

Zarządzanie bezpieczeństwem informacji

Firma Galach Consulting Sp. z o.o., NIP 5213704182/ KRS: 0000571975 (dalej Partner PWCyber), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przekazanych w ramach Programu PWCyber (zwanymi dalej „Materiałami”), w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych. Partner oświadcza, że materiały nie naruszają praw osób trzecich.

Spis treści

Wprowadzenie	3
Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji	3
Zasady bezpiecznego przetwarzania informacji	5
Zarządzanie bezpieczeństwem w obszarze IT	12
Zarządzanie bezpieczeństwem fizycznym i środowiskowym	16
Bezpieczeństwo informacji w zarządzaniu personelem	17
Bezpieczeństwo informacji w zarządzaniu dostawcami	18
Zarządzanie ciągłością przetwarzania informacji	20
Dokumentacja zarządzania bezpieczeństwem informacji	21
Nadzór nad bezpieczeństwem przetwarzania informacji	22

Wprowadzenie

Zarządzanie bezpieczeństwem informacji obejmuje działania mające na celu identyfikację potrzeb w zakresie ochrony aktywów informacyjnych, ich realizację, ocenę skuteczności oraz wprowadzanie działań doskonalących, zapewniających coraz skuteczniejsze zabezpieczenie przed zagrożeniami. Wprowadzenie procesów zarządzania bezpieczeństwem informacji wynika zarówno z wymagań prawnych i regulacyjnych (w tym UKSC¹, KRI², DORA³) jak i oczywistych potrzeb organizacji narażonej na różnorakie zagrożenia, w tym cyberataki.

Celem niniejszego przewodnika jest wsparcie we wdrożeniu procesów zarządzania bezpieczeństwem informacji. Należy zaznaczyć jednak, że przewodnik nie opisuje całości działań, które są niezbędne do certyfikacji systemu zarządzania bezpieczeństwem informacji lub systemu zarządzania ciągłością działania na zgodność z właściwymi normami (ISO/IEC 27001, ISO 22301).

Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji

Zarządzanie ryzykiem jest kluczowym elementem zarządzania bezpieczeństwem informacji, pozwala bowiem na zidentyfikowanie potrzeb w zakresie ochrony aktywów informacyjnych oraz wybór środków adekwatnych do potrzeb organizacji. Proces zarządzania ryzykiem składa się z następujących elementów:

- Identyfikacji ryzyka.
- Analizy ryzyka.
- Oceny ryzyka.
- Zdefiniowania i wdrożenia planów postępowania z ryzykiem.

¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560, z późn. zm.)

² Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773)

³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (ang. Digital Operational Resilience Act)

Identyfikacja ryzyka obejmuje zidentyfikowanie czynników, które mogą spowodować naruszenie bezpieczeństwa aktywów informacyjnych, a w szczególności ich poufności, integralności i dostępności. Czynniki te mogą być związane z:

- Celowym działaniem (na przykład cyberataki, akty sabotażu).
- Błędem ludzkim (na przykład nieprawidłowe wprowadzenie lub usunięcie danych, błędna konfiguracja oprogramowania).
- Awarią techniczną (na przykład awaria sprzętu informatycznego, awaria zasilania).
- Działaniem siły wyższej (na przykład zalanie pomieszczenia w wyniku powodzi, uszkodzenie instalacji elektrycznej w wyniku uderzenia pioruna).

Ryzyko może być identyfikowane na dwa sposoby:

- W oparciu o scenariusze dotyczące całej organizacji, dotyczące wielu aktywów (na przykład pożar serwerowni skutkujący zniszczeniem serwerów tam znajdujących się lub wprowadzenie złośliwego oprogramowania skutkującego zainfekowaniem całej infrastruktury informatycznej).
- W rozbiciu na poszczególne aktywa (na przykład cyberataki w odniesieniu do poszczególnych systemów informatycznych).

Możliwe jest też podejście mieszane, uwzględniające zarówno scenariusze globalne jak i przypisane do poszczególnych aktywów.

Analiza ryzyka obejmuje oszacowanie poziomu ryzyka, którego wielkość zależy od prawdopodobieństwa wystąpienia strat spowodowanych czynnikiem określonym w ramach identyfikacji ryzyka oraz skutków ich wystąpienia. Skutki powinny być oceniane oddzielnie z uwagi na naruszenie poufności, integralności i dostępności, gdyż mogą one znacznie różnić się pomiędzy poszczególnymi atrybutami bezpieczeństwa.

Podczas analizy ryzyka w ramach zarządzania bezpieczeństwem informacji najczęściej stosuje się miary opisowe (np. niskie, średnie, wysokie), precyzując, co rozumiemy pod poszczególnymi pojęciami. Szacując poziom ryzyka należy wziąć pod uwagę posiadane zabezpieczenia, jak również podatności na czynniki ryzyka (np. serwerownia jest podatna na zalanie, jeżeli znajduje się w piwnicy budynku).

W ramach oceny ryzyka podejmowana jest decyzja co do jego akceptacji.

W przypadku braku akceptacji konieczne jest podjęcie działań zmierzających do obniżenia poziomu ryzyka. Działania te powinny być udokumentowane w planie postępowania z ryzykiem – w praktyce jest to dokument określający wymagane

działania prowadzące do obniżenia poziomu ryzyka, terminy ich realizacji i osoby odpowiedzialne, a także sposób weryfikacji skuteczności podjętych działań. Realizacja planów postępowania z ryzykiem powinna być monitorowana i nadzorowana.

Sposób postępowania z ryzykiem w obszarze zarządzania bezpieczeństwem informacji może obejmować:

- Modyfikowanie ryzyka poprzez wdrożenie działań zmniejszających jego wielkość. Najczęściej modyfikowanie ryzyka polega na wprowadzeniu zabezpieczeń, zarówno o charakterze technicznym jak i organizacyjnym, ograniczających prawdopodobieństwo wystąpienia strat spowodowanych naruszeniem bezpieczeństwa.
- Dzielenie ryzyka poprzez przeniesienie części strat na inny podmiot – przykładem jest tu zakup polisy ubezpieczeniowej, która ma pokryć przynajmniej część strat związanych z naruszeniem bezpieczeństwa.
- Unikanie ryzyka poprzez zmianę sposobu działania tak, że czynnik mogący spowodować naruszenie bezpieczeństwa przestaje występować (przykładem jest wycofanie z użytku komputerów przenośnych co powoduje, że znika ryzyko ich zagubienia).
- Zachowanie ryzyka, polegające na jego akceptacji.

Czynności związane z identyfikowaniem, analizą i oceną ryzyka oraz inicjowaniem działań związanych z postępowaniem z ryzykiem powinny być przeprowadzane:

- Okresowo (z reguły przyjmuje się częstotliwość raz do roku).
- W przypadku zmian, które mogą wpłynąć na poziom ryzyka. Dotyczy to zarówno zmian w zakresie samej organizacji (np. zmiana struktury organizacyjnej, stosowanej technologii, lokalizacji itp.) jak i zmian w środowisku, w którym organizacja funkcjonuje, w tym zmian prawnych i regulacyjnych.
- W przypadku, gdy wystąpiły incydenty bezpieczeństwa, które nie były ujęte w identyfikacji ryzyka lub które mogą świadczyć o niedoszacowaniu ryzyka.

Zasady bezpiecznego przetwarzania informacji

Kluczowym elementem zarządzania bezpieczeństwem informacji jest ustanowienie, zakomunikowanie i egzekwowanie zasad bezpiecznego przetwarzania⁴ informacji.

⁴ Przetwarzanie to wszelkie operacje wykonywane na danych, zarówno w sposób zautomatyzowany, jak i ręczny, obejmujące ich zbieranie, przechowywanie, modyfikowanie, udostępnianie oraz usuwanie.

Zasady bezpieczeństwa informacji dotyczyć będą wszystkich podmiotów, które przetwarzają informacje w ramach działań organizacji – dotyczy to zatem nie tylko pracowników etatowych, ale także zleceniobiorców, kontraktorów, a także pracowników podmiotów zewnętrznych świadczących usługi związane z przetwarzaniem informacji należących do organizacji.

Zasady bezpieczeństwa powinny odnosić się do informacji przetwarzanych w dowolnej postaci. Poniżej przedstawiono wybrane zagadnienia, które należy rozważyć w kontekście definiowania i wdrażania zasad bezpiecznego przetwarzania informacji.

W zakresie informacji przetwarzanych w dowolnej postaci:

- Pozyskiwanie, przetwarzanie i wykorzystywanie informacji wyłącznie z zachowaniem przepisów obowiązującego prawa, w szczególności dotyczy to informacji podlegających ochronie w związku z ochroną praw autorskich i informacji stanowiących dane osobowe.
- Realizacja obowiązków prawnych związanych z przetwarzaniem określonego rodzaju informacji – dotyczy to między innymi danych osobowych i realizacji praw podmiotów danych.
- Przekazywanie informacji wyłącznie osobom uprawnionym do jej otrzymania.
- Przechowywanie informacji w formie udokumentowanej przez czas uzasadniony wymaganiami organizacji, w tym wynikającymi z wymagań prawnych i kontraktowych.
- Dbałość o poprawność dokumentowanej informacji oraz reagowanie w przypadku stwierdzenia braku jej poprawności.
- Określenie zasad reagowania w przypadku podejrzenia naruszenia bezpieczeństwa informacji, w tym sposobu zgłaszania takich zdarzeń.
- Określenie zasad reagowania w przypadku podejrzenia niedostatecznego zabezpieczenia przetwarzanych informacji.
- Sposób zabezpieczenia pomieszczeń, w których informacje są przechowywane i składowane.
- Ograniczenia dotyczące wykonywania fotografii i nagrywania filmów na terenie obiektów organizacji – w sytuacjach gdy jest to uzasadnione charakterem obiektu i przetwarzanych na jego terenie danych.

W zakresie informacji przetwarzanych z wykorzystaniem systemów informatycznych:

- Zasady korzystania ze służbowego sprzętu informatycznego i służbowego oprogramowania.
- Zasady i ograniczenia związane z korzystaniem ze sprzętu prywatnego do celów służbowych.
- Bezpieczne korzystanie z haseł i innych mechanizmów uwierzytelniających, w sposób ograniczający ryzyko ich pozyskania przez osoby nieuprawnione.
- Blokowanie komputera w przypadku odejścia od stanowiska pracy.
- Stosowanie zasady czystego ekranu.
- Lokalizacja ekranu w sposób ograniczający ryzyko jego podejrzenia przez osoby nieuprawnione wchodzące do pomieszczenia lub znajdujące się poza pomieszczeniem – na przykład na zewnątrz budynku.
- Właściwe przechowywanie danych, w sposób zapewniający ochronę ich poufności i dostępności – w szczególności dotyczy to przechowywania danych na dyskach sieciowych, w katalogach przeznaczonych do przechowywania określonych typów danych (co wiąże się z odpowiednio nadanymi uprawnieniami do tych katalogów).
- Zasady korzystania z zasobów Internetu, w tym w zakresie odwiedzania stron internetowych, pozyskiwania plików z Internetu i ich wykorzystywania w bieżącej pracy.
- Zasady i ograniczenia dotyczące korzystania z serwisów społecznościowych, w tym w związku z publikowaniem informacji o charakterze służbowym i wykorzystywania informacji publikowanych w mediach społecznościowych do wykonywania obowiązków służbowych.
- Zasady bezpiecznego korzystania z poczty elektronicznej – dotyczy to w szczególności weryfikacji poprawności adresów odbiorców wiadomości, stosowania – tam gdzie jest to niezbędne w związku z rodzajem przesyłanych informacji – ochrony kryptograficznej, stosowania – tam gdzie jest to niezbędne z uwagi na ochronę danych osobowych – pola UDW, a także zwrócenia uwagi na treść załączonej w mailu poprzedniej korespondencji (może ona zawierać informacje, które nie powinny być przesyłane adresatom).

-
- Zasady stosowania przez użytkowników mechanizmów ochrony kryptograficznej – jest to szczególnie istotne w przypadku, gdy ochrona kryptograficzna ogranicza się do tworzenia zabezpieczonych hasłem skompresowanych archiwów i ich przekazywania innym kanałem komunikacyjnym.
 - W przypadku pracowników korzystających z podpisu elektronicznego – zasady używania powyższego, w tym postępowanie w przypadku utraty urządzenia do składania podpisu.
 - Zasady bezpiecznego korzystania z narzędzi do prowadzenia telekonferencji i komunikatorów ograniczające ryzyko dostępu osób nieuprawnionych do przekazywanych informacji.
 - Zasady postępowania z nośnikami przenośnymi, w tym wskazanie sytuacji, w których zapisanie danych na nośniku jest dopuszczalne oraz wymagań dotyczących zabezpieczenia nośnika.
 - Zasady i ograniczenia związane z korzystaniem z narzędzi do transferu danych, w tym w oparciu o usługi chmury obliczeniowej i wymagania dotyczące zabezpieczenia danych przesyłanych przy użyciu tych narzędzi, o ile są one dopuszczone do użytku w organizacji.
 - Podstawowe zasady ochrony antywirusowej i ochrony przed atakami socjotechnicznymi uwzględniające pocztę elektroniczną, komunikatory, strony www, nośniki przenośne, kontakt telefoniczny i bezpośredni.
 - Zasady i ograniczenia związane z korzystaniem z publicznie dostępnych narzędzi generatywnej sztucznej inteligencji, w szczególności w związku z ryzykiem ujawnienia wrażliwych informacji oraz w związku z ryzykiem wykorzystania do wykonywania zadań służbowych fałszywych informacji udostępnionych przez te narzędzia.
 - Zasady bezpiecznego maskowania danych (w tym zakrywania niepożądanych danych w plikach pdf).
 - Zasady pracy zdalnej ograniczające ryzyko utraty sprzętu informatycznego (określenie zasad bezpiecznego transportu i przechowywania sprzętu) oraz dostępu osób nieuprawnionych do sprzętu i przetwarzanych danych. Zasady te powinny regulować również kwestię pracy w miejscach publicznych, gdzie istnieje podwyższone ryzyko kradzieży sprzętu, a także podejrzenia wyświetlanych treści przez osoby nieuprawnione. Przedmiotowe zasady powinny

obejmować również przetwarzanie danych z wykorzystaniem urządzeń mobilnych (smartfony, tablety).

- Zasady reagowania na zdarzenia mogące świadczyć o naruszeniu bezpieczeństwa, w tym wskazanie symptomów takich naruszeń, działań podejmowanych niezwłocznie po ich odnotowaniu oraz sposób zgłaszania zdarzenia służbom informatycznym w organizacji.

W zakresie informacji przetwarzanych w formie papierowej:

- Sposób bezpiecznego przechowywania i przekazywania dokumentów papierowych.
- Sposób ewidencji przepływu dokumentacji papierowej.
- Zasady bezpiecznego korzystania z drukarek, skanerów i urządzeń kopiujących.
- Wymagania dotyczące niszczenia dokumentów papierowych.
- Wymagania dotyczące porządkowania miejsc spotkań, w których mogą znajdować się informacje zapisane w postaci notatek, zapisów na tablicy, flipcharcie itp.

W zakresie informacji przekazywanych w formie ustnej, w tym podczas rozmowy telefonicznej:

- Prowadzenie rozmowy w sposób minimalizujący ryzyko podsłuchania przez inne osoby znajdujące się w pobliżu.
- Unikanie nagrywania komunikatów zawierających wrażliwe informacje na automatycznej sekretarce – problem może pojawić się w przypadku błędnie wybranego numeru telefonu.

Część z wymienionych powyżej zasad może być zróżnicowana w zależności od charakteru informacji – w szczególności w przypadku informacji mniej wrażliwych organizacja może dopuścić brak określonych zabezpieczeń, na przykład może dopuścić przesyłanie informacji bez uprzedniego zaszyfrowania. Aby w sposób przejrzysty określić wymagania dotyczące zabezpieczenia różnych rodzajów informacji stosuje się ich klasyfikację. **Zasady dotyczące klasyfikacji obejmować powinny:**

- Definicje poszczególnych klas informacji.
- Kryteria, według których informacje są przypisywane do poszczególnych klas wraz z określeniem odpowiedzialności za klasyfikowanie informacji.

-
- Sposób oznaczania, do jakiej klasy została przypisana informacja. Przydatne mogą być tutaj narzędzia informatyczne wspierające ten proces.
 - Zasady zabezpieczenia informacji należących do poszczególnych klas. Zasady te, przynajmniej w pewnym zakresie, mogą być wymuszone przez rozwiązania techniczne (na przykład system DLP⁵ wspierający kontrolę przepływu danych klasyfikowanych).

Zasady opisane powyżej powinny być wprowadzone regulacjami obowiązującymi w organizacji, uwzględniającymi również odpowiedzialność za ochronę aktywów informacyjnych. Odpowiedzialność ta spoczywa w szczególności na:

- Kadrze kierowniczej odpowiedzialnej za bezpieczeństwo w całej organizacji, jak również w poszczególnych komórkach organizacyjnych, realizowanych procesach i projektach.
- Pracownikach służb informatycznych odpowiedzialnych za utrzymanie, zabezpieczenie i właściwe zarządzanie infrastrukturą informatyczną, z uwzględnieniem należytej ochrony przetwarzanych informacji.
- Pracownikach odpowiedzialnych za bezpieczeństwo i administrację obiektami należącymi do organizacji, w tym budynkami i pomieszczeniami, w szczególności w zakresie wdrażania, eksploatacji i konserwacji systemów bezpieczeństwa technicznego i środowiskowego oraz koordynacji zadań realizowanych przez pracowników ochrony fizycznej.
- Pracownikach odpowiedzialnych za procesy zakupowe i współpracę z dostawcami z uwagi na konieczność uwzględnienia wymagań bezpieczeństwa w ramach realizowanych przez nich zadań.
- Pracownikach odpowiedzialnych za obsługę prawną i obszar zgodności w zakresie identyfikacji zmian w przepisach prawnych i regulacyjnych i analizę ich wpływu na obowiązujące w organizacji zasady bezpiecznego przetwarzania informacji i środki zapewniające ochronę aktywów informacyjnych.
- Inspektorze Ochrony Danych (o ile został powołany), w zakresie określonym w art. 39 RODO⁶.

⁵ Rozwiązania zapobiegające nieuprawnionemu ujawnieniu lub wyciekowi informacji (ang. Data Loss Prevention)

⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego

- Wszystkich pracowników i współpracowników przetwarzających informacje lub mających dostęp do aktywów informacyjnych, którzy są zobowiązani do przestrzegania wewnętrznych zasad obowiązujących w organizacji.
- Pracownikach podmiotów zewnętrznych świadczących usługi dla organizacji w zakresie wynikającym z wymagań kontraktowych określających zasady ochrony aktywów informacyjnych.

W ramach systemu zarządzania bezpieczeństwem informacji powinny być utworzone i przypisane role:

- Pełnomocnika systemu zarządzania odpowiedzialnego za całość zadań związanych z utrzymaniem, stosowaniem i doskonaleniem zasad zarządzania ochroną aktywów informacyjnych.
- Audytorów wewnętrznych odpowiedzialnych za realizację audytów wewnętrznych, wskazanych w części poświęconej nadzorowi nad zarządzaniem bezpieczeństwem informacji.

Oprócz zapoznania pracowników i współpracowników z obowiązującymi zasadami poprzez udostępnienie im wprowadzonych w organizacji regulacji **niezbędne są działania szkoleniowe i uświadamiające**. Powinny one w szczególności obejmować:

- Szkolenia kadry kierowniczej w zakresie obowiązków związanych z zarządzaniem bezpieczeństwem informacji.
- Szkolenia uświadamiające zagrożenia dla bezpieczeństwa informacji, w tym cyberzagrożenia oraz działania niezbędne do przeciwstawiania się im.
- Kampanie informacyjne, w szczególności dotyczące nowego typu zagrożeń oraz przypominające zasady bezpieczeństwa.
- Testy symulujące zagrożenia, w tym testy socjotechniczne.
- Szkolenia budujące kompetencje niezbędne do bezpiecznego przetwarzania informacji oraz do zarządzania systemami bezpieczeństwa, adekwatnie do zakresu zadań uczestniczących w nich osób.

Szkolenie prezentujące podstawowe zasady bezpieczeństwa powinny być prowadzone dla:

przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

-
- Nowych pracowników i współpracowników w ramach on-boardingu.
 - Dotychczasowych pracowników i współpracowników – okresowo
 - Pracowników podmiotów zewnętrznych realizujących zadania związane z przetwarzaniem wrażliwych informacji należących do organizacji.

Wiedza pozyskana w trakcie szkoleń powinna podlegać weryfikacji poprzez przeprowadzanie testów kompetencyjnych.

Zarządzanie bezpieczeństwem w obszarze IT

Zarządzanie bezpieczeństwem w obszarze IT obejmuje szereg procesów zapewniających ochronę informacji przetwarzanych z wykorzystaniem infrastruktury informatycznej, w tym urządzeń końcowych i mobilnych. Do procesów tych należą w szczególności:

- Zarządzanie tożsamością w infrastrukturze informatycznej, w tym tworzenie, blokowanie i usuwanie kont w systemach informatycznych. Zarządzanie tożsamością nie ogranicza się do kont użytkowników, powinno również obejmować konta systemowe. Ponadto, w ramach zarządzania tożsamością należy wziąć pod uwagę praktykę blokowania kont w przypadku dłuższej nieobecności użytkownika.
- Zarządzanie danymi uwierzytelniającymi, w tym ich tworzenie, przekazywanie użytkownikom (dotyczy haseł inicjalnych i danych wykorzystywanych przy uwierzytelnieniu wieloskładnikowym), umożliwienie resetu danych uwierzytelniających. Zarządzanie danymi uwierzytelniającymi obejmuje również zapewnienie dostępu do kont awaryjnych oraz komunikację pomiędzy systemami.
- Nadawanie i modyfikowanie uprawnień, w tym formalne wnioskowanie o nadanie uprawnień, akceptowanie i realizowanie wniosków z uwzględnieniem zasad minimalnych uprawnień, wiedzy uzasadnionej i segregacji zadań. Podobnie jak w przypadku tożsamości, zarządzanie uprawnieniami nie ogranicza się do kont użytkowników. W przypadku zarządzania tożsamością i zarządzania uprawnieniami należy uwzględnić nadawanie uprawnień na czas określony, gdy jest to uzasadnione sposobem realizacji przez użytkownika zadań na rzecz organizacji.

-
- Odbieranie uprawnień – zarówno w przypadku zakończenia współpracy z organizacją, jak i w przypadku, gdy uprawnienia nie są już potrzebne do realizacji zadań.
 - Przeprowadzanie przeglądu kont i uprawnień, pod kątem zasadności posiadania dostępu do aktywów informacyjnych. Przeglądy powinny być przeprowadzane okresowo, a także w przypadku wystąpienia zmian uzasadniający dodatkowy przegląd. Elementem procesu przeglądu kont jest również identyfikowanie kont, które nie są wykorzystywane.
 - Zarządzanie dostępem uprzywilejowanym w sposób ograniczający ryzyko nieuprawnionego wykorzystania uprawnień administracyjnych oraz gwarantujący rozliczalność dostępu (np. poprzez unikanie stosowania wspólnych kont administracyjnych). Zarządzanie dostępem uprzywilejowanym wiązać się może z utwardzeniem konfiguracji infrastruktury informatycznej oraz wprowadzeniem zabezpieczeń ograniczających ryzyko przejęcia kont administracyjnych (np. rozwiązania klasy PAM⁷).
 - Zarządzanie aktywami, w tym utrzymywanie aktualnego rejestru aktywów, określenie ich właścicieli oraz powiązanie z procesami biznesowymi i analizą ryzyka.
 - Zarządzanie cyklem życia sprzętu informatycznego: przygotowanie, wydanie do eksploatacji, serwis i konserwacja w ramach eksploatacji, bezpieczne wycofanie sprzętu z eksploatacji. Przygotowanie sprzętu obejmuje w szczególności instalację i aktualizację oprogramowania oraz jego skonfigurowanie zgodnie z zasadami bezpieczeństwa obowiązującymi w organizacji. Działania serwisowe muszą zapewniać ochronę informacji, zwłaszcza w zakresie poufności, a także rozliczalność prac serwisowych. Wycofanie sprzętu obejmuje również bezpieczne usunięcie danych przechowywanych na tym sprzęcie - w niektórych przypadkach może być zasadnym zarchiwizowanie tych danych.
 - Wprowadzanie zmian w infrastrukturze informatycznej w sposób zapewniający jej bezpieczeństwo, w tym analizowanie dopuszczalności zmiany, jej planowanie i testowanie, zapewnienie możliwości powrotu w przypadku niepowodzenia, dokumentowanie zmiany. Należy pamiętać, że sposób postępowania może być różny zależnie od charakteru zmiany, jej zakresu i ryzyka z nią związanego.

⁷ Ang. Privileged Access Management - to systemy, które umożliwiają kontrolowanie i monitorowanie kont uprzywilejowanych, takich jak administratorzy systemów, serwerów czy baz danych.

-
- Wprowadzanie nowych rozwiązań informatycznych. W ramach tego procesu należy określić minimalne wymagania dla takich rozwiązań, zasady planowania i realizacji wdrożeń, testowania i odbioru. W przypadku prac programistycznych realizowanych przez organizację lub na jej zlecenie należy określić i egzekwować wymagania bezpieczeństwa dla tworzonego oprogramowania, w tym podstawowe praktyki bezpiecznego pisania oprogramowania, zasady dostępu do kodu, zatwierdzania w nim zmian oraz weryfikacji poprawności i bezpieczeństwa. Dodatkowo, w przypadku prac zleconych należy uwzględnić kwestię zapewnienia praw własności i dostępności kodu źródłowego.
 - Zarządzanie architekturą bezpieczeństwa uwzględniające specyfikę infrastruktury informatycznej, wymagania prawne i regulacyjne, wnioski wypływające z analizy ryzyka i procesu monitorowania zagrożeń.
 - Zarządzanie konfiguracją w celu określenia standardów konfiguracji dla wykorzystywanego sprzętu, oprogramowania i usług oraz ograniczenia ryzyka występowania incydentów poprzez wykorzystanie dostępnych zabezpieczeń oraz wyłączenie zbędnych funkcjonalności mogących być celem potencjalnego ataku.
 - Zarządzanie infrastrukturą sieciową, obejmujące projektowanie i utrzymywanie segmentacji sieci, zarządzanie usługami sieciowymi, połączeniami zewnętrznymi, dostępem zdalnym, komunikacją pomiędzy strefami bezpieczeństwa oraz monitorowanie bezpieczeństwa ruchu sieciowego.
 - Zarządzanie usługami w ramach chmury obliczeniowej, w tym dostosowywanie rozwiązań do zmian w usługach chmurowych, a także opracowanie, utrzymywanie i okresowe testowanie planów wyjścia z usługi chmurowej.
 - Zarządzanie odstępstwami od przyjętych standardów bezpieczeństwa, w przypadku, gdy standardy te nie mogą być spełnione. Proces powinien uwzględniać planowanie i realizację działań zmierzających do usunięcia tych odstępstw.
 - Zarządzanie dokumentacją infrastruktury informatycznej i systemów bezpieczeństwa.
 - Monitorowanie infrastruktury informatycznej, reagowanie na anomalie i incydenty bezpieczeństwa. Należy uwzględnić zarówno wymagania w zakresie konfiguracji mechanizmów zbierania i przechowywania logów, synchronizacji czasu oraz generowania alertów, jak i zasady postępowania w przypadku

wystąpienia naruszenia bezpieczeństwa. Reagowanie na incydenty musi uwzględniać wymagania prawne adekwatne do charakteru przetwarzanych informacji (wynikające m.in. z UKSC i RODO), powinno zapewniać nie tylko usunięcie skutków incydentu i przywrócenie prawidłowego przetwarzania informacji, ale również analizę przyczyn i zapobieżenie podobnym zdarzeniom w przyszłości. W tym celu niezbędnym może być zebranie i przeanalizowanie właściwego materiału dowodowego, co również powinno zostać uwzględnione w zarządzaniu bezpieczeństwem IT.

- Monitorowanie parametrów pojemnościowych infrastruktury informatycznej, reagowanie na anomalie, a także planowanie wymagań pojemnościowych w przyszłości i podejmowanie działań dostosowawczych.
- Monitorowanie zagrożeń w celu podjęcia działań ograniczających ich możliwy negatywny efekt. Należy dodać, iż monitorowanie zagrożeń nie powinno ograniczać się wyłącznie do obszaru infrastruktury informatycznej, ale obejmować całą organizację, w tym wszystkie procesy przetwarzania informacji.
- Zarządzanie podatnościami, w tym ich identyfikowanie, analizowanie i usuwanie. Należy pamiętać, że niektóre podatności nie mogą być usunięte w trybie natychmiastowym – w takich przypadkach należy podjąć działania mitygujące, zaś podatność usunąć niezwłocznie, gdy będzie to możliwe.
- Zarządzanie oprogramowaniem, w tym dopuszczanie nowego oprogramowania do eksploatacji po weryfikacji jego bezpieczeństwa i poprawności działania, instalowanie oraz wycofywanie oprogramowania z eksploatacji (na przykład w sytuacji zakończenia wsparcia przez producenta). Z procesem tym jest powiązane zarządzanie licencjami zapewniające z jednej strony posiadanie wymaganej liczby licencji, z drugiej zaś optymalizację ich ilości.
- Zarządzanie aktualizacjami oprogramowania, uwzględniające weryfikację poprawności działania systemów po instalacji aktualizacji.
- Zarządzanie danymi, w tym usuwanie zbędnych danych (zgodnie z zasadami retencji). Zarządzanie danymi może również dotyczyć danych testowych, obejmując ich wytwarzanie lub pozyskiwanie z danych produkcyjnych oraz zarządzanie dalszym cyklem ich życia. Zarządzanie danymi testowymi powiązane jest z procesem wprowadzania zmian lub nowych rozwiązań.
- Zabezpieczenie dostępności poprzez wykonywanie kopii zapasowych. Zarządzanie kopiami zapasowymi powinno uwzględniać kwestię

przechowywania backupów poza miejscem przetwarzania, bezpieczeństwo transferu kopii zapasowych do miejsca składowania, a także okresowe testowanie możliwości odtworzeniowych. Sposób wykonywania kopii zapasowych musi uwzględniać ochronę przed zagrożeniami skutkującymi utratą danych, w tym atakami ransomware.

- Zarządzanie kryptografią, w tym zarządzaniem cyklem życia kluczy kryptograficznych i certyfikatów, uwzględnienie obsługi incydentów związanych z kompromitacją kluczy, a także zapewnienie możliwości awaryjnego odszyfrowania danych składowanych.
- Zarządzanie zarejestrowanymi domenami, w tym nadzór nad odnawianiem domen.
- Bieżącą administrację i nadzór nad systemami informatycznymi, infrastrukturą sieciową i systemami bezpieczeństwa. Istotne czynności administracyjne powinny być dokumentowane.

Zarządzanie bezpieczeństwem fizycznym i środowiskowym

Ochrona informacji wiąże się z zabezpieczeniem obszarów i pomieszczeń, w których są one przetwarzane, a także zapewnieniem właściwych warunków środowiskowych dla sprzętu informatycznego. Zarządzanie bezpieczeństwem informacji w tym obszarze powinno w szczególności obejmować:

- Architekturę środków bezpieczeństwa, uwzględniających ochronę przed dostępem osób nieuprawnionych, monitorowanie obszaru i wykrywanie nieuprawnionego wejścia, zapewnienie właściwych warunków środowiskowych (temperatury, wilgotności, zasilania), ochronę przeciwpożarową, ochronę przed zalaniem pomieszczeń, itp.
- Nadzór nad ruchem osobowym i materiałowym.
- Nadawanie i odbieranie uprawnień do dostępu do pomieszczeń, w tym zarządzanie uprawnieniami w systemach SKD⁸ i SSWiN⁹.

⁸ System kontroli dostępu

⁹ System sygnalizacji włamania i napadu

-
- Zarządzanie kluczami do pomieszczeń z zapewnieniem rozliczalności wydania i zdania.
 - Zarządzanie nagraniami z systemu telewizji dozorowej, w tym ich usuwanie po okresie przechowywania.
 - Przegląd nagrań i logów.
 - Okresową konserwację i testy środków bezpieczeństwa.
 - Nadzór i koordynację służb ochrony fizycznej.
 - Reagowanie na incydenty bezpieczeństwa.

Bezpieczeństwo informacji w zarządzaniu personelem

Czynnik ludzki ma kluczowy wpływ na bezpieczeństwo przetwarzanych informacji. Z tego względu procesy zarządzania personelem muszą uwzględniać aspekty bezpieczeństwa informacji, w szczególności zaś obejmować:

- Uwzględnienie w strukturze organizacyjnej ról i zadań związanych z zarządzaniem bezpieczeństwem informacji i nadzorem nad realizacją procesów w tym zakresie.
- Uwzględnienie, w zakresie zadań na poszczególnych stanowiskach pracy, czynności i odpowiedzialności związanych z ochroną informacji i zarządzaniem jej bezpieczeństwem. Należy pamiętać o odpowiedzialności kadry kierowniczej za nadzór nad stosowaniem obowiązujących w organizacji zasad bezpieczeństwa informacji w podległych jej komórkach organizacyjnych i procesach.
- Uwzględnienie, w umowach z personelem oraz innych dokumentach regulujących zasady wykonywania zadań na rzecz organizacji (na przykład w regulaminie pracy), klauzul dotyczących ochrony informacji, zachowania poufności oraz konsekwencji nieprzestrzegania tych zasad. Należy pamiętać o ewentualnych ograniczeniach wynikających z prawa pracy.
- Zapewnienie weryfikacji wiarygodności, rękojmi zaufania i posiadanych kompetencji w procesie rekrutacji, z uwzględnieniem ewentualnych ograniczeń prawnych. Udokumentowanie zakresu i wyników weryfikacji w ramach zapisów prowadzonych w procesie rekrutacji.

-
- Uwzględnienie, w ramach weryfikacji pracownika w trakcie okresu próbnego, kompetencji w zakresie ochrony informacji i podejścia do przestrzegania obowiązujących w organizacji w tym zakresie regulacji.
 - Uwzględnienie, w ramach prowadzonych ocen okresowych, zagadnień związanych z przestrzeganiem zasad ochrony informacji.
 - Ujęcie zagadnień związanych z zarządzaniem bezpieczeństwem informacji w planowaniu ścieżek szkoleniowych i ścieżek rozwoju, w zakresie adekwatnym do pełnionych zadań.
 - Zapewnienie rozliczalności przekazania i zwrotu nośników i środków przetwarzania informacji.
 - Zasady postępowania w przypadku zakończenia pracy lub współpracy, uwzględniające rozliczenie pracownika lub współpracownika, odebranie uprawnień do systemów informatycznych oraz odebranie uprawnień do wstępu na teren obiektów organizacji. Elementem procedury zakończenia współpracy może być również spotkanie przypominające o zobowiązaniach w zakresie ochrony informacji (w tym ich nieujawniania) pozostających w mocy po zakończeniu współpracy (tzw. exit interview).
 - Zasady postępowania w przypadki zmiany zakresu obowiązków, powiązane ze zmianą posiadanych przez pracownika lub współpracownika uprawnień.

Bezpieczeństwo informacji w zarządzaniu dostawcami

Procesy zakupowe oraz procesy zarządzania dostawcami, w tym usługodawcami, powinny uwzględniać aspekty ochrony informacji, w tym w związku z powierzaniem przetwarzania informacji podmiotom zewnętrznym oraz w związku z wykorzystywaniem dostarczanych przez te podmioty produktów i usług.

W szczególności należy wziąć pod uwagę:

- Specyfikację wymagań w zakresie ochrony informacji dla dostarczanych produktów i usług.
- Wiarygodność potencjalnych dostawców i ich zdolność do zapewnienia należytej ochrony powierzanych informacji. W przypadku kluczowych dostawców ocena wiarygodności nie powinna ograniczać się wyłącznie do etapu wyboru dostawcy, ale powinna być przeprowadzana okresowo, w ramach nadzoru nad dostawcą,

zwłaszcza, gdy pojawiają się wątpliwości co do jego wiarygodności (np. incydenty z udziałem dostawcy, materiały prasowe o negatywnym wydźwięku itp.), a także w przypadku zmian, które mogą wpłynąć na możliwość należytego świadczenia usług przez dostawcę (np. zmiany właścicielskie, zmiany profilu działalności).

- Minimalizację ryzyka związanego z uzależnieniem organizacji od dostawcy.
- Ograniczenia prawne związane z możliwością korzystania z produktów i usług dostawcy, w tym wynikające z uznania go za dostawcę wysokiego ryzyka.
- Identyfikację i zarządzanie ryzykiem związanym z bezpieczeństwem łańcucha dostaw. Zakres działań związanych z oceną podwykonawców i poddostawców będzie uzależniony od charakteru dostaw lub usługi – obejmować może zarówno ocenę przed zawarciem umowy jak i dalsze działania związane z nadzorem nad jej realizacją – pamiętając, że stroną umowy jest dostawca i to on jest odpowiedzialny za zapewnienie możliwości nadzoru nad podwykonawcami. Należy również mieć na uwadze ograniczenia dostawcy w zakresie nadzoru nad poddostawcami - przykładem może być sytuacja, gdy kontrahent wykorzystuje usługi globalnej chmury publicznej.
- Klauzule umowne precyzujące wymagania w zakresie bezpieczeństwa informacji. Wymagania te nie muszą ograniczać się do ogólnych klauzul o zachowaniu poufności i stosowania dobrych praktyk w zakresie zarządzania bezpieczeństwem, ale mogą definiować wymagane środki bezpieczeństwa informacji – zarówno techniczne jak i organizacyjne, w tym związane z kompetencjami i świadomością personelu.
- Wymagania prawne związane ze współpracą z dostawcą, w tym związane z powierzeniem przetwarzania danych osobowych. Powyższe wiąże się z zawarciem umowy o powierzeniu przetwarzania danych osobowych, ale również (co jest elementem powyżej umowy) kwestią podpowierzenia przetwarzania i identyfikacji podprocesorów (co z kolei wiąże się z problemem bezpieczeństwa łańcucha dostaw) oraz rzeczywistym miejscem przetwarzania powierzonych danych osobowych, z uwzględnieniem działań podprocesorów.
- Prawo do przeprowadzania audytu strony drugiej lub zlecenia przeprowadzania takiego audytu podmiotowi zewnętrznemu. Należy doprecyzować sposób, zasady i terminy przeprowadzania audytu, uwzględniając fakt, że prawo do przeprowadzenia audytu wprost wynika z art. 28 RODO regulującego kwestię powierzenia przetwarzania danych osobowych.

-
- Monitorowanie jakości świadczonych usług, w tym z uwagi na aspekty bezpieczeństwa informacji i inicjowanie działań naprawczych w sytuacjach tego wymagających.

Zarządzanie ciągłością przetwarzania informacji

Zapewnienie ciągłości przetwarzania informacji obejmuje zarówno wprowadzenie środków ograniczających ryzyko przerwy w realizacji procesów jak i zaplanowanie działań umożliwiających kontynuację krytycznych procesów w sytuacji kryzysowej. Zarządzanie ciągłością działania, oprócz uwzględnienia w ramach zarządzania ryzykiem i działaniach szkoleniowo-uświadamiających, obejmować powinno:

- Identyfikację wymagań, w tym określenie dopuszczalnych przestojów w realizacji procesów, dopuszczalnej utraty danych przetwarzanych w organizacji, a także dopuszczalnego spadku wydajności w sytuacji kryzysowej. Wymagania te są określane w ramach analizy wpływu na działalność (*BIA – ang. Business Impact Analysis*). Podobnie jak w przypadku zarządzania ryzykiem, analiza BIA powinna być okresowo ponawiana, a wnioski z niej wynikające powinny być uwzględniane przy aktualizacji zarządzania ciągłością działania organizacji.
- Określenie i wdrożenie strategii określającej podejście do zapewnienia ciągłości działania na poziomie adekwatnym do zidentyfikowanych wymagań.
- Plany ciągłości działania określające sposób postępowania w celu zapewnienia ciągłości realizacji krytycznych procesów. Uruchomienie planów wynika z wystąpienia incydentu skutkującego istotnym zakłóceniem działania organizacji –niezbędne jest zatem powiązanie działań w zakresie zarządzania ciągłością działania z zarządzaniem incydentami.
- Procedury odtworzeniowe zapewniające przywrócenie organizacji do stanu sprzed sytuacji kryzysowej.
- Zasady komunikacji w sytuacji kryzysowej. Obejmują one zarówno komunikację wewnętrzną, w tym związaną z realizacją planów ciągłości działania i procedur odtworzeniowych, jak i komunikację zewnętrzną, w tym z klientami i dostawcami. Zasady te powinny w szczególności uwzględniać fakt braku dostępu do określonych metod komunikacji spowodowany wystąpieniem sytuacji kryzysowej.
- Przeprowadzanie okresowych testów ciągłości działania i testów odtworzeniowych. Działania te powinny uwzględniać nie tylko weryfikację

gotowości organizacji do stawienia czoła sytuacji kryzysowej ale również umożliwiać przygotowanie personelu do efektywnej realizacji planów i procedur.

Dokumentacja zarządzania bezpieczeństwem informacji

Struktura dokumentacji zarządzania bezpieczeństwem informacji powinna być dostosowana do specyfiki danej organizacji i zgodna ze stosowanymi w tej organizacji praktykami. Istotne jest aby:

- Dokumentacja była opracowywana w sposób zapewniający możliwość jej dystrybucji zgodnie z zasadą wiedzy uzasadnionej. Oznacza to, między innymi, wydzielenie dokumentów, których treść jest przeznaczona dla ograniczonej grupy odbiorców i unikanie sytuacji, w których dokumenty te będą rozpowszechniane w organizacji.
- Został zachowany spójny format dokumentacji, zapewniający możliwość kontroli wersji i jednoznaczne określenie aktualnej wersji dokumentacji.
- Dokumentacja była formalnie zatwierdzana jako obowiązująca w organizacji.
- Dokumentacja była dystrybuowana w sposób umożliwiający zapoznanie się z nią przez osoby upoważnione.
- Poprzednie wersje dokumentacji były archiwizowane zgodnie z zasadami obowiązującymi w organizacji, zaś zbędne wersje były usuwane.
- Dokumentacja podlegała przeglądom pod kątem jej aktualności. Przeglądy powinny być przeprowadzane okresowo, a także w przypadku wystąpienia zdarzeń, które mogą świadczyć o konieczności jej zaktualizowania – związanych zarówno ze zmianami w organizacji i jej środowisku jak i zidentyfikowanymi przypadkami nieskuteczności procesów zarządzania bezpieczeństwem.
- Wprowadzanie nowych dokumentów i ich nowych wersji było poprzedzone uzgodnieniami w celu potwierdzenia przydatności dla organizacji.

Elementem dokumentacji zarządzania bezpieczeństwem informacji są również zapisy potwierdzające realizację wymaganych działań. Z praktycznego punktu widzenia pożądanym jest aby, tam gdzie jest to możliwe, zapisy takie były tworzone w sposób automatyczny, wykorzystując funkcjonalność systemów informatycznych i zabezpieczeń technicznych. Z uwagi na możliwą obecność danych wrażliwych dostęp do zapisów powinien być ograniczony i kontrolowany. Same zapisy powinny być

przechowywane w sposób ograniczający ryzyko ich uszkodzenia lub modyfikacji, przez czas wynikający z wprowadzonych w organizacji regulacji, z uwzględnieniem obowiązujących wymagań prawnych.

Nadzór nad bezpieczeństwem przetwarzania informacji

Nadzór nad bezpieczeństwem przetwarzania informacji ma na celu nie tylko weryfikację zgodności z przyjętymi zasadami, ale również ocenę ich efektywności i realizację działań doskonalących. W skład nadzoru mogą wchodzić działania obejmujące w szczególności:

- Pomiar skuteczności i efektywności procesów zarządzania bezpieczeństwem w oparciu o kluczowe wskaźniki efektywności (KPI¹⁰).
- Identyfikację możliwych zmian w poziomie zidentyfikowanego ryzyka w oparciu o kluczowe wskaźniki ryzyka (KRI¹¹).
- Audyty wewnętrzne i zewnętrzne.
- Audyty dostawców.
- Testy bezpieczeństwa infrastruktury informatycznej, systemów i aplikacji.
- Przeglądy konfiguracji systemów informatycznych.
- Testy socjotechniczne.
- Przeglądy potwierdzające przydatność, adekwatność i skuteczność zarządzania bezpieczeństwem informacji.

W wyniku powyższych mogą być identyfikowane i wdrażane działania korekcyjne usuwające zidentyfikowane problemy wraz z działaniami korygującymi usuwającymi przyczynę ich wystąpienia, a także działania doskonalące w zakresie zarządzania bezpieczeństwem informacji.

¹⁰ ang. *key performance indicator*

¹¹ ang. *key risk indicator*