługują rozwiązań wymaganych przez dane zabezpieczenie, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

AC-1 – KONTROLA DOSTĘPU POLITYKA I PROCEDURY

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Umiarkowany**	**Wysoki**
AC-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT. Dostawcy oraz osoby przeprowadzające prace konserwacyjne mogą uzyskiwać dostęp do systemów OT w wielu lokalizacjach danego obiektu oraz na dużym obszarze geograficznym. Dostęp może być możliwy w miejscach, które nie są widoczne, takich jak siłownie czy maszynownie, podwieszane sufity, stacje terenowe, sterownie oraz przepompownie.

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Umiarkowany**	**Wysoki**
AC-2	**Zarządzanie kontami**	**Wybrano**	**Wybrano**	**Wybrano**
AC-2 (1)	*ZARZĄDZANIE KONTAMI | AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU*		Wybrano	Wybrano
AC-2 (2)	*ZARZĄDZANIE KONTAMI | AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM I AWARYJNYM*		**Wybrano**	**Wybrano**
AC-2 (3)	*ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT*		Wybrano	Wybrano
AC-2 (4)	*ZARZĄDZANIE KONTAMI | AUTOMATYCZNE DZIAŁANIA AUDYTOWE*		Wybrano	Wybrano
AC-2 (5)	*ZARZĄDZANIE KONTAMI | WYLOGOWANIE PRZEZ UŻYTKOWNIKA PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI*		**Wybrano**	**Wybrano**
AC-2 (11)	*ZARZĄDZANIE KONTAMI | WARUNKI UŻYTKOWANIA*			Wybrano
AC-2 (12)	*ZARZĄDZANIE KONTAMI | MONITOROWANIE KONTA POD WZGLĘDEM NIETYPOWYCH ZASTOSOWAŃ*			Wybrano
AC-2 (13)	*ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA*		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: W kontekście systemów OT środki zapewniające bezpieczeństwo fizyczne, bezpieczeństwo pracowników, wykrywanie włamań lub działania audytowe mogą realizować założenie tego środka bezpieczeństwa.

Zabezpieczenie rozszerzone: (1) (3) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (2) Omówienie zabezpieczenia w kontekście systemów OT: Niniejsze zabezpieczenie nie jest stosowane, gdy systemy OT (na przykład

urządzenia terenowe) nie obsługują kont tymczasowych lub awaryjnych. Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur zarządzania.

Zabezpieczenie rozszerzone: (5) Omówienie zabezpieczenia w kontekście systemów OT: W przypadku tego zabezpieczenia rozszerzonego należy określić w zasadach (politykach) czas wylogowania użytkowników w przypadku nieaktywności. Niniejsze zabezpieczenie rozszerzone nie obejmuje automatycznego egzekwowania zasad. Na organizacji spoczywa odpowiedzialność za określenie, czy zabezpieczenie rozszerzone jest stosowne w przypadku danej misji lub funkcji systemu OT, a także ustalenie czasu oraz scenariuszy stosowania. W przypadku braku stosownych ram czasowych lub scenariuszy stosowania, parametry ustanowione przez organizację powinny odzwierciedlać ten stan.

Zabezpieczenie rozszerzone: (11) (12) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (13) Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny zadbać o koordynację zespołów odpowiedzialnych za systemy OT, działu kadr, pracowników odpowiedzialnych za systemy IT oraz pracowników działu ochrony fizycznej w celu sprawnego przeprowadzenia procesu zwolnienia osób wysokiego ryzyka.

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Numer zabezpieczenia	**Nazwa zabezpieczenia** Nazwa zabezpieczenia rozszerzonego	**Zabezpieczenie bazowe** **Poziom wpływu na system informacyjny**		
		Niski	**Umiarkowany**	**Wysoki**
AC-3	**Egzekwowanie uprawnień dostępu**	**Wybrano**	**Wybrano**	**Wybrano**
AC-3 (11)	*EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OGRANICZENIE DOSTĘPU DO OKREŚLONYCH RODZAJÓW INFORMACJI*			**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja musi zapewnić, że mechanizmy egzekwowania uprawnień dostępu nie wpłyną negatywnie na wydajność i działanie systemów OT. Przykładowe zabezpieczenia kompensacyjne

obejmują enkapsulację. Należy określić precyzyjne zasady kontroli dostępu logicznego do nieadresowalnych i nieroutowalnych zasobów systemowych oraz związanych z nimi informacji i danych. Mechanizmy kontroli dostępu obejmują sprzęt, oprogramowanie układowe i oprogramowanie, które odpowiadają za sterowanie urządzeniem lub uzyskują dostęp do urządzenia, takie jak sterowniki urządzeń i sterowniki łączności. Kontrola dostępu fizycznego może stanowić zabezpieczenie kompensacyjne stosowane w miejscu kontroli dostępu logicznego. W przypadku jego zastosowania może jednak nie być możliwe osiągnięcie odpowiedniej szczegółowości, zwłaszcza gdy użytkownicy muszą mieć dostęp do różnych funkcji.

Zabezpieczenie rozszerzone: (11) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna określić oraz ograniczyć dostęp do informacji, który może wpływać na środowisko OT. Musi także mieć na uwadze rodzaje informacji, które mogą być wrażliwe, zastrzeżone, zawierają tajemnice handlowe lub mogą mieć wpływ na bezpieczeństwo.

Uzasadnienie uwzględnienia zabezpieczenia AC-3 (11) do WYSOKIEGO poziomu wpływu: Utrata dostępności, integralności i poufności niektórych rodzajów informacji, przetwarzanych w systemie OT o wysokim poziomie wpływu może spowodować poważne lub katastrofalne skutki dla działalności organizacji, a także jej zasobów oraz pracowników, obejmujące poważne ograniczenie lub utratę zdolności do realizacji swoich misji, utratę zasobów organizacyjnych, a także śmierć lub urazy zagrażające życiu osób.

AC-4 EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-4	**Egzekwowanie zasad przepływu informacji**		**Wybrano**	**Wybrano**
AC-4 (4)	*EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | KONTROLA PRZEPŁYWU ZASZYFROWANYCH INFORMACJI*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady przepływu informacji mogą być egzekwowane przy pomocy zestawu logicznych i fizycznych technik

ograniczania przepływu. Egzekwowanie zasad przepływu informacji jest także możliwe w związku z kontrolą treści wiadomości. Ruch przychodzący lub wychodzący związany z protokołami stosowanymi przez przemysłowe systemy OT może być ograniczony przy pomocy reguł egzekwowanych przez urządzenie sieciowe umieszczone pomiędzy sieciami OT i IT. W przypadku komunikacji nieroutowalnej, takiej jak połączenia szeregowe, urządzenia mogą być skonfigurowane w taki sposób, aby ograniczać polecenia związane z określonymi znacznikami urządzenia OT. Egzekwowanie zasad przepływu informacji może być usprawniane dzięki oznaczaniu fizycznych złączy kolorystycznie lub etykietami w celu ułatwienia konfiguracji sieci. Należy fizycznie odłączyć od sieci urządzenia, które nie muszą łączyć się z innymi urządzeniami lub sieciami.

Zabezpieczenie rozszerzone: (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

AC-5 ROZDZIAŁ OBOWIĄZKÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-5	**Rozdział obowiązków**		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonego bezpieczeństwa pracowników oraz przeprowadzanie audytów. Organizacja powinna przeanalizować stosowność pełnienia wielu krytycznych funkcji przez jedną osobę.

AC-6 ZASADA MINIMALNYCH UPRAWNIEŃ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-6	**Zasada minimalnych uprawnień**		**Wybrano**	**Wybrano**
AC-6 (1)	*ZASADA MINIMALNYCH UPRAWNIEŃ | UPOWAŻNIONY DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA*		**Wybrano**	**Wybrano**

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-6 (2)	*ZASADA MINIMALNYCH UPRAWNIEŃ | NIEUPRZYWILEJOWANY DOSTĘP DLA FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM*		**Wybrano**	**Wybrano**
AC-6 (3)	*ZASADA MINIMALNYCH UPRAWNIEŃ | DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ*			**Wybrano**
AC-6 (5)	*ZASADA MINIMALNYCH UPRAWNIEŃ | UPRZYWILEJOWANE KONTA*		**Wybrano**	**Wybrano**
AC-6 (7)	*ZASADA MINIMALNYCH UPRAWNIEŃ | PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA*		Wybrano	Wybrano
AC-6 (9)	*ZASADA MINIMALNYCH UPRAWNIEŃ | KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI*		**Wybrano**	**Wybrano**
AC-6 (10)	*ZASADA MINIMALNYCH UPRAWNIEŃ | ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI*		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie zwiększonego bezpieczeństwa pracowników oraz przeprowadzanie audytów. Organizacja powinna przeanalizować stosowność posiadania wielu krytycznych uprawnień przez jedną osobę. Modele uprawnień stosowane w systemach mogą być dostosowane z myślą o zapewnianiu integralności i dostępności, na przykład w taki sposób, by niższy poziom uprawnień obejmował wyłącznie możliwość odczytu danych, z kolei wyższy poziom uprawnień może zapewniać dostęp do funkcji zapisu).

Zabezpieczenie rozszerzone: (1) (2) (3) (5) (9) Omówienie zabezpieczenia w kontekście systemów OT: Gdy komponenty systemów OT (takie jak na przykład sterowniki PLC) nie obsługują funkcji rejestrowania uprzywilejowanych funkcji, można użyć innych komponentów systemu w granicach autoryzacji (np. stacji roboczych lub środków monitorowania dostępu fizycznego).

Zabezpieczenie rozszerzone: (7) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (10) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują dokładniejsze audytowanie.

AC-7 NIEUDANE PRÓBY LOGOWANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-7	Nieudane próby logowania	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Wiele systemów OT działa w trybie ciągłym, a operatorzy pozostają zalogowani do systemu przez cały czas. W takich przypadkach można zastosować funkcję wymuszania ponownego logowania. Przykładowe zabezpieczenia kompensacyjne obejmują rejestrowanie lub zapisywanie wszystkich nieudanych prób logowania i powiadamianie pracowników odpowiedzialnych za bezpieczeństwo systemów OT za pomocą alarmów lub innych rozwiązań, gdy przekroczona zostanie określona przez organizację liczba kolejnych nieudanych prób logowania. Limity nieudanych prób logowania powinny być egzekwowane w przypadku kont (np. konta administratora) lub systemów (np. stacji roboczych), które nie są wymagane w celu zapewnienia nieprzerwanego działania systemu.

AC-8 POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-8	Powiadomienie o zasadach użycia systemu	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: W przypadku wielu systemów OT wymagane jest nieprzerwane działanie, ponadto systemy OT mogą nie obsługiwać funkcji powiadomień o zasadach użycia systemu lub nie są w stanie ich skutecznie przekazywać. Przykładowe zabezpieczenia kompensacyjne obejmują umieszczanie fizycznych powiadomień w miejscach, w których wykorzystywane są systemy OT lub prowadzenie cyklicznych szkoleń dotyczących korzystania z systemów przed uzyskaniem zezwolenia na dostęp do systemu.

AC-10 KONTROLA LICZBY JEDNOCZESNYCH SESJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-10	**Kontrola liczby jednoczesnych sesji**			**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Liczba, typ kont oraz uprawnienia jednoczesnych sesji powinny uwzględniać role i obowiązki poszczególnych osób używających systemu. Przykładowe zabezpieczenia kompensacyjne obejmują szczegółowe audytowanie.

AC-11 BLOKADA URZĄDZENIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-11	**Blokada urządzenia**		**Wybrano**	**Wybrano**
AC-11 (1)	*BLOKADA URZĄDZENIA | WYGASZACZ EKRANU*		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Niniejsze zabezpieczenie dotyczy środowisk, w których pracownicy znajdują się w pobliżu wyświetlaczy systemu. Może zostać dostosowane, gdy systemy nie posiadają wyświetlaczy, działają w obiekcie, w którym są egzekwowane zasady kontroli dostępu, znajdują się w zamkniętej obudowie oraz w sytuacjach, gdy wymagana jest natychmiastowa reakcja operatora w sytuacjach awaryjnych. Przykładowe zabezpieczenia kompensacyjne obejmują umieszczenie wyświetlacza w miejscu objętym kontrolą dostępu fizycznego, do którego dostęp mają wyłącznie osoby posiadające wymagane uprawnienia, dla których wyświetlane informacje stanowią wiedzę konieczną.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: W celu uniemożliwienia dostępu do wyświetlacza lub ochronie systemu przed próbą podłączenia wyświetlacza można zastosować zabezpieczenia fizyczne. W przypadkach, gdy nie jest możliwe ukrycie wyświetlanych informacji, należy zastosować niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa.

AC-12 ZAKOŃCZENIE SESJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-12	**Zakończenie sesji**		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują dokładniejsze audytowanie bądź ograniczenie uprawnień zdalnego dostępu do najważniejszych pracowników.

AC-14 DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-14	**Działania dozwolone bez identyfikacji lub uwierzytelnienia**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AC-17 DOSTĘP ZDALNY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-17	**Zdalny dostęp**	**Wybrano**	**Wybrano**	**Wybrano**
AC-17 (1)	*DOSTEP ZDALNY | AUTOMATYCZNE MONITOROWANIE I KONTROLA*		**Wybrano**	**Wybrano**
AC-17 (2)	*DOSTEP ZDALNY | OCHRONA POUFNOŚCI I INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA*		**Wybrano**	**Wybrano**
AC-17 (3)	*DOSTEP ZDALNY | ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU*		**Wybrano**	**Wybrano**
AC-17 (4)	*DOSTEP ZDALNY | POLECENIA UPRZYWILEJOWANE I DOSTĘP*		Wybrano	Wybrano
AC-17 (9)	*DOSTEP ZDALNY | ODŁĄCZENIE LUB WYŁĄCZENIE DOSTĘPU*	**Dodano**	**Dodano**	**Dodano**
AC-17 (10)	*DOSTEP ZDALNY | UWIERZYTELNIANIE ZDALNYCH POLECEŃ*		Dodano	Dodano

Tłumaczenie

Omówienie zabezpieczenia w kontekście systemów OT: W przypadkach, gdy nie jest możliwe wykorzystanie wszystkich lub wybranych elementów środka zabezpieczeń w danym systemie OT, należy zastosować inne mechanizmy lub procedury jako zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur. Zabezpieczenia kompensacyjne mogą obejmować ograniczenie możliwości uzyskania dostępu zdalnego do określonego przedziału czasowego lub wykonanie połączenia z miejsca, w którym działa system OT do uwierzytelnionego podmiotu zdalnego.

Zabezpieczenie rozszerzone: (2) Omówienie zabezpieczenia w kontekście systemów OT: Należy zastosować rozwiązania oparte na szyfrowaniu w celu zapewnienia poufności i integralności sesji zdalnego dostępu. Choć wiele urządzeń wykorzystywanych w systemach OT nie obsługuje nowoczesnych standardów szyfrowania, takie funkcje mogą realizować dodatkowe urządzenia (np. bramki VPN). Nie należy mylić tego zabezpieczenia ze środkiem bezpieczeństwa SC-8 – Poufność i integralność transmisji, który odnosi się do wymagań dotyczących poufności i integralności wszelkiej komunikacji, w tym łączności między urządzeniami OT.

Zabezpieczenie rozszerzone: (3) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują ręczne uwierzytelnianie podmiotu łączącego się z systemem w przypadku każdego połączenia.

Zabezpieczenie rozszerzone: (4) (10) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (9) Omówienie zabezpieczenia w kontekście systemów OT: Wdrożenie funkcji rozłączania sesji zdalnego dostępu nie powinno wpływać na działanie systemu OT. Pracownicy odpowiedzialni za systemy OT powinni zostać przeszkoleni w zakresie korzystania z funkcji rozłączenia sesji zdalnego dostępu.

Uzasadnienie uwzględnienia zabezpieczenia AC-17 (9) do NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Ze względu na popularyzację funkcji dostępu zdalnego w coraz większej liczbie systemów OT,

możliwość odłączenia lub wyłączenia zdalnego dostępu ma kluczowe znaczenie dla zarządzania ryzykiem i może być wymagana do zapewnienia bezpieczeństwa oraz niezawodności ich działania.

Uzasadnienie uwzględnienia zabezpieczenia AC-17 (10) do UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Możliwość uwierzytelniania zdalnych poleceń jest kluczowa dla zapobiegania wykonywania nieautoryzowanych poleceń, których wykonanie może prowadzić do wystąpienia zdarzeń skutkujących obrażeniami lub śmiercią osób, zniszczeniem mienia, uszkodzeniem cennych zasobów, uniemożliwieniem realizacji misji lub funkcji biznesowych, a także naruszeniem zasad ochrony wrażliwych informacji.

AC-18 DOSTĘP BEZPRZEWODOWY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-18	**Dostęp bezprzewodowy**	**Wybrano**	**Wybrano**	**Wybrano**
AC-18 (1)	*DOSTĘP BEZPRZEWODOWY | UWIERZYTELNIANIE ORAZ SZYFROWANIE*		**Wybrano**	**Wybrano**
AC-18 (3)	*DOSTĘP BEZPRZEWODOWY | DEZAKTYWACJA SIECI BEZPRZEWODOWEJ*		Wybrano	Wybrano
AC-18 (4)	*DOSTĘP BEZPRZEWODOWY | OGRANICZENIE DOKONYWANIA KONFIGURACJI PRZEZ UŻYTKOWNIKÓW*			Wybrano
AC-18 (5)	*DOSTĘP BEZPRZEWODOWY | POZIOMY MOCY ANTEN I TRANSMISJI*			**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: W przypadkach, gdy nie jest możliwe wykorzystanie wszystkich lub wybranych elementów środka zabezpieczeń w danym systemie OT, należy zastosować inne mechanizmy lub procedury jako zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Możliwość włączenia funkcji uwierzytelniania i szyfrowania jest uzależniona od

możliwości danego środowiska OT. Jeśli urządzenia i użytkownicy nie mogą być uwierzytelniani i szyfrowani ze względu na ograniczenia związane z działaniem systemów lub brak stosownych możliwości technologicznych, należy wdrożyć zabezpieczenia kompensacyjne obejmujące dokładniejsze audytowanie dostępu bezprzewodowego, ograniczenie uprawnień do dostępu bezprzewodowego do najważniejszych osób lub wdrożenie zabezpieczenia rozszerzonego AC-18 (5) w celu ograniczenia zasięgu dostępu bezprzewodowego.

Zabezpieczenie rozszerzone: (3) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (5) Zarówno dostęp do połączeń bezprzewodowych, jak i zakłócenia sygnałów mogą stanowić źródła problemów w środowiskach OT. Anteny i poziomy mocy powinny zostać ustalone w taki sposób, aby umożliwić spełnianie wymogów dotyczących dostępności. Z punktu widzenia poufności, anteny oraz poziomy mocy mogą zostać dostosowane w taki sposób, aby ograniczyć możliwość połączenia się z siecią poza bezpośrednim otoczeniem systemu.

AC-19 KONTROLA DOSTĘPU DO URZĄDZEŃ MOBILNYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-19	**Kontrola dostępu do urządzeń przenośnych**	Wybrano	Wybrano	Wybrano
AC-19 (5)	*KONTROLA DOSTĘPU DO URZĄDZEŃ MOBILNYCH | SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA LUB WYBRANYCH ZASOBÓW URZĄDZENIA*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AC-20 WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-20	**Wykorzystanie systemów zewnętrznych**	**Wybrano**	**Wybrano**	**Wybrano**

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-20 (1)	*WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYC | OGRANICZENIA AUTORYZOWANEGO DOSTĘPU*		Wybrano	Wybrano
AC-20 (2)	*WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH | PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE - OGRANICZONE ZASTOSOWANIE*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny dostosować definicję pojęcia „systemu zewnętrznego", aby odzwierciedlała zakres odpowiedzialności organizacji, a także wewnętrzne podziały organizacyjne oraz istniejące powiązania pomiędzy nimi. Organizacja może uznać, że dany system stanowi system zewnętrzny, jeśli wykonuje inne funkcje, egzekwuje inne zasady, podlega innym jednostkom zarządzającym lub nie pozwala na weryfikację wdrożonych środków bezpieczeństwa w stopniu zapewniającym zaufanie. Przykładowo system OT i system przetwarzający dane przedsiębiorstwa mogą zostać uznane za zewnętrzne względem siebie w zależności od granic autoryzacji systemów działających w organizacji.

Kolejnym typowym przykładem tej zależności jest dostęp do systemów OT uzyskiwany przez partnerów biznesowych, na przykład przez dostawców lub przedsiębiorstwa świadczące usługi wsparcia. Opracowanie stosownej definicji systemów zewnętrznych oraz zaufanie względem nich jest wymagane w odniesieniu do funkcji, celów, technologii i ograniczeń systemów OT, aby było możliwe ustalenie i udokumentowanie technicznego lub biznesowego uzasadnienia użycia oraz akceptacji ryzyka nierozerwalnie związanego z korzystaniem z systemu zewnętrznego.

Zabezpieczenie rozszerzone: (1) (2) Brak omówienia zabezpieczenia w kontekście systemów OT.

AC-21 UDOSTĘPNIANIE INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-21	**Udostępnianie informacji**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AC-22 TREŚCI PUBLICZNIE DOSTĘPNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AC-22	Treści publicznie dostępne	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Z zasady publiczny dostęp do systemów OT powinien być niedozwolony. Wybrane informacje mogą zostać przesłane do publicznie dostępnego systemu, co może wymagać zastosowania dodatkowych środków bezpieczeństwa. Na organizacji ciąży obowiązek sprawdzenia, które informacje są udostępniane przed ich publikacją.

F.7.2. UŚWIADAMIANIE I SZKOLENIA – KATEGORIA AT

AT-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AT-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

AT-2 SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AT-2	**Szkolenie w zakresie uświadamiania bezpieczeństwa**	**Wybrano**	**Wybrano**	**Wybrano**
AT-2 (2)	*SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAGROŻENIE WEWNĘTRZNE*	Wybrano	Wybrano	Wybrano
AT-2 (3)	*SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | INŻYNIERIA SPOŁECZNA I POZYSKIWANIE DANYCH*		Wybrano	Wybrano
AT-2 (4)	*SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | PODEJRZANA TRANSMISJA I ANOMALIE ZACHOWANIA SYSTEMU*		**Dodano**	**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Szkolenie w zakresie uświadamiania bezpieczeństwa winno obejmować początkowe (wstępne) i okresowe

Tłumaczenie

zapoznanie z procedurami i zasadami dotyczącymi systemów OT, standardowymi procedurami operacyjnymi, trendami w sektorze bezpieczeństwa oraz podatnościami. Program szkoleń w zakresie uświadamiania bezpieczeństwa dotyczących systemów OT powinien być zgodny z wymogami określonymi w zasadach szkoleń w zakresie uświadamiania bezpieczeństwa ustanowionymi przez organizację.

Zabezpieczenie rozszerzone: (2) (3) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (4) Omówienie zabezpieczenia w kontekście systemów OT: Należy identyfikować oraz informować o podejrzanych i niestandardowych zachowaniach w środowisku OT. Niektóre przykłady takich zachowań mogą obejmować sterowniki PLC przełączone do trybu programowania, gdy powinny znajdować się w trybie pracy, wyłączenie procesu bez znanej przyczyny, działanie złośliwego programowania na urządzeniu HMI, nieoczekiwany ruch kursora lub pojawienie się w procesie zmiany, która nie została dokonana przez operatora.

Uzasadnienie uwzględnienia zabezpieczenia AT-2 (4) do UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Szkolenie pracowników odpowiedzialnych za systemy OT w zakresie wykrywania podejrzanych transmisji oraz anomalii, a także działań, które należy podjąć w przypadku wystąpienia takich zdarzeń, może stanowić ważny dodatek do mechanizmów wykrywania zagrożeń oraz ochrony systemu, zapewniając skuteczniejsze reagowanie na zagrożenia.

AT-3 SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AT-3	Szkolenie w zakresie bezpieczeństwa opartego na rolach	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Szkolenie w zakresie bezpieczeństwa winno obejmować początkowe i okresowe zapoznanie się z procedurami i zasadami dotyczącymi systemów OT, standardowymi procedurami

operacyjnymi, trendami w sektorze bezpieczeństwa oraz podatnościami. Program szkoleń w zakresie bezpieczeństwa dotyczących systemów OT powinien być zgodny z wymogami określonymi w zasadach szkoleń w zakresie uświadamiania bezpieczeństwa ustanowionymi przez organizację. Szkolenie może być dostosowane do konkretnych ról pracowników odpowiedzialnych za systemy OT, wśród których można wymienić operatorów, pracowników odpowiedzialnych za utrzymanie, inżynierów, nadzorców i administratorów.

AT-4 DOKUMENTACJA SZKOLENIOWA

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
AT-4	**Dokumentacja szkoleniowa**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.3. AUDYT I ROZLICZALNOŚĆ – KATEGORIA AU

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Audyt i rozliczalność"

Co do zasady starsze systemy OT nie obejmują ani nie oferują informacji dotyczących audytu bezpieczeństwa ani narzędzi audytowania. W sytuacjach, gdy systemy OT nie są w stanie obsługiwać wymogów związanych z audytem i rozliczalnością, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Organizacje mogą na przykład zastanowić się, czy informacje dotyczące audytu bezpieczeństwa są dostępne z oddzielnych systemów lub komponentów systemu (np. magazynu danych, zapór, systemów bezpieczeństwa fizycznego). Dodatkowe przykłady zabezpieczeń kompensacyjnych zostały podane w opisie każdego środka bezpieczeństwa.

AU-1 POLITYKA I PROCEDURY AUDYTU I ROZLICZALNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-1	Polityka i procedury	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

AU-2 AUDYT ZDARZEŃ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-2	Audyt zdarzeń	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny rozważyć uwzględnienie stosownych zdarzeń dotyczących systemów OT (takich jak: alerty, alarmy, zmiany konfiguracji i stanu systemu, działania operatora) w dziennikach zdarzeń, które mogą być oznaczone jako zdarzenia na potrzeby audytu.

AU-3 ZAWARTOŚĆ REJESTRÓW AUDYTU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-3	**Zawartość rejestrów audytu**	Wybrano	Wybrano	Wybrano
AU-3 (1)	*ZAWARTOŚĆ REJESTRÓW AUDYTU | DODATKOWE INFORMACJE KONTROLNE*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AU-4 POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-4	**Pojemność pamięci zapisów audytu**	Wybrano	Wybrano	Wybrano
AU-4 (1)	*POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU | TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH*	Dodano	Dodano	Dodano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie uwzględnienia zabezpieczenia AU-4 (1) do NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Wymagania ustanowione w organizacji mogą prowadzić do konieczności przechowywania bardzo dużych ilości danych, przekraczających możliwości komponentów systemu OT.

AU-5 REAKCJA NA BŁĘDY PROCESÓW AUDYTU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-5	**Reakcja na błędy procesów audytu**	Wybrano	Wybrano	Wybrano
AU-5 (1)	*REAKCJA NA BŁĘDY PROCESÓW AUDYTU | OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU*			Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-5 (2)	*REAKCJA NA BŁĘDY PROCESÓW AUDYTU | ALERTY CZASU RZECZYWISTEGO*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AU-6 PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-6	**Przegląd zapisu audytu, analiza i raportowanie**	Wybrano	Wybrano	Wybrano
AU-6 (1)	*PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE | ZAUTOMATYZOWANA INTEGRACJA PROCESÓW*		**Wybrano**	**Wybrano**
AU-6 (3)	*PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA ZBIORÓW AUDYTU*		Wybrano	Wybrano
AU-6 (5)	*PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE | ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU*			Wybrano
AU-6 (6)	*PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie ręcznych mechanizmów lub procedur. W przypadku urządzeń, które nie umożliwiają gromadzenia zapisów z audytów, konieczny może być okresowy przegląd ręczny.

Zabezpieczenie rozszerzone: (3) (5) (6) Brak omówienia zabezpieczenia w kontekście systemów OT.

AU-7 REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-7	**Redukcja treści zapisów z audytu i generowanie raportów**		Wybrano	Wybrano
AU-7 (1)	*REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYZACJA PROCESU*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AU-8 ZNACZNIKI CZASU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-8	**Znaczniki czasu**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują korzystanie z oddzielnego systemu stanowiącego główne źródło czasu. Dodatkowe informacje znajdują się w opisie powiązanego środka bezpieczeństwa SC-45.

AU-9 OCHRONA INFORMACJI AUDYTOWYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-9	**Ochrona informacji audytowych**	Wybrano	Wybrano	Wybrano
AU-9 (2)	*OCHRONA INFORMACJI AUDYTOWYCH | BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE*			Wybrano
AU-9 (3)	*OCHRONA INFORMACJI AUDYTOWYCH | OCHRONA KRYPTOGRAFICZNA*			Wybrano
AU-9 (4)	*OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP DLA PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AU-10 NIEZAPRZECZALNOŚĆ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-10	**Niezaprzeczalność**			**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Urządzenia OT mogą nie wymuszać niezaprzeczalności zapisów audytu, co może powodować konieczność wdrożenia zabezpieczeń kompensacyjnych. Przykładowe zabezpieczenia kompensacyjne obejmują systemy bezpieczeństwa fizycznego, kamery wykorzystywane w celu monitorowania dostępu użytkowników lub wykorzystanie oddzielnego urządzenia w celu gromadzenia plików i zapisów dziennika.

AU-11 RETENCJA ZAPISÓW AUDYTU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-11	**Retencja zapisów audytu**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

AU-12 TWORZENIE ZAPISÓW AUDYTU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
AU-12	**Tworzenie zapisów audytu**	Wybrano	Wybrano	Wybrano
AU-12 (1)	*TWORZENIE ZAPISÓW AUDYTU | OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU*			**Wybrano**
AU-12 (3)	*TWORZENIE ZAPISÓW AUDYTU | ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY*			**Wybrano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują zapewnienie skorelowanych czasowo zapisów audytu w oddzielnym systemie.

Zabezpieczenie rozszerzone: (3) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują stosowanie niezautomatyzowanych mechanizmów lub procedur zarządzania.

F.7.4. OCENA, AUTORYZACJA I MONITOROWANIE – KATEGORIA CA

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Ocena, autoryzacja i monitorowanie”

W sytuacjach, gdy systemy OT nie obsługują rozwiązań dotyczących oceny, autoryzacji oraz monitorowania wymaganych przez dane zabezpieczenie, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

CA-1 – POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

CA-2 OCENA ZABEZPIECZEŃ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-2	**Ocena zabezpieczeń**	**Wybrano**	**Wybrano**	**Wybrano**
CA-2 (1)	*OCENA ZABEZPIECZEŃ | NIEZALEŻNI AUDYTORZY*		Wybrano	Wybrano
CA-2 (2)	*OCENA ZABEZPIECZEŃ | OCENY SPECJALISTYCZNE*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Oceny winny być przeprowadzane i dokumentowane przez wykwalifikowanych audytorów, doświadczonych w ocenie systemów OT, upoważnionych przez organizację. Osoba lub grupa przeprowadzająca ocenę powinna w pełni rozumieć zasady i procedury bezpieczeństwa informacji, zasady i procedury bezpieczeństwa dotyczące systemów OT oraz specyficzne zagrożenia dla zdrowia, bezpieczeństwa i środowiska związane

z konkretnym obiektem bądź procesem w organizacji. Organizacja powinna dołożyć wszelkich starań, by ocena nie wpłynęła na działanie systemu ani nie spowoduje jego przypadkowej modyfikacji. Jeśli działania związane z oceną muszą być przeprowadzone na produkcyjnym systemie OT, konieczne może być wyłączenie go przed przeprowadzeniem oceny lub zaplanowanie tych działań w taki sposób, by w miarę możliwości odbywały się podczas planowanych przestojów systemu OT.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (2) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna przeprowadzić analizę ryzyka w celu wyboru ocenianego systemu (na przykład systemu produkcyjnego, systemu testowego lub laboratoryjnego).

CA-3 WYMIANA INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
CA-3	**Wymiana informacji**	**Wybrano**	**Wybrano**	**Wybrano**
CA-3 (6)	*WYMIANA INFORMACJI | AUTORYZACJA PRZESYŁU*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna przeprowadzić analizy ryzyka i korzyści, aby stwierdzić, czy system OT powinien być połączony z innymi systemami. Osoba autoryzująca (*ang. authorizing official – AO*) powinna dobrze poznać zasady i procedury bezpieczeństwa informacji, a także zasady i procedury bezpieczeństwa dotyczące systemów OT, ryzyko dotyczące systemów operacyjnych organizacji, osób, innych organizacji i państwa związane z połączeniem z innymi systemami. Powinna także znać osoby i organizacje, które obsługują i utrzymują poszczególne systemy, w tym przedsiębiorstwa zewnętrzne świadczące usługi konserwacji oraz dostawców usług. Dodatkowo AO powinna być świadoma szczególnych zagrożeń dla zdrowia, bezpieczeństwa i środowiska związanych z konkretnym połączeniem. Połączenia ze środowiska OT do innych stref bezpieczeństwa mogą wykraczać poza granicę autoryzacji, co może wymagać zatwierdzenia połączenia przez dwie różne osoby autoryzujące. Decyzje o akceptacji ryzyka winne być udokumentowane.

Zabezpieczenie rozszerzone: (6) Brak omówienia zabezpieczenia w kontekście systemów OT.

CA-5 PLAN I ETAPY DZIAŁANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-5	**Plan i etapy działania**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Działania naprawcze wskazane w opracowanych ocenach mogą nie być możliwe do natychmiastowego wdrożenia w środowisku OT. W związku z tym można wdrożyć tymczasowe środki przeciwdziałania w celu zmniejszenia ryzyka w ramach planu usuwania podatności lub planu i etapów działania.

CA-6 AUTORYZACJA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-6	**Autoryzacja**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CA-7 CIĄGŁE MONITOROWANIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-7	**Ciągłe monitorowanie**	**Wybrano**	**Wybrano**	**Wybrano**
CA-7 (1)	*CIĄGŁE MONITOROWANIE | NIEZALEŻNA OCENA*		Wybrano	Wybrano
CA-7 (4)	*CIĄGŁE MONITOROWANIE | MONITOROWANIE RYZYKA*	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Programy ciągłego monitorowania systemów OT są projektowane, dokumentowane i wdrażane z udziałem pracowników odpowiedzialnych za systemy OT. Organizacja powinna dołożyć wszelkich starań, by procesy związane z ciągłym monitorowaniem nie wpływały na działanie systemów OT. Osoba lub grupa osób planująca oraz przeprowadzająca działania związane z ciągłym monitorowaniem systemów OT winna

wdrożyć program monitorowania zachowujący zgodność z zasadami i procedurami bezpieczeństwa informacji, zasadami i procedurami bezpieczeństwa dotyczącymi systemów OT oraz uwzględniający zagrożenia dla zdrowia, bezpieczeństwa i środowiska związane z konkretnym obiektem bądź procesem w organizacji. Ciągłe monitorowanie może być zautomatyzowane lub realizowane ręcznie z częstotliwością wystarczającą do podejmowania decyzji opartych na ryzyku. Organizacja może na przykład ręcznie monitorować dzienniki zdarzeń z określoną częstotliwością – rzadziej w przypadku odizolowanych systemów charakteryzujących się niższym poziomem ryzyka, z kolei częściej w przypadku systemów sieciowych charakteryzujących się wyższym poziomem ryzyka.

Zabezpieczenie rozszerzone: (1) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

CA-8 BADANIE TESTY PENETRACYJNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-8	**Testy penetracyjne**			**Wybrano**
CA-8 (1)	*BADANIE PENETRACYJNE | NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY*			~~Usunięto~~

Omówienie zabezpieczenia w kontekście systemów OT: W przypadku sieci OT wszelkie badania penetracyjne winny wiązać się z zachowaniem najwyższej ostrożności, aby zapewnić, że nie wpłyną one negatywnie na działanie systemów OT. Z zasady systemy OT charakteryzują się wysoką wrażliwością na czas procesów i dysponują ograniczonymi zasobami. Przykładowe zabezpieczenia kompensacyjne obejmują wykorzystanie repliki systemu, a także wirtualizowanego lub symulowanego systemu do przeprowadzania badań penetracyjnych. Produkcyjny system OT może wymagać wyłączenia przed przeprowadzeniem badań. W sytuacji, gdy systemy OT są wyłączane w celu badań penetracyjnych, w miarę możliwości należy zaplanować ich przeprowadzenie podczas planowanych przestojów. Jeśli badania penetracyjne mają zostać przeprowadzone w sieciach innych niż OT, należy zachować szczególną ostrożność, aby nie nastąpiło przypadkowe naruszenie zasad bezpieczeństwa systemów i sieci OT.

Uzasadnienie usunięcia zabezpieczenia CA-8 (1) z WYSOKIEGO poziomu wpływu: W celu przeprowadzenia skutecznego testowania penetracyjnego systemów OT niezbędna jest specjalistyczna wiedza, a wybór niezależnych wykonawców posiadających odpowiedni zestaw umiejętności lub wiedzę do przeprowadzenia badań penetracyjnych środowiska OT może okazać się niemożliwy. Choć co do zasady testowanie penetracyjne powinno być przeprowadzane przez niezależny podmiot lub zespół, wybór takiego zespołu może okazać się niewykonalny w przypadku wszystkich systemów OT o wysokim poziomie wpływu.

CA-9 POŁĄCZENIA WEWNĄTRZSYSTEMOWE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CA-9	Połączenia wewnątrzsystemowe	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny przeprowadzić analizę ryzyka i korzyści w celu ustalenia, czy urządzenia i komponenty systemu OT powinny być podłączone do innych komponentów systemu, a następnie udokumentować te połączenia. AO winna w pełni rozumieć potencjalne ryzyko związane z zatwierdzaniem poszczególnych połączeń lub klas podłączanych komponentów systemu. AO może na przykład zatwierdzić podłączenie dowolnych czujników ograniczonych do zakresu od 4 do 20 miliamperów (mA); z kolei inne typy połączeń (np. szeregowe lub Ethernet) mogą wymagać oddzielnego zatwierdzenia. Decyzje o akceptacji ryzyka winne być udokumentowane.

F.7.5. ZARZĄDZANIE KONFIGURACJĄ – KATEGORIA CM

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Zarządzanie konfiguracją”

Gdy system OT nie może zostać skonfigurowany w taki sposób, by ograniczyć możliwość korzystania ze zbędnych funkcji lub nie obsługuje zautomatyzowanych mechanizmów realizujących funkcje zarządzania konfiguracją, należy zastosować niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

CM-1 – POLITYKA I PROCEDURY

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
CM-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

CM-2 KONFIGURACJA BAZOWA

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
CM-2	**Konfiguracja bazowa**	Wybrano	Wybrano	Wybrano
CM-2 (2)	*KONFIGURACJA BAZOWA | AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ*		Wybrano	Wybrano
CM-2 (3)	*KONFIGURACJA BAZOWA | RETENCJA ZACHOWANYCH KONFIGURACJI*		Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-2 (7)	*KONFIGURACJA BAZOWA | KONFIGUROWANIE SYSTEMÓW I KOMPONENTÓW W OBSZARACH WYSOKIEGO RYZYKA*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-3 ZABEZPIECZANIE ZMIAN KONFIGURACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-3	**Zabezpieczanie zmian konfiguracji**		**Wybrano**	**Wybrano**
CM-3 (1)	*ZABEZPIECZANIE ZMIAN KONFIGURACJI | AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ WPROWADZANIA ZMIAN*			Wybrano
CM-3 (2)	*ZABEZPIECZANIE ZMIAN KONFIGURACJI | TESTY, WALIDACJA I ZMIANY DOKUMENTÓW*		Wybrano	Wybrano
CM-3 (4)	*ZABEZPIECZANIE ZMIAN KONFIGURACJI | FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI*		Wybrano	Wybrano
CM-3 (6)	*ZABEZPIECZANIE ZMIAN KONFIGURACJI | ZARZĄDZANIE KRYPTOGRAFICZNE*			Wybrano
CM-3 (7)	*ZABEZPIECZANIE ZMIAN KONFIGURACJI | PRZEGLĄD ZMIAN W SYSTEMIE*			
CM-3 (8)	*ZABEZPIECZANIE ZMIAN KONFIGURACJI | ZAPOBIEGANIE LUB OGRANICZANIE ZMIAN KONFIGURACJI*			

Omówienie zabezpieczenia w kontekście systemów OT: Procedury związane z zabezpieczaniem zmian konfiguracji powinny być zgodne z praktykami zarządzania zmianami obowiązującymi w organizacji.

Zabezpieczenie rozszerzone: (1) (2) (4) (6) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (7) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna uwzględniać wymogi dotyczące systemów OT przy określaniu częstotliwości oraz okoliczności przeprowadzania przeglądów zmian w systemie. Pomiarowe systemy bezpieczeństwa mogą wymagać przeglądów zmian przeprowadzanych z określoną częstotliwością, aby możliwe było zapewnienie, że nie zostały wprowadzone żadne zmiany w komponentach logicznych funkcji pomiarowej bezpieczeństwa.

Zabezpieczenie rozszerzone: (8) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna zapobiegać wprowadzaniu lub ograniczyć możliwość wprowadzenia zmian konfiguracji w oparciu o ustalone ryzyko, na podstawie którego można ustalić, że system nie powinien być modyfikowany bez dodatkowych zezwoleń i stosownych dopuszczeń. Wybrane sterowniki PLC są wyposażone w fizyczne przełączniki, które muszą zostać wykorzystane w celu przełączenia sterownika do trybu umożliwiającego dokonanie zmian. Fizyczne przełączniki mogą zabezpieczać możliwość dokonania zmian w konfiguracji poprzez wprowadzenie wymogu uzyskania fizycznego dostępu do urządzenia w celu dokonania zmiany w systemie.

CM-4 ANALIZY WPŁYWU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-4	**Analizy wpływu**	**Wybrano**	**Wybrano**	**Wybrano**
CM-4 (1)	*ANALIZY WPŁYWU | ODDZIELNE ŚRODOWISKA TESTOWE*			Wybrano
CM-4 (2)	*ANALIZY WPŁYWU | WERYFIKACJA ZABEZPIECZEŃ*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna uwzględnić wzajemne zależności pomiędzy różnymi aspektami bezpieczeństwa systemów OT. Pracownicy odpowiedzialni za bezpieczeństwo systemów OT powinni uczestniczyć w procesie zarządzania zmianami w procesie, jeśli zmiana w systemie może mieć wpływ na jego bezpieczeństwo.

Zabezpieczenie rozszerzone: (1) (2) Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-5 OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
CM-5	**Ograniczenia możliwości dokonywania zmian**	**Wybrano**	**Wybrano**	**Wybrano**
CM-5 (1)	*OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Niektóre urządzenia OT są wyposażone w przełączniki umożliwiające zmianę konfiguracji oraz trybu ich pracy. Jeśli takie rozwiązania istnieją, należy z nich korzystać w celu ochrony urządzeń przed możliwością dokonania nieautoryzowanych zmian. Wiele sterowników PLC jest wyposażonych w przełączniki, które umożliwiają przełączenie ich do trybu programowania lub trybu pracy. Sterowniki te powinny zostać skonfigurowane w trybie pracy lub trybie zdalnym, aby zapobiec nieautoryzowanym zmianom konfiguracji. Należy także usunąć z urządzenia wymagane w tym celu klucze i stosownie je zabezpieczyć.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-6 USTAWIENIA KONFIGURACYJNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
CM-6	**Ustawienia konfiguracyjne**	Wybrano	Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-6 (1)	*USTAWIENIA KONFIGURACYJNE | AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA*			Wybrano
CM-6 (2)	*USTAWIENIA KONFIGURACYJNE | ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-7 ZASADA MINIMALNEJ FUNKCJONALNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-7	**Zasada minimalnej funkcjonalności**	**Wybrano**	**Wybrano**	**Wybrano**
CM-7 (1)	*ZASADA MINIMALNEJ FUNKCJONALNOŚCI | PRZEGLĄDY OKRESOWE*		Wybrano	Wybrano
CM-7 (2)	*ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAPOBIEGANIE WYKONYWANIU PROGRAMU*		Wybrano	Wybrano
CM-7 (5)	*ZASADA MINIMALNEJ FUNKCJONALNOŚCI | AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA")*		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna postępować zgodnie z zasadą minimalnej funkcjonalności, umożliwiając działanie określonych funkcji, protokołów oraz usług wymaganych w celu prawidłowego działania i realizacji funkcji przez systemy OT. W przypadku interfejsów

nieroutowalnych, takich jak połączenia szeregowe, stosowne przerwania mogą zostać wyłączone a ustawienia mogą zostać skonfigurowane w trybie tylko do odczytu dla wszystkich użytkowników z wyjątkiem użytkowników uprzywilejowanych, aby w ten sposób ograniczyć funkcjonalność. Porty stanową część przestrzeni adresowej w protokołach sieciowych i często są powiązane z określonymi protokołami lub funkcjami. W przypadku protokołów routowalnych istnieje możliwość wyłączenia portów na wielu urządzeniach sieciowych, co pozwala na ograniczenie funkcjonalności do minimum wymaganego do działania.

Zabezpieczenie rozszerzone: (1) (2) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (5) Omówienie zabezpieczenia w kontekście systemów OT: Lista aplikacji uruchamianych w środowiskach OT jest względnie niezmienna, co umożliwia stosowanie listy autoryzowanego oprogramowania. Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych zaleca korzystanie z listy dozwolonych aplikacji w środowiskach i systemach OT.

CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-8	**Inwentaryzacja komponentów systemu**	Wybrano	Wybrano	Wybrano
CM-8 (1)	*INWENTARYZACJA KOMPONENTÓW SYSTEMU | AKTUALIZACJE INSTALACJI I USUWANIA KOMPONENTÓW*		Wybrano	Wybrano
CM-8 (2)	*INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNA KONSERWACJA (UTRZYMYWANIE)*			Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-8 (3)	*INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH*		Wybrano	Wybrano
CM-8 (4)	*INWENTARYZACJA KOMPONENTÓW SYSTEMU | INFORMACJA DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-9 PLAN ZARZĄDZANIA KONFIGURACJĄ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-9	**Plan zarządzania konfiguracją**		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Plany zarządzania konfiguracją dotyczą zarówno wewnętrznych, jak i zewnętrznych pracowników oraz podmiotów (np. wykonawców, integratorów) odpowiedzialnych za konfigurację urządzeń.

CM-10 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-10	**Ograniczenia w użyciu oprogramowania**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-11 OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-11	**Oprogramowanie instalowane przez użytkownika**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CM-12 LOKACJA (POŁOŻENIE) INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CM-12	**Położenie (lokacja) informacji**		**Wybrano**	**Wybrano**
CM-12 (1)	*LOKACJA (POŁOŻENIE) INFORMACJI | AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny wskazać typy informacji oraz komponenty, aby analizować, w jakich miejscach informacje są przetwarzane i przechowywane. Informacje ważne z punktu widzenia środowisk OT mogą obejmować hasła do kont współdzielonych, kopie zapasowe konfiguracji sterowników PLC, szczegółowe schematy połączeń sieciowych i oceny ryzyka określające zagrożenia dotyczące danego środowiska.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.6. PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA – KATEGORIA CP

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Planowanie awaryjne / Ciągłość działania”

Systemy OT często charakteryzują się niezmiennością lokalizacji i brakiem możliwości przeniesienia, ponadto problemem bywa niska dostępność zamienników oraz części zamiennych wybranych komponentów. Nawet niewielka awaria może uniemożliwić realizację podstawowych misji i funkcji biznesowych przy zachowaniu pełnej ciągłości lub ograniczenie przestoju do minimum. W przypadkach, w których organizacja nie jest w stanie zapewnić niezbędnych podstawowych usług, wsparcia lub zautomatyzowanych mechanizmów awaryjnych, należy zastosować inne mechanizmy lub procedury jako zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

CP-1 – POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

CP-2 PLAN CIĄGŁOŚCI DZIAŁANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-2	**Plan ciągłości działania**	**Wybrano**	**Wybrano**	**Wybrano**
CP-2 (1)	*PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z POWIĄZANYMI PLANAMI*		Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-2 (2)	*PLAN CIĄGŁOŚCI DZIAŁANIA | PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA*			Wybrano
CP-2 (3)	*PLAN CIĄGŁOŚCI DZIAŁANIA | WZNAWIANIE PODSTAWIOWYCH DZIAŁAŃ I FUNKCJI BIZNESOWYCH*		Wybrano	Wybrano
CP-2 (5)	*PLAN CIĄGŁOŚCI DZIAŁANIA | KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH*			Wybrano
CP-2 (8)	*PLAN CIĄGŁOŚCI DZIAŁANIA | IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna określić plany awaryjne dla poszczególnych kategorii zakłóceń oraz awarii. W przypadku wystąpienia sytuacji awaryjnej, urządzenia OT powinny realizować zaprogramowane funkcje, na przykład powiadomić operatora o awarii, a następnie przerwać pracę bądź powiadomić operatora, a następnie bezpiecznie wyłączyć proces przemysłowy lub kontynuować pracę na podstawie ostatniej bezpiecznej konfiguracji przed wystąpieniem awarii. Plany ciągłości działania dotyczące poważnych zakłóceń i awarii mogą wymagać zaangażowania wyspecjalizowanych organizacji, takich jak na przykład FEMA, służby ratownicze czy organy regulacyjne.

Zabezpieczenie rozszerzone: (1) (2) (3) (5) (8) Brak omówienia zabezpieczenia w kontekście systemów OT.

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-3	**Szkolenie w zakresie planowania ciągłości działania**	Wybrano	Wybrano	Wybrano
CP-3 (1)	*SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | WYDARZENIA SYMULOWANE*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CP-4 TESTOWANIE PLANU AWARYJNEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-4	**Testowanie planu ciągłości działania**	Wybrano	Wybrano	Wybrano
CP-4 (1)	*TESTOWANIE PLANU AWARYJNEGO | KOORDYNACJA Z POWIĄZANYMI PLANAMI*		Wybrano	Wybrano
CP-4 (2)	*TESTOWANIE PLANU AWARYJNEGO | ZAPASOWE MIEJSCE PRZETWARZANIA*			**Wybrano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (2) Omówienie zabezpieczenia w kontekście systemów OT: Nie wszystkie systemy mogą posiadać zapasowe miejsce przetwarzania, jak wskazano w opisie środka bezpieczeństwa CP-7.

CP-6 ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-6	**Zapasowe miejsce przechowywania kopii**		**Wybrano**	**Wybrano**
CP-6 (1)	*ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | SEPARACJA OD MIEJSCA GŁÓWNEGO*		Wybrano	Wybrano
CP-6 (2)	*ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | CZAS ODZYSKIWANIA I PUNKT ODTWORZENIA DANYCH*			Wybrano
CP-6 (3)	*ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | DOSTĘPNOŚĆ*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

CP-7 ZAPASOWE MIEJSCE PRZETWARZANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-7	**Zapasowe miejsce przetwarzania**		**Wybrano**	**Wybrano**
CP-7 (1)	*ZAPASOWE MIEJSCE PRZETWARZANIA | ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ*		Wybrano	Wybrano
CP-7 (2)	*ZAPASOWE MIEJSCE PRZETWARZANIA | DOSTĘPNOŚĆ*		Wybrano	Wybrano
CP-7 (3)	*ZAPASOWE MIEJSCE PRZETWARZANIA | PRIORYTET USŁUG*		Wybrano	Wybrano
CP-7 (4)	*ZAPASOWE MIEJSCE PRZETWARZANIA | GOTOWOŚĆ DO UŻYCIA*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Wiele serwerów nadzorujących lub optymalizujących procesy (na przykład serwery znajdujące się na poziomach 3 i wyższych w modelu Purdue) zarządzające całym zakładem może być

Tłumaczenie

obsługiwanych z zapasowego miejsca przetwarzania. Z zasady nie jest możliwe, by urządzenia terenowe (czujniki i elementy wykonawcze) oraz systemy sterowania (czyli urządzenia poziomów 1 i 0 modelu Purdue) mogły być obsługiwanie z zapasowego miejsca przetwarzania.

Zabezpieczenie rozszerzone: (1) (2) (3) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

CP-8 USŁUGI TELEKOMUNIKACYJNE

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
CP-8	**Usługi telekomunikacyjne**		**Wybrano**	**Wybrano**
CP-8 (1)	*USŁUGI TELEKOMUNIKACYJNE | PRIORYTETY ŚWIADCZENIA USŁUG*		Wybrano	Wybrano
CP-8 (2)	*USŁUGI TELEKOMUNIKACYJNE | POJEDYNCZE PUNKTY AWARII*		Wybrano	Wybrano
CP-8 (3)	*USŁUGI TELEKOMUNIKACYJNE | ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH*			Wybrano
CP-8 (4)	*USŁUGI TELEKOMUNIKACYJNE | PLAN AWARYJNY DOSTAWCY*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zagadnienia związane z jakością usługi dotyczące systemów OT obejmują opóźnienia i przepustowość.
Zabezpieczenie rozszerzone: (1) (2) (3) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

CP-9 KOPIA ZAPASOWA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
CP-9	**Kopia zapasowa**	Wybrano	Wybrano	Wybrano
CP-9 (1)	*KOPIA ZAPASOWA | BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI*		**Wybrano**	**Wybrano**
CP-9 (2)	*KOPIA ZAPASOWA | TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH*			**Wybrano**
CP-9 (3)	*KOPIA ZAPASOWA | SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH*			Wybrano
CP-9 (5)	*KOPIA ZAPASOWA | PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI*			Wybrano
CP-9 (8)	*KOPIA ZAPASOWA | OCHRONA KRYPTOGRAFICZNA*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) (2) Omówienie zabezpieczenia w kontekście systemów OT: Weryfikacja niezawodności i integralności zwiększa pewność odtworzenia systemu w przypadku wystąpienia incydentu i minimalizuje wpływ związany z przestojami i awariami. Możliwość testowania kopii zapasowych jest często uzależniona od dostępności zasobów pozwalających na odwzorowanie docelowego środowiska, na przykład dostępności zapasowych urządzeń i komponentów na potrzeby testów. Testowanie kopii zapasowych i ich odtwarzania w systemach OT często jest możliwe wyłącznie w przypadku systemów obejmujących

nadmiarowe komponenty lub organizacji posiadających zapasowe urządzenia. W wybranych przypadkach proces wykorzystywania próbek jest ograniczony wyłącznie do nadmiarowych systemów. Zabezpieczenia kompensacyjne mogą obejmować alternatywne metody testowania kopii zapasowych, takie jak sprawdzanie poprawności skrótów kryptograficznych lub sum kontrolnych.

Zabezpieczenie rozszerzone: (3) (5) (8) Brak omówienia zabezpieczenia w kontekście systemów OT.

CP-10 ODZYSKIWANIE I ODTWARZANIE SYSTEMU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-10	**Odzyskiwanie i odtwarzanie systemu**	**Wybrano**	**Wybrano**	**Wybrano**
CP-10 (2)	*ODZYSKIWANIE I ODTWARZANIE SYSTEMU | ODTWARZANIE TRANSAKCJI*		Wybrano	Wybrano
CP-10 (4)	*ODZYSKIWANIE I ODTWARZANIE SYSTEMU | PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM*			Wybrano
CP-10 (6)	*ODZYSKIWANIE I ODTWARZANIE SYSTEMU | OCHRONA KOMPONENTÓW*		**Dodano**	**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Odtworzenie systemów OT wymaga ustalenia, czy zmienne dotyczące stanu systemu powinny zostać przywrócone do wartości początkowych, czy raczej wartości sprzed wystąpienia zakłócenia. Przykładem może być rozważenie, czy zawory powinny zostać ustawione w stanie pełnego otwarcia, pełnego zamknięcia lub do ustawienia sprzed wystąpienia awarii. Przywrócenie zmiennych stanu systemu może zakłócić trwające procesy

fizyczne – na przykład zamknięcie zaworów może wpłynąć na chłodzenie komponentów systemu.

Zabezpieczenie rozszerzone: (2) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (6) Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny uwzględnić przedziały czasowe przywracania i odtwarzania systemów ustalając zapasowe urządzenia, które powinny być przechowywane, a także wziąć pod uwagę zagrożenia środowiskowe, które mogą doprowadzić do awarii lub uszkodzenia urządzeń. Lokalizacje i środowiska przechowywania powinny zostać dobrane z myślą o wymogach urządzeń wykorzystywanych do tworzenia kopii.

Uzasadnienie uwzględnienia zabezpieczenia CP-10 (6) w zakresie UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Komponenty systemów OT przechowywane bez odpowiedniej ochrony przed zagrożeniami środowiskowymi i nieautoryzowanym dostępem fizycznym lub logicznym mogą być podatne na naruszenie zasad ochrony lub uszkodzenie. Niektóre komponenty mogą zawierać wbudowaną elektronikę, która musi być chroniona przed zagrożeniami środowiskowymi.

CP-12 TRYB BEZPIECZNY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
CP-12	**Tryb bezpieczny**	Dodano	Dodano	Dodano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie uwzględnienia środka bezpieczeństwa CP-12 w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Zabezpieczenie zapewnia ramy, dzięki którym organizacja może planować zasady oraz procedury skutecznego działania w przypadku wystąpienia niekontrolowanych sytuacji dotyczących systemów IT i OT w środowisku eksploatacji w celu zminimalizowania potencjalnego wpływu na bezpieczeństwo i środowisko.

F.7.7. IDENTYFIKACJA I UWIERZYTELNIANIE – KATEGORIA IA

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Identyfikacja i uwierzytelnianie”

Przed wdrożeniem zabezpieczeń należących do kategorii IA – Identyfikacja i uwierzytelnianie, organizacja powinna wziąć pod uwagę, że ich stosowanie wiąże się z koniecznością znalezienia kompromisów pomiędzy poziomem bezpieczeństwa i prywatności a możliwymi opóźnieniami, osiągami i wydajnością systemu. Organizacja powinna na przykład przeanalizować, czy opóźnienia wynikające z zastosowania mechanizmów uwierzytelniania opartych na metodach kryptograficznych mogą mieć negatywny wpływ na wydajność systemów OT.

W sytuacjach, gdy systemy OT nie obsługują rozwiązań wymaganych przez wymagania w zakresie identyfikacji i uwierzytelniania, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

IA-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

IA-2 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-2	**Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)**	**Wybrano**	**Wybrano**	**Wybrano**
IA-2 (1)	*IDENTYFIKACJA I UWIERZYTELNIANIE | UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT UPRZYWILEJOWANYCH*	**Wybrano**	**Wybrano**	**Wybrano**

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
IA-2 (2)	*IDENTYFIKACJA I UWIERZYTELNIANIE | UWIERZYTELNIANIE WIELOSKŁADNIKOWE DOSTĘPU DO KONT NIEUPRZYWILEJOWANYCH*	**Wybrano**	**Wybrano**	**Wybrano**
IA-2 (5)	*IDENTYFIKACJA I UWIERZYTELNIANIE | UWIERZYTELNIANIE INDYWIDUALNE PRZED UWIERZYTELNIANIEM GRUPOWYM*			**Wybrano**
IA-2 (8)	*IDENTYFIKACJA I UWIERZYTELNIANIE | DOSTĘP DO KONT – ODPORNOŚĆ NA POWTARZANIE*	Wybrano	Wybrano	Wybrano
IA-2 (12)	*IDENTYFIKACJA I UWIERZYTELNIANIE | AUTORYZACJA DANYCH DOSTĘPOWYCH*	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Gdy w organizacji wymagane jest stosowanie kont współdzielonych, stosowne zabezpieczenia kompensacyjne mogą obejmować zapewnienie zwiększonego bezpieczeństwa fizycznego, bezpieczeństwa pracowników oraz audytowanie. W przypadku niektórych systemów OT, zapewnienie operatorowi możliwości niezwłocznej reakcji ma kluczowe znaczenie. Należy zapewnić, by obsługa systemów OT nie była ograniczona lub utrudniona przez wymogi w zakresie identyfikacji lub uwierzytelniania. Dostęp do tych systemów może być ograniczony przez odpowiednie zabezpieczenia dostępu fizycznego.

Zabezpieczenie rozszerzone: (1) (2) Omówienie zabezpieczenia w kontekście systemów OT: Odpowiednim zabezpieczeniem kompensacyjnym mogą być ograniczenia dostępu fizycznego, które mogą stanowić jeden ze składników uwierzytelniania, pod warunkiem, że system nie jest dostępny zdalnie.

Zabezpieczenie rozszerzone: (5) Omówienie zabezpieczenia w kontekście systemów OT: W przypadku dostępu lokalnego zabezpieczenia dostępu fizycznego oraz tworzenie plików dziennika mogą stanowić alternatywę dla uwierzytelniania poszczególnych użytkowników systemu OT. W przypadku dostępu zdalnego mechanizm uwierzytelniania dostępu zdalnego pozwoli na identyfikację, autoryzację oraz rejestrowanie indywidualnego dostępu przed zezwoleniem na korzystanie z kont współdzielonych.

Zabezpieczenie rozszerzone: (8) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (12) Omówienie zabezpieczenia w kontekście systemów OT: Autoryzacja danych dostępowych dotyczy wyłącznie jednostek rządowych wymienionych w definicji zawartej w Memorandum OMB M-19-17 [OMB-M1917]. Pozostałe organizacje winny zapoznać się z opisem zabezpieczeń rozszerzonych IA-2 (1) (2), które określają wytyczne dotyczące poświadczeń w przypadku uwierzytelniania wieloskładnikowego. Wiele systemów OT nie umożliwia autoryzacji danych dostępowych, w związku z czym wymagają zastosowania zabezpieczeń kompensacyjnych.

IA-3 IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-3	**Identyfikacja i uwierzytelnianie urządzenia**	Dodano	Wybrano	Wybrano
IA-3 (1)	*IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE*			
IA-3 (4)	*IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA | ATESTACJA URZĄDZENIA*			

Omówienie zabezpieczenia w kontekście systemów OT: W przypadku systemów OT funkcje uwierzytelniania urządzeń mogą nie być dostępne. Jeśli urządzenia znajdują się w jednej lokalizacji, zabezpieczenia dostępu fizycznego, które zapobiegają nieautoryzowanej komunikacji między urządzeniami, mogą być stosowane jako zabezpieczenia kompensacyjne. W przypadku komunikacji zdalnej może być wymagane zastosowanie dodatkowych urządzeń, aby spełnić wymagania dotyczące uwierzytelniania.

Zabezpieczenie rozszerzone: (1) (4) Omówienie zabezpieczenia w kontekście systemów OT: W przypadku systemów OT, które obejmują urządzenia przemysłowego internetu rzeczy, wybrane zabezpieczenia rozszerzone mogą być wymagane w celu ochrony komunikacji między urządzeniami.

Uzasadnienie uwzględnienia zabezpieczenia IA-3 (11) w ramach NISKIEGO poziomu wpływu: Biorąc pod uwagę różnorodność urządzeń OT i ich lokalizacji, organizacje muszą rozważyć, czy urządzenia OT, które mogą być podatne na manipulacje lub spoofing, wymagają identyfikacji i uwierzytelniania, a jeśli tak, to dla jakich typów połączeń są one wymagane.

IA-4 ZARZĄDZANIE IDENTYFIKATOREM

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
IA-4	**Zarządzanie identyfikatorem**	Wybrano	Wybrano	Wybrano
IA-4 (4)	*ZARZĄDZANIE IDENTYFIKATOREM | IDENTYFIKACJA STATUSU UŻYTKOWNIKA*		**Wybrano**	**Wybrano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (4) Omówienie zabezpieczenia w kontekście systemów OT: To zabezpieczenie rozszerzone jest zazwyczaj wdrażane na szczeblu organizacyjnym, nie zaś na poziomie systemu. Zarządzanie ryzykiem dotyczącym niektórych systemów i środowisk OT może jednak wymagać by identyfikatory (np. karty dostępu pracowników) miały różne oznaczenia wskazujące na status poszczególnych osób – wykonawców, obcokrajowców oraz użytkowników spoza organizacji.

IA-5 ZARZĄDZANIE METODAMI UWIERZYTELNIANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
IA-5	**Zarządzanie metodami uwierzytelniania**	**Wybrano**	**Wybrano**	**Wybrano**
IA-5 (1)	*ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE OPARTE O HASŁA*	Wybrano	Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
IA-5 (2)	*ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO*		Wybrano	Wybrano
IA-5 (6)	*ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | OCHRONA METOD UWIERZYTELNIANIA*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują zabezpieczenie dostępu fizycznego oraz enkapsulację systemów OT w celu umożliwienia uwierzytelniania użytkowników poza systemami OT.

Zabezpieczenie rozszerzone: (1) (2) (6) Brak omówienia zabezpieczenia w kontekście systemów OT.

IA-6 OCHRONA PROCESU UWIERZYTELNIANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
IA-6	**Ochrona procesu uwierzytelniania**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Podstawowym założeniem tego zabezpieczenia jest to, że system jest wyposażony w interfejs wizualny, który przekazuje informacje zwrotne na temat informacji uwierzytelniających podczas procesu uwierzytelniania. W przypadku, gdy system OT wykorzystuje interfejs, który nie pozwala na przekazywanie takich informacji (na przykład realizując uwierzytelnianie oparte na protokole), zabezpieczenie może zostać dostosowane.

IA-7 MODUŁ KRYPTOGRAFICZNY UWIERZYTELNIANIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-7	**Uwierzytelnianie modułu kryptograficznego**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

IA-8 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-8	**Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji)**	**Wybrano**	**Wybrano**	**Wybrano**
IA-8 (1)	*IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE*	**Wybrano**	**Wybrano**	**Wybrano**
IA-8 (2)	*IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH*	**Wybrano**	**Wybrano**	**Wybrano**
IA-8 (4)	*IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE*	**Wybrano**	**Wybrano**	**Wybrano**

Tłumaczenie

Omówienie zabezpieczenia w kontekście systemów OT: Omówienie zabezpieczenia w kontekście systemów OT dotyczące środka bezpieczeństwa IA-2 [Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)] odnosi się także do użytkowników spoza organizacji.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Autoryzacja danych dostępowych dotyczy wyłącznie jednostek rządowych wymienionych w definicji zawartej w Memorandum OMB M-19-17 [OMB-M1917], takich jak organy rządowe czy wykonawcy.

Zabezpieczenie rozszerzone: (2) (4) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują wdrożenie odpowiednich funkcji poza systemami OT oraz zastosowanie uwierzytelniania wieloskładnikowego.

IA-11 PONOWNE UWIERZYTELNIENIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-11	**Ponowne uwierzytelnienie**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

IA-12 POTWIERDZENIE TOŻSAMOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-12	**Potwierdzanie tożsamości**		**Wybrano**	**Wybrano**
IA-12 (1)	*POTWIERDZENIE TOŻSAMOŚCI | AUTORYZACJA PRZEŁOŻONEGO*			**Dodano**
IA-12 (2)	*POTWIERDZENIE TOŻSAMOŚCI | DOWODZENIE TOŻSAMOŚCI*		**Wybrano**	**Wybrano**
IA-12 (3)	*POTWIERDZENIE TOŻSAMOŚCI | POTWIERDZANIE I WERYFIKACJA DOWODÓW TOŻSAMOŚCI*		**Wybrano**	**Wybrano**

Tłumaczenie

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IA-12 (4)	*POTWIERDZENIE TOŻSAMOŚCI | OSOBISTE ZATWIERDZENIE I WERYFIKACJA*			**Wybrano**
IA-12 (5)	*POTWIERDZENIE TOŻSAMOŚCI | POTWIERDZENIE ADRESU*		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Potwierdzanie tożsamości to proces realizowany przez różne jednostki w organizacji. Istniejące systemy organizacyjne, takie jak procesy kadrowe lub procedury IT, powinny zostać wykorzystane w celu realizacji założeń tego zabezpieczenia.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Realizacja zadań przez pracowników utrzymania, inżynierów oraz przedstawicieli podmiotów zewnętrznych może wymagać dostępu do systemów OT. Na organizacji spoczywa odpowiedzialność za wyznaczenie osoby autoryzującej (AO) weryfikującej tożsamość pracowników przed zezwoleniem na dostęp do środowiska OT. Należy także rozważyć uzyskanie w takich sytuacjach zgody przełożonego lub sponsora, na przykład przedstawiciela działu operacyjnego.

Zabezpieczenie rozszerzone: (2) (3) (4) (5) Omówienie zabezpieczenia w kontekście systemów OT: Jeśli zabezpieczenia te są stosowane w organizacji, należy wykorzystać istniejące procesy. Przykładowo dział kadr może posiadać system pozwalający na weryfikację dowodów tożsamości. Zespoły odpowiedzialne za bezpieczeństwo systemów OT nie muszą opracowywać niezależnego systemu w celu realizacji założeń tego zabezpieczenia.

Uzasadnienie uwzględnienia zabezpieczenia IA-12 (1) w zakresie WYSOKIEGO poziomu wpływu: Przełożony lub sponsor powinien mieć świadomość każdej sytuacji, w której pracownicy uzyskują dostęp do środowiska OT, ponieważ nieautoryzowane lub przypadkowe uzyskanie dostępu może wiązać się ze skutkami dotyczącymi procesu fizycznego.

F.7.8. REAGOWANIE NA INCYDENTY – KATEGORIA IR

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Reagowanie na Incydenty”

Zautomatyzowane mechanizmy i rozwiązania w zakresie wykrywania incydentów związanych z bezpieczeństwem zwykle nie stanowią części systemów OT ani nie są z nimi połączone.

IR-1 – POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

IR-2 SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-2	**Szkolenie w zakresie reagowania na incydenty**	Wybrano	Wybrano	Wybrano
IR-2 (1)	*SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | WYDARZENIA SYMULOWANE*			Wybrano
IR-2 (2)	*SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

IR-3 TESTOWANIE REAGOWANIA NA INCYDENTY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-3	**Testowanie reagowania na incydenty**		Wybrano	Wybrano
IR-3 (2)	TESTOWANIE REAGOWANIA NA *INCYDENTY | KOORDYNACJA* Z POWIĄZANYMI PLANAMI		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

IR-4 OBSŁUGA INCYDENTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-4	**Obsługa incydentów**	**Wybrano**	**Wybrano**	**Wybrano**
IR-4 (1)	*OBSŁUGA INCYDENTÓW | AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ*		Wybrano	Wybrano
IR-4 (4)	*OBSŁUGA INCYDENTÓW | KORELACJA INFORMACJI*			Wybrano
IR-4 (11)	*OBSŁUGA INCYDENTÓW | ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: W ramach działań i kompetencji dotyczących obsługi incydentów organizacja koordynuje działania z podmiotami zewnętrznymi – producentami, integratorami oraz dostawcami, aby zapewnić im możliwość reagowania na zdarzenia dotyczące wbudowanych komponentów i urządzeń.

Zabezpieczenie rozszerzone: (1) (4) (11) Brak omówienia zabezpieczenia w kontekście systemów OT.

IR-5 MONITOROWANIE INCYDENTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-5	**Monitorowanie incydentów**	Wybrano	Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-5 (1)	*MONITOROWANIE INCYDENTÓW | AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

IR-6 ZGŁASZANIE INCYDENTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
IR-6	**Zgłaszanie incydentów**	**Wybrano**	**Wybrano**	**Wybrano**
IR-6 (1)	*ZGŁASZANIE INCYDENTÓW | ZGŁASZANIE AUTOMATYCZNE*		**Wybrano**	**Wybrano**
IR-6 (3)	*ZGŁASZANIE INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja winna zgłaszać incydenty bez zbędnej zwłoki. CISA współpracuje z międzynarodowymi zespołami reagowania na incydenty komputerowe (*ang. computer emergency response teams – CERT*), zarówno publicznymi, jak i działającymi w sektorze prywatnym, w celu zapewnienia wymiany informacji dotyczących incydentów związanych z bezpieczeństwem systemów sterowania i środkami przeciwdziałania.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Zautomatyzowane mechanizmy i rozwiązania w zakresie zgłaszania incydentów związanych z bezpieczeństwem zwykle nie stanowią części systemów OT ani nie są z nimi połączone.

Zabezpieczenie rozszerzone: (3) Brak omówienia zabezpieczenia w kontekście systemów OT.

IR-7 WSPARCIE REAGOWANIA NA INCYDENTY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
IR-7	**Wsparcie reagowania na incydenty**	Wybrano	Wybrano	Wybrano
IR-7 (1)	*WSPARCIE REAGOWANIA NA INCYDENTY | AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

IR-8 PLAN REAGOWANIA NA INCYDENTY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
IR-8	**Plan reagowania na incydenty**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.9. UTRZYMANIE I WSPARCIE – KATEGORIA MA

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Utrzymanie i wsparcie”

Zautomatyzowane mechanizmy wykorzystywane do planowania, przeprowadzania i dokumentowania prac utrzymaniowych oraz działań związanych ze wsparciem zwykle nie stanowią części systemów OT ani nie są z nimi połączone.

W sytuacjach, gdy systemy OT nie obsługują rozwiązań w zakresie utrzymania i konserwacji wymaganych przez dane zabezpieczenie, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

MA-1 – POLITYKA I PROCEDURY

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
MA-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

MA-2 NADZÓR NAD UTRZYMANIEM

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
MA-2	**Nadzór nad utrzymaniem**	Wybrano	Wybrano	Wybrano
MA-2 (2)	*NADZÓR NAD UTRZYMANIEM | AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MA-3 NARZĘDZIA UTRZYMANIOWE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
MA-3	**Narzędzia utrzymaniowe**		Wybrano	Wybrano
MA-3 (1)	*NARZĘDZIA UTRZYMANIOWE | SPRAWDZANIE NARZĘDZI*		Wybrano	Wybrano
MA-3 (2)	*NARZĘDZIA UTRZYMANIOWE | SPRAWDZANIE NOŚNIKÓW DANYCH*		Wybrano	Wybrano
MA-3 (3)	*NARZĘDZIA UTRZYMANIOWE | ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MA-4 UTRZYMANIE ZDALNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	**Umiarkowany**	**Wysoki**
MA-4	**Utrzymanie zdalne**	Wybrano	Wybrano	Wybrano
MA-4 (1)	*UTRZYMANIE ZDALNE | AUDYT I PRZEGLĄD*		Dodano	Dodano
MA-4 (3)	*UTRZYMANIE ZDALNE | PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA*			**Wybrano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (3) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja może wymagać skorzystania ze zdalnych usług utrzymania, wsparcia i diagnostyki w celu odtworzenia podstawowych funkcji lub przywrócenia usług systemu OT. Przykładowe zabezpieczenia kompensacyjne obejmują ograniczenie zakresu usług konserwacyjnych i diagnostycznych do niezbędnego minimum oraz staranne monitorowanie i audytowanie prac realizowanych w ramach zdalnego utrzymania, a także zdalnej konserwacji i diagnostyki.

Uzasadnienie uwzględnienia zabezpieczenia MA-4 (1) w zakresie UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Działanie środowisk OT jest często w dużym stopniu uzależnione do usług zewnętrznych dostawców w zakresie utrzymania i konserwacji. Z tego powodu organizacje winny mieć możliwość analizy plików dziennika dotyczących prac konserwacyjnych.

MA-5 PERSONEL UTZRYMANIOWY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MA-5	**Personel utrzymaniowy**	Wybrano	Wybrano	Wybrano
MA-5 (1)	*PERSONEL UTRZYMANIOWY | OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MA-6 TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MA-6	**Terminowość przeprowadzania konserwacji**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MA-7 KONSERWACJA W TERENIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MA-7	**Konserwacja w terenie**	**Dodano**	**Dodano**	**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje winny wskazać systemy OT i komponenty systemów objęte szczególnymi wymogami dotyczącymi kalibracji, utrzymania lub innymi wymaganiami i ograniczyć zakres prac konserwacyjnych do określonych obiektów. Przykłady takich systemów mogą obejmować systemy o krytycznym znaczeniu dla bezpieczeństwa lub systemy, w których tolerancje dokładności są ograniczone i wymagane są dodatkowe kontrole jakości.

Uzasadnienie uwzględnienia środka bezpieczeństwa MA-7 w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Niektóre urządzenia OT są objęte szczególnymi wymaganiami dotyczącymi kalibracji, utrzymania i modyfikacji wynikającymi z przepisów, regulacji lub norm bezpieczeństwa. Zróżnicowanie lokalizacji może wpływać na jakość i dokładność prac utrzymaniowych w terenie.

F.7.10. OCHRONA NOŚNIKÓW DANYCH – KATEGORIA MP

MP-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-1	Polityka i procedury	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

MP-2 DOSTĘP DO NOŚNIKÓW DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-2	Dostęp do nośników danych	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MP-3 OZNAKOWANIE NOŚNIKÓW DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-3	Oznakowanie nośników danych		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MP-4 PRZECHOWYWANIE NOŚNIKÓW DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-4	Przechowywanie nośników danych		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MP-5 TRANSPORT NOŚNIKÓW DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-5	**Transport nośników danych**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MP-6 SANITYZACJA NOŚNIKÓW DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-6	**Sanityzacja nośników danych**	Wybrano	Wybrano	Wybrano
MP-6 (1)	*SANITYZACJA NOŚNIKÓW DANYCH | PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA*			Wybrano
MP-6 (2)	*SANITYZACJA NOŚNIKÓW DANYCH | TESTOWANIE SPRZĘTU*			Wybrano
MP-6 (3)	*SANITYZACJA NOŚNIKÓW DANYCH | TECHNIKI NIEDESTRUKCYJNE*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

MP-7 UŻYWANIE NOŚNIKÓW DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
MP-7	**Używanie nośników danych**	Wybrano	Wybrano	Wybrano

F.7.11. OCHRONA FIZYCZNA I ŚRODOWISKOWA – KATEGORIA PE

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Ochrona fizyczna i środowiskowa”

Zabezpieczenia należące do kategorii ochrony fizycznej i środowiskowej są często wykorzystywane w roli zabezpieczeń kompensacyjnych w przypadku wielu systemów OT, w związku z czym ich stosowanie jest szczególnie ważne. Każde zabezpieczenie kompensacyjne winno ograniczać ryzyko do akceptowalnego poziomu.

PE-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-1	Polityka i procedury	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT. Komponenty OT mogą być rozmieszczone na dużym obszarze zakładu lub geograficznym, zarazem mogą stanowić punkt dostępu do całej sieci OT w organizacji. W tym kontekście mogą także obowiązywać zabezpieczenia wynikające z przepisów i regulacji.

PE-2 ZEZWOLENIA NA DOSTĘP FIZYCZNY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-2	Zezwolenia na dostęp fizyczny	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-3 KONTROLA DOSTĘPU FIZYCZNEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-3	**Kontrola dostępu fizycznego**	**Wybrano**	**Wybrano**	**Wybrano**
PE-3 (1)	*KONTROLA DOSTĘPU FIZYCZNEGO | DOSTĘP DO SYSTEMU*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja winna uwzględniać wzajemne zależności pomiędzy różnymi aspektami bezpieczeństwa systemów OT oraz wymogi w zakresie dostępu do systemów w sytuacjach awaryjnych. W sytuacji awaryjnej organizacja może ograniczyć dostęp do obiektów i zasobów OT wyłącznie do upoważnionych osób. Systemy OT często obejmują urządzenia, które nie są wyposażone w kompleksowe funkcje kontroli dostępu ani nie są w stanie ich obsługiwać ze względu na restrykcyjne ograniczenia dotyczące bezpieczeństwa lub szybkości działania. Organizacja powinna zastosować zabezpieczenia dostępu fizycznego oraz środki bezpieczeństwa wchodzące w skład architektury obrony w głąb, jeśli jest to wymagane i możliwe w celu uzupełnienia zabezpieczeń systemów OT, gdy mechanizmy elektroniczne nie są w stanie zaspokoić wymagań bezpieczeństwa określonych w planie bezpieczeństwa organizacji.
Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-4 KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-4	**Kontrola dostępu do medium transmisyjnego**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-5 KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-5	**Kontrola dostępu do urządzeń wejścia - wyjścia**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-6 MONITOROWANIE DOSTĘPU FIZYCZNEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-6	**Monitorowanie dostępu fizycznego**	Wybrano	Wybrano	Wybrano
PE-6 (1)	*MONITOROWANIE DOSTĘPU FIZYCZNEGO | ALARMY WŁAMANIOWE I URZĄDZENIA NADZORUJĄCE*		Wybrano	Wybrano
PE-6 (4)	*MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW*		Dodano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) (4) Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie uwzględnienia zabezpieczenia PE-6 (4) w zakresie UMIARKOWANEGO poziomu wpływu: Wiele komponentów systemów OT znajduje się w odległych geograficznie i rozproszonych lokalizacjach. Wybrane komponenty systemów mogą być umieszczone pod sufitami, pod podłogą lub w szafach rozdzielczych. Zabezpieczenia dostępu fizycznego są wykorzystywane w wielu przypadkach w roli zabezpieczeń kompensacyjnych, gdy nie istnieje możliwość wykorzystania logicznych funkcji kontroli dostępu.

PE-8 REJESTRY DOSTĘPU GOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-8	**Rejestracja dostępu gości**	Wybrano	Wybrano	Wybrano
PE-8 (1)	*REJESTRY DOSTĘPU GOŚCI | AUTOMATYCZNA REJESTRACJA / PRZEGLĄD*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-9 WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-9	**Wyposażenie energetyczne i okablowanie**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-10 WYŁĄCZENIE AWARYJNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-10	**Wyłączenie awaryjne**		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Odłączenie zasilania niektórych systemów OT może być niemożliwe lub nie jest zalecane. Proces określania parametrów zabezpieczenia zdefiniowanych przez organizację powinien przebiegać w porozumieniu z pracownikami odpowiedzialnymi za bezpieczeństwo oraz za systemy OT. Przykładowe zabezpieczenia kompensacyjne obejmują projektowanie systemów, które w przypadku awarii powracają do ostatniego znanego bezpiecznego stanu oraz wdrożenie procedur awaryjnych.

PE-11 ZASILANIE AWARYJNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-11	**Zasilanie awaryjne**		Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-11 (1)	*ZASILANIE AWARYJNE | ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA*			Wybrano
PE-11 (2)	*ZASILANIE AWARYJNE | ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA*			

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-12 OŚWIETLENIE AWARYJNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-12	**Oświetlenie awaryjne**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-13 OCHRONA PRZECIWPOŻAROWA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-13	**Ochrona przeciwpożarowa**	**Wybrano**	**Wybrano**	**Wybrano**
PE-13 (1)	*OCHRONA PRZECIWPOŻAROWA | SYSTEMY DETEKCJI - AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE*		Wybrano	Wybrano
PE-13 (2)	*OCHRONA PRZECIWPOŻAROWA | SYSTEMY GASZĄCE - AUTOMATYCZNA AKTYWACJA I POWIADOMIENIE*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Systemy ochrony przeciwpożarowej powinny być dobierane z uwzględnieniem wymogów i charakterystyki środowiska OT. Na przykład stosowanie zraszaczy w wybranych środowiskach może stanowić poważne niebezpieczeństwo.

Zabezpieczenie rozszerzone: (1) (2) Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-14 ZABEZPIECZENIA ŚRODOWISKOWE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-14	**Zabezpieczenia środowiskowe**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Systemy sterowania temperaturą i wilgotnością powietrza stanowią zwykle elementy innych systemów OT (np. systemów ogrzewania, wentylacji i klimatyzacji, obsługujących procesy lub oświetleniowych), mogą także stanowić samodzielne i oddzielne systemy OT. Systemy OT mogą działać w ekstremalnych warunkach, zarówno wewnątrz budynków, jak i na zewnątrz. Parametry robocze – temperatura i wilgotność powietrza, a także parametry eksploatacji są określone w specyfikacji projektowej oraz danych technicznych systemów OT. Obwody zasilania, szafy dystrybucyjne, routery i przełączniki odpowiedzialne za obsługę systemów ochrony przeciwpożarowej i bezpieczeństwa pracowników muszą pracować w odpowiedniej temperaturze i wilgotności.
W przypadku braku możliwości wdrożenia zabezpieczeń środowiskowych, należy używać urządzeń zaprojektowanych z myślą o odporności na zagrożenia środowiskowe związane z danym systemem OT.

PE-15 OCHRONA PRZED ZALANIEM

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-15	**Ochrona przed zalaniem**	**Wybrano**	**Wybrano**	**Wybrano**
PE-15 (1)	*OCHRONA PRZED ZALANIEM | AUTOMATYCZNE WYKRYWANIE*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Ochrona przed zalaniem oraz wykorzystanie zaworów odcinających dopływ wody oraz izolujących poszczególne obwody stanowią działania stosowane w kontekście wybranych systemów OT. Systemy OT wykorzystywane w przemyśle produkcyjnym, elektrowniach wodnych, sektorze transportu, żeglugi oraz w przedsiębiorstwach wodno-kanalizacyjnych opierają się na

przemieszczaniu się wody i są projektowane z myślą o pracy z określoną ilością wody, a także ustalonych parametrach przepływu i ciśnienia. Obwody zasilania, szafy dystrybucyjne, routery i przełączniki, które obsługują systemy ochrony przeciwpożarowej i bezpieczeństwa pracowników powinny być zaprojektowane w taki sposób, by zalanie nie spowodowało awarii systemu (na przykład w przypadku pożaru, spryskiwacze nie powinny zalać serwerów sterujących systemem przeciwpożarowym, routerów lub przełączników ani nie spowodują zwarcia alarmów, systemów ewakuacyjnych, oświetlenia awaryjnego lub systemów gaśniczych).

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-16 DOSTAWA I USUWANIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-16	Dostawa i usuwanie	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-17 ZAPASOWE MIEJSCE PRACY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-17	Zapasowe miejsce pracy		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-18 LOKALIZACJA KOMPONENTÓW SYSTEMU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-18	Lokalizacja komponentów systemu			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PE-21 OCHRONA PRZED IMPULSEM ELEKTROMAGNETYCZNYM

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-21	**Ochrona przed impulsem elektromagnetycznym**			

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje wykorzystujące systemy OT mogą wdrożyć ochronę przed impulsem elektromagnetycznym w celu zapobiegania zagrożeniom agresywnym lub środowiskowym. Zachęcamy do stosowania wytycznych Krajowego Centrum Koordynacyjnego ds. Komunikacji (*ang. National Coordinating Center for Communications – NCC*) na temat ochrony przed impulsami elektromagnetycznymi (Guidelines on EM pulse protection).

PE-22 ZNAKOWANIE KOMPONENTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PE-22	**Znakowanie komponentów**		**Dodano**	**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Komponenty sprzętowe winne być oznaczone lub etykietowane w celu określenia informacji, które są przetwarzane, przechowywane lub przesyłane przy ich użyciu. Oznaczenia komponentów mogą być użyteczne w celu szybkiej identyfikacji systemów bezpieczeństwa i sterowania, urządzeń OT i IT oraz systemów połączonych z sieciami wewnętrznymi i zewnętrznymi. Oznaczenie komponentów zmniejsza prawdopodobieństwo wprowadzenia nieprawidłowej konfiguracji, niezamierzonej zmiany lub przeprowadzenia konserwacji niewłaściwego urządzenia.

Uzasadnienie uwzględnienia środka bezpieczeństwa PE-22 w zakresie UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Systemy OT są wyjątkowymi rozwiązaniami ze względu na fakt, że wyglądem mogą przypominać komponenty IT, jednocześnie realizując zupełnie inne funkcje. Wprowadzenie widocznych rozróżnień komponentów realizujących różne funkcje może pomóc w ograniczeniu liczby incydentów związanych z niezawodnością spowodowanych błędami dotyczącymi konserwacji i utrzymania.

F.7.12. PLANOWANIE – KATEGORIA PL

PL-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-1	Polityka i procedury	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

PL-2 PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-2	Plany bezpieczeństwa systemu ii ochrony prywatności	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Gdy systemy są ze sobą ściśle powiązane, niezbędna jest koordynacja planowania. System o niskim poziomie wypływu może bowiem wpływać niekorzystnie na system o wyższym poziomie wpływu.

PL-4 ZASADY POSTĘPOWANIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-4	Zasady postępowania	Wybrano	Wybrano	Wybrano
PL-4 (1)	*ZASADY POSTĘPOWANIA | MEDIA SPOŁECZNOŚCIOWE I OGRANICZENIA KORZYSTANIA ZE STRON / APLIKACJI ZEWNĘTRZNYCH*	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PL-7 KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-7	Koncepcja bezpieczeństwa działań operacyjnych			

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny rozważyć opracowanie procedur operacyjnych i zbadanie, w jaki sposób odnoszą się one do technologii IT i OT wykorzystywanych w danym środowisku eksploatacji.

PL-8 ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-8	**Architektury bezpieczeństwa i ochrony prywatności**		Wybrano	Wybrano
PL-8 (1)	*ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI | ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)*			

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Podejście oparte na obronie w głąb (lub obronie warstwowej) stanowi powszechną praktykę w obszarze architektur bezpieczeństwa środowisk OT.

PL-9 ZARZĄDZANIE CENTRALNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-10	**Wybór zabezpieczeń bazowych**	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Jeśli architektura zapewnia taką możliwość, należy rozważyć opcję centralnego zarządzania usuwaniem awarii, ochronę przed złośliwym kodem, a także rejestrowanie i wykrywanie incydentów.

PL-10 WYBÓR ZABEZPIECZEŃ BAZOWYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-10	**Wybór zabezpieczeń bazowych**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PL-11 DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PL-11	**Dostosowanie zabezpieczeń bazowych**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.13. PROGRAM BEZPIECZEŃSTWA INFORMACJI OBEJMUJĄCY CAŁĄ ORGANIZACJĘ

PROGRAMY ZARZĄDZANIA – KATEGORIA PM

Charakterystyka kategorii zabezpieczeń związanych z zarządzaniem programem bezpieczeństwa informacji obejmującym całą organizację

Zabezpieczenia związane z zarządzaniem programem bezpieczeństwa informacji w całej organizacji są wdrażane w celu wspierania realizacji programu bezpieczeństwa informacji. Nie są one powiązane z zabezpieczeniami bazowymi, a jednocześnie są niezależne od poszczególnych poziomów wpływu na system.

Wdrożenie tych zabezpieczeń powinno uwzględniać wyjątkowe właściwości systemów OT, wymagania dotyczące tych systemów, powiązania z innymi systemami oraz ich wpływ na inne programy związane z działaniem systemów OT, takie jak programy dotyczące bezpieczeństwa, wydajności, niezawodności czy odporności. W tym celu program bezpieczeństwa powinien opierać się na interdyscyplinarnych zespołach, które będą w stanie wypracować kompromis pomiędzy interesami, celami i zakresami odpowiedzialności, takimi jak możliwości, adaptowalność, odporność, bezpieczeństwo, ochrona, użyteczność i wydajność.

PM-1 PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*
PM-1	**Plan programu bezpieczeństwa informacji**

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-2 ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*
PM-2	**Role kierownicze programu bezpieczeństwa informacji**

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-3 ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-3	Zasoby w zakresie bezpieczeństwa informacji i ochrony prywatności

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-4 PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-4	Plan działania i etapy wprowadzania zabezpieczeń

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-5 INWENTARYZACJA SYSTEMU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-5	Inwentaryzacja systemu

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-6 MIARY WYDAJNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-6	Miary skuteczności

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-7 STRUKTURA ORGANIZACYJNA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-7	Struktura organizacyjna

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-8 PLAN INFRASTRUKTURY KRYTYCZNEJ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-8	Plan infrastruktury krytycznej

Brak omówienia zabezpieczenia w kontekście systemów OT.

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny zapoznawać się z wymogami i wytycznymi dotyczącymi ochrony określonymi w rozporządzeniach wykonawczych, wytycznych stosownych ministerstw i urzędów oraz organizacji sektorowych.

PM-9 STRATEGIA ZARZĄDZANIA RYZYKIEM

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-9	Strategia zarządzania ryzykiem

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-10 PROCES AUTORYZACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-10	Proces autoryzacji

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-11 DEFINICJA MISJI I PROCESU BIZNESOWEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-11	Definicja misji i procesu biznesowego

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-12 ZAGROŻENIA WEWNĘTRZNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-12	Zagrożenia wewnętrzne

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-13 PESONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-13	Personel bezpieczeństwa i ochrony prywatności

PM-14 TESTOWANIE, SZKOLENIA I MONITOROWANIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-14	Testowanie, szkolenia i monitorowanie

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-15 GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-15	Grupy i stowarzyszenia zajmujące się bezpieczeństwem i ochroną prywatności

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny być zaznajomione z działalnością grup oraz stowarzyszeń zajmujących się bezpieczeństwem i ochroną prywatności, w tym jednostek rządowych, centrów wymiany informacji i analiz, a także organizacji branżowych i sektorowych.

PM-16 OSTRZEGANIE O ZAGROŻENIACH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-16	Ostrzeganie o zagrożeniach

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny nawiązywać współpracę oraz udostępniać informacje na temat potencjalnych incydentów bez zbędnej zwłoki. CISA pełni funkcję scentralizowanej jednostki odpowiedzialnej za koordynowanie zagadnień związanych z bezpieczeństwem oraz komunikacją dotyczącą cyberbezpieczeństwa. Organizacje powinny rozważyć wdrożenie rozwiązań pozwalających na udostępnianie informacji jawnych, a także klasyfikowanych.

PM-17 OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-17	Ochrona nadzorowanych informacji jawnych przetwarzanych w systemach zewnętrznych

Omówienie zabezpieczenia w kontekście systemów OT: Zabezpieczenie to dotyczy jednostek rządowych oraz innych organizacji, które pracują z organami rządowymi i przetwarzają nadzorowane informacje jawne.

PM-18 PLAN PROGRAMU OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-18	Plan programu ochrony prywatności

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-19 ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-19	Role kierownicze programu ochrony prywatności

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-20 ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-20	Rozpowszechnianie informacji o programie ochrony prywatności
PM-20 (1)	*ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI | POLITYKA PRYWATNOŚCI PREZENTOWANE NA STRONACH INTERNETOWYCH, W APLIKACJACH I USŁUGACH CYFROWYCH*

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-21 REJESTROWANIE UJAWNIEŃ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-21	Rejestrowanie ujawnień

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-22 ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-22	Zarządzanie jakością danych osobowych

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-23 ORGAN ZARZĄDZANIA DANYMI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-23	Organ zarządzania danymi

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-24 RADA DS. INTEGRALNOŚCI DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-24	Rada ds. integralności danych

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-25 MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-25	Minimalizacja danych osobowych wykorzystywanych w testach, szkoleniach i badaniach

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-26 ZARZĄDZANIE SKARGAMI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-26	Zarządzanie skargami

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-27 SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-27	Sprawozdawczość w zakresie ochrony prywatności

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-28 OPRACOWYWANIE RAM RYZYKA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-28	Opracowywanie ram ryzyka

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-29 ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-29	Role kierownicze programu zarządzania ryzykiem

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-30 STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-30	Strategia zarządzania ryzykiem w łańcuchu dostaw
PM-30 (1)	*STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW | DOSTAWCY ELEMENTÓW KRYTYCZNYCH LUB ISTOTNYCH Z PUNKTU WIDZENIA MISJI*

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-31 STRATEGIA CIĄGŁEGO MONITORINGU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-31	Strategia ciągłego monitorowania

Brak omówienia zabezpieczenia w kontekście systemów OT.

PM-32 PRZEZNACZENIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*
PM-32	Przeznaczenie

Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.14. BEZPIECZEŃSTWO OSOBOWE – KATEGORIA PS

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Bezpieczeństwo osobowe”

Zapewnienie bezpieczeństwa pracowników wymaga współpracy między pracownikami odpowiedzialnymi za systemy OT oraz IT, a także pracowników działu bezpieczeństwa oraz działu kadr.

PS-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-1	Polityka i procedury	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

PS-2 OKREŚLANIE RYZYKA DLA STANOWISKA PRACY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-2	Określanie ryzyka dla stanowiska pracy	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje prywatne powinny opierać się na istniejących regulacjach sektorowych, przepisach prawa, zasadach i wytycznych w celu określenia ryzyka dla poszczególnych stanowisk pracy.

PS-3 DOBÓR PERSONELU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-3	Dobór personelu	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PS-4 ZAKOŃCZENIE ZATRUDNIENIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-4	Zakończenie zatrudnienia	Wybrano	Wybrano	Wybrano

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-4 (2)	*ZAKOŃCZENIE ZATRUDNIENIA | AUTOMATYCZNE POWIADAMIANIE*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PS-5 OBSADZENIE LUB PRZENIESIENIE STANOWISKA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-5	**Obsadzenie lub przeniesienie stanowiska**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PS-6 UMOWY DOSTĘPU / WSPÓŁPRACY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-6	**Umowy dostępu / współpracy**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PS-7 BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-7	**Bezpieczeństwo osobowe stron trzecich**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PS-8 SANKCJE PERSONALNE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-8	**Sankcje personalne**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

PS-9 OPISY STANOWISK PRACY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
PS-9	**Opisy stanowisk pracy**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.15. OCENA RYZYKA – KATEGORIA RA

Wiele organizacji opierających się na systemach OT opracowuje programy szacowania i oceny ryzyka, które można wykorzystać na potrzeby analizy ryzyka związanego z cyberbezpieczeństwem.

RA-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
RA-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

RA-2 KATEGORYZACJA BEZPIECZEŃSTWA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
RA-2	**Kategoryzacja bezpieczeństwa**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: W celu określenia poziomu wpływu systemów OT można odwołać się do wstępnych ocen ryzyka, ocen bezpieczeństwa funkcjonalnego i innych ocen ryzyka opracowanych przez organizację.

RA-3 SZACOWANIE RYZYKA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
RA-3	**Szacowanie ryzyka**	Wybrano	Wybrano	Wybrano
RA-3 (1)	*SZACOWANIE RYZYKA | SZACOWANIE RYZYKA ŁAŃCUCHA DOSTAW*	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

RA-5 MONITOROWANIE I SKANOWANIE PODATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
RA-5	**Monitorowanie i skanowanie podatności**	**Wybrano**	**Wybrano**	**Wybrano**

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
RA-5 (2)	*MONITOROWANIE I SKANOWANIE PODATNOŚCI | NADZOROWANIE WYKRYTYCH PODATNOŚCI*	Wybrano	Wybrano	Wybrano
RA-5 (4)	*MONITOROWANIE I SKANOWANIE PODATNOŚCI | WYKRYWANIE SKANOWANIA*			**Wybrano**
RA-5 (5)	*MONITOROWANIE I SKANOWANIE PODATNOŚCI | DOSTĘP UPRZYWILEJOWANY*		Wybrano	Wybrano
RA-5 (11)	*MONITOROWANIE I SKANOWANIE PODATNOŚCI | AUTOMATYCZNE ANALIZY TRENDÓW*	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Na podstawie szacowanego ryzyka organizacja winna określić sposoby monitorowania i skanowania podatności w zabezpieczeniach swojego systemu. Takie sposoby mogą obejmować aktywne skanowanie, pasywne monitorowanie lub zabezpieczenia kompensacyjne, w zależności od systemu. Analiza podatności może być przeprowadzona na przykład za pomocą systemu pasywnego monitorowania i kontroli wizualnej w celu aktualizacji inwentaryzacji zasobów. Inwentaryzację można następnie porównać z listami znanych podatności (np. informacjami CISA i krajową bazą danych dotyczących podatności na zagrożenia NIST). Produkcyjny system OT może wymagać wyłączenia przed przeprowadzeniem aktywnego skanowania. Skanowanie należy zaplanować w taki sposób, by odbywało się podczas planowanych przestojów, jeśli jest to możliwe. Jeśli narzędzia do skanowania podatności mają być wykorzystywane w sieciach innych niż OT, należy zachować szczególną ostrożność, aby nie nastąpiło przypadkowe skanowanie systemów i sieci OT. Automatyczne skanowanie sieci nie obejmuje łączności nieroutowalnej, na przykład komunikacji szeregowej. Zabezpieczenia kompensacyjne obejmują zbudowanie repliki lub symulowanie systemu w celu przeprowadzenia skanowania lub wykorzystywanie rozwiązań skanowania podatności działających na hostach.

Zabezpieczenie rozszerzone: (2) (5) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (4) Omówienie zabezpieczenia w kontekście systemów OT: Przykłady informacji wykrywanych w środowiskach OT mogą obejmować informacje o kluczowych pracownikach oraz dane techniczne związane z systemami i konfiguracjami. Lokalizacje, które mogą wymagać monitorowania lub skanowania, obejmują fora techniczne, blogi oraz strony internetowe producentów oraz dostawców.

Zabezpieczenie rozszerzone: (11) Omówienie zabezpieczenia w kontekście systemów OT: W przypadku organizacji rządowych wiążąca jest dyrektywa operacyjna CISA 20-01, która wymaga, by poszczególne jednostki władzy wykonawczej opracowały i opublikowały zasady ujawniania podatności dotyczących systemów i usług dostępnych przez Internet oraz utrzymywały procesy wspierające realizację tych zadań. Zasady ujawniania podatności mogą zostać wdrożone na szczeblu organizacji – nie muszą być ustalane dla każdego pojedynczego systemu. Organizacje rządowe oraz podmioty prywatne mogą zrealizować założenia tego zabezpieczenia poprzez utworzenie i monitorowanie skrzynki poczty elektronicznej oraz opublikowanie jej adresu na publicznej stronie internetowej, aby osoby zainteresowane mogły kontaktować się z organizacją w sprawie ujawnień.

RA-7 REAKCJA NA RYZYKO

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
RA-7	**Reakcja na ryzyko**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

RA-9 ANALIZA KRYTYCZNOŚCI

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
RA-9	**Analiza krytyczności**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

F.7.16. NABYWANIE SYSTEMU I USŁUG – KATEGORIA SA

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Nabywanie systemu i usług”

W sytuacjach, gdy systemy OT nie spełniają wymogów związanych z zabezpieczeniami w zakresie nabywania systemów i usług, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

SA-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

SA-2 PRZYDZIAŁ ZASOBÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-2	**Przydział zasobów**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-3 CYKL ŻYCIA SYSTEMU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-3	**Cykl życia systemu**	Wybrano	Wybrano	Wybrano
SA-3 (1)	*CYKL ŻYCIA SYSTEMU | ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM*			
SA-3 (3)	*CYKL ŻYCIA SYSTEMU | ODŚWIEŻANIE TECHNOLOGII*			

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Organizacje, które nie utrzymują lokalnych środowisk przedprodukcyjnych i korzystają z usług zewnętrznych integratorów powinny dołożyć wszelkich starań, by umowy zawierały zapisy mające na celu ograniczanie ryzyka związanego z bezpieczeństwem i prywatnością.

Zabezpieczenie rozszerzone: (3) Omówienie zabezpieczenia w kontekście systemów OT: Przewidywany okres eksploatacji systemów OT jest dłuższy niż w przypadku większości typowych komponentów IT. Należy uwzględnić odświeżenie technologii w procesie planowania budżetu, aby ograniczyć korzystanie z przestarzałych systemów, które stanowią zagrożenie dla bezpieczeństwa lub niezawodności.

SA-4 PROCES NABYCIA

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Zmienione poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SA-4	**Proces nabycia**	**Wybrano**	**Wybrano**	**Wybrano**
SA-4 (1)	*PROCES NABYCIA | WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ*		**Wybrano**	**Wybrano**
SA-4 (2)	*PROCES NABYCIA | PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ*		**Wybrano**	**Wybrano**
SA-4 (5)	*PROCES NABYCIA | KONFIGURACJA SYSTEMU, KOMPONENTÓW I USŁUG*			Wybrano
SA-4 (9)	*PROCES NABYCIA | FUNKCJE, PORTY, PROTOKOŁY / USŁUGI*		**Wybrano**	**Wybrano**
SA-4 (10)	*PROCES NABYCIA | WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW*	**Wybrano**	**Wybrano**	**Wybrano**
SA-4 (12)	*PROCES NABYCIA | WŁASNOŚĆ DANYCH*	Dodano	Dodano	Dodano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny nawiązać współpracę z producentami systemów OT, aby uświadamiać ich na temat potrzeb w zakresie cyberbezpieczeństwa. Projekt nabycia systemu SCADA/systemu sterowania *(ang. SCADA/Control Systems Procurement Project*) zawiera przykładowe wymagania w zakresie cyberbezpieczeństwa dotyczące systemu OT.

Zabezpieczenie rozszerzone: (1) (2) (9) Omówienie zabezpieczenia w kontekście systemów OT: Podczas nabywania systemów oraz komponentów systemu OT może okazać się, że kwestie dotyczące bezpieczeństwa nie zostały uwzględnione w projekcie. Osoby odpowiedzialne za nabycie systemów powinny rozważyć możliwość wyboru innych produktów, zakupu dodatkowych urządzeń lub zaplanowania zabezpieczeń kompensacyjnych.

Zabezpieczenie rozszerzone: (10) Omówienie zabezpieczenia w kontekście systemów OT: Wymóg korzystania z zatwierdzonych produktów dotyczy wyłącznie organizacji postępujących zgodnie z wytycznymi Memorandum OMB M-19-17 [OMB-M1917], takich jak organy rządowe czy wykonawcy. Przykładowe zabezpieczenia kompensacyjne obejmują wykorzystanie produktów umieszczonych w wykazie produktów zatwierdzonych FIPS 201 w celu realizacji funkcji uwierzytelniania w połączeniu z produktami OT.

Zabezpieczenie rozszerzone: (5) (12) Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie uwzględnienia zabezpieczenia SA-4 (12) w zakresie NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Dane wrażliwe lub własnościowe organizacji związane z systemami OT są często przekazywane wykonawcom w ramach pracy nad projektami oraz usług wsparcia. W związku z tym należy określić własność danych przed ich przekazaniem dostawcy lub integratorowi. Należy ustalić zakres udostępniania danych innym podmiotom oraz podjąć ustalenia dotyczące usuwania danych po zakończeniu projektu. Systemy OT obsługiwane przez wykonawców na zlecenie organizacji mogą być objęte tymi samymi wymogami (wynikającymi z przepisów, regulacji itp.) dotyczącymi własności i przechowywania danych.

SA-5 DOKUMENTACJA SYSTEMU

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SA-5	**Dokumentacja systemu**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-8 ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-8	**Zasady inżynierii bezpieczeństwa i ochrony prywatności**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-9 USŁUGI SYSTEMU ZEWNĘTRZNEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-9	**Usługi systemu zewnętrznego**	Wybrano	Wybrano	Wybrano
SA-9 (2)	*USŁUGI SYSTEMU ZEWNĘTRZNEGO | IDENTYFIKACJA FUNKCJI, PORTÓW, PROTOKOŁÓW I USŁUG*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-10 ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-10	**Zarządzanie konfiguracją dewelopera**		**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Pracownicy posiadający wiedzę na temat wymogów bezpieczeństwa i prywatności powinni uczestniczyć w procesie zarządzania zmianami w konfiguracji dewelopera.

SA-11 TESTOWANIE I OCENA PRZEZ DEWELOPERA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-11	**Testowanie i ocena przez dewelopera**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-15 PROCES ROZWOJU, STANDARDY I NARZĘDZIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-15	**Proces rozwoju, standardy i narzędzia**		Wybrano	Wybrano
SA-15 (3)	*PROCES ROZWOJU, NORMY I NARZĘDZIA | ANALIZA KRYTYCZNOŚCI*		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-16 SZKOLENIA PROWADZONE PRZEZ DEWELOPERA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-16	**Szkolenia prowadzone przez dewelopera**			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-17 ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-17	**Architektura oraz projekt bezpieczeństwa i ochrony prywatności dewelopera**			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-21 DOBÓR DEWELOPERÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-21	**Dobór deweloperów**			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SA-22 KOMPONENTY SYSTEMU BEZ WSPARCIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SA-22	**Komponenty systemu bez wsparcia**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: W skład systemów OT mogą wchodzić komponenty, które nie są już objęte wsparciem dewelopera, producenta lub dostawcy i nie zostały dotychczas wymienione ze względów operacyjnych, bezpieczeństwa, dostępności lub okresu eksploatacji. Organizacja powinna wskazać alternatywne metody wsparcia i utrzymania takich komponentów systemu i rozważyć wdrożenie dodatkowych zabezpieczeń kompensacyjnych w celu ograniczenia wpływu znanych zagrożeń i podatności na komponenty systemu bez wsparcia.

F.7.17. OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH – KATEGORIA SC

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Ochrona systemów i sieci telekomunikacyjnych”

Organizacje powinny wdrażać rozwiązania kryptograficzne wyłącznie po przeprowadzeniu kompleksowej analizy potrzeb w zakresie bezpieczeństwa i potencjalnego wpływu takich rozwiązań na wydajność systemu. Organizacja powinna na przykład przeanalizować, czy opóźnienia wynikające z zastosowania metod kryptograficznych mogą mieć negatywny wpływ na wydajność systemów OT. Choć starsze urządzenia, które wciąż występują w wielu systemach OT, nie są wyposażone w funkcje kryptograficzne i nie są w stanie obsługiwać szyfrowania, organizacje mogą zastosować zabezpieczenia kompensacyjne, na przykład enkapsulację takich urządzeń i systemów, by zrealizować wymogi danego zabezpieczenia.

W sytuacjach, gdy systemy OT nie obsługują rozwiązań wymaganych przez zabezpieczenia dotyczące ochrony systemów i sieci telekomunikacyjnych, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

SC-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-1	Polityka i procedury	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

SC-2 ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-2	Rozdzielenie funkcjonalności systemu i użytkownika		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Rozdzielenie fizyczne

funkcjonalności obejmuje wykorzystywanie oddzielnych systemów do zarządzania systemami OT oraz do obsługi komponentów OT. Separacja logiczna obejmuje wykorzystywanie różnych kont użytkowników przez administratorów i operatorów. Przykładowe zabezpieczenia kompensacyjne obejmują szczegółowe audytowanie.

SC-3 IZOLACJA FUNKCJI BEZPIECZEŃSTWA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-3	Izolacja funkcji bezpieczeństwa			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny rozważyć wdrożenie tego zabezpieczenia na etapie projektowania nowych architektur lub aktualizacji istniejących komponentów. Przykładowe zabezpieczenia kompensacyjne obejmują kontrolę dostępu.

SC-4 INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-4	Informacje na współdzielonych zasobach systemowych		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Stosowanie tego zabezpieczenia jest szczególnie istotne w przypadku systemów OT, które przetwarzają wrażliwe dane. Przykładowe zabezpieczenia kompensacyjne obejmują projektowanie systemu OT w taki sposób, by zapobiec współdzieleniu zasobów systemowych.

SC-5 OCHRONA PRZED BLOKADĄ USŁUG (DoS)

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-5	Ochrona przed blokadą usług (DoS)	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Niektóre urządzenia i komponenty systemów OT mogą być bardziej podatne na ataki blokady usług (DoS) ze względu na dużą zależność pewnych procesów od czasu. Na podstawie analizy opartej na ryzyku organizacja powinna ustalić priorytetowe obszary ochrony przed

atakami DoS oraz ustanowić stosowne zasady i procedury.

SC-7 OCHRONA POŁĄCZEŃ BRZEGOWYCH

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Zmienione poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SC-7	**Ochrona połączeń brzegowych**	Wybrano	Wybrano	Wybrano
SC-7 (3)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | PUNKTY DOSTĘPOWE*		Wybrano	Wybrano
SC-7 (4)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE*		Wybrano	Wybrano
SC-7 (5)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK*		Wybrano	Wybrano
SC-7 (7)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | DZIELONE TUNELOWANIE DLA URZĄDZEŃ ZDALNYCH*		Wybrano	Wybrano
SC-7 (8)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY*		Wybrano	Wybrano
SC-7 (18)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | BŁĄD BEZPIECZEŃSTWA*		**Dodano**	**Wybrano**
SC-7 (21)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA ELEMENTÓW SYSTEMU*			Wybrano
SC-7 (28)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | POŁĄCZENIA Z SIECIAMI PUBLICZNYMI*	**Dodano**	**Dodano**	**Dodano**
SC-7 (29)	*OCHRONA POŁĄCZEŃ BRZEGOWYCH | SEPARACJA PODSIECI W CELU ODIZOLOWANIA FUNKCJI*	**Dodano**	**Dodano**	**Dodano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (3) (4) (5) (7) (8) (21) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (18) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja powinna ustalić najbardziej odpowiedni tryb awarii – na przykład zezwolenie na dowolny ruch lub zablokowanie całej łączności.

Zabezpieczenie rozszerzone: (28) Omówienie zabezpieczenia w kontekście systemów OT: Organizacje winny rozważyć potrzebę bezpośredniego połączenia poszczególnych systemów OT z sieciami publicznymi, biorąc pod uwagę potencjalne korzyści, dodatkowe wektory zagrożeń i potencjalne negatywne skutki związane z każdym rodzajem połączenia i dostępu.

Zabezpieczenie rozszerzone: (29) Omówienie zabezpieczenia w kontekście systemów OT: Zastosowanie podsieci pozwala na izolację funkcji o niskim poziomie ryzyka od funkcji o wysokim poziomie ryzyka, a także funkcji sterowania oraz bezpieczeństwa. Podsieci powinny być stosowane wyłącznie w połączeniu z innymi technikami ochrony połączeń brzegowych.

Uzasadnienie uwzględnienia zabezpieczenia SC-7 (18) w zakresie UMIARKOWANEGO poziomu wpływu: Możliwość wyboru trybu awarii fizycznych elementów sieci OT odróżnia systemy OT od systemów IT. Dokonanie odpowiedniego wyboru może mieć kluczowy wpływ na złagodzenie skutków awarii.

Uzasadnienie uwzględnienia zabezpieczenia SC-7 (28) w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Dostęp do systemów oraz komponentów systemów OT powinien być ograniczony wyłącznie do osób, w przypadku których jest niezbędny w celu wykonywania pracy i prawidłowego działania systemu. Połączenia między systemami OT i sieciami publicznymi mają ograniczone zastosowanie w środowiskach OT, jednocześnie prowadząc do znaczącego wzrostu potencjalnego ryzyka.

Uzasadnienie uwzględnienia zabezpieczenia SC-7 (29) w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: W środowiskach OT stosowanie podsieci i podział na strefy stanowią powszechne praktyki w zakresie izolacji funkcji.

SC-8 POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-8	**Poufność i integralność transmisji**		Wybrano	Wybrano
SC-8 (1)	*POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OCHRONA KRYPTOGRAFICZNA*		**Wybrano**	**Wybrano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Tłumaczenie

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Zakładając transmisję danych i informacji przez niezaufane segmenty sieci, organizacja winna rozważyć zastosowanie wszystkich dostępnych mechanizmów ochrony integralności opartych na rozwiązaniach kryptograficznych (np. podpis cyfrowy, stosowanie funkcji skrótów) w celu ochrony poufności i integralności informacji. Przykładowe zabezpieczenia kompensacyjne obejmują zabezpieczenia fizyczne, takie jak bezpieczne przepusty (połączenie punkt-punkt) między dwoma komponentami systemu.

SC-10 ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-10	**Zakończenie połączenia sieciowego**		~~Usunięto~~	~~Usunięto~~

Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie usunięcia środka bezpieczeństwa SC-10 z UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Cel niniejszego zabezpieczenia został przedstawiony w opisie zabezpieczenia rozszerzonego AC-17 (9) dla systemów OT.

SC-12 GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-12	**Generowanie i zarządzanie kluczami kryptograficznymi**	Wybrano	Wybrano	Wybrano
SC-12 (1)	*GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | DOSTĘPNOŚĆ*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SC-13 OCHRONA KRYPTOGRAFICZNA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-13	**Ochrona kryptograficzna**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SC-15 WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa Nazwa zabezpieczenia rozszerzonego:	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-15	**Współpracujące urządzenia i aplikacje**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SC-17 CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-17	**Certyfikaty infrastruktury klucza publicznego**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SC-18 KOD MOBILNY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-18	**Kod mobilny**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SC-20 BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-20	**Bezpieczeństwo nazw domen / adresów IP (autentyczność pochodzenia)**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Bezpieczne usługi nazw domen i adresów należy wdrożyć wyłącznie po przeprowadzeniu stosownych analiz oraz ustaleniu, że ich zastosowanie nie wpłynie negatywnie na wydajność systemów OT.

SC-21 BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-21	**Bezpieczeństwo nazw domen / usługa ustalania adresu IP**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Bezpieczne usługi nazw domen i adresów należy wdrożyć wyłącznie po przeprowadzeniu stosownych analiz oraz ustaleniu, że ich zastosowanie nie wpłynie negatywnie na wydajność systemów OT.

SC-22 ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-22	Architektura nazw domen / adresów IP / zamawianie usługi DNS	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Bezpieczne usługi nazw domen i adresów należy wdrożyć wyłącznie po przeprowadzeniu stosownych analiz oraz ustaleniu, że ich zastosowanie nie wpłynie negatywnie na wydajność systemów OT.

SC-23 AUTENTYCZNOŚĆ SESJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-23	Autentyczność sesji		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują funkcje audytu.

SC-24 PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-24	Przejście do określonego stanu systemu po błędzie		Dodano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Jednym z obszarów odpowiedzialności organizacji jest wybór odpowiedniego stanu, do którego przechodzi system w przypadku awarii. Gromadzenie informacji o stanie systemów OT obejmuje zapewnienie spójności zmiennych dotyczących stanów systemów OT z fizycznym stanem systemu OT (np. informacji o tym, czy zawory są otwarte lub zamknięte, czy łączność jest dozwolona lub zablokowana, czy proces przebiega prawidłowo).

Uzasadnienie uwzględnienia środka bezpieczeństwa SC-24 w ramach UMIARKOWANEGO poziomu wpływu: W ramach architektury i projektu systemu OT

organizacja powinna dokonać wyboru stosownego stanu systemu na podstawie funkcji systemu OT oraz jego środowiska eksploatacji. Możliwość wyboru trybu, do którego przejdą fizyczne komponenty systemów OT w przypadku awarii odróżnia systemy OT od systemów IT. Dokonanie odpowiedniego wyboru może mieć kluczowy wpływ na złagodzenie skutków awarii, która może wpłynąć na realizowane procesy fizyczne (na przykład awaria zaworów w pozycji zamkniętej może zakłócić działanie chłodzenia systemu).

SC-28 OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SC-28	**Ochrona danych w składowaniu / Kopie konfiguracji systemu**		**Wybrano**	**Wybrano**
SC-28 (1)	*OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | OCHRONA KRYPTOGRAFICZNA*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Rozwiązania oparte na mechanizmach kryptograficznych należy wdrożyć wyłącznie po przeprowadzeniu stosownych analiz oraz ustaleniu, że ich zastosowanie nie wpłynie negatywnie na wydajność systemów OT. W sytuacji, w której wykorzystanie mechanizmów kryptograficznych okaże się niemożliwe w przypadku wybranych komponentów systemów OT, stosowne zabezpieczenia kompensacyjne mogą obejmować przeniesienie danych do lokalizacji, która obsługuje mechanizmy kryptograficzne.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

SC-32 DZIELENIE SYSTEMU NA PARTYCJE

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SC-32	**Dzielenie systemu na partycje**			
SC-32 (1)	*DZIELENIE SYSTEMU NA PARTYCJE | FIZYCZNE WYDZIELONE DOMENY DLA FUNKCJI UPRZYWILEJOWANYCH*			

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny rozważyć fizyczne rozdzielenie domen dla funkcji uprzywilejowanych, w tym funkcji wpływających na bezpieczeństwo systemów.

SC-39 IZOLACJA PROCESÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-39	Izolacja procesów	Wybrano	Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują wydzielanie procesów w celu realizowania ich za pośrednictwem innych platform.

SC-41 DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA/WYJŚCIA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-41	Dostęp do portów i urządzeń wejścia / wyjścia	Dodano	Dodano	Dodano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie uwzględnienia środka bezpieczeństwa SC-41 w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Zakres funkcji systemów OT jest zwykle określany odgórnie i nie ulega częstym zmianom.

SC-45 SYNCHRONIZACJA CZASU SYSTEMOWEGO

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-45	Synchronizacja czasu systemowego	Dodano	Dodano	Dodano
SC-45 (1)	*SYNCHRONIZACJA CZASU SYSTEMOWEGO | SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA*			

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje winny koordynować synchronizację czasu w systemach OT, aby zapewnić możliwości ustalania przyczyn problemów oraz prowadzenie dochodzeń w przypadku incydentu.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Synchronizacja z autoryzowanym źródłem czasu odniesienia może stanowić zabezpieczenie w sytuacji, gdy gromadzone dane są zestawiane z danymi systemów znajdującymi się poza granicami organizacji. Systemy OT powinny wykorzystywać znaczniki czasu oparte na stosownych mechanizmach i standardach, takich jak GPS lub IEEE 1588.

Uzasadnienie uwzględnienia środka bezpieczeństwa SC-45 w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Względny czas systemowy może stanowić ważny element zapewniania bezpieczeństwa oraz niezawodnej realizacji podstawowych funkcji systemów OT. Synchronizacja czasu może również usprawnić analizę przyczyn awarii i zdarzeń dzięki zapewnieniu, że dzienniki audytu pochodzące z różnych systemów opierają się na tym samym czasie, co pozwala na skorelowanie zdarzeń występujących jednocześnie w wielu systemach.

SC-47 ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Zmienione poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SC-47	**Alternatywne ścieżki komunikacyjne**			**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Organizacje powinny ustalić wykaz systemów wymagających alternatywnych ścieżek komunikacyjnych w celu zapewnienia, że utrata łączności nie będzie w stanie spowodować utraty wglądu w proces lub utraty możliwości sterowania, a także incydentu bezpieczeństwa.

Uzasadnienie uwzględnienia środka bezpieczeństwa SC-47 w ramach WYSOKIEGO poziomu wpływu: Aby zapewnić ciągłość działania podczas incydentu, organizacje powinny rozważyć ustanowienie alternatywnych ścieżek komunikacyjnych do celów kierowania i sterowania (*ang. command-and-control*), aby umożliwić podejmowanie i prowadzenie działań dotyczących systemów o wysokim poziomie wpływu, gdy utrata dostępności lub integralności może spowodować poważne lub katastrofalne negatywne skutki, w tym dotyczące bezpieczeństwa i świadczenia usług krytycznych.

SC-51 OCHRONA SPRZĘTOWA

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SC-51	**Ochrona sprzętowa**			

Omówienie zabezpieczenia w kontekście systemów OT: Niektóre systemy OT zapewniają funkcję ochrony przed zapisem opartą na fizycznych przełącznikach blokady zapisu wymagających użycia klucza lub zmiany pozycji. Organizacje powinny określić wykaz systemów, w których należy włączyć ochronę przed zapisem, a także opracować proces wyłączania trybu ochrony przed zapisem w systemie.

F.7.18. INTEGRALNOŚĆ SYSTEMU I INFORMACJI – KATEGORIA SI

Informacje dotyczące dostosowywania zabezpieczeń należących do kategorii „Integralność systemu i informacji”

W sytuacjach, gdy systemy OT nie obsługują rozwiązań wymaganych przez zabezpieczenia dotyczące zapewnienia integralności systemu i informacji, należy zastosować zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa. Przykłady zabezpieczeń kompensacyjnych są podane w opisie każdego środka bezpieczeństwa.

SI-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady winny odnosić się do wyjątkowych właściwości systemów OT oraz wynikających z nich wymagań, a także powiązań z systemami innymi niż systemy OT.

SI-2 USUWANIE USTEREK

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-2	**Usuwanie usterek**	**Wybrano**	**Wybrano**	**Wybrano**
SI-2 (2)	*USUWANIE USTEREK | ZAUTOMATYZOWANE USUWANIE USTEREK*		Wybrano	Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Usuwanie usterek i instalowanie poprawek bywa złożonym procesem, ponieważ wiele systemów OT pracuje pod kontrolą systemów operacyjnych oraz wykorzystuje oprogramowanie, które nie jest już wspierane przez producenta. Operatorzy OT mogą również nie mieć odpowiednich możliwości testowania poprawek, w związku z czym mogą musieć polegać na dostawcach w zakresie testowania poprawności działania poprawki. W niektórych sytuacjach organizacje mogą być zmuszone do zaakceptowania dodatkowego ryzyka, jeśli nie są dostępne poprawki producenta, instalacja poprawek wymaga dodatkowego czasu na ukończenie weryfikacji lub testów, lub jeśli wymaga

zatrzymania procesów i przestoju systemu. W takich sytuacjach należy wdrożyć zabezpieczenia kompensacyjne (np. ograniczyć narażenie podatnego systemu, ograniczyć podatne usługi, wdrożyć poprawki na poziomie wirtualnym). Należy także rozważyć wdrożenie innych zabezpieczeń kompensacyjnych, które nie zmniejszają ryzyka szczątkowego, lecz poprawiają zdolność reagowania, na przykład poprzez zapewnienie szybszej reakcji w przypadku wystąpienia incydentu, a także opracowanie planu zapewniającego możliwość wykrycia wykorzystania podatności w systemie OT. Testowanie poprawek dotyczących systemów OT może być niemożliwe przy wykorzystaniu zasobów dostępnych dla danej organizacji.

Zabezpieczenie rozszerzone: (2) Brak omówienia zabezpieczenia w kontekście systemów OT.

SI-3 ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-3	**Zabezpieczenie przed złośliwym kodem**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Rozwiązania w zakresie ochrony przed złośliwym kodem należy wdrożyć wyłącznie po przeprowadzeniu stosownych analiz oraz ustaleniu, że ich zastosowanie nie wpłynie negatywnie na wydajność systemów OT. Tego rodzaju narzędzia należy skonfigurować w taki sposób, by zminimalizować ich potencjalny wpływ na systemy OT (na przykład domyślnym zachowaniem powinno być stosowanie powiadomień zamiast kwarantanny). Przykładowe zabezpieczenia kompensacyjne obejmują zwiększone monitorowanie ruchu i audyty.

SI-4 MONITOROWANIE SYSTEMU

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-4	**Monitorowanie systemu**	**Wybrano**	**Wybrano**	**Wybrano**
SI-4 (2)	*MONITOROWANIE SYSTEMU | AUTOMATYCZNE NARZĘDZIA I MECHANIZMY ANALIZY W CZASIE RZECZYWISTYM*		**Wybrano**	**Wybrano**

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-4 (4)	*MONITOROWANIE SYSTEMU | WEJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY*		Wybrano	Wybrano
SI-4 (5)	*MONITOROWANIE SYSTEMU | ALERTY SYSTEMOWE*		**Wybrano**	**Wybrano**
SI-4 (10)	*MONITOROWANIE SYSTEMU | INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW*			Wybrano
SI-4 (12)	*MONITOROWANIE SYSTEMU | AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ*			Wybrano
SI-4 (14)	*MONITOROWANIE SYSTEMU | WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH*			Wybrano
SI-4 (20)	*MONITOROWANIE SYSTEMU | UPRZYWILEJOWANI UŻYTKOWNICY*			Wybrano
SI-4 (22)	*MONITOROWANIE SYSTEMU | NIEAUTORYZOWANE USŁUGI SIECIOWE*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: Organizacja musi zapewnić, że stosowanie narzędzi i technik monitorowania nie wpłynie negatywnie na wydajność i działanie systemów OT. Przykładowe zabezpieczenia kompensacyjne obejmują wdrożenie stosownych mechanizmów monitorowania sieci, procesów i dostępu fizycznego.

Zabezpieczenie rozszerzone: (2) Omówienie zabezpieczenia w kontekście systemów OT: W sytuacji, w której system OT nie może zostać skonfigurowany w sposób umożliwiający stosowanie zautomatyzowanych narzędzi do analizy zdarzeń w czasie zbliżonym do rzeczywistego, należy zastosować niezautomatyzowane mechanizmy lub procedury jako zabezpieczenia kompensacyjne opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa.

Zabezpieczenie rozszerzone: (4) (10) (12) (14) (20) (22) Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (5) Omówienie zabezpieczenia w kontekście systemów OT: Przykładowe zabezpieczenia kompensacyjne obejmują ręczne generowanie alertów.

SI-5 ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-5	**Alerty bezpieczeństwa, porady i dyrektywy**	**Wybrano**	**Wybrano**	**Wybrano**
SI-5 (1)	*ALERTY BEZPIECZEŃSTWA, PORADY | AUTOMATYCZNE ALERTY I ZALECENIA*			Wybrano

Omówienie zabezpieczenia w kontekście systemów OT: CISA publikuje alerty bezpieczeństwa i informacje dotyczące systemów OT na swojej stronie https://www.cisa.gov/uscert/ics. Centra wymiany informacji i analiz zajmujące się poszczególnymi sektorami często opracowują stosowne informacje oraz alerty, które można znaleźć na stronie https://www.nationalisacs.org/.

Zabezpieczenie rozszerzone: (1) Brak omówienia zabezpieczenia w kontekście systemów OT.

SI-6 WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-6	**Weryfikacja funkcji bezpieczeństwa i ochrony prywatności**			**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Po stwierdzeniu wystąpienia anomalii ponowne uruchomienie systemu OT może być niemożliwe. Z tego powodu należy planować takie działania zgodnie z wymaganiami operacyjnymi dotyczącymi systemów OT.

SI-7 APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-7	**Aplikacje, oprogramowanie układowe i integralność informacji**		**Wybrano**	**Wybrano**
SI-7 (1)	*APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | KONTROLE INTEGRALNOŚCI*		**Wybrano**	**Wybrano**

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-7 (2)	*APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI*			**Wybrano**
SI-7 (5)	*APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI*			**Wybrano**
SI-7 (7)	*APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | INTEGRACJA WYKRYWANIA I ODPOWIEDZI*		**Wybrano**	**Wybrano**
SI-7 (15)	*APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTORYZACJA KODU*			**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Do zakresu odpowiedzialności organizacji należy określenie, czy korzystanie z rozwiązań umożliwiających weryfikację integralności może wpływać negatywnie na działanie systemu sterowania przemysłowego. W takim wypadku organizacja powinna wdrożyć zabezpieczenia kompensacyjne, takie jak ręczne weryfikacje integralności, które nie wpływają na wydajność systemu.

Zabezpieczenia rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Organizacja musi zapewnić, że stosowanie narzędzi i technik weryfikacji integralności nie wpłynie negatywnie na wydajność i działanie systemów OT.

Zabezpieczenie rozszerzone: (2) Omówienie zabezpieczenia w kontekście systemów OT: Gdy wdrożenie automatycznych narzędzi weryfikujących integralność jest niemożliwe, należy wdrożyć niezautomatyzowane mechanizmy lub procedury. Przykładowe zabezpieczenia kompensacyjne obejmują przeprowadzanie planowych ręcznych inspekcji w celu wykrycia naruszeń integralności.

Zabezpieczenie rozszerzone: (5) Omówienie zabezpieczenia w kontekście systemów OT: Po stwierdzeniu wystąpienia anomalii ponowne uruchomienie systemu sterowania przemysłowego może być niemożliwe. Z tego powodu należy planować takie działania zgodnie z wymaganiami operacyjnymi dotyczącymi systemów ICS.

Zabezpieczenie rozszerzone: (7) Omówienie zabezpieczenia w kontekście systemów OT: Gdy system sterowania przemysłowego nie jest wyposażony w funkcje umożliwiające automatyczne wykrywanie nieautoryzowanych zmian istotnych dla bezpieczeństwa, należy wdrożyć zabezpieczenia kompensacyjne, takie jak niezautomatyzowane mechanizmy lub procedury, opracowane zgodnie z ogólnymi wytycznymi dotyczącymi dostosowywania środków bezpieczeństwa.

Zabezpieczenie rozszerzone: (15) Omówienie zabezpieczenia w kontekście systemów OT: Autoryzacja kodu daje pewność, że aplikacje oraz oprogramowanie układowe w systemach OT nie padły ofiarą sabotażu. Jeśli zautomatyzowane mechanizmy autoryzacji kodu nie są dostępne lub nie mogą zostać wykorzystane, organizacje mogą autoryzować kod za pomocą szeregu technik, w tym weryfikacji skrótów kryptograficznych, pobierania oprogramowania z zaufanych źródeł, weryfikacji numerów wersji u źródła lub testowania aplikacji i oprogramowania układowego w środowiskach offline lub testowych.

SI-8 OCHRONA PRZED SPAMEM

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-8	**Ochrona przed spamem**		**Wybrano**	**Wybrano**
SI-8 (2)	*OCHRONA PRZED SPAMEM | AUTOMATYCZNE AKTUALIZACJE*		~~Usunięto~~	~~Usunięto~~

Omówienie zabezpieczenia w kontekście systemów OT: Wdrożenie ochrony przed spamem w systemach OT polega na wyłączeniu mechanizmów, funkcji oraz usług (w tym poczty elektronicznej czy przeglądarek internetowych) na poszczególnych urządzeniach i komponentach systemów OT.

Uzasadnienie usunięcia zabezpieczenia SI-8 (2) z UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Mechanizmy wykorzystywane w celu przesyłania i dostarczania spamu winny być wyłączone lub usunięte w systemach OT, zatem automatyczne aktualizacje nie są konieczne.

SI-10 WERYFIKACJA WPROWADZANYCH INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-10	**Weryfikacja wprowadzanych informacji**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SI-11 OBSŁUGA BŁĘDÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-11	**Obsługa błędów**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SI-12 ZARZĄDZANIE I RETENCJA DANYCH

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-12	**Zarządzanie i retencja danych**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SI-13 PRZEWIDYWANIE AWARII

Nr Zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-13	**Przewidywanie awarii**			Dodano

Brak omówienia zabezpieczenia w kontekście systemów OT.

Uzasadnienie uwzględnienia środka bezpieczeństwa SI-13 w ramach WYSOKIEGO poziomu wpływu: Systemy OT są projektowane i realizowane z uwzględnieniem pewnych warunków oraz założeń dotyczących środowiska eksploatacji oraz trybu pracy. Wiele systemów OT podlega znacznie dłuższej eksploatacji niż inne typowe systemy, co może spowodować ujawnienie wad ukrytych, które byłyby niewidoczne w innych środowiskach i warunkach. Błąd przepełnienia zakresu liczb całkowitych może nigdy nie wystąpić w systemach, które są uruchamiane ponownie z odpowiednią częstotliwością, co uniemożliwia wystąpienie błędu. Zarówno doświadczenia, jak i dochodzenia

przeprowadzone w następstwie anomalii i incydentów w systemach OT mogą doprowadzić do wskazania pewnych problemów, które były nieznane i nie zostały przewidziane.
W takich sytuacjach zalecane jest wdrożenie stosownych działań zapobiegawczych oraz naprawczych (np. ponowne uruchomienie systemu lub aplikacji), jednak ich stosowanie może być niemożliwe ze względu na wymogi dotyczące środowisk i systemów OT.

SI-16 OCHRONA PAMIĘCI

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-16	**Ochrona pamięci**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SI-17 PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Zmienione poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SI-17	**Procedury testowania awaryjnego**	**Dodano**	**Dodano**	**Dodano**

Omówienie zabezpieczenia w kontekście systemów OT: Wybrane warunki wystąpienia awarii oraz stosowne odpowiadające im procedury mogą być różne w zależności od określonego poziomu bazowego. To samo zdarzenie może wywołać różne reakcje w zależności od poziomu wpływu. W celu realizacji procedur testowania awaryjnego można wykorzystać mechaniczne i analogowe systemy. Stany awaryjne powinny uwzględniać potencjalny wpływ na bezpieczeństwo ludzi, systemy fizyczne i środowisko. Dodatkowe wytyczne znajdują się w opisie powiązanego środka bezpieczeństwa CP-6.

Uzasadnienie uwzględnienia środka bezpieczeństwa SI-17 w ramach NISKIEGO, UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Celem tego zabezpieczenia jest ustanowienie w organizacji ram pozwalających na określenie zasad i procedur postępowania w przypadku wystąpienia awarii i innych incydentów. Opracowanie i udokumentowanie procesu decyzyjnego dotyczącego incydentów i sposobów reagowania w obliczu zmian w środowisku eksploatacji stanowi element procesu zarządzania ryzykiem.

SI-22 RÓŻNICOWANIE INFORMACJI

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SI-22	Różnicowanie informacji			

Omówienie zabezpieczenia w kontekście systemów OT: Wiele systemów OT przetwarza zróżnicowane informacje w celu osiągania zadanej niezawodności. Niektóre przykłady zróżnicowanych informacji występujących w systemach OT obejmują odpytywanie czujników oraz określanie stanu systemu.

F.7.19. ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW – KATEGORIA SR

SR-1 POLITYKA I PROCEDURY

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-1	**Polityka i procedury**	**Wybrano**	**Wybrano**	**Wybrano**

Omówienie zabezpieczenia w kontekście systemów OT: Zasady i procedury dotyczące łańcucha dostaw związanego z systemami OT powinny uwzględniać zarówno otrzymane, jak i wyprodukowane komponenty. Wiele systemów OT opiera się na starszych komponentach, które nie są w stanie sprostać oczekiwaniom nowoczesnego łańcucha dostaw. Należy opracować odpowiednie zabezpieczenia kompensacyjne starszych systemów, które umożliwią spełnianie wymogów i oczekiwań łańcucha dostaw organizacji.

SR-2 PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-2	**Plan zarządzania ryzykiem w łańcuchu dostaw**	Wybrano	Wybrano	Wybrano
SR-2 (1)	*PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW | POWOŁANIE ZESPOŁU ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW*	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SR-3 ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Zmienione poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-3	**Zabezpieczenia i procesy w łańcuchu dostaw**	Wybrano	Wybrano	Wybrano
SR-3 (1)	*ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | ZRÓŻNICOWANA BAZA DOSTAW*			

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Korzystanie z usług wielu dostawców związanych z systemami OT może pozwolić

na zwiększenie niezawodności dzięki ograniczeniu typowych powodów awarii. Nie zawsze jest to jednak możliwe ze względu na fakt, że w przypadku wielu technologii liczba dostępnych produktów spełniających stosowne wymagania jest ograniczona.

SR-5 STRATEGIE, NARZĘDZIA I METODY NABYCIA

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Zmienione poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SR-5	**Strategie, narzędzia i metody nabycia**	Wybrano	Wybrano	Wybrano
SR-5 (1)	*STRATEGIE, NARZĘDZIA I METODY NABYCIA | ODPOWIEDNIE ZAOPATRZENIE*		**Dodano**	**Dodano**

Brak omówienia zabezpieczenia w kontekście systemów OT.

Zabezpieczenie rozszerzone: (1) Omówienie zabezpieczenia w kontekście systemów OT: Należy nawiązywać kontakty z dostawcami i producentami, a także opracować strategie dotyczące części zamiennych, aby zapewnić dostępność krytycznych komponentów w celu zaspokojenia potrzeb operacyjnych.

Uzasadnienie uwzględnienia zabezpieczenia SR-5 (1) w zakresie UMIARKOWANEGO oraz WYSOKIEGO poziomu wpływu: Systemy OT i ich komponenty są często budowane z myślą o konkretnych zastosowaniach, a liczba producentów i dostawców poszczególnych komponentów bywa często ograniczona. Organizacje powinny opracować wykaz krytycznych komponentów systemów OT i wdrożyć stosowne zabezpieczenia, aby zapewnić ich dostępność w przypadku zakłóceń w łańcuchu dostaw.

SR-6 OCENY I RECENZJE DOSTAWCÓW

Nr zabezpieczenia	**Nazwa środka bezpieczeństwa** *Nazwa zabezpieczenia rozszerzonego:*	**Poziomy bazowe zabezpieczeń**		
		Niski	**Umiarkowany**	**Wysoki**
SR-6	**Oceny i przeglądy dostawców**		Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SR-8 UMOWY DOTYCZĄCE POWIADOMIEŃ

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-8	**Umowy dotyczące powiadomień**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SR-9 ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-9	**Odporność na manipulacje i wykrywanie sabotażu**			Wybrano
SR-9 (1)	*ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU | WIELOETAPOWY CYKL ŻYCIA SYSTEMU*			Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SR-10 KONTROLA SYSTEMÓW / KOMPONENTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-10	**Kontrola systemów / komponentów**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SR-11 AUTENTYCZNOŚĆ KOMPONENTU

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-11	**Autentyczność komponentów**	Wybrano	Wybrano	Wybrano
SR-11 (1)	*AUTENTYCZNOŚĆ KOMPONENTU | SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM*	Wybrano	Wybrano	Wybrano
SR-11 (2)	*AUTENTYCZNOŚĆ KOMPONENTU | ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW*	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

SR-12 USUWANIE KOMPONENTÓW

Nr zabezpieczenia	Nazwa środka bezpieczeństwa *Nazwa zabezpieczenia rozszerzonego:*	Poziomy bazowe zabezpieczeń		
		Niski	Umiarkowany	Wysoki
SR-12	**Usuwanie komponentów**	Wybrano	Wybrano	Wybrano

Brak omówienia zabezpieczenia w kontekście systemów OT.

ZAŁĄCZNIK G – LISTA ZMIAN

Niniejszy dokument jest trzecią wersją publikacji NIST SP 800-82. Aktualizacje w tej wersji obejmują:

- Rozszerzenie zakresu stosowania z systemów sterowania przemysłowego na szeroko pojęte systemy OT.
- Informacje dotyczące podatności oraz zagrożeń dotyczących systemów OT.
- Aktualizacje dotyczące zarządzania ryzykiem związanym z technologią operacyjną, a także zaleceń w zakresie dobrych praktyk i architektur.
- Aktualizacje dotyczące bieżących działań w zakresie bezpieczeństwa technologii operacyjnej.
- Aktualizacje dotyczące narzędzi oraz zdolności do ochrony technologii operacyjnych.
- Zmiany dostosowujące treść publikacji do innych norm i wytycznych dotyczących bezpieczeństwa technologii operacyjnych, w tym ram cyberbezpieczeństwa.
- Nowe wytyczne ujednolicające treść publikacji z informacjami dotyczącymi zabezpieczeń opisanych w dokumencie NIST SP 800-53, Rev. 5 / NSC 800-53 [NSC 800-53].
- Dodatkowe informacje dotyczące technologii operacyjnych na potrzeby zabezpieczeń opisanych w dokumencie NIST SP 800-53, Rev. 5 / NSC 800-53 [NSC 800-53], które zapewniają dostosowanie do poziomu bazowych (minimalnych) zabezpieczeń systemów technologii operacyjnej o niskim, umiarkowanym i wysokim poziomie wpływu.