Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

Sprawozdanie

Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

za 2024 rok

2025

TLP: CLEAR

Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2024 rok

Spis treści

Spis Rysunków: 11
Spis Tabel: 11
Wstęp 13
1 Podsumowanie zarządcze 14
2 Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa 16
2.1.1 Przegląd Krajobrazu Cyberprzestrzeni 2024 r. 16
2.1.2 Zgłoszenia i incydenty cyberbezpieczeństwa 17
2.1.2.1 **Incydenty:** 17
2.1.2.2 **Zgłoszenia:** 17
2.1.3 Umocowanie instytucjonalne Pełnomocnika 18
2.1.4 Kolegium do Spraw Cyberbezpieczeństwa 19
2.1.5 Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC) 20
2.1.6 Rekomendacje i Komunikaty Pełnomocnika Rządu ds. Cyberbezpieczeństwa 20
2.1.7 Zespół Incydentów Krytycznych 21
2.1.8 Struktura KSC 22
2.2 Analiza i szacowanie ryzyka dla Krajowego Systemu Cyberbezpieczeństwa (KSC) na poziomie strategicznym 23
2.2.1 Cele analizy: 23
2.2.2 Analiza SWOT KSC 23
2.2.3 Analiza PESTLE KSC 23
2.2.4 Matryca oceny ryzyka 24
2.2.5 Rejestr ryzyka: 25
2.2.6 Podsumowanie 29
3 CSIRT-y poziomu krajowego 31
3.1 CSIRT GOV 32
3.1.1 Dane liczbowe dotyczące zgłoszeń i incydentów z podziałem zgodnym z art. 2 pkt. 5-9 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (KSC): 32
3.1.2 Działania prowadzone przez CSIRT GOV w obszarze cyberprzestrzeni RP 33
3.1.3 Zadania realizowane w 2024 r. 34
3.1.3.1 W 2024 r. ABW realizowała inne niż ww. zadania w ramach zespołu CSIRT — tj. czynności związane z bezpieczeństwem cyberprzestrzeni RP. Zaliczyć do nich można m.in.: 34
3.1.3.2 Analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa 35
3.1.3.3 Zidentyfikowane najpoważniejsze zagrożenia systemowe dla krajowego systemu cyberbezpieczeństwa 35
3.1.3.4 Zidentyfikowane najpoważniejsze zagrożenia techniczne dla systemów teleinformatycznych 36
3.1.3.5 Grupy APT 36
3.1.3.6 Identyfikowane najważniejsze zagrożenia, trendy i kampanie, wraz z opisem najważniejszych incydentów oraz stosowanych taktyk, technik i procedur (TTPs) 36
3.1.4 Wnioski i rekomendacje 37
3.1.5 Planowane działania w 2025 r. 37
3.1.6 Prognoza sytuacji w cyberprzestrzeni na lata 2025-2026 38
3.2 **CSIRT MON** 39

3.2.1 Dane liczbowe dotyczące zgłoszeń i incydentów z podziałem zgodnym z art. 2 pkt. 5-9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa 39
3.2.2 Opis najważniejszych incydentów 39
3.2.3 Informacje nt. grup (APT, cyberprzestępczych, haktywistycznych) dokonujących cyberataków wymierzonych w Polskę 40
3.2.4 Zidentyfikowane najpoważniejsze zagrożenia. 41
3.3 CSIRT NASK 42
3.3.1 Dane dotyczące liczby zgłoszeń i incydentów w 2024 r. 42
3.3.2 Incydenty ustawowe w podziale na sektory w 2024 r. 42
3.3.3 Najczęstsze typy incydentów wg taksonomii eCSIRT.net w 2024 r. 42
3.3.4 Zgłoszenia SMS oraz wzorce fałszywych wiadomości SMS 43
3.3.5 Zgłoszenia nielegalnych treści 43
3.3.6 Incydenty zarejestrowane przez zespół Dyżurnet.pl od 1 stycznia do 31 grudnia 2024 r. 43
3.3.7 Działania grup APT obserwowane przez CSIRT NASK w 2024 r. 44
3.3.8 Wybrane kampanie 44
3.3.8.1 UNC1151/Ghostwriter 44
3.3.8.2 APT28/Fancy Bear/Forest Blizzard 47
3.3.9 Współpraca krajowa i międzynarodowa oraz udział w projekcie FETTA 48
3.3.10 Opis najważniejszych realizowanych działań w obszarze cyberbezpieczeństwa 49
3.3.11 Analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa 50
3.3.12 Zidentyfikowane najpoważniejsze zagrożenia Techniczne dla systemów teleinformatycznych: 50
3.3.13 Zidentyfikowane najpoważniejsze zagrożenia Systemowe dla krajowego systemu cyberbezpieczeństwa: 51
3.3.14 Wnioski i rekomendacje 51
3.3.15 Planowane działania w 2025 r. 51
3.3.16 Przewidywania dotyczące sytuacji w cyberprzestrzeni na lata 2025–2026 52
4 Organy właściwe do spraw cyberbezpieczeństwa i sektorowe zespoły cyberbezpieczeństwa 53
4.1 Sektor energii (MKiŚ) 54
4.1.1 Działania zrealizowane w 2024 r. 54
4.1.1.1 Identyfikacja oraz prowadzenie postępowań administracyjnych wobec operatorów usług kluczowych z sektora energii 54
4.1.1.2 Nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa 54
4.1.1.3 Prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa sektora energii 55
4.1.1.4 Udział w ćwiczeniach cyberbezpieczeństwa poziomu krajowego i międzynarodowego 55
4.1.1.5 Zespół ds. monitorowania cyberbezpieczeństwa sektora energii 55
4.1.1.6 Współpraca międzynarodowa 56
4.1.2 Inne zadania 57
4.1.3 Analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa 57
4.1.4 Wnioski i rekomendacje. 58
4.1.5 Planowane działania w 2025 r. 59
4.2 Działania Ministra Obrony Narodowej jako organu właściwego do spraw cyberbezpieczeństwa 60
4.3 Sektor bankowy i infrastruktury rynków finansowych (KNF) 61

4.3.1 Zadania 61
4.3.1.1 Analiza podmiotów rynku finansowego w zakresie spełnienia kryteriów 61
4.3.1.2 Bieżący nadzór, w tym przekazywanie informacji oraz kontrole Operatorów Usług Kluczowych 61
4.3.1.3 Działania edukacyjne 61
4.3.1.4 DORA (Digital Operational Resilience Act) 62
4.3.1.5 EU-SCICF – koordynacja cyberincydentów charakterze systemowym 62
4.3.2 Działalność sektorowa zespołu Cyberbezpieczeństwa CSIRT KNF 62
4.3.2.1 Przeciwdziałanie atakom ransomware 62
4.3.2.2 Bezpieczeństwo Infrastruktury Podmiotów Nadzorowanych 62
4.3.2.3 Wymiana Informacji o Cyberzagrożeniach 63
4.3.2.4 Ochrona Nieprofesjonalnych Uczestników Rynku 63
4.3.3 Planowane działania w 2025 r. 63
4.4 Sektor ochrony zdrowia (z wyłączeniem podmiotów podległych MON) (MZ) 64
4.4.1 Podjęte przedsięwzięcia 64
4.4.2 Pozostałe zadania 65
4.4.3 Planowane działania w 2025 r. 65
4.4.4 Centrum e- Zdrowia (CeZ) – CSIRT CeZ 65
4.4.4.1 Statystyki obsłużonych incydentów 65
4.4.4.2 Opis najważniejszych incydentów 66
4.4.4.3 Liczba przeskanowanych podmiotów i wykrytych podatności 67
4.4.4.4 Najczęściej występujące podatności i błędy konfiguracyjne: 67
4.4.4.5 Podsumowanie 67
4.4.4.6 Statystyki błędów konfiguracyjnych i podatności 67
4.4.4.6.1 Zakres danych 68
4.4.4.7 Najczęściej występujące błędy konfiguracyjne 68
4.4.4.8 Wyniki i statystyki 68
4.4.4.9 Dane z innych źródeł, w tym od osób prywatnych 69
4.4.4.10 Podsumowanie 69
4.4.4.10.1 Współpraca z innymi zespołami cyberbezpieczeństwa 69
4.4.4.10.2 Podnoszenie świadomości o cyberzagrożeniach 70
4.4.4.10.3 Analiza sektora 70
4.4.4.11 Wnioski 71
4.4.5 Planowane działania 72
4.5 Działania Ministra Infrastruktury jako organu właściwego do spraw cybebrzpieczeństwa (MI) 73
4.5.1 Zadania i Działania statutowe, jako organu właściwego 73
4.5.2 Prace nad nowelizacją ustawy o KSC 73
4.5.3 CSIRT sektorowy 73
4.5.4 Zakłócenia sygnału GNSS 74
4.5.5 Centra Wymiany Informacji i Analiz (ISAC) 74
4.5.6 Dojrzałość podmiotów z nadzorowanych sektorów w obszarze cyberbezpieczeństwa i ich gotowość do wejścia w życie Dyrektywy NIS2 74
4.5.7 Współpraca z Urzędem Lotnictwa Cywilnego 74

4.5.8 System S46 ... 75
4.5.9 Udział w wydarzeniach ... 75
4.5.10 Pozostałe zagadnienia ... 75
4.5.11 Wnioski i rekomendacje ... 75
4.5.12 Planowane działania w 2025 r. ... 76
4.6 Działania Ministra Cyfryzacji jako organu właściwego do spraw cybebrzpieczeństwa (MC) ... 77
4.6.1 Realizowane zadania ... 77
4.6.2 Forum Organów Właściwych ... 77
4.6.3 System S46 ... 77
4.6.4 Budowa sektorowego zespołu cyberbezpieczeństwa CSIRT-Cyfra ... 78
5 Służby Specjalne ... 79
5.1 Agencja Wywiadu (AW) ... 80
5.1.1 Rozwój krajowego systemu cyberbezpieczeństwa ... 80
5.1.1.1 Wdrożenie i ocena funkcjonowania przepisów o KSC ... 80
5.1.1.2 Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa ... 80
5.1.1.3 Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym ... 80
5.1.1.4 Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej ... 81
5.1.1.5 Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym ... 81
5.1.1.6 Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym ... 81
5.1.1.7 Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń ... 81
5.1.1.8 Bezpieczeństwo łańcucha dostaw ... 81
5.1.1.9 Testy i audyty cyberbezpieczeństwa ... 82
5.1.2 Zwiększenie potencjału - Podmiot realizujacy zadania Strategii ... 82
5.1.2.1 Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa ... 82
5.1.2.2 Nastawienie na rozwój współpracy między sektorem publicznym i prywatnym ... 82
5.1.3 Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa RP ... 82
5.1.3.1 Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni ... 83
5.1.3.2 Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym ... 83
5.2 Agencja Bezpieczeństwa Wewnętrznego (ABW) ... 83
5.3 Służba Wywiadu Wojskowego (SWW) ... 83
5.4 Służba Kontrwywiadu Wojskowego (SKW) ... 84
5.4.1 Działania SKW mające na celu przeciwdziałanie aktywności Rosyjskich Służb Specjalnych (RSS) 84
5.4.1.1 Ocena skuteczności i efektów przeciwdziałania aktywności SVR ukierunkowanej na systemy informatyczne ambasad oraz oprogramowania „TeamCity” ... 84
5.4.1.2 Operacja DYINGEMBER ... 84
5.4.2 Inne zidentyfikowane zagrożeniea w których rozpoznaniu brało udział SKW - Manipulacja systemai steroania stsemów oczyszczania wody ... 84
5.4.3 Prognozy i przewidywania ... 85
5.4.3.1 wykorzytsanbe urządzeń SOHO do prowadzenia budowy infrastruktury operacyjenj ... 85

5.4.3.2 zagrożenia dla systemów przemysłowych ... 85
6 Zwalczanie cyberprzestępczości ... 86
6.1 Ministerstwo Sprawiedliwości (MS) ... 87
6.1.1 Podjęte przedsięwzięcia ... 87
6.1.2 Wnioski i rekomendacje ... 87
6.2 Prokuratura Krajowa ... 89
6.2.1 Podjęte działania ... 89
6.2.2 Działania planowane do relaizacji w latach 2025 — 2027 ... 89
6.2.3 Dane statystyczne dot. działalności ... 90
6.3 Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) ... 91
6.3.1 Zadania CBZC ... 91
6.3.2 Działania podjęte w 2024 r. ... 92
6.3.3 Dane dotyczące wyników w zwalczaniu cyberprzestępczości w kategoriach będących w szczególnym zainteresowaniu CBZC za rok 2024 ... 92
6.3.4 Rekomendacje ... 92
6.4 Komenda Główna Polcji (KGP) ... 93
6.4.1 Zadania i rola KGP ... 93
6.4.2 Rekomendacje: ... 94
6.5 Centralne Biuro Antykorupcyjne (CBA) ... 95
6.5.1 Zadania ... 95
7 Ministerstwo Obrony Narodowej (MON) ... 96
7.1 Działania realizowane przez resort obrony narodowej w zakresie cyberbezpieczeństwa, w szczególności służące realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 96
7.1.1 Wdrożenie i ocena funkcjonowania przepisów o krajowym systemie cyberbezpieczeństwa ... 96
7.1.2 Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa ... 96
7.1.3 Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej 97
7.1.4 Zwiększanie zdolności do zwalczania cyberprzestępczości,w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym ... 97
7.1.5 Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń ... 97
7.1.6 Bezpieczeństwo łańcucha dostaw oraz testy i audyty bezpieczeństwa ... 97
7.1.7 Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa ... 97
7.1.8 Zwiększanie kompetencji instytucjonalnych oraz realizacja współpracy między sektorem publinczym i prywatnym ... 98
7.1.9 Zwiększenie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa RP ... 99
7.1.10 Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli ... 100
7.1.11 Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym ... 100
7.1.12 Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym z podmiotami zewnętrznymi ... 101
7.2 Wnioski i rekomendacje ... 101
7.3 Predykcje dotyczące sytuacji w cyberprzestrzeni na lata 2025-2026. ... 103
7.4 Planowane działania w 2025 r. ... 103
8 Inne instytucje współtworzące KSC ... 104
8.1 Ministerstwo Edukacji Narodowej (MEN) ... 104

8.1.1 Polityka Cyfrowej Transformacji Edukacji (PCTE) ... 104
8.1.2 Inne zadnia związane z cyberbezpieczeństwem ... 104
8.1.3 Wnioski i rekomendacje ... 105
8.2 Ministerstwo Spraw Wewnętrznych i Administracji (MSWIA) ... 106
8.2.1 Opis najważniejszych realizowanych działań dotyczących cyberbezpieczeństwa w obszarze odpowiedzialności Ministra SWiA ... 106
8.2.1.1 Działania realizowane przez MSWiA ... 107
8.2.1.2 Działania realizowane przez Policję ... 109
8.2.1.3 Działania realizowane przez Straż Graniczną ... 109
8.2.1.4 Działania realizowane przez Państwową Straż Pożarną ... 110
8.2.1.5 Działania realizowane przez Służbę Ochrony Państwa ... 111
8.2.2 Wnioski i rekomendacje ... 111
8.2.2.1 Zapewnienie odpowiednich zasobów dla cyberbezpieczeństwa ... 111
8.2.2.2 Ochrona informacji o infrastrukturze krytycznej ... 112
8.2.2.3 Brak umocowań dla usług chmurowych w zakresie informacji klauzulowanych ... 113
8.2.2.4 Powszechne wykorzystywanie rozwiązań chmurowych (cloud) ... 113
8.2.2.5 Wprowadzenie systemów AI do infrastruktury bezpieczeństwa ... 114
8.2.2.6 Uruchomienie Systemu Bezpiecznej Łączności Państwowej (SBŁP) ... 114
8.2.2.7 Realizacja celu odporności NATO „Odporne Systemy Łączności Cywilnej” ... 116
8.2.2.8 Modernizacja infrastruktury TESTA-ng ... 116
8.2.2.9 Uruchomienie bezpiecznej łączności satelitarnej *Secure Connectivity* ... 116
8.2.2.10 Budowa centrów kompetencyjnych odpowiedzialnych za zapewnienie cyberbezpieczeństwa dla komunikacji krytycznej ... 117
8.2.3 Przewidywania dotyczące sytuacji w cyberprzestrzeni na lata 2025-2026 ... 117
8.3 Rządowe Centrum Bezpieczeństwa (RCB) ... 119
8.3.1 Zrealizowane przedsięwzięcia ... 119
8.4 Rada do Spraw Cyfryzacji (RdsC) ... 120
8.4.1 O radzie ... 120
8.4.2 Zrealizowane przedsięwzięcia ... 120
8.4.3 Podjęte stanowiska ... 121
8.5 Ministerstwo Rozwoju i Technologii (MRiT) ... 122
8.5.1 Podjęte przedsięwzięcia – „Biznes.gov.pl” ... 122
8.6 Ministerstwo Finansów (MF) ... 123
8.6.1 Opis najważniejszych realizowanych działań w obszarze cyberbezpieczeństwa. ... 123
8.6.2 Zidentyfikowane najpoważniejsze zagrożenia systemowe dla krajowego systemu cyberbezpieczeństwa: ... 124
8.6.3 Planowane działania w 2025 r. ... 124
8.7 Urząd Komunikacji Elektronicznej (UKE) ... 125
8.7.1 Najważniejsze działania w obszarze cyberbezpieczeństwa ... 125
8.7.1.1 Wdrożenie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej ... 125
8.7.1.2 Budowa świadomości w obszarze cyberbezpieczeństwa ... 125
8.7.2 Funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa ... 125
8.7.3 Zagrożenia dla sektora komunikacji elektronicznej i kraju ... 125

8.7.4 Wnioski i rekomendacje 125
8.7.5 Zasadnicze przedsięwzięcia planowane do realizacji w 2025 roku: owered by TCPDF (www.tcpdf.org) 126
8.7.6 Przewidywania dotyczące sytuacji w cyberprzestrzeni w latach 2025–2026: 126
8.8 Urząd Ochrony Danych Osobowych (UODO) 127
8.8.1 Podjęte przedsięwzięcia 127
8.8.2 Ocena funkcjonowania KSC 127
8.8.3 Planowane działania w 2025 r. 128
8.8.4 Prognoza sytuacji w cyberprzestrzeni na lata 2025-2026 128
9 Realizowane działania w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym 129
9.1 Rozwój krajowego systemu cyberbezpieczeństwa 129
9.1.1 Centrum Cyberbezpieczeństwa NASK (CCN) 129
9.1.2 Nowelizacja Rozporządzenia Rady Ministrów w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa 129
9.1.3 Projekty w ramach Krajowego Planu Odbudowy (KPO) 129
9.1.4 Plany działania przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń 130
9.1.5 Wdrożenie Dyrektywy NIS 2 131
9.1.6 Ustawa o kryptoaktywach 131
9.1.7 Standardy i Rekomendacje Cyberbezpieczeństwa 131
9.1.8 Projekt „PIONIER-Q w ramach European Quantum Communication Infrastructure” 132
9.2 Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty 133
9.2.1 System Komunikacji Rządowej – niejawnej (SKR-Z) 133
9.2.2 Projekt „Bezpieczny Komunikator” - Threema OnPrem 133
9.2.3 Usługa „Zastrzeż PESEL” 133
9.2.4 Usługa „Bezpiecznie w sieci” 133
9.2.5 Program „Cyberbezpieczny Samorząd” 134
9.2.6 Projekt „Osłona informacyjna kampanii wyborczej 2024 r.” 134
9.3 Realizowane zadania NASK-PIB w ramach udzielonej dotacji: 135
9.3.1 System „AntyDDoS” 135
9.3.2 Fundusz Cyberbezpieczeństwa – Świadczenie teleinformatyczne 136
9.3.3 Stopnie alarmowe CRP 136
9.4 Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa 137
9.4.1 Program Współpracy w Cyberbezpieczeństwie (PWCyber) 137
9.4.2 Upowszechnianie usług chmurowych w administracji rządowej 138
9.4.3 Prace nad dokumentem strategicznym w dziedzinie informatyzacji państwa 140
9.4.4 Forum Ochrony Infrastruktury Krytycznej Ministra Cyfryzacji 141
9.4.5 Krajowy planu działania do programu polityki „Droga ku cyfrowej dekadzie” do 2030 r. 141
9.4.6 Pozyskanie platfrmy Cyber Threat Intelligence, CTI 141
9.5 Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa 143
9.5.1 Portal „BezpieczeneDane.gov.pl” 143
9.5.2 Ustawa o ochronie małoletnich przed dostępem do treści nieodpowiednich w internecie 143
9.5.3 Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej 143

9.5.4 Program „Higiena Cyfrowa” 144
9.5.5 Monitoring treści o potencjale dezinformacyjnym w mediach społecznościowych 144
9.5.6 Projekt „Szkoła Międzypokoleniowa” 144
9.5.7 Usługa „Baza Wiedzy” 145
9.5.8 Certyfikacja w cyberbezpieczeństwie 145
9.5.9 Program „CYBERSECIDENT” 146
9.5.10 Zwalczanie niegodziwego traktowania dzieci w celach seksualnych w Internecie 146
9.5.11 Projekt „SecureV” - Szkolenia z cyberbezpieczeństwa dla najważniejszych osób w państwie 146
9.5.12 Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa 147
9.5.13 Projekty wspierające edukacje o cyberbezpieczeństwie – „Cyberlekcje” 148
9.5.14 „Baza wiedzy” o cyberbezpieczeństwie na portalu gov.pl 148
9.5.15 Ćwiczenia cyberbezpieczeństwa UE 148
9.5.16 Ćwiczenia KSC – „KSC-EXE 2024” 149
9.6 Budowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa 151
9.6.1 Współpraca w ramach Unii Europejskiej 151
9.6.1.1 Zespół „Cyberprzestrzeni” 151
9.6.1.2 Pojedynczy Punkt Kontaktowy 151
9.6.1.3 Prace legislacyjne w ramach UE 151
9.6.2 Współpraca w ramach ENISA 152
9.6.3 Współpraca bilateralna i multilateralna 152
9.6.4 Counter Ransomware Initiatives 153
9.6.5 Wsparcie dla Ukrainy i współpraca z Ukrainą 153
9.6.6 Mechanizm talliński 153
9.6.7 Inne organizacje międzynarodowe 153
9.6.8 Rozpoczęcie realizacji projektu „National Coordination Centre – Poland”, współfinansowanego z Programu Cyfrowa Europa 154
9.6.9 Rozpoczęcie naboru do Społeczności Kompetentnej w zakresie Cyberbezpieczeństwa 154
9.6.10 Realizacja inicjatyw promujących polskie innowacje w cyberbezpieczeństwie 154
9.6.11 Stworzenie nowych możliwości udzielania wsparcia w ramach pomocy de minimis dla polskich przedsiębiorców w obszarze cyberbezpieczeństwa. 155
9.6.12 Wsparcie dla budowania międzysektorowych i transgranicznych partnerstw pomiędzy podmiotami działającymi w obszarze cyberbezpieczeństwa. 155
9.6.13 Zachęcanie młodych talentów do podjęcia kariery w cyberbezpieczeństwie 155
10 Wnioski i rekomendacje 156
10.1.1 Poziom Realizacji wniosków ze Sprawozdania z roku 2023 156
11 Wnioski i rekomendacje za rok 2024 158
12 Planowane działania w 2025 r. 162
12.1.1 Nowelizacja ustawy o KSC 162
12.1.2 Przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029 162
12.1.3 Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42) 162
12.1.4 Dalsza realizacja projektu „National Coordination Centre – Poland” 162
12.1.5 Realizacja badania polskich małych i średnich przedsiębiorców działających w obszarze cyberbezpieczeństwa 163

12.1.6 Przeprowadzenie konkursu grantowego dla przedsiębiorców działających w branży cyberbezpieczeństwa 163
12.1.7 Dalsze bUdowanie społeczności kompetentnej w obszarze cyberbezpieczeństwa 163
13 Oznaczenia TLP **164**

SPIS RYSUNKÓW:

Rysunek 1. Schemat Krajowego Systemu Cyberbezpieczeństwa 22
Rysunek 2. Wykres porównujący liczbę incydentów obsłużonych przez właściwy CSIRT w latach 2023 i 2024 31
Rysunek 3. Incydenty zarejestrowane przez DYŻURNET.PL 43
Rysunek 4. Treść propagandowa zamieszczona przez grupę UNC1151 na stronie Polskiej Agencji Antydopingowej 46
Rysunek 5. Przykład treści dezinformacyjnej w serwisie Telegram 47
Rysunek 6. Przykład wiadomości użytej przez grupę APT28 do dystrybucji szkodliwego oprogramowania 47
Rysunek 7. Diagram przedstawiający poszczególne etapy infekcji 48
Rysunek 9. Liczba wykrytych podatności z klasyfikacją 67
Rysunek 10. Wykryte podatności w 2024 r. 69
Rysunek 14. Wyniki ankiety 70
Rysunek 11. Wyniki ankiety 70
Rysunek 12. Wyniki ankiety 70
Rysunek 13. Wyniki ankiety 70
Rysunek 15. Logo Cyberbezpieczny Samorząd 134
Rysunek 16. Logo programu AntyDDoS 136
Rysunek 17. Logo PWCyber 137
Rysunek 18. Uczestnicy konferencji podsumowującej pięciolecie programu PWCyber 138
Rysunek 19. Konferencja prasowa dot. publikacji Strategii Cyfryzacji Polski 140
Rysunek 20. Bezpiecznedane.gov.pl 143
Rysunek 21. Podpisanie projektu 145
Rysunek 22. Cyberlekcje 148
Rysunek 23. Ćwiczenia KSC-EXE 2024 149
Rysunek 24. Mechanizm Talliński 153
Rysunek 25. NCC-PL 154

SPIS TABEL:

Tabela 1. Zestawienie liczby zarejestrowanych incydentów 17
Tabela 2. Zestawienie liczby incydentów w klasyfikacji zgodnej z UKSC 17
Tabela 3. Zestawienie zgłoszeń i incydentów dla CSIRT NASK 18
Tabela 4. Zestawienie dwuletnie zgłoszeń i incydentów dla CSIRT NASK 18
Tabela 5. Zestawienie zgłoszeń i incydentów dla CSIRT GOV 18
Tabela 6. Zestawienie liczby incydentów zarejestrowanych w CSIRT MON 18
Tabela 7 Zestawienie tematyki Kolegium ds. Cyberbezpieczeństwa 20

Tabela 8 Zestawienie rekomendacji Pełnomocnika 21
Tabela 9 Zestawienie komunikatów Pełnomocnika 21
Tabela 10. Analiza SWOT dla KSC 23
Tabela 11. Analiza typu PESTLE dla KSC 23
Tabela 12. Skala oceny ryzyka 24
Tabela 13. Matryca oceny ryzyka dla KSC 24
Tabela 14. Rejestr ryzyka. 25
Tabela 15. Kwalifikacja incydentów 32
Tabela 16. Sektory występowania incydentów 32
Tabela 17. Kwalifikacja incydentów wg. KSC 33
Tabela 18. Kwalifikacja incydentów wg KSC 39
Tabela 19. Zestawienie zgłoszeń i incydentów 42
Tabela 20. Kwalifikacja incydentów wg. KSC 42
Tabela 21. Najpopularniejsze rodzaje ataków 43
Tabela 22. Liczba zgłoszeń wiadomości SMS oraz wzorce fałszywych wiadomości SMS 43
Tabela 23. Aktowość grup APT w ujęciu miesięcznym 44
Tabela 24. Dane zidentyfikowane przez CSIRT KNF w 2024 r. 63
Tabela 25. Incydenty obsłużone przez CSIRT CeZ w 2024r. 66
Tabela 26. Podział incydentów ze względu na typ w 2024r. 66
Tabela 27. Zestawienie liczby wykrytych podatności 67
Tabela 28. Zestawienie wykrytych podatności 68
Tabela 29. Raport z systemu N6 69
Tabela 34. Występowanie poszczególnych typów incydentów z podziałem na miesiące w 2024r. 71
Tabela 35. Osądzeni, skazani za wybrane przestępstwa w I instancji sądów rejonowych 88
Tabela 36. dane dot. osądzonych i skazanych za przestępstwo z art. 165 § 1 i 3 kk w I instancji sądów okręgowych za lata 2023 i 2024 r. 88
Tabela 37. Dane statystyczne dot. działalności Prokuratury Krajowej w zakresie zwalczania cyberprzestępczości 90
Tabela 38. Dane CBZC w zakresie realizacji zadań 92
Tabela 39. Zidentyfikowane kampanie 124
Tabela 40. Szkolenia w ramach programu SecureV 147
Tabela 41. Poziom realizacji wniosków z ze Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2023 156
Tabela 42. Oznaczenia TLP 164

WSTĘP

Rok 2024 był okresem intensywnych działań, dużych wyzwań i znaczących osiągnięć w obszarze cyberbezpieczeństwa w Polsce. W obliczu wzrostu poziomu zagrożeń i systematycznie rosnącej liczbie coraz bardziej zaawansowanych ataków w przestrzeni cyfrowej, wysiłki podmiotów tworzących krajowy system cyberbezpieczeństwa (KSC) skoncentrowane były na budowaniu odporności i zwiększaniu poziomu bezpieczeństwa Rzeczypospolitej Polski. W minionym roku podjęte zostały znaczne wysiłki celem wsparcia rozwoju technologii oraz wzmocnienie kompetencji specjalistów odpowiedzialnych za ochronę cyberprzestrzeni.

Niniejsze Sprawozdanie powstało na podstawie art. 63 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1] (dalej: UKSC). Stosownie do ww. przepisu Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (dalej: Pełnomocnik) opracowuje i przedkłada Radzie Ministrów w terminie do dnia 31 marca każdego roku Sprawozdanie za poprzedni rok kalendarzowy zawierające informacje o prowadzonej działalności w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym.

Dokument został opracowany przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji przy wykorzystaniu danych, informacji i materiałów własnych oraz udostępnionych przez instytucje publiczne, w tym w szczególności zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego, organy właściwe ds. cyberbezpieczeństwa, służby specjalne, organy ścigania oraz wymiaru sprawiedliwości i inne instytucje publiczne.

W niniejszym Sprawozdaniu przedstawione zostały kluczowe inicjatywy i przedsięwzięcia, które zostały podjęte w 2024 roku oraz rekomendacje na kolejne lata, mające na celu dalsze wzmacnianie cyberbezpieczeństwa w Polsce.

Informacje o charakterze wrażliwym i niejawne zostały zawarte w niejawnym[2] załączniku do niniejszego Sprawozdania, który zostanie udostępniony uprawnionym podmiotom.

Krzysztof Gawkowski

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Wiceprezes Rady Ministrów

Minister Cyfryzacji

[1] Dz.U. z 2024 r. poz. 1077

[2] W rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2024 r. poz. 632).

1 PODSUMOWANIE ZARZĄDCZE

Rok 2024 był czasem wyraźnego rozkwitu Krajowego Systemu Cyberbezpieczeństwa (KSC). Ten funkcjonujący od 2018 r. system przez lata działalności potwierdził swój potencjał i stał się jedną z kluczowych płaszczyzn funkcjonowania państwa. Przechodzi on rokrocznie kolejne, rzeczywiste testy swojej efektywności i sprawczości. Widoczna gołym okiem, stale przyśpieszająca cyfryzacja nie tylko życia społecznego, ale także procesów biznesowych i informacyjnych sprawia, skokowy wzrost znaczenia sfery cyfrowej dla stabilnego rozwoju cywilizacyjnego społeczeństwa. Powyższe jest również niezbędne dla zapewnienia ogólnego poziomu bezpieczeństwa i stabilności funkcjonować państwa w warunkach trudnego otoczenia polityczno-społecznego w jakim się obecnie znajdujemy. Jest to szczególnie dostrzegalne kontekście kolejnego roku pełnoskalowego i wielopłaszczyznowego konfliktu zbrojnego na Ukrainie, który bezpośrednio dotyka polskiej sfery cyfrowej. Polska jako państwo przyfrontowe będące głównym *hubem* logistycznym udzielanej pomocy wojskowej i politycznej dla państwa ukraińskiego, znajduje się pod stałą presją działań hybrydowych prowadzonych ze strony Rosji (FR) i Białorusi. W zakres ww. złośliwych aktywności wchodzą zarówno wrogie działania aktywne grup APT (*ang. Advanced Persistetnt Threat*) związanych bezpośrednio ze służbami specjalnymi państw nieprzyjaznych Polsce, jak również zależne od władz oraz pośrednio przez nie sterowane i inspirowane grupy haktywistyczne, czy ugrupowania zorganizowanej przestępczości kryminalnej prowadzącej szkodliwą aktywność hakerską w przestrzeni cyfrowej. Powyższe ma odzwierciedlenie w danych liczbowych dokumentujących, kolejny roczny wzrost liczby cyberataków na polskie podmioty.

Należy zaznaczyć, że 2024 rok, był również czasem swoistego nabrzmiewania fali nadchodzących technologicznych rewolucji związanych m.in. z rozwiązaniami chmurowymi, implementacją w narzędziach cyfrowych mechanizmów opartych o algorytmy sztucznej inteligencji (AI) i uczenia maszynowego czy początku międzynarodowego wyścigu w zakresie rozwiązań kwantowych oraz układów scalonych opartych o krzem. Wszystkie ww. aspekty obejmują swoim oddziaływaniem sferę bezpieczeństwa teleinformatycznego, stanowiącego *clue* istnienia KSC oraz będą stanowiły ogromne wyzwanie dla efektywności systemu w nadchodzących latach. Dlatego też KSC wymaga wzmożonej uwagi i wysiłków koordynacyjnych, celem zachowania swojego wysokiego stopnia sprawczości w dynamicznie zmieniającym się otoczeniu technologicznym i legislacyjnym.

Na chwile obecną w KSC strategiczną rolę odgrywa Ministerstwo Cyfryzacji – w strukturze kierownictwa resortu umocowana jest funkcja Pełnomocnika Rządu ds. Cyberbezpieczeństwa, które odpowiada m.in. za kreowanie i organizowanie ww. systemu.

Zgodnie z przyjętą praktyką zarządczą KSC, na poziomie operacyjnym realizowane są procesy reagowania na zagrożenia bezpieczeństwa teleinformatycznego. Kluczowa rola w tym zakresie przypisana jest do trzech zespołów reagowania na incydenty - CSIRTów poziomu krajowego (CSIRT NASK, CSIRT GOV, CSIRT MON), dysponujących newralgicznymi wiedzą i kompetencjami w zapewnianiu bezpieczeństwa KSC w warstwie technicznej.

Należy zaznaczyć, że w swoich w swoich sektorach wzrasta aktywność działalności organów właściwych, z których część powołała własne sektorowe zespoły cyberbezpieczeństwa (CSIRT KNF, CEZ), a cześć rozpoczęła proces ich utworzenia. Projektowana nowelizacja UKSC przewiduje przeformowanie tych podmiotów w CSIRT-y sektorowe.

Dla stabilności KSC na poziomie strategiczno-politycznym kluczowe znaczenie ma organ doradczy, jakim jest Kolegium ds. Cyberbezpieczeństwa. W jego skład wchodzą reprezentanci najważniejszych instytucji odpowiedzialnych za bezpieczeństwo narodowe i publiczne RP.

Ponadto w 2024 roku, coraz większą rolę w bieżącej koordynacji działań i reagowaniu na incydenty, odgrywało Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC), ustanowione przez Ministerstwo Cyfryzacji przy wsparciu Ministerstwa Obrony Narodowej (MON) i Rządowego Centrum Bezpieczeństwa (RCB). W spotkaniach uczestniczyli przedstawiciele kluczowych instytucji dla bezpieczeństwa teleinformatycznego na poziomie krajowym. Należy również pamiętać o kluczowej roli służb kontrwywiadowczych i wywiadowczych w zapewnianiu bezpieczeństwa narodowego, także w cyberprzestrzeni oraz roli organów ścigania w zwalczaniu cyberprzestępczości. Dlatego

funkcjonowanie PCOC jest niezbędne dla płynnej wymiany informacji pomiędzy instytucjami zapewniającymi bezpieczeństwo cyberprzestrzeni i obywateli RP, którzy się w niej poruszają.

Niniejsze Sprawozdanie obejmuje kluczowe działania podejmowane w celu zwiększenia poziomu bezpieczeństwa cyberprzestrzeni w Polsce. Priorytetem było rozwijanie zaawansowanych narzędzi i systemów technologicznych, które zapewniają cyberbezpieczeństwo. Równie istotnym elementem było zapewnienie odpowiednich zasobów kadrowych z właściwymi kompetencjami, co umożliwiło świadczenie teleinformatyczne, pozwalające na wynagrodzenie specjalistów ds. cyberbezpieczeństwa w sektorze publicznym na poziomie zbliżonym do płac w sektorze prywatnym. W zakresie działań edukacyjnych i szkoleniowych na poziomie ogólnospołecznym, konieczne jest kontynuowanie działań mających na celu podnoszenie wiedzy zarówno w zakresie podstawowej higieny cyfrowej i świadomości zagrożeń, jak i rozwijaniu specjalistycznych kompetencji technicznych.

W roku 2025, Krajowy System Cyberbezpieczeństwa będzie podlegał istotnym zmianom, wynikającym z konieczności wdrożenia do polskiego porządku prawnego dyrektywy NIS2 oraz innego prawodawstwa Unii Europejskiej (m.in. *Toolbox 5g*). Powyższe zostanie zrealizowane poprzez uchwalenie procedowanej nowelizacji UKSC. Ponadto zostanie przyjęta nowa Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029, zawierająca wnioski i doświadczenia z dotychczasowego funkcjonowania KSC oraz która zaadoptuje wyzwania związane z postępem technologicznym, zmianami społecznymi i prawnymi oraz ewolucją środowiska bezpieczeństwa.

Jednym z głównych wniosków dotyczących usprawnienia funkcjonowania KSC jest potrzeba utworzenia centralnego podmiotu koordynującego cyberbezpieczeństwo na szczeblu krajowym. Takie rozwiązanie znacząco poprawiłoby zarządzanie bezpieczeństwem cyberprzestrzeni w Polsce oraz umożliwiłoby bardziej efektywne i szybsze reagowanie na pojawiające się zagrożenia. Docelowo odciążyłoby również aktualnie zaangażowane instytucje w realizacji obowiązków wynikających z UKSC, co skutkowałoby możliwością zaangażowania zasobów do realizacji innych kluczowych dla bezpieczeństwa państwa, ustawowych zadań tych instytucji.

2 PEŁNOMOCNIK RZĄDU DO SPRAW CYBERBEZPIECZEŃSTWA

2.1.1 PRZEGLĄD KRAJOBRAZU CYBERPRZESTRZENI 2024 R.

2024 rok był kolejnym rokiem cechującym się wzrostem poziom zagrożeń w cyberprzestrzeni w skali globalnej. Polska również odnotowała ich wysoki poziom. Zarejestrowano wzrost aktywność grup prowadzących nielegalne działania w świecie cyfrowym, oraz odnotowany został wyraźny wzrost liczby incydentów cyberbezpieczeństwa przez CSIRTy poziomu krajowego.

Rozprzestrzenianie się cyberataków wynikało również z pojawienia się nowych typów zagrożeń, które powstały w wyniku rozwoju innowacyjnych technologii oraz ich rosnącej dostępności, jak modele AI.

W nadchodzących latach przewiduje się dalsze nasilenie trendu wzrostu skali cyberataków. Już obecnie zauważalna jest tendencja wzrostowa w zakresie występowania grup hackerskich motywowanych finansowo, często działających w ramach międzynarodowej przestępczości zorganizowanej. Liczba incydentów bezpieczeństwa związanych z internetowymi oszustwami finansowymi stanowi największą część wszystkich zarejestrowanych zdarzeń, i częściej opiera się na wykorzystywaniu szeroko pojętych technik socjotechnicznych niż na zaawansowanych technologicznie atakach związanych z m.in. infekowaniem systemów czy wykorzystywaniem podatności bezpieczeństwa.

Ponadto należy zwrócić szczególną uwagę na ataki typu APT oraz sponsorowane przez państwa nieprzychylne Polsce. Mogą cechować się długotrwałym charakterem, wykorzystaniem zaawansowanych narzędzi, nowatorskich technologii oraz specjalistycznej wiedzy napastników. Są one wysoce zaawansowane, trudne do wykrycia, a adekwatna reakcja na nie wymaga wielowarstwowej struktury systemów ochronnych oraz specjalistycznej wiedzy i często doświadczenia pracowników zespołów bezpieczeństw IT.

Dotychczas obserwowane trudności w jednostkach publicznych związane z rekrutacją wykwalifikowanej kadry na kluczowe stanowiska odpowiedzialne za bezpieczeństwo zasobów, jak również znaczne obciążenie obecnych pracowników licznymi obowiązkami mogą w pewnym momencie doprowadzić do przeciążania systemu zabezpieczeń.

Wzrost napięć w sferze bezpieczeństwa międzynarodowego, zwłaszcza przeciągający się konflikt na Ukrainie w zestawieniu z rosnącą liczbą systemów (przy jednocześnie często niewystarczających zasobach ludzkich i finansowych w niektórych instytucjach, głównie lokalnych), mogą mieć poważne konsekwencje nie tylko dla poszczególnych podmiotów, ale całego systemu bezpieczeństwa publicznego czy narodowego.

Rosnące koszty infrastruktury bezpieczeństwa stanowią poważne obciążenie dla jednostek sektora finansów publicznych. Konieczne są dalsze działania wzmacniające KSC, koordynacja działań, zwiększenie potencjału instytucji oraz zapewnienie odpowiednich środków finansowych na rozwój kadrowy i technologiczny.

Nieustanny konflikt w cyberprzestrzeni, wojna Rosji z Ukrainą, hybrydowe działania przeciwko Zachodowi, wojny handlowe i technologiczne, dynamiczna digitalizacja oraz rozwój przełomowych technologii to kluczowe czynniki diametralnie zmieniające świat. Nowe technologie, takie jak AI, chmura obliczeniowa, big data, informatyka kwantowa i łączność nowej generacji, odgrywają kluczową rolę w cyberbezpieczeństwie. AI umożliwia szybkie wykrywanie i reagowanie na zagrożenia poprzez analizę dużych zbiorów danych w czasie rzeczywistym. Systemy oparte o AI adaptują się do nowych zagrożeń, automatycznie aktualizują strategie obronne, szybko reagują na incydenty i przewidują ataki dzięki algorytmom uczenia maszynowego.

W 2024 roku Polska była obiektem licznych cyberataków, w tym operacji wrogich państw, mających na celu pozyskanie informacji, rozpoznanie systemów ICT, zakłócenie infrastruktury krytycznej oraz szerzenie dezinformacji. Jednakże wyłącznie CSIRT NASK zanotował wzrost liczby zarejestrowanych incydentów. Pozostałe CSIRTy poziomu krajowego odnotowały spadek rejestracji liczby incydentów w stosunku do roku poprzedniego, co świadczy, że stały zakres odpowiedzialności wpływa na stabilność całego systemy oraz o rosnącej świadomości obywateli nt. znaczenia zgłaszania zagrożeń.

2.1.2 ZGŁOSZENIA I INCYDENTY CYBERBEZPIECZEŃSTWA

2.1.2.1 INCYDENTY:

W 2024 r. CSIRTy poziomu krajowego sumarycznie zarejestrowały 111 660 incydentów bezpieczeństwa teleinformatycznego, z czego CSIRT NASK zarejestrował 103 449 (wzrost 29% rdr), CSIRT GOV 3 991 (spadek 16% rdr), natomiast CSIRT MON 4 220 (spadek 28% rdr). Powyższe zestawienie liczby incydentów, zostało zawarte w tabeli poniżej (tab.1). Analiza wskaźników wskazuje wyraźny trend wzrostowy rejestrowanych incydentów w skali krajowej (23% rdr).

Tabela 1. Zestawienie liczby zarejestrowanych incydentów

CSIRT poziomu krajowego:	2023 r.	2024 r.	Zmiana procentowa:.
CSIRT NASK	80 267	103 449	+29%
CSIRT GOV	4 676	3 991	-15%
CSIRT MON	5 841	4 220	-28%
Sumaryczna roczna liczba zarejestrowanych incydentów:	90 784	111 660	+23%

Natomiast w zestawieniu z rokiem poprzednim w 2024 r. stwierdzono zmianę w zakresie wzrostu liczby incydentów w klasyfikacji zgodnej z art. 2 pkt. 5-9 UKSC. Zarejestrowano większą o 57% liczbę incydentów poważnych oraz większą o 58% liczbę incydentów w podmiotach publicznych, co zostało zawarte w tabeli poniżej.

Tabela 2. Zestawienie liczby incydentów w klasyfikacji zgodnej z UKSC

	Rodzaje incydentów zgodnie z art. 2 pkt. 5-9 UKSC							
	Krytyczne		Poważne		Istotne		W podmiotach publicznych	
	2023	2024	2023	2024	2023	2024	2023	2024
CSIRT NASK	0	0	40	57	0	0	2 184	3 450
CSIRT GOV	0	0	0	6	0	0	0	3
CSIRT MON	0	0	0	0	0	0	0	0
Suma:	0	0	40	63	0	0	2 184	3 453
Zmiana:				+57%				+58%

2.1.2.2 ZGŁOSZENIA:

W zakresie zgłoszeń w 2024 r. CSIRTy poziomu krajowego (CSIRT NASK oraz CSIRT GOV) otrzymały łącznie 627 339 zgłoszeń naruszeń bezpieczeństwa systemów teleinformatycznych, co stanowi wzrost o 60% w stosunku do roku poprzedniego (390 977).

Szczególnie istotna zmiana nastąpiła w zestawieniu zgłoszeń obsługiwanych przez NASK, które cechowało się wzrostem sumy o 64%, wzrostem liczby incydentów z 80 267 do 103 449 oraz średnią dzienną liczbą incydentów z 220 na 283 co stanowiło wzrost o 29%. Stosunek liczby incydentów do zarejestrowanych zgłoszeń spadł o 5% w skali roku.

Tabela 3. Zestawienie zgłoszeń i incydentów dla CSIRT NASK

CSIRT NASK					
Rok	Zgłoszenia	Średnia dzienna	Incydenty	Średnia dzienna	Stosunek incydentów do zgłoszeń
2023	371 089	1 017	80 267	220	22%
2024	609 900	1 671	103 449	283	17%
Zmiana	+64%		+29%		-5%

Tabela 4. Zestawienie dwuletnie zgłoszeń i incydentów dla CSIRT NASK

CSIRT NASK											
	Zgłoszenia				Incydenty				Stosunek incydentów do zgłoszeń		
Rok	Roczna liczba zgłoszeń	Średnia dzienna	Zmiana rok do roku	Zmiana rok do 2 lat	Roczna liczba incydentów	Średnia dzienna	Zmiana rok do roku	Zmiana tok do 2 lat	Stosunek incydentów do zgłoszeń	Zmiana rok do roku	Zmiana rok do 2 lat
2022	322 500	884	-	-	39 700	109	-	-	12%	-	-
2023	371 089	1 017	+15%	-	80 267	220	+102%	-	22%	+10%	-
2024	**609 900**	**1 671**	+64%	+89%	**103 449**	**283**	+28%	+160%	**17%**	-5%	+5%

Zestawienie zgłoszeń i incydentów obsługiwanych przez CSIRT GOV uległa zauważalnej poprawie. Liczba zgłoszeń w ujęciu rocznym zmniejszyła się o 12% z 19 888 do 17 439, natomiast liczba incydentów spadła o 15% z 4 676 do 3 991, co dało średnią dzienną w wysokości 11 zarejestrowanych incydentów dziennie.

Tabela 5. Zestawienie zgłoszeń i incydentów dla CSIRT GOV

CSIRT GOV					
Rok	Zgłoszenia	Średnia dzienna	Incydenty	Średnia dzienna	Stosunek incydentów do zgłoszeń
2023	19 888	54	4 676	13	24%
2024	17 439	48	3 991	11	23%
Zmiana	-12%		-15%		-1%

Liczba incydentów zarejestrowanych w 2024 r. w CSIRT MON spadła o 28% z 5 841 do 4 220 dając średnio 11 incydentów zarejestrowanych dziennie.

Tabela 6. Zestawienie liczby incydentów zarejestrowanych w CSIRT MON

CSIRT MON		
Rok	Incydenty	Średnia dzienna
2023	5 841	16
2024	4 220	12
Zmiana	-28%	

2.1.3 UMOCOWANIE INSTYTUCJONALNE PEŁNOMOCNIKA

Art. 60 UKSC stanowi, iż Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa odpowiada za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa

w Rzeczypospolitej Polskiej. W 2024 r. analogicznie do roku poprzedniego[3] funkcję Pełnomocnika pełnił Minister Cyfryzacji. Tak skonstruowane umocowanie instytucjonalne Pełnomocnika, w postaci swoistej unii personalnej z kierownictwem resortu cyfryzacji, odpowiedzialnego za KSC, zapewnia maksymalizację efektywności realizowanych przedsięwzięć, co jest szczególnie istotne w czasie dynamicznej cyfryzacji życia publicznego oraz związanymi z tym rosnącą skalą i poziomem zagrożeń.

Dzięki wyżej opisanej konstrukcji – liczba oraz złożoność zadań na poziomie krajowym, podejmowanych przez Ministerstwo Cyfryzacji (ministra właściwego ds. informatyzacji) zostały poprawnie i efektywnie skoordynowane z działaniami podejmowanymi przez inne podmioty odpowiadające za zapewnianie cyberbezpieczeństwa RP.

Pełnomocnik wraz z Ministerstwem Cyfryzacji stanowią centralny element kształtujący krajowy system cyberbezpieczeństwa, który zgodnie z art. 4 UKSC jest tworzony przez podmioty m.in. takie jak: operatorzy usług kluczowych, dostawcy usług cyfrowych, CSIRTy poziomu krajowego (CSIRT MON, CSIRT NASK, CSIRT GOV), sektorowe zespoły cyberbezpieczeństwa, jednostki sektora finansów publicznych, instytuty badawcze, urzędy centralne, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, oraz Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa (w rozumieniu UKSC).

2.1.4 KOLEGIUM DO SPRAW CYBERBEZPIECZEŃSTWA

Na podstawie art. 64 UKSC przy Radzie Ministrów działa Kolegium do Spraw Cyberbezpieczeństwa, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

Do zadań Kolegium należy także opracowywanie rekomendacji dla Rady Ministrów dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Posiedzenia Kolegium są organizowane przez Ministerstwo Cyfryzacji, które obsługuje Sekretarza Kolegium.

Przebieg prac Kolegium oraz treść wyrażonych stanowisk, rekomendacji oraz opinii posiadają charakter niejawny w rozumieniu ustawy o ochronie informacji niejawnych.

W 2024 r. odbyło się 5 posiedzeń Kolegium. Tematyka poruszana w minionym roku dotyczyła zagadnień wymienionych w poniższej tabeli:

[3] Z czasową przerwą wynikającą z konieczności umocowania się Rady Ministrów po wyborach parlamentarnych.

Tabela 7 Zestawienie tematyki Kolegium ds. Cyberbezpieczeństwa

Posiedzenie	Tematyka obrad:	Data
1.	1. Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w przedmiocie wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa w zakresie maksymalnych kwoty prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego na rok 2024.	16.01.2024r.
2.	1. Zaprezentowanie podsumowania Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2023 rok; 2. Omówienie harmonogramu prac Kolegium w drugim półroczu br. - przedstawienie propozycji zagadnień przez członków Kolegium; 3. Wydanie opinii Kolegium w zakresie stosowania rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa w trybie uproszczonym; 4. Wydanie opinii Kolegium w przedmiocie wniosku o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa.	26.03.2024r.
3.	1. Przedstawienie warunków akcyjnych przez UKE; 2. Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w sprawie aukcji UKE i wymagań bezpieczeństwa dla sieci 5G w paśmie 700 oraz 800 MHz.	3.10.2024r.
4.	1. Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w zakresie, aktualizacji wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa dotyczących prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego na rok 2024; 2. Przedstawienie zagadnienia nadużyć finansowych w przestrzeni cyfrowej – wystąpienie przedstawiciela KNF.	21.11.2024r.
5.	1. Wydanie opinii Kolegium do Spraw Cyberbezpieczeństwa w przedmiocie wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa w zakresie maksymalnych kwot prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego na rok 2025; 2. Przedstawienie opinii ABW oraz NASK w sprawie bezpieczeństwa wyborów prezydenckich 2025.	19.12.2024r.

2.1.5 POŁĄCZONE CENTRUM OPERACYJNE CYBERBEZPIECZEŃSTWA (PCOC)

W celu efektywnej koordynacji i bieżącego zarządzania cyberbezpieczeństwem na poziomie krajowym Ministerstwo Cyfryzacji we współpracy z RCB organizują spotkania w formacie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa.

PCOC jest to nieformalna platforma koordynacyjna Ministra Cyfryzacji. Wykorzystywana jest do szybkiej wymiany danych i informacji w zakresie zdarzeń w cyberprzestrzeni na poziomie krajowym. Pozwala na znaczące skrócenie czasu reakcji na zdarzenia i podniesienie poziomu cyberbezpieczeństwa RP, w szczególności w zakresie reagowania na pojawiające się incydenty cyberbezpieczeństwa. PCOC jest cyklicznym, zwykle cotygodniowym gremium zrzeszającym przedstawicieli CSIRTów poziomu krajowego oraz innych instytucji o kluczowym znaczeniu dla prawidłowego funkcjonowania KSC, oraz innych sfer bezpieczeństwa państwa. Spotkania mają charakter niejawny. Tematyka poruszana w trakcie posiedzeń oscyluje wokół technicznych aspektów omawianych zdarzeń w cyberprzestrzeni.

PCOC funkcjonuje od 2022 r. Celem zapewnienia odpowiednich środków technicznych niezbędnych dla funkcjonowania PCOC, resort cyfryzacji w latach minionych zlecił NASK-PIB zadanie pn. „Wyposażenie uczestników Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) w niezbędne urządzenia i sprzęt ICT". Wskazane podmioty biorące udział w spotkaniach koordynacyjnych PCOC zostały wyposażone w urządzenia i sprzęt ICT pozwalające na podłączenie do wojskowej sieci MILNET-Z. Ww. sieć umożliwia wymianę danych i informacji pomiędzy podmiotami uczestnikami, nie tylko jawnych, ale również tych objętych klauzulą tajności.

2.1.6 REKOMENDACJE I KOMUNIKATY PEŁNOMOCNIKA RZĄDU DS. CYBERBEZPIECZEŃSTWA

W 2024 r. Pełnomocnik aktywnie wykorzystywał mechanizm rekomendacji opisany w art. 33 ust. 4a ustawy dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 poz. 913 i 1703).

Rekomendacje zostały udzielone po uprzednich konsultacjach z zespołami CSIRT poziomu krajowego oraz po zasięgnięciu opinii Kolegium do Spraw Cyberbezpieczeństwa.

W minionym roku zostały wydane 3 rekomendacje Pełnomocnika.

Tabela 8 Zestawienie rekomendacji Pełnomocnika

Rekomendacje			
LP.	**Tematyka**	**Adres pełnej treści**	**Data**
1.	Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca aktualizacji produktów Fortinet	https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-aktualizacji-produktow-fortinet	28.03.2024r.
2.	Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca Biuletynów Informacji Publicznej	https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-biuletynow-informacji-publicznej	11.06.2024r.
3.	Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca oprogramowania Zimbra Collaboration	https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-oprogramowania-zimbra-collaboration	15.11.2024r.

Ponadto Pełnomocnik wydał 4 komunikaty w sprawach ważnych z perspektywy KSC.

Tabela 9 Zestawienie komunikatów Pełnomocnika

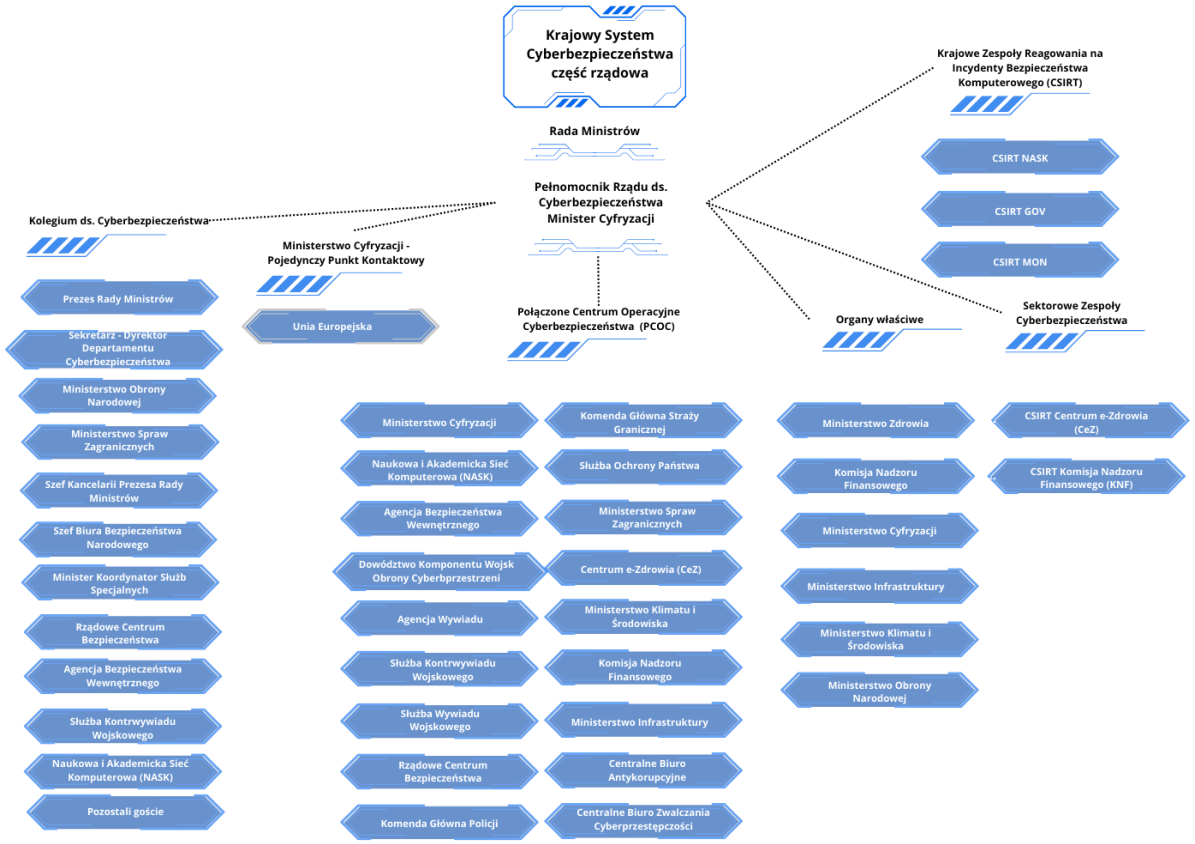
Komunikaty			
LP.	**Tematyka**	**Adres do pełnej treści**	**Data**
1.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie ataków DDoS	https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-ds-cyberbezpieczenstwa3	18.03.2024r.
2.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie zabezpieczenia infrastruktury teleinformatycznej administracji samorządowej na terenach zagrożonych powodzią	https://www.gov.pl/web/cyfryzacja/komunikat-w-sprawie-zabezpieczenia-infrastruktury-teleinformatycznej-administracji-samorzadowej-na-terenach-zagrozonych-powodzia	16.09.2024r.
3.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie oszustw w komunikacji z osobami publicznymi	https://www.gov.pl/web/baza-wiedzy/komunikat-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-w-sprawie-oszustw-w-komunikacji-z-osobami-publicznymi	27.09.2024r.
4.	Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie wzrostu liczby incydentów w polskiej cyberprzestrzeni, które dotyczą wycieków danych	https://www.gov.pl/web/cyfryzacja/wzrost-liczby-incydentow-zwiazanych-z-wyciekiem-danych--zalecenia-pelnomocnik-rzadu-do-spraw-cyberbezpieczenstwa	18.10.2024r.

2.1.7 ZESPÓŁ INCYDENTÓW KRYTYCZNYCH

Zespół jest obsługiwany przez RCB. W celu konsolidacji zadań w zakresie cyberbezpieczeństwa w przygotowywanej nowelizacji UKSC przewiduje się przeniesienie obsługi Zespołu do urzędu obsługującego Pełnomocnika.

2.1.8 STRUKTURA KSC

Rysunek 1. Schemat Krajowego Systemu Cyberbezpieczeństwa



2.2 ANALIZA I SZACOWANIE RYZYKA DLA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA (KSC) NA POZIOMIE STRATEGICZNYM

2.2.1 CELE ANALIZY:

Cele analizy wynikają bezpośrednio z celów wdrożenia krajowego systemu cyberbezpieczeństwa zawartych w art. 3 UKSC.

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie:

1. cyberbezpieczeństwa na poziomie krajowym;
2. niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług;
3. zapewnienie obsługi incydentów.

2.2.2 ANALIZA SWOT KSC

Tabela 10. Analiza SWOT dla KSC

Mocne strony (Strengths)	Słabe strony (Weaknesses)
1. Kompleksowe podejście do cyberbezpieczeństwa 2. Współpraca międzysektorowa 3. Szybkie reagowanie na incydenty	1. Niedobór zasobów ludzkich 2. Złożoność procedur 3. Ograniczone zasoby finansowe
Szanse (Opportunities)	**Zagrożenia (Threats)**
1. Nowelizacja ustawy 2. Współpraca międzynarodowa 3. Konsolidacja działań na poziomie krajowym	1. Rosnąca liczba cyberataków 2. Zmieniające się przepisy 3. Niedostateczna świadomość

2.2.3 ANALIZA PESTLE KSC

Tabela 11. Analiza typu PESTLE dla KSC

Polityczne (Political)	Ekonomiczne (Economic)	Społeczne (Social)	Technologiczne (Technological)	Prawne (Legal)	Środowiskowe (Environmental)
1.Regulacje i przepisy 2.Współpraca międzynarodowa	1.Koszty wdrożenia 2.Wsparcie finansowe	1. Świadomość społeczna. 2. Edukacja i szkolenia	1.Postęp technologiczny 2.Innowacje	1. Przepisy prawne 2. Ochrona danych	1. Zarządzanie zasobami 2. Zrównoważony rozwój

2.2.4 MATRYCA OCENY RYZYKA

Przy ocenie ryzyka dla Krajowego Systemu Cyberbezpieczeństwa (KSC) zastosowano skalę trzystopniową oraz kolorystyczną, która obejmuje poziomy: niskie, średnie i wysokie ryzyko. Skala została zastosowana zarówno do matrycy oceny ryzyka, jak rejestru ryzyka.

Tabela 12. Skala oceny ryzyka

Prawdopodobieństwo:	**Niskie**: Mało prawdopodobne, że ryzyko się zmaterializuje.
	Średnie: Możliwe, że ryzyko się zmaterializuje.
	Wysokie: Bardzo prawdopodobne, że ryzyko się zmaterializuje.
Wpływ	**Niski**: Minimalny wpływ na realizację celów KSC.
	Średni: Znaczący, ale zarządzalny wpływ na realizację celów KSC.
	Wysoki: Poważny wpływ na realizację celów KSC, mogący prowadzić do poważnych zakłóceń.

Tabela 13. Matryca oceny ryzyka dla KSC

Ryzyko	Prawdopodobieństwo	Wpływ	Ocena Ryzyka
Polityczne			
Zmiany legislacyjne	Wysokie	Wysoki	**Wysokie**
Geopolityczne napięcia	Wysokie	Wysoki	**Wysokie**
Polityka wewnętrzna	Niskie	Niski	**Niskie**
Ekonomiczne			
Koszty wdrożenia	Wysokie	Wysoki	**Wysokie**
Wpływ na gospodarkę	Wysokie	Wysoki	**Średnie**
Finansowanie	Średnie	Średni	**Średnie**
Społeczne			
Świadomość społeczna	Wysokie	Wysoki	**Wysokie**
Zaufanie publiczne	Średnie	Średni	**Średnie**
Edukacja	Średnie	Średni	**Średnie**
Technologiczne			
Szybki rozwój technologii	Wysokie	Wysoki	**Wysokie**
Złożoność infrastruktury	Wysokie	Wysoki	**Wysokie**
Nowe zagrożenia	Wysokie	Wysoki	**Wysokie**
Prawne			
Zgodność z regulacjami	Wysokie	Wysoki	**Średnie**
Ochrona danych osobowych	Wysokie	Wysoki	**Średnie**
Sankcje	Średnie	Średni	**Niskie**
Środowiskowe			
Zarządzanie zasobami	Średnie	Średni	**Średnie**
Zrównoważony rozwój	Średnie	Średni	**Średnie**
Zmiany klimatyczne	Niskie	Niski	**Niskie**
Organizacyjne			
Struktura organizacyjna	Średnie	Średni	**Średnie**
Kultura organizacyjna	Średnie	Średni	**Średnie**
Zarządzanie zmianą	Średnie	Średni	**Średnie**
Operacyjne			

Zarządzanie incydentami	Wysokie	Wysoki	**Wysokie**
Ciągłość działania	Wysokie	Wysoki	**Wysokie**
Bezpieczeństwo fizyczne	Średnie	Średni	**Średnie**
Techniczne			
Wady systemów	Wysokie	Wysoki	**Wysokie**
Integracja systemów	Średnie	Średni	**Średnie**
Zarządzanie aktualizacjami	Wysokie	Wysoki	**Wysokie**

2.2.5 REJESTR RYZYKA:

Tabela 14. Rejestr ryzyka.

Ryzyko	Opis ryzyka	Potencjalne Skutki:	Środki Zaradcze:
Polityczne			
Zmiany legislacyjne	Zmiany w przepisach prawnych, w tym implementacja przepisów prawa międzynarodowego mogą wpływać na wymagania dotyczące cyberbezpieczeństwa, jak i na obowiązki podmiotów prywatnych i publicznych, oraz na standaryzacje rozwiązań prawnych w tym technicznych zgodnych z narzuconymi wymogami.	Zwiększenie kosztów zgodności z przepisami. Potrzeba szybkiej adaptacji do nowych regulacji. Zmiana organizacji i struktury KSC, w tym formy zarządzania i koordynacji realizacji działań n szczeblu krajowym. Możliwość nałożenia kar na RP za nieprzestrzeganie przepisów.	Konsolidacja na poziomie krajowym możliwych do realizacji narzędzi celem spełniania wymagań. Działania deregulacyjne oraz harmonizacyjne wielu aktów prawa dotyczących cyberbezpieczeństwa.
Geopolityczne napięcia	Napięcia w stosunkach międzynarodowych, konflikty międzynarodowe, konflikt zbrojny w państwach sąsiadujących z RP. Ww. czynniki mogą prowadzić do wzrostu polaryzacji sojuszniczych bloków politycznych na arenie międzynarodowej, łącznie ze zmianami organizacji zasad budowania relacji między państwami i prowadzenia krajowej polityki zagranicznej.	Polityka sankcyjna mocarstw w zakresie realizacji współpracy politycznej, obejmować może ograniczenia w zakresie dostępu do nowych technologii, w tym technologii przełomowych, wrażliwych i kluczowych dla zrównoważonego rozwoju. Ograniczenia w zakresie dostępu do nowych rozwiązań technologicznych i wiedzy, mogą skutkować zahamowaniem rozwoju i budowaniem dysproporcji w zakresie rozwoju cywilizacyjnego między państwami. W zakresie cyberataków ze strony państw zaangażowanych w konflikty zbrojne, mogą nastąpić działania wymierzone w m.in. infrastrukturę krytyczną i/lub ukierunkowane na wiele podmiotów kluczowych dla bezpieczeństwa publicznego RP jednocześnie, prowadząc do czasowego ograniczenia działalności newralgicznych systemów państwa powodując wyraźne, negatywne efekty społeczne i gospodarcze.	Wzmocnienie współpracy międzynarodowej w zakresie cyberbezpieczeństwa i wymiany technologicznej oraz rozwoju. Wsparcie krajowej nauki i podmiotów technologicznych. Inwestycje w zaawansowane systemy wykrywania i reagowania na zagrożenia. Regularne testowanie odporności systemów na cyberataki.
Polityka wewnętrzna	Zmiany w polityce wewnętrznej, takie jak zmiany rządów czy kierunków polityki na szczeblu krajowym, mogą wpływać na priorytety i finansowanie działań	Zmniejszenie budżetu na cyberbezpieczeństwo. Zmiana priorytetów w zakresie ochrony funkcjonowania KSC. Potencjalne opóźnienia w realizacji projektów	Ustanowienie międzyresortowych zespołów ds. cyberbezpieczeństwa w celu zapewnienia spójności działań.

	związanych z cyberbezpieczeństwem.	związanych z cyberbezpieczeństwem. Osłabienie koordynacji działań między różnymi agencjami rządowymi.	Zapewnienie warunków długoterminowego finansowania kluczowych przedsięwzięć.
Ekonomiczne			
Koszty wdrożenia	Wdrożenie zmian w KSC wiąże się z wysokimi kosztami finansowymi i organizacyjnymi. Koszty będą obejmować zmiany struktury zarządzania oraz koordynacji KSC. Utworzenie instytucji o charakterze sektorowym wymagających zakupu pozyskania zasobów technicznych i ludzkich. systemów.	Znaczne obciążenie budżetu organizacji. Możliwość opóźnień w realizacji innych projektów z powodu alokacji zasobów finansowych na cyberbezpieczeństwo. Konieczność pozyskania dodatkowego finansowania.	Planowanie budżetu z uwzględnieniem kosztów cyberbezpieczeństwa. Konsolidacja zakupów i rozwoju rozwiązań IT dla grupo podmiotów. Wdrażanie rozwiązań open-source, celem redukcji kosztów.
Wpływ na gospodarkę	Cyberataki mogą mieć poważne konsekwencje dla gospodarki, w tym zakłócenia w funkcjonowaniu przedsiębiorstw, utratę danych oraz spadek zaufania do systemów cyfrowych.	Straty finansowe dla firm i instytucji. Spadek produktywności z powodu przestojów w działalności. Zmniejszenie inwestycji w sektorze cyfrowym z powodu obaw o bezpieczeństwo, spadek zaufania publicznego do wprowadzonych zmian osłabiający ich efektywność kosztową. Utrata własności intelektualnej i innowacji.	Wzmocnienie współpracy międzysektorowej w zakresie cyberbezpieczeństwa (implementacja S-46). Inwestycje w edukację i szkolenia z zakresu cyberbezpieczeństwa. Wdrażanie zaawansowanych technologii ochrony danych i systemów.
Finansowanie	Brak odpowiedniego finansowania może utrudnić wdrożenie i utrzymanie skutecznych systemów cyberbezpieczeństwa, co zwiększa ryzyko podatności na cyberataki.	Niewystarczające zabezpieczenia systemów informatycznych. Zwiększone ryzyko incydentów bezpieczeństwa. Potencjalne straty finansowe i reputacyjne.	Poszukiwanie różnych źródeł finansowania, w tym grantów i funduszy unijnych. Współpraca z sektorem prywatnym w celu pozyskania i dystrybucji środków. Regularne przeglądy budżetu i alokacja zasobów na cyberbezpieczeństwo.
Społeczne			
Świadomość społeczna	Niski poziom świadomości społecznej na temat zagrożeń cyfrowych może prowadzić do nieodpowiednich zachowań użytkowników, co zwiększa ryzyko incydentów bezpieczeństwa.	Wzrost liczby udanych cyberataków. Utrata danych osobowych i finansowych. Zmniejszenie ogólnego poziomu bezpieczeństwa systemów informacyjnych.	Kampanie edukacyjne i informacyjne na temat cyberbezpieczeństwa. Regularne szkolenia dla obywateli i pracowników instytucji publicznych. Współpraca z mediami w celu zwiększenia świadomości społecznej.
Zaufanie publiczne	Brak zaufania publicznego do systemów cyfrowych i instytucji odpowiedzialnych za cyberbezpieczeństwo może prowadzić do niechęci do korzystania z usług cyfrowych i technologii.	Spadek korzystania z usług cyfrowych. Zmniejszenie inwestycji w technologie cyfrowe. Wzrost obaw społecznych dotyczących prywatności i bezpieczeństwa danych. Odrzucanie systemów i polityk bezpieczeństwa ze względu na brak zaufania do sensowności ich stosowanie.	Transparentna komunikacja na temat działań podejmowanych w zakresie cyberbezpieczeństwa. Budowanie zaufania poprzez szybkie i skuteczne reagowanie na incydenty bezpieczeństwa. Wdrażanie i promowanie najlepszych praktyk w zakresie ochrony danych osobowych. Stosowanie rozwiązań typu open-source w administracji publicznej
Edukacja	Brak odpowiedniej edukacji w zakresie cyberbezpieczeństwa może prowadzić do niskiego poziomu wiedzy i umiejętności	Wzrost liczby incydentów bezpieczeństwa. Niska skuteczność działań prewencyjnych.	Wprowadzenie programów edukacyjnych z zakresu cyberbezpieczeństwa w szkołach i uczelniach.

	wśród obywateli, co zwiększa ryzyko cyberataków.	Zwiększone koszty związane z reagowaniem na incydenty.	Organizowanie warsztatów oraz szkoleń dla różnych grup wiekowych i społecznych. Promowanie ciągłego doskonalenia zawodowego w zakresie cyberbezpieczeństwa.
Technologiczne			
Szybki rozwój technologii	Szybki rozwój technologii, takich jak sztuczna inteligencja (AI), masowe wykorzystanie internetu Rzeczy (IoT) i blockchain, komputerów kwantowych - stwarza nowe możliwości rozwoju cywilizacyjnego, ale również nowe zagrożenia dla cyberbezpieczeństwa.	Wzrost liczby i złożoności cyberataków. Trudności w nadążaniu za nowymi technologiami i ich zabezpieczeniami. Zwiększone ryzyko wykorzystania nowych technologii przez cyberprzestępców. Wzrost złożoności stosowanych rozwiązań powoduje wzrost zapotrzebowania specjalistyczne kadry.	Inwestycje w badania i rozwój technologii zabezpieczeń. Regularne aktualizacje i testowanie systemów bezpieczeństwa. Współpraca z ekspertami i firmami technologicznymi w celu monitorowania nowych zagrożeń. Tworzenie standardów bezpieczeństwa oraz strategii przeciwdziałania zagrożeniom.
Złożoność infrastruktury	Złożoność infrastruktury informatycznej, w tym systemów bezpieczeństwa, może prowadzić do trudności w zarządzaniu i zabezpieczaniu wszystkich elementów systemu oraz spadku kompatybilności stosowanych rozwiązań.	Wzrost podatności na cyberataki. Trudności w identyfikacji i reagowaniu na incydenty bezpieczeństwa. Wzrost wielkości i różnorodności środowiska IT podającego ochronie. Możliwość zakłóceń w działaniu kluczowych usług.	Konsolidacja i unifikacja rozwiązań IT w podmiotach publicznych. Wdrożenie zaawansowanych systemów wykrywania włamań i zarządzania incydentami (S46).
Nowe zagrożenia	Pojawiające się nowe zagrożenia (głównie typu „usług na zlecenie", takie jak ransomware, zaawansowane ataki phishingowe i wykorzystanie AI przez cyberprzestępców, stanowią poważne wyzwanie dla cyberbezpieczeństwa.	Wzrost liczby incydentów bezpieczeństwa. Straty finansowe i reputacyjne. Zwiększone koszty związane z reagowaniem na incydenty.	Edukacja i szkolenia dla pracowników w zakresie rozpoznawania i reagowania na nowe zagrożenia. Wykorzystanie zaawansowanych technologii, takich jak AI, do wykrywania i neutralizowania zagrożeń. Wzmacnianie wykrywalności przestępstw i egzekucji kar.
Prawne			
Zgodność z regulacjami	Niezgodność z obowiązującymi regulacjami prawnymi dotyczącymi cyberbezpieczeństwa może prowadzić do poważnych konsekwencji prawnych i finansowych.	Wysokie kary finansowe za nieprzestrzeganie przepisów. Utrata zaufania klientów i partnerów biznesowych. Możliwość wstrzymania działalności operacyjnej.	Regularne audyty zgodności z regulacjami. Wdrożenie systemów zarządzania zgodnością (compliance). Szkolenia dla pracowników w zakresie obowiązujących przepisów.
Ochrona danych osobowych	Naruszenie przepisów dotyczących ochrony danych osobowych, takich jak RODO, może prowadzić do poważnych konsekwencji prawnych i reputacyjnych.	Wysokie kary finansowe za naruszenie przepisów o ochronie danych. Utrata zaufania klientów i partnerów biznesowych. Możliwość wstrzymania działalności operacyjnej.	Wdrożenie polityk i procedur ochrony danych osobowych. Regularne szkolenia dla pracowników w zakresie ochrony danych. Monitorowanie i audytowanie procesów przetwarzania danych osobowych.
Sankcje	Naruszenie międzynarodowych sankcji może prowadzić do poważnych konsekwencji prawnych i finansowych, a także do utraty reputacji.	Wysokie kary finansowe za naruszenie sankcji. Utrata zaufania klientów i partnerów biznesowych. Możliwość wstrzymania działalności operacyjnej.	Monitorowanie zmian w przepisach dotyczących sankcji. Wdrożenie systemów zarządzania zgodnością z sankcjami.

			Szkolenia dla pracowników w zakresie obowiązujących sankcji.
Środowiskowe			
Zarządzanie zasobami	Niewłaściwe zarządzanie zasobami naturalnymi i technologicznymi może prowadzić do problemów z dostępnością i bezpieczeństwem infrastruktury teleinformatycznej.	Zakłócenia w dostępie do kluczowych zasobów, takich jak energia i woda. Zwiększone ryzyko awarii systemów informatycznych oraz ograniczona dostępność do zasobów danych. Wzrost kosztów operacyjnych związanych z zarządzaniem zasobami.	Wdrożenie systemów monitorowania i zarządzania zasobami. Optymalizacja zużycia zasobów poprzez zastosowanie technologii oszczędzających energię. Regularne audyty i przeglądy zarządzania zasobami.
Zrównoważony rozwój	Brak uwzględnienia zasad zrównoważonego rozwoju w strategiach cyberbezpieczeństwa może prowadzić do długoterminowych problemów środowiskowych i społecznych.	Negatywny wpływ na środowisko naturalne. Zmniejszenie zaufania społecznego do instytucji odpowiedzialnych za cyberbezpieczeństwo. Wzrost kosztów związanych z naprawą szkód środowiskowych.	Integracja zasad zrównoważonego rozwoju w strategiach cyberbezpieczeństwa. Promowanie ekologicznych praktyk w zarządzaniu infrastrukturą IT. Współpraca z organizacjami zajmującymi się ochroną środowiska.
Zmiany klimatyczne	Zmiany klimatyczne mogą prowadzić do ekstremalnych zjawisk pogodowych, które mogą zakłócać działanie infrastruktury krytycznej i systemów informatycznych.	Zakłócenia w działaniu kluczowych usług z powodu ekstremalnych zjawisk pogodowych. Zwiększone ryzyko awarii systemów informatycznych. Wzrost kosztów związanych z naprawą i odbudową infrastruktury.	Wdrożenie planów awaryjnych na wypadek ekstremalnych zjawisk pogodowych. Inwestycje w odporne na zmiany klimatyczne technologie i infrastruktury. Regularne testowanie i aktualizacja planów zarządzania kryzysowego.
Organizacyjne			
Struktura organizacyjna	Niewłaściwa struktura organizacyjna, niedostosowana do wielkości systemu może prowadzić do nieefektywnego zarządzania cyberbezpieczeństwem, braku jasnych ról i odpowiedzialności oraz problemów z komunikacją.	Opóźnienia w reagowaniu na incydenty bezpieczeństwa. Niewłaściwe zarządzanie zasobami i priorytetami. Zwiększone ryzyko błędów i zaniedbań.	Jasne określenie ról i odpowiedzialności w zakresie cyberbezpieczeństwa. Regularne przeglądy i aktualizacje struktury organizacyjnej. Wdrożenie efektywnych kanałów komunikacji wewnętrznej. Utworzenie podmiotu koordynującego działania wraz z narzędziami egzekwowania decyzji.
Kultura organizacyjna	Brak kultury bezpieczeństwa w podmiotach może prowadzić do niskiego poziomu świadomości zagrożeń i nieodpowiednich zachowań pracowników.	Wzrost liczby incydentów bezpieczeństwa. Utrata danych i naruszenie prywatności. Spadek zaufania do systemu centralnego.	Promowanie kultury bezpieczeństwa poprzez szkolenia i kampanie edukacyjne. Wdrażanie polityk i procedur bezpieczeństwa jako integralnej części kultury organizacyjnej. Regularne audyty i oceny kultury bezpieczeństwa w organizacji.
Zarządzanie zmianą	Niewłaściwe zarządzanie zmianą może prowadzić do problemów z wdrażaniem nowych technologii i procedur, co zwiększa ryzyko błędów i podatności na zagrożenia.	Zakłócenia w działaniu systemów informatycznych. Wzrost ryzyka incydentów bezpieczeństwa. Niezadowolenie pracowników i spadek efektywności.	Wdrożenie formalnych procedur zarządzania zmianą. Szkolenia dla pracowników w zakresie zarządzania zmianą. Regularne przeglądy i aktualizacje procedur zarządzania zmianą

Operacyjne			
Zarządzanie incydentami	Niewłaściwe zarządzanie incydentami cyberbezpieczeństwa może prowadzić do poważnych konsekwencji, takich jak utrata danych, zakłócenia w działaniu systemów oraz straty finansowe.	Wzrost liczby incydentów bezpieczeństwa. Długotrwałe zakłócenia w działaniu kluczowych usług. Straty finansowe i reputacyjne.	Wdrożenie formalnych procedur zarządzania incydentami. Regularne szkolenia dla personelu w zakresie reagowania na incydenty. Wykorzystanie zaawansowanych narzędzi do monitorowania i analizy incydentów. Utworzenie podmiotu koordynującego.
Ciągłość działania	Brak odpowiednich planów ciągłości działania może prowadzić do długotrwałych zakłóceń w świadczeniu kluczowych usług w przypadku awarii systemów informatycznych.	Przestoje w działaniu kluczowych usług. Straty finansowe i operacyjne. Utrata zaufania klientów i partnerów biznesowych.	Opracowanie i wdrożenie planów ciągłości działania. Regularne testowanie i aktualizacja planów awaryjnych. Inwestycje w technologie zapewniające szybkie przywracanie systemów po awarii.
Bezpieczeństwo fizyczne	Naruszenia bezpieczeństwa fizycznego, takie jak nieautoryzowany dostęp do infrastruktury, mogą prowadzić do poważnych incydentów cyberbezpieczeństwa.	Fizyczne uszkodzenie infrastruktury IT. Kradzież danych i sprzętu. Zwiększone ryzyko cyberataków.	Wdrożenie zaawansowanych systemów kontroli dostępu. Regularne audyty i testy bezpieczeństwa fizycznego. Szkolenia dla personelu w zakresie procedur bezpieczeństwa fizycznego.
Techniczne			
Wady systemów	Wady systemów informatycznych, takie jak luki w zabezpieczeniach, mogą być wykorzystywane przez cyberprzestępców do przeprowadzania ataków.	Utrata danych i naruszenie prywatności. Zakłócenia w działaniu kluczowych usług. Straty finansowe i reputacyjne.	Regularne audyty bezpieczeństwa systemów. Wdrożenie zaawansowanych systemów wykrywania i zapobiegania włamaniom. Aktualizowanie systemów w celu eliminacji znanych luk. Rekomendacje Pełnomocnika w sprawie stosowania rozwiązań.
Integracja systemów	Integracja różnych systemów informatycznych może prowadzić do problemów z kompatybilnością i zwiększać ryzyko podatności na ataki.	Trudności w zarządzaniu i monitorowaniu zintegrowanych systemów. Zwiększone ryzyko awarii i zakłóceń w działaniu systemów. Możliwość wystąpienia luk bezpieczeństwa w punktach integracji.	Staranna analiza i planowanie integracji systemów. Wdrożenie narzędzi do monitorowania i zarządzania zintegrowanymi systemami. Regularne testy penetracyjne i audyty bezpieczeństwa integracji.
Zarządzanie aktualizacjami	Niewłaściwe zarządzanie aktualizacjami oprogramowania może prowadzić do pozostawienia systemów podatnych na znane zagrożenia.	Wzrost liczby incydentów bezpieczeństwa. Zakłócenia w działaniu systemów informatycznych. Straty finansowe i reputacyjne.	Opracowanie strategii zarządzania aktualizacjami. Wykorzystanie narzędzi do automatyzacji procesu aktualizacji. Regularne testowanie aktualizacji przed wdrożeniem oraz monitorowanie ich skutków.

2.2.6 PODSUMOWANIE

Analiza ryzyka dla Krajowego Systemu Cyberbezpieczeństwa została przeprowadzona w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym, niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz zapewnienia obsługi incydentów, zgodnie z celami zawartymi w art. 3 UKSC. Analiza ta, została utworzona z perspektywy poziomu strategicznego, dlatego też liczba ryzyka została ograniczona wyłącznie i zgodnie z grupowaniem zmieszczonym w tabeli, pokazuje, że istnieje

wiele czynników, które mogą wpływać na realizację celów ustawowych. Ryzyko związane z politycznymi, ekonomicznymi, społecznymi, technologicznymi i prawnymi aspektami wymaga szczególnej uwagi i odpowiednich działań zaradczych. Ww. grupach zostały wskazane ryzyka wymagające szczególnej uwagi nie zamykające zbioru ryzyka dla KSC. Należy pamiętać, że analiza została przygotowana na wysokim poziomie ogólności eliminując z oceny tysiące mikroprocesów wpływających na stabilne i efektywne funkcjonowanie KSC na niższych poziomach zarządzania systemem.

Dobór ww. grup ryzyka sprawia, że analiza stała się praktycznym i funkcjonalnym narzędziem wspierającym proces decyzyjny na poziomie strategicznym oraz obrazuje jednocześnie krajobraz zagrożeń dla KSC. Wdrożenie skutecznych mechanizmów zarządzania ryzykiem oraz ciągłe monitorowanie i aktualizowanie jest kluczowe dla zapewnienia bezpieczeństwa cyfrowego na poziomie krajowym.

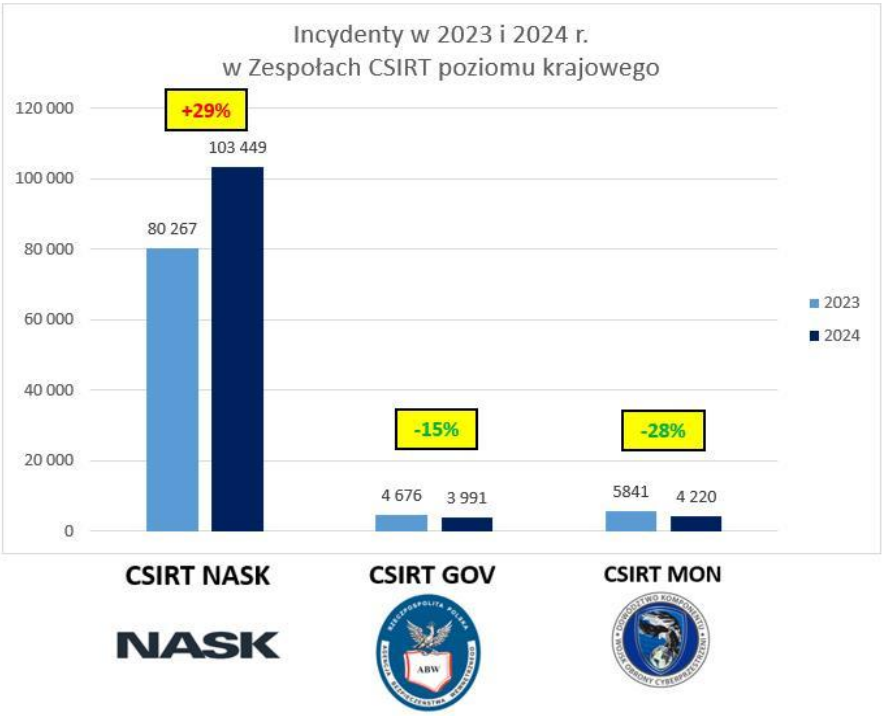
3 CSIRT-Y POZIOMU KRAJOWEGO

W ramach Krajowego Systemu Cyberbezpieczeństwa na poziomie operacyjnym funkcjonują trzy zespoły CSIRT poziomu krajowego:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Zadania CSIRT-ów określa rozdział 6. UKSC. Każdy z nich cechuje się swoją specyfiką z uwagi na obszar odpowiedzialności (*constituency*). W pewnym uproszczeniu można stwierdzić, że CSIRT GOV odpowiada za administrację państwową i infrastrukturę krytyczną; CSIRT NASK za administrację samorządową, niektóre instytucje publiczne, operatorów usług kluczowych i dostawców usług cyfrowych (za wyjątkiem tych podległych pod MON), sektor przedsiębiorstw i „zwykłych obywateli"; a CSIRT MON za Siły Zbrojne RP, resort obrony narodowej (w tym jego jednostki i komórki organizacyjne), jak również niektóre inne podmioty realizujące zadania na rzecz Sił Zbrojnych RP, jak np. część przedsiębiorstw zbrojeniowych.

Rysunek 2. Wykres porównujący liczbę incydentów obsłużonych przez właściwy CSIRT w latach 2023 i 2024



3.1 CSIRT GOV

3.1.1 DANE LICZBOWE DOTYCZĄCE ZGŁOSZEŃ I INCYDENTÓW Z PODZIAŁEM ZGODNYM Z ART. 2 PKT. 5-9 USTAWY Z DNIA 5 LIPCA 2018 R. O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA (KSC):

Zespół CSIRT GOV od 1 stycznia do 31 grudnia 2024 r. **zarejestrował 3 991 incydentów** w rozumieniu ustawy o KSC. Zostały one zaklasyfikowane jako**:**

Tabela 15. Kwalifikacja incydentów

Kwalifikacja incydentów	Liczba
Podatność	**105**
Publikacja	**902**
Socjotechnika	**815**
Niedostępność	**478**
Atak	**261**
Kaskada	**235**
Skanowanie	**108**
Treści	**56**
Wirus	**31**

Wskazane incydenty wystąpiły w następujących sektorach:

Tabela 16. Sektory występowania incydentów

Sektory występowania	Liczba
Instytucja	**817**
Operator infrastruktury krytycznej	**783**
Organ państwowy	**627**
Urząd	**559**
Ministerstwo	**501**
Służba	**313**
Pozostałe	**391**

Wśród powyższych incydentów odnotowano:

Tabela 17. Kwalifikacja incydentów wg. KSC

Charakterystyka wg. KSC	Liczba
Incydenty krytyczne	**0**
Incydenty poważne	**6 (5 - sektor Energia, 1 - sektor Transport)**
Incydenty istotne	**0**
Incydenty w podmiotach publicznych	**3**

W 2024 r. wszystkie incydenty poważne wynikały z awarii i nie nosiły znamion ataku teleinformatycznego. Incydenty w podmiocie publicznym wystąpiły w różnego typu instytucjach administracji publicznej i dotyczyły m.in. ataków DDoS czy też infekcji złośliwym oprogramowaniem.

3.1.2 DZIAŁANIA PROWADZONE PRZEZ CSIRT GOV W OBSZARZE CYBERPRZESTRZENI RP

Do głównych zadań działającego w strukturach ABW Zespołu CSRT GOV (w tym związanych z podnoszeniem efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa) należy m.in.:

- wspieranie podmiotów administracji publicznej oraz operatorów usług kluczowych infrastruktury krytycznej w zakresie rozpoznawania i przeciwdziałania zagrożeniom cyberbezpieczeństwa,
- podnoszenie poziomu świadomości i wiedzy na temat zagrożeń cybernetycznych poprzez wydawanie rekomendacji dotyczących stosowania dobrych praktyk w zakresie zabezpieczania i bezpiecznego użytkowania środowiska IT,
- prowadzenie szkoleń dla osób sprawujących funkcje publiczne, podmiotów administracji rządowej, operatorów usług kluczowych i operatorów infrastruktury krytycznej dotyczących zagrożeń w cyberprzestrzeni, a także ukierunkowanych na podnoszenie kwalifikacji i kompetencji w zakresie cyberbezpieczeństwa,
- zarządzanie i rozwijanie systemu wczesnego ostrzegania **ARAKIS GOV (w 2024 r. system ten zanotował łącznie 1 947 791 593 przepływów, co przełożyło się na 3 322 068 wygenerowanych alarmów**, jednocześnie we wskazanym okresie ABW podłączyła do niego 5 nowych podmiotów),
- prowadzenie ocen bezpieczeństwa systemów teleinformatycznych (w 2024 r. Zespół CSIRT GOV przeprowadził tego rodzaju czynności w 15 instytucjach administracji rządowej oraz u operatorów infrastruktury krytycznej, w których przebadał łącznie 161 segmentów sieci/systemów teleinformatycznych oraz 26 domen/subdomen oraz stron www),
- przyjmowanie i analiza zgłoszeń o incydentach oraz wydawanie rekomendacji zgłaszającym, mających na celu podniesienie poziomu bezpieczeństwa systemów IT, a także formułowanie rekomendacji wprowadzenia działań zmierzających do minimalizacji lub neutralizacji zagrożeń, w tym przywrócenia prawidłowego działania systemów teleinformatycznych **(w 2024 r. do Zespołu CSRT GOV wpłynęło 17 439 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego, na podstawie których zarejestrowano 3 991 faktycznych incydentów** ich obsługa realizowana była w ramach krajowego systemu cyberbezpieczeństwa we współpracy z pozostałymi uczestnikami tego systemu),
- dystrybucja ostrzeżeń o zagrożeniach bezpieczeństwa systemów teleinformatycznych oraz przekazywanie rekomendacji w zakresie zagadnień organizacyjnych i technicznych, mających na celu podniesienie poziomu bezpieczeństwa systemów IT (w 2024 r. **Zespół CSIRT GOV rozesłał do podmiotów administracji publicznej i operatorów infrastruktury krytycznej 518 ostrzeżeń o potencjalnym lub wykrytym zagrożeniu.** Ich tematyka obejmowała zarówno informacje

o podatnościach w oprogramowaniu, konieczność blokowania szkodliwych adresów IP, jak i kampaniach phishingowych),

- współpraca z CSIRT MON i CSIRT NASK oraz sektorowymi zespołami cyberbezpieczeństwa w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni RP, w szczególności dotycząca sposobów obsługi incydentów, wymiany informacji technicznych i systemowych, w tym w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa,
- wykorzystywanie systemu S46 do rejestrowania i obsługi incydentów teleinformatycznych w zakresie cyberbezpieczeństwa występujących u operatorów infrastruktury krytycznej oraz operatorów usług kluczowych, jak również wydawania ostrzeżeń o zidentyfikowanych zagrożeniach dla systemów i sieci teleinformatycznych,
- współpraca z CSIRT MON oraz CSIRT NASK przy identyfikacji i reagowaniu na zdarzenia o charakterze określonym w art. 2 pkt. 5-9 KSC (incydent, incydent krytyczny, incydent poważny, incydent istotny, incydent w podmiocie publicznym), a także wsparcie podmiotów dotkniętych incydentem oraz ostrzeganie podmiotów zagrożonych,
- kooperacja z organami odpowiedzialnymi za rozpoznawanie przestępstw popełnianych w cyberprzestrzeni oraz ściganie ich sprawców,
- współpraca z podmiotami krajowego systemu cyberbezpieczeństwa,
- udział w międzynarodowych forach wymiany informacji o zagrożeniach cybernetycznych (np. CSIRTs Network, Malware Information Sharing Platform w ramach NATO),
- zaangażowanie ABW w kwestie bezpieczeństwa związane z realizacją ww. projektów i inicjatyw:
  - rozwiązania organizacyjno-techniczne wspierające realizację ustawy o ochronie ludności i obronie cywilnej, której istotnym komponentem jest System Bezpiecznej Łączności Państwowej,
  - budowa Krajowego Centrum Przetwarzania Danych,
  - implementacja Dyrektywy NIS2 (cyberbezpieczeństwo w ujęciu ogólnokrajowym),
  - implementacja DORA (cyberodporność sektora finansowego),
  - implementacja AI Act (wykorzystanie sztucznej inteligencji).

3.1.3 ZADANIA REALIZOWANE W 2024 R.

3.1.3.1 W 2024 R. ABW REALIZOWAŁA INNE NIŻ WW. ZADANIA W RAMACH ZESPOŁU CSIRT — TJ. CZYNNOŚCI ZWIĄZANE Z BEZPIECZEŃSTWEM CYBERPRZESTRZENI RP. ZALICZYĆ DO NICH MOŻNA M.IN.:

- identyfikację osób publikujących treści zagrażające bezpieczeństwu wewnętrznemu państwa, powiązanych z działalnością terrorystyczną lub ekstremistyczną i wykorzystujących zaawansowane narzędzia anonimizacji (takie jak sieci TOR czy VPN) w celu ukrycia swojej tożsamości, a także blokowanie na podstawie dostępnych rozwiązań prawnych szkodliwych przekazów,
- analizę projektów aktów normatywnych powszechnie obowiązujących, które swoim zakresem obejmowały kwestie dotyczące cyberbezpieczeństwa oraz przygotowywanie stanowisk Szefa ABW wobec tych regulacji (do najistotniejszych projektów, wobec których wniesiono uwagi należały m.in.:
  - projekt ustawy — Prawo komunikacji elektronicznej
  - projekt ustawy o zmianie ustawy o działaniach antyterrorystycznych oraz ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
  - projekt ustawy o zmianie ustawy o aplikacji mObywatel,
  - projekt ustawy o systemach sztucznej inteligencji),
- S46 to ogólnokrajowy system komunikacyjno-analityczny rozwijany przez Naukową i Akademicką Sieć Komputerową — Państwowy Instytut Badawczy. Powstał on w oparciu o art. 46 UKSC celem wspierania współpracy i wymiany informacji,

- opiniowanie i analizowanie projektów aktów prawa Unii Europejskiej dotyczących m.in. obszarów cyberbezpieczeństwa, sztucznej inteligencji czy łączności elektronicznej, pod kątem ich wpływu na bezpieczeństwo RP oraz realizację ustawowych zadań ABW.

3.1.3.2 ANALIZA I OCENA FUNKCJONOWANIA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

- Kluczowym aktem prawnym regulującym sposób funkcjonowania krajowego systemu cyberbezpieczeństwa jest przyjęta ponad 6 lat temu UKSC. W kontekście zadań ABW innym, głównym źródłem obowiązków prawnych (wpisujących się w obszar odpowiedzialności Agencji oraz korespondujących z UKSC) jest ustawa o ABW oraz AW m.in. w zakresie tzw. oceny bezpieczeństwa (art. 32a) czy też zarządzania systemem wczesnego ostrzegania ARAKIS GOV (art. 32a).

Oceniając zaś sposób funkcjonowania krajowego systemu cyberbezpieczeństwa warto podkreślić, że zawarte w ww. aktach normatywnych rozwiązania prawne znajdują praktyczne zastosowanie, czego wyrazem pozostaje:

- udział przedstawicieli ABW w reagowaniu na poważne incydenty bezpieczeństwa, w tym zwłaszcza związane z trwającą obecnie agresją Federacji Rosyjskiej na Ukrainę,
- realizowane przez Agencję na przestrzeni ostatnich lat oceny bezpieczeństwa systemów i sieci teleinformatycznych,
- liczne wdrożenia systemu ARAKIS GOV,
- wykorzystanie instrumentów prawnych wprowadzonych ustawą o działaniach antyterrorystycznych, w tym w szczególności stopni alarmowych CRP,
- uczestnictwo w licznych gremiach koordynujących zarządzanie szeroko rozumianą transformacją cyfrową państwa oraz dbałością o bezpieczeństwo teleinformatyczne systemów kluczowych dla ciągłości jego działania (np. Kolegium ds. Cyberbezpieczeństwa czy Zespół Incydentów Krytycznych).

3.1.3.3 ZIDENTYFIKOWANE NAJPOWAŻNIEJSZE ZAGROŻENIA SYSTEMOWE DLA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

W ocenie ABW za kluczowe źródło zagrożeń dla funkcjonowania krajowego systemu cyberbezpieczeństwa należy uznać brak precyzyjnego uregulowania poniższych obszarów:

- bezpieczeństwo łańcucha dostaw, którego egzemplifikacją jest kwestia regulacji dotyczących tzw. dostawców wysokiego ryzyka,
- rozwiązania sprzętowe i programowe eksploatowane w systemach kluczowych dla funkcjonowania państwa (w tym w ramach infrastruktury krytycznej),
- dopuszczalność stosowania rozwiązań infrastrukturalnych (zarówno w zakresie Centrów Przetwarzania Danych, jak i sieci IT) w odniesieniu do ww. systemów kluczowych dla funkcjonowania państwa — m. in. uregulowanie dopuszczalności stosowania chmury obliczeniowej (publicznej, rządowej),
- bezpieczeństwo poczty w sektorze GOV oraz ochrona danych przetwarzanych przez urzędników państwowych,
- ochrona danych medycznych obywateli RP, a także dotyczących służb państwowych,
- bezpieczne stosowanie tzw. technologii przełomowych, w tym zwłaszcza sztucznej inteligencji, w kontekście wykorzystania tzw. deepfake'ów na potrzeby oszustw (np. fałszywych inwestycji) czy też szerzenia dezinformacji.

Ponadto należy zaznaczyć, że istotnym wyzwaniem dla Polski będzie konieczność dostosowania krajowego systemu cyberbezpieczeństwa do przyjętych przepisów Dyrektywy NIS2, która swoim zakresem obejmuje również instytucje publiczne, dotychczas pominięte w ramach obowiązującej wersji UKSC.

3.1.3.4 ZIDENTYFIKOWANE NAJPOWAŻNIEJSZE ZAGROŻENIA TECHNICZNE DLA SYSTEMÓW TELEINFORMATYCZNYCH

W kontekście odnotowanych w RP cyberataków należy zwrócić uwagę m.in. na następujące kwestie.;

- niezmiennie wysoką popularność ataków z wykorzystaniem elementów socjotechniki i ataków typu ransomware,
- rosnącą popularność różnego typu oszustw (np. wykorzystujących wizerunek spółek Skarbu Państwa, urzędów państwowych oraz przedstawicieli organów państwa),
- zwiększające się wykorzystanie alternatywnych środków komunikacji (np. komunikatory internetowe), co pozwala na obchodzenie wymagań i zabezpieczeń wprowadzonych ustawą z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej,
- dużą skalę dezinformacji, w tym bazującej na produktach generatywnej sztucznej inteligencji,
- rosnącą liczbę wykorzystywanych podatności, w tym aktywne stosowanie przez adwersarzy podatności typu zero-day;
- wzrastające zagrożenie dla infrastruktury teleinformatycznej podmiotów poprzez ataki na łańcuch dostaw.

Spośród incydentów zarejestrowanych przez CSIRT GOV największa ich liczba została zakwalifikowana jako podatność, na którą składają się zagrożenia polegające na błędnej konfiguracji bądź nieaktualnej wersji oprogramowania zasobów dostępnych z poziomu sieci internet. Wykryte luki bezpieczeństwa zwiększają ryzyko nieautoryzowanego dostępu, przejęcia kontroli nad systemami czy wycieku danych wrażliwych z zasobów instytucji.

W 2024 r. liczne incydenty zaklasyfikowano jako publikacje. Dotyczyły one ujawnienia wrażliwych informacji z wycieków danych (często poddostawców), dezinformację czy nieautoryzowaną modyfikację treści na stronach i zasobach instytucji (np. publikacja w Polskiej Agencji Prasowej o rzekomej mobilizacji z 31 maja 2024 r.).

W 2024 r. miały miejsce ataki grup ransomware na firmy świadczące usługi teleinformatyczne na rzecz operatorów infrastruktury krytycznej. Przedmiotowe ataki wskazują na potrzebę stałego weryfikowania zabezpieczeń zarówno usług kluczowych, jak i wspierających. Zidentyfikowane wycieki danych zawierały w sobie nierzadko informacje osobowe, dotyczące przedsiębiorstwa lub jego infrastruktury teleinformatycznej.

3.1.3.5 GRUPY APT

Wśród głównych celów leżących w zainteresowaniu grup APT (ang. *Advanced Persistent Threat*) w 2024 r. znalazły się ministerstwa oraz operatorzy infrastruktury krytycznej z sektora energii oraz transportu (kolejowego i lotniczego). Odnotowane zostały próby kompromitacji serwerów pocztowych oraz inne ataki mające na celu pozyskanie dostępu do sieci, systemów i danych organizacji. Trend ten stanowił kontynuację działań rosyjskich adwersarzy zaobserwowanych w 2023 r.

3.1.3.6 IDENTYFIKOWANE NAJWAŻNIEJSZE ZAGROŻENIA, TRENDY I KAMPANIE, WRAZ Z OPISEM NAJWAŻNIEJSZYCH INCYDENTÓW ORAZ STOSOWANYCH TAKTYK, TECHNIK I PROCEDUR (TTPS)

- Najważniejszym zagrożeniem, z trendem wzrostowym w 2024 r., były ataki na łańcuch dostaw, w tym przede wszystkim incydenty w firmach Aiut Sp. z o.o. i Atende S.A. (z powodu których zostały wydane m.in. zalecenia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa). Dane z wycieków zawierały informacje takie jak: szczegóły stosowanej infrastruktury teleinformatycznej oraz automatyki przemysłowej, realizowane inwestycje, specyfikacje stosowanych rozwiązań teleinformatycznych instytucji czy też poświadczenia do kont w infrastrukturze instytucji.
- Istotnym, stale utrzymującym się zagrożeniem w cyberprzestrzeni RP były ataki grup APT na podmioty pozostające we właściwości CSIRT GOV. Biorąc pod uwagę te zagrożenia, można wskazać najczęściej identyfikowane taktyki, metody oraz procedury ataków stosowane przez tego typu grupy.

W odniesieniu do infrastruktury, aktorzy wykorzystują do ataków przede wszystkim sieci anonimizujące, np. różnego rodzaju węzły proxy czy komercyjne serwisy VPN. Nierzadko przejmowane są urządzenia sieciowe posiadające podatności (szczególnie typu EOL), które następnie służą do kamuflażu dalszych działań lub są wykorzystywane jako serwery C&C.

W ramach rekonesansu służącego przygotowaniom do ataków, aktorzy dokonują rozpoznania infrastruktury w oparciu o skanowanie pod kątem otwartych portów lub usług czy też w celu ujawnienia ewentualnych podatności. W zakresie kampanii socjotechnicznych stosowne rozpoznanie bazuje na danych publikowanych na stronach internetowych czy udostępnianych na portalach społecznościowych przez osoby lub podmioty. Źródłem wiedzy w ramach rekonesansu są także wycieki dostępne w sieciach typu darknet lub informacje pozyskane w wyniku wcześniejszych kompromitacji.

- Często stosowanym wektorem kompromitacji w dalszym ciągu są wiadomości z użyciem elementów socjotechniki, wykorzystujące fałszywe panele logowania do różnych usług, np. poczty Outlook czy też dystrybuujące złośliwe załączniki lub zawierające odesłanie do dokumentów (ich pobranie wiąże się z wykonaniem złośliwego kodu i uzyskaniem zdalnego dostępu do urządzenia).
- Szczególnym rodzajem technik jest uzyskiwanie dostępu do infrastruktury LAN poprzez urządzenia VPN, stosując techniki typu bruteforce i password spraying, jak również wykorzystanie podatności typu RCE na urządzeniu.

Po uzyskaniu dostępu do infrastruktury aktorzy eskalują następnie uprawnienia w systemach i sieciach, jak również starają się utrzymać trwały dostęp do skompromitowanych zasobów. Obserwowane jest również wykorzystywanie skompromitowanych systemów do prowadzenia dalszych działań przeciwko kolejnym celom, uwiarygodniając źródło ruchu sieciowego czy korespondencji email, jak również prowadzenia eksfiltracji danych.

3.1.4 WNIOSKI I REKOMENDACJE

W kontekście wskazanych powyżej najpoważniejszych zagrożeń w cyberprzestrzeni za kluczowe należy uznać podjęcie działań celem umożliwienia kontroli ryzyka z nich wynikającego, na poziomie akceptowalnym dla bezpieczeństwa państwa. W ocenie ABW powinna się tam znaleźć m.in.:

- klarowna i obiektywna ocena obecnego stanu w zakresie przygotowania poszczególnych instytucji oraz gotowości rozwiązań prawno-organizacyjno-technicznych do mierzenia się z głównymi wyzwaniami dla bezpieczeństwa cyberprzestrzeni,
- definicja pożądanego stanu docelowego w ww. zakresie,
- portfolio programów i projektów ukierunkowanych na osiągnięcie ww. stanu docelowego.

3.1.5 PLANOWANE DZIAŁANIA W 2025 R.

W ramach planów ABW na 2025 r. w kontekście zapewnienia cyberbezpieczeństwa RP za kluczowe należy uznać:

- kontynuację realizacji zadań nałożonych na CSIRT GOV przez UKSC, ustawę o ABW oraz AW, ustawę o działaniach antyterrorystycznych oraz stosowne rozporządzenia, w szczególności dotyczące: identyfikacji i ostrzegania o zagrożeniach, rejestracji i obsługi incydentów teleinformatycznych, prowadzenia ocen bezpieczeństwa systemów i sieci IT, dalszego rozwoju i podłączania nowych podmiotów do systemu ARAKIS GOV oraz współpracy krajowej i zagranicznej,
- bieżące zaangażowanie w proces rozpoznania i minimalizowania zagrożeń systemowych i technicznych związanych z cyberbezpieczeństwem,
- wzmocnienie potencjału kadrowego, organizacyjnego i technicznego ABW w kontekście skutecznego i efektywnego rozpoznawania współczesnych zagrożeń, w tym dotyczących cyberszpiegostwa i cyberterroryzmu.

3.1.6 PROGNOZA SYTUACJI W CYBERPRZESTRZENI NA LATA 2025-2026

Analiza zmian zachodzących w cyberprzestrzeni RP w 2024 r. prowadzi m.in. do następujących wniosków:

- częściej mogą występować ataki na łańcuch dostaw, będące równie dewastacyjne w skutkach co bezpośredni atak na infrastrukturę podmiotu,
- wybiórcze wdrażanie zabezpieczeń typu MFA (lub jego jednoznaczny brak) przez instytucje stanowić będzie nieustanne zagrożenie dla operatorów infrastruktury krytycznej, a przede wszystkim administracji państwowej,
- przewiduje się utrzymanie trendu wzrostowego wykorzystania podatności o *różnym poziomie skomplikowania i krytyczności* w systemach instytucji.

3.2 CSIRT MON

3.2.1 DANE LICZBOWE DOTYCZĄCE ZGŁOSZEŃ I INCYDENTÓW Z PODZIAŁEM ZGODNYM Z ART. 2 PKT. 5-9 USTAWY Z DNIA 5 LIPCA 2018 R. O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

W 2024 r. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC)/CSIRT MON zarejestrował 4220 incydentów.
Ponadto:

- W 2024 r. DKWOC/CSIRT MON nie zarejestrował żadnego incydentu sklasyfikowanego jako krytyczny.
- W 2024 r. DKWOC/CSIRT MON nie zarejestrował żadnego zgłoszenia od operatora usługi kluczowej dot. incydentu poważnego.
- W 2024 r. DKWOC/CSIRT MON nie zarejestrował żadnego zgłoszenia od dostawcy usługi cyfrowej dot. incydentu istotnego.

Tabela 18. Kwalifikacja incydentów wg KSC

Zagrożenia cyberbezpieczeństwa	Liczba
Incydenty krytyczne	**0**
Incydenty poważne	**0**
Incydenty istotne	**0**
Zarejestrowane incydenty	**4 220**

3.2.2 OPIS NAJWAŻNIEJSZYCH INCYDENTÓW

W 2024 roku odnotowano próby ataków na infrastrukturę oraz użytkowników resortu obrony narodowej (RON). **Głównym wektorem ataku pozostaje phishing**, który w większości przypadków ukierunkowany jest na wykradanie poświadczeń logowania lub innych wrażliwych metadanych umożliwiających adwersarzowi nieuprawniony dostęp do systemów teleinformatycznych resortu. **Wektor ten jest wykorzystywany zarówno przez zagrożenia o charakterze oportunistycznym jak i przez adwersarzy klasy APT**.

W ramach prowadzonych działań **DKWOC/CSIRT MON zidentyfikował trend wzrostowy liczby incydentów powiązanych z atakami na popularne komunikatory internetowe oraz urządzenia mobilne**. **W ocenie DKWOC/CSIRT MON trend ten będzie utrzymywał się w 2025 r.**

W toku prowadzonych analiz zidentyfikowano szereg incydentów dot. naruszeń bezpieczeństwa związanych z wykradaniem poświadczeń logowania. Jest to spowodowane najprawdopodobniej infekcją urządzeń prywatnych, które nie są objęte systemami monitorowania cyberbezpieczeństwa przez DKWOC/CSIRT MON.

Kolejną kategorią zdarzeń są ataki typu supply–chain. W minionym roku odnotowano wzrost liczby ataków na podmioty współpracujące z RON, które mogą potencjalnie przetwarzać informacje wrażliwe dla resortu. W ocenie DKWOC/CSIRT MON wynika to faktu, iż adwersarz upatruje możliwości

pozyskania cennych informacji dotyczących dziedziny obronności poprzez systemy teleinformatyczne podmiotów, których zabezpieczenia są potencjalnie łatwiejsze do przełamania.

3.2.3 INFORMACJE NT. GRUP (APT, CYBERPRZESTĘPCZYCH, HAKTYWISTYCZNYCH) DOKONUJĄCYCH CYBERATAKÓW WYMIERZONYCH W POLSKĘ

Zasadnicza aktywność w cyberprzestrzeni w 2024 r. w obszarze odpowiedzialności DKWOC/CSIRT MON, podobnie jak w 2023 r., została zdeterminowana trwającym konfliktem oraz aktywną postawą Polski w zakresie wsparcia Ukrainy. W 2024 roku znaczący wpływ na bezpieczeństwo systemów IT RON miały zagrożenia wynikające z działań klastrów aktywności o charakterze APT kojarzonych głównie z działalnością inspirowaną, sponsorowaną lub pozostającą w strukturach państwa. Wachlarz aktywności grup APT jest bardzo szeroki i obejmuje m.in. planowe rozpoznawanie infrastruktury teleinformatycznej, prowadzenie działań cyberszpiegowskich, pozyskiwanie wrażliwych informacji, które następnie służą dezinformacji, zakłócaniu funkcjonowania sieci oraz systemów IT, a nawet niszczeniu przechowywanych w nich informacji.

a) **Aktywność grup powiązanych z Federacją Rosyjską obserwowane w 2024 r.**

W 2024 roku DKWOC/CSIRT MON zidentyfikował aktywność wymierzoną przeciwko systemom RON, którą przypisuje się grupom APT powiązanym ze służbami specjalnymi Federacji Rosyjskiej. Zaobserwowano działania polegające na: aktywnym rozpoznaniu infrastruktury RON, atakach phishingowych oraz atakach typu brute force ze szczególnym nastawieniem na systemy poczty elektronicznej. W ocenie DKWOC/CSIRT MON celem zidentyfikowanych aktywności adwersarzy prawdopodobnie było pozyskiwanie wrażliwych informacji dotyczących procesu dostaw do Ukrainy.

b) **Aktywność grup powiązanych z Republiką Białorusi w 2024 r.**

W zakresie aktywności grup APT powiązanych z Republiką Białorusi, DKWOC/CSIRT MON wraz z partnerami krajowymi identyfikował szeroko zakrojone kampanie phishingowe wymierzone głównie w obywateli Polski (w tym żołnierzy i pracowników RON), a także Litwy i Ukrainy. Kampanie charakteryzowały się różnorodnością technik, w tym dystrybucją złośliwego oprogramowania, wyłudzaniem poświadczeń logowania oraz podszywaniem się pod organizacje charytatywne.

Phishing był dominującą metodą działania adwersarza, przy czym szczególną uwagę zwracały ataki wymierzone w użytkowników o znaczeniu strategicznym. Adwersarz stosował fałszywe strony logowania do poczty e-mail. Jednocześnie, prowadził działania dystrybucyjne z wykorzystaniem złośliwego oprogramowania. W niektórych przypadkach adwersarz wykorzystywał metody socjotechniczne polegające na dystrybucji zainfekowanych dokumentów urzędowych, co wskazuje na próbę dotarcia do specyficznych grup ofiar, w tym instytucji rządowych i wojskowych. W ocenie DKWOC/CSIRT MON działania te mają na celu zakłócenie bezpieczeństwa regionu i są częścią szerszej strategii prowadzenia operacji przez grupy APT powiązane z Republiką Białorusi.

c) **Aktywność grup haktywistycznych w 2024 r.**

W 2024 r. DKWOC/CSIRT MON, w obszarze swojej odpowiedzialności, zidentyfikował jedną grupę haktywistyczną wykazującą aktywność. Unnamed Leshy[4], w ocenie DKWOC/CSIRT MON, realizuje działania zgodne z interesem strategicznym Federacji Rosyjskiej i odpowiada za przeprowadzenie ataków typu DDoS przeciwko podmiotom prywatnym i publicznym, w szczególności powiązanym z donacjami dla Ukrainy.

[4] NoName057(10) - DKWOC/CSIRT MON opracowując Model zagrożeń dla systemów IT RON na 2024 r. zastosował własną nomenklaturę nazewniczą dla zbiorów i klastrów aktywności stanowiących największe zagrożenie

3.2.4 ZIDENTYFIKOWANE NAJPOWAŻNIEJSZE ZAGROŻENIA.

W 2024 roku znaczący wpływ na bezpieczeństwo systemów IT RON miały zagrożenia wynikające z działań grup APT. Aktywność tych grup kojarzona jest głównie z działalnością sponsorowaną lub będącą częścią struktur państwa. Spektrum działań grup APT obejmuje różnorodne czynności: od systematycznie realizowanego rozpoznania infrastruktury teleinformatycznej, poprzez cyberszpiegostwo, zakłócanie działania systemów IT i sieci, aż po niszczenie danych, które się w nich znajdują. Do najpoważniejszych zagrożeń ze strony grup APT można zaliczyć:

- Ataki spear-phishingowe mające na celu wykradanie poświadczeń logowania lub infekcji urządzenia złośliwym oprogramowaniem.
- Skompromitowanie komercyjnych dostawców usług i rozwiązań IT.
- Wykorzystywanie przez grupy APT podatności typu zero-day.
- Ataki typu brute force w celu uzyskania dostępu do zasobów sieciowych i skrzynek pocztowych.

W licznych atakach grupy APT wykorzystywały skompromitowane prywatne urządzenia sieciowe (m.in. zlokalizowane w Polsce) oraz posługiwały się infrastrukturą anonimizującą typu VPN/proxy w celu ukrycia źródła ataku oraz atrybucji.

Więcej informacji dot. działalności MON w cyberprzestrzeni zostało zawarte w rozdziale 7. Ministerstwo Obrony Narodowej oraz w 4.2 Działania Ministra Obrony Narodowej jako organu właściwego do spraw cyberbezpieczeństwa.

3.3 CSIRT NASK

3.3.1 DANE DOTYCZĄCE LICZBY ZGŁOSZEŃ I INCYDENTÓW W 2024 R.

Zgłoszenia i incydenty cyberbezpieczeństwa zarejestrowane przez CSIRT NASK od 1 stycznia do 31 grudnia 2024 r.

Tabela 19. Zestawienie zgłoszeń i incydentów

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	600 990
w tym zarejestrowane (obsłużone) incydenty	103 449

Incydenty zgłoszone ustawowo do CSIRT NASK od 1 stycznia do 31 grudnia 2024 r.

Tabela 20. Kwalifikacja incydentów wg. KSC

Zagrożenia cyberbezpieczeństwa	Liczba
Incydenty krytyczne	0
Incydenty poważne	57
Incydenty istotne	0
Incydenty w podmiotach publicznych	3 450

3.3.2 INCYDENTY USTAWOWE W PODZIALE NA SEKTORY W 2024 R.

Wśród **57** incydentów poważnych odnotowanych w 2024 r. **44** zdarzenia miały miejsce w sektorze **bankowości i infrastruktury rynków finansowych**. Pozostałe incydenty poważne dotyczyły **sektora ochrony zdrowia** (**11**) oraz **sektora transportu** (**2**). Wśród **3 450** incydentów w podmiotach publicznych, zgłoszonych ustawowo do CSIRT NASK od stycznia do grudnia 2024 r., **ponad połowę (55%) stanowiły incydenty w administracji publicznej**. W analizowanym okresie **nie zarejestrowano żadnego incydentu krytycznego ani też żadnego incydentu istotnego**.

3.3.3 NAJCZĘSTSZE TYPY INCYDENTÓW WG TAKSONOMII ECSIRT.NET W 2024 R.

W 2024 r. zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**98 tys.**) stanowiły one **95%**. Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). W 2024 r. odnotowano **40,1 tys.** takich incydentów.

Oszuści stosowali różnorodne scenariusze. W dalszym ciągu często występowały oszustwa inwestycyjne, w których podszywali się pod różne koncerny paliwowo-energetyczne, firmy oraz instytucje. Wiele z tych oszustw zaczynało się reklamami wykorzystującymi wizerunki znanych osób – polityków, sportowców, aktorów, które zamieszczano w mediach społecznościowych. Linki przekierowywały na strony, na których potencjalnym ofiarom obiecywano wysokie zyski, ale prawdziwym celem oszustów było wyłudzenie pieniędzy. Ponadto na liście oszustw komputerowych znalazły się też m.in. fałszywe sklepy internetowe. Natomiast wśród popularnych kampanii phishingowych były m.in. przypadki nieuprawnionego wykorzystywania wizerunku serwisów OLX, Allegro oraz Facebook.

Kolejnym najczęściej występującym rodzajem zagrożeń było szkodliwe oprogramowanie. W 2024 r. tego typu incydentów zarejestrowano **1 891.** Wśród odnotowanych incydentów z tej kategorii dominowały szeroko rozsyłane wiadomości e-mail ze szkodliwym załącznikiem. Załącznik zawierał najczęściej tzw. infostealer, czyli oprogramowanie służące do wykradania haseł i innych poufnych informacji z zainfekowanych komputerów. Wśród najczęściej występujących infostealerów można wyróżnić takie rodziny, jak Formbook, Remcos, Lumma Stealer czy Agent Tesla.

W tym zestawieniu trzecią pozycję zajmują podatne usługi. W minionym roku tego typu zagrożeń odnotowano **1 634**, w tym 260 incydentów zostało zarejestrowanych na podstawie wyników skanowania z systemu Artemis, 726 incydentów po analizie wyników skanowania urządzeń przemysłowych przez system Snitch oraz 119 na podstawie wysyłek podatności, dotyczących krytycznych podatności w produktach IT wykorzystywanych w Polsce. Pozostałe incydenty dotyczyły bieżącej obsługi zgłaszanych zagrożeń.

Tabela 21. Najpopularniejsze rodzaje ataków

Top 3 zarejestrowanych incydentów wg rodzaju	Liczba
Oszustwa komputerowe	**97 995**
Szkodliwe oprogramowanie	**1 891**
Podatne usługi	**1 634**

3.3.4 ZGŁOSZENIA SMS ORAZ WZORCE FAŁSZYWYCH WIADOMOŚCI SMS

CSIRT NASK monitoruje występowanie smishingu oraz tworzy wzorce wiadomości, które posiadają cechy pozwalające na uznanie ich za smishing. Działania te wykonuje na podstawie zgłoszeń podejrzanych wiadomości tekstowych (SMS) otrzymanych od odbiorców tych wiadomości oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów. Podejrzane SMS- y można zgłaszać do CSIRT NASK poprzez bezpłatny skrócony numer **8080**.

Tabela 22. Liczba zgłoszeń wiadomości SMS oraz wzorce fałszywych wiadomości SMS

Zgłoszenia wiadomości SMS oraz wzorce fałszywych wiadomości SMS	Liczba
Zgłoszenia wiadomości SMS	**354 566**
Wzorce fałszywych wiadomości SMS	**746**

3.3.5 ZGŁOSZENIA NIELEGALNYCH TREŚCI

Oddzielną grupę stanowią incydenty związane z publikacją potencjalnie nielegalnych treści w Internecie, w szczególności materiały przedstawiające seksualne wykorzystywanie dzieci lub inne szkodliwe treści skierowane przeciwko bezpieczeństwu małoletnich. Tego typu zagrożenia obsługiwane są przez zespół Dyżurnet.pl.

3.3.6 INCYDENTY ZAREJESTROWANE PRZEZ ZESPÓŁ DYŻURNET.PL OD 1 STYCZNIA DO 31 GRUDNIA 2024 R.

Rysunek 3. Incydenty zarejestrowane przez DYŻURNET.PL

Incydenty zarejestrowane przez zespół Dyżurnet.pl	Liczba
Przeanalizowane incydenty*, w tym:	**27 787**
treści przedstawiające seksualne wykorzystywanie dzieci (CSAM**)	**11 147**
*Incydent to zgłoszenie poddane analizie oraz odpowiednio zaklasyfikowane przez ekspertów Dyżurnet.pl. Liczba wszystkich zgłoszeń potencjalnie nielegalnych treści. ** CSAM (Child Sexual Abuse Materials), tj. materiały przedstawiające seksualne wykorzystywanie dziecka.	

3.3.7 DZIAŁANIA GRUP APT OBSERWOWANE PRZEZ CSIRT NASK W 2024 R.

W 2024 r. CERT Polska/CSIRT NASK ponownie zaobserwował wysoki poziom aktywności grup APT, wiązanych z obcymi państwami. Grupy prowadziły swoje działania zarówno w celach wywiadowczych, jak i propagandowych. Większość obserwowanej aktywności atakujących związana była z wyłudzaniem danych uwierzytelniających do skrzynek pocztowych, dystrybucją szkodliwego oprogramowania, a także z atakami na systemy przemysłowe. W 2024 r. celem ataków były już nie tylko największe firmy czy instytucje publiczne, lecz także mniejsze firmy, mające znaczenie w łańcuchach dostaw, a nawet osoby blisko związane z atakowanymi (członkowie ich rodzin czy znajomi).

Przypadki opisywane poniżej stanowią wyłącznie fragment działalności grup APT, monitorowanej przez CERT Polska/CSIRT NASK, i nie odzwierciedlają w pełni skali znanych ataków tych grup na polskie instytucje.

Większość zaobserwowanych ataków dotyczyła grup związanych z Federacją Rosyjską oraz Republiką Białorusi.

Tabela 23. Aktowość grup APT w ujęciu miesięcznym

Aktywność grup APT obserwowanych przez CERT Polska/CSIRT NASK*	**2024**											
	sty	**lut**	**mar**	**kwi**	**maj**	**cze**	**lip**	**sie**	**wrz**	**paź**	**lis**	**gru**
UNC1151/Ghostwriter (Rosja/Białoruś)		■	■	■		■		■	■	■	■	■
APT28/Fancy Bear/ Forest Blizzard (Rosja)	■	■	■	■	■	■	■		■	■		
APT29/Cozy Bear/ Midnight Blizzard (Rosja)										■		
Sandworm/Voodo Bear/Seashell Blizzard (Rosja)				■						■		
Turla/Venomous Bear/ Secret Blizzard (Rosja)	■	■			■							
APT-UNK3	■											
APT-UNK4							■					

* *Aktywność grup APT obserwowanych przez CERT Polska/CSIRT NASK w 2024 r. została oznaczona na zielono.*

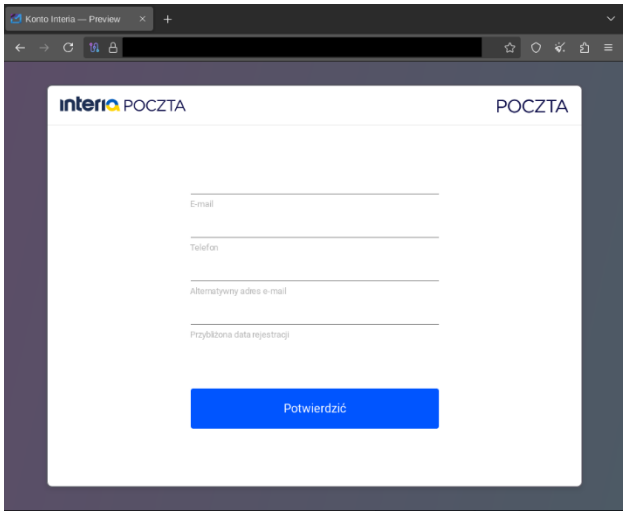
3.3.8 WYBRANE KAMPANIE

3.3.8.1 UNC1151/GHOSTWRITER

W 2024 r. grupa UNC1151 kontynuowała intensywne działania, które były już odnotowywane w poprzednich latach, i ponownie została uznana za najaktywniejszą organizację wśród grup

obserwowanych przez CSIRT NASK. Według publikacji firm Mandiant[5] i Google[6] grupa UNC1151 z dużym prawdopodobieństwem powiązana jest z rządem Białorusi, ale według innych źródeł ma również związek z rosyjskimi służbami specjalnymi [7]. W ostatnim roku grupa ta wykazała się niezwykle różnorodnymi metodami ataku, obejmującymi zarówno ataki phishingowe na klientów serwisów pocztowych, jak i infekcje złośliwym oprogramowaniem. Grupa angażowała się także w działania propagandowe, które dotyczyły polskich olimpijczyków, konfliktu zbrojnego na Ukrainie oraz ćwiczeń wojskowych, odbywających się na terenie Polski. Tak szerokie spektrum działania grupy wskazuje, że dąży ona nie tylko do realizacji celów wywiadowczych, lecz także do wpływania na opinię publiczną w kluczowych kwestiach społeczno-politycznych.

Równanie 1. Fałszywy panel logowania grupy UNC1151 do serwisu pocztowego Interia



Przez większość roku grupa UNC1151 prowadziła intensywną kampanię mailową, w której pod pretekstem zawieszenia konta oraz konieczności zmiany hasła nakłaniała użytkowników do podania swoich danych logowania do serwisów pocztowych. Zgodnie z posiadanymi przez nas informacjami oraz na podstawie skali zgłoszeń otrzymanych od obywateli możemy ocenić, że działania te miały charakter zakrojony na dużą skalę – celem były osoby wykonujące różne zadania czy funkcje społeczne.

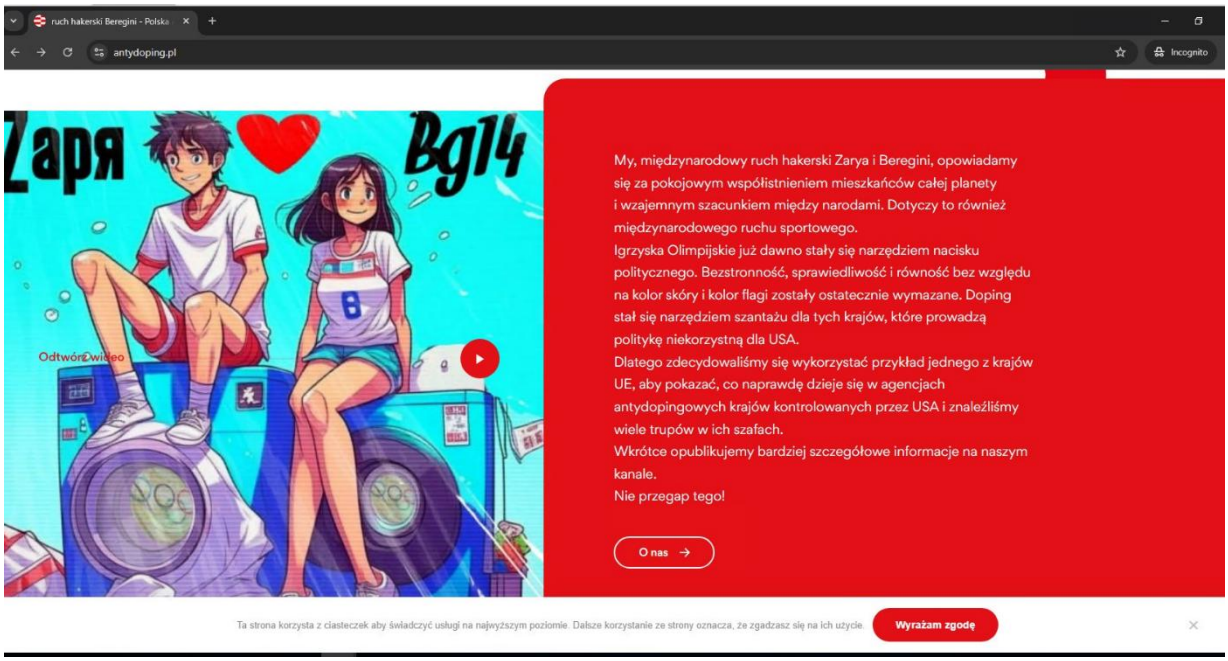
W atakach z użyciem szkodliwego oprogramowania grupa wykorzystywała motyw zaproszeń na branżowe spotkania i konferencje, aby zachęcić użytkowników do pobrania pliku archiwum załączonego do wiadomości e-mail. W archiwach znajdowały się pliki w formacie CHM (Compiled HTML Help), które po otwarciu wyświetlały nieświadomemu użytkownikowi zaproszenie na prawdziwe wydarzenie, jednocześnie uruchamiając złośliwy kod. Na dalszym etapie infekcji zainfekowane systemy pobierały Cobalt Strike, narzędzie umożliwiające zdalne przejęcie kontroli nad systemem, co pozwala na wykonywanie różnorodnych działań, takich jak kradzież danych, rozprzestrzenianie się w sieci, instalacja dodatkowych narzędzi atakującego.

W czerwcu 2024 r. zespół CERT Polska nawiązał komunikację z Polską Agencją Antydopingową (POLADA) w sprawie prawdopodobnej infekcji szkodliwym oprogramowaniem, a następnie podjął się przeprowadzenia pełnej analizy incydentu. Podczas analizy ustalono, że za atakiem stał prawdopodobnie aktor, który wykorzystał podatność w jednym z systemów w polskiej instytucji, a następnie odsprzedał dostęp do infrastruktury, tzw. access broker. Na podstawie odnalezionych artefaktów stwierdzono, że w wyniku tego działania dostęp do systemów organizacji uzyskała grupa UNC1115, która następnie

[5] https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
[6] https://blog.google/threat-analysis-group/update-threat-landscape-ukraine
[7] https://www.gov.pl/web/sluzby-specjalne/ustalenia-abw-i-skw-dot-atakow-hakerskich

wykradła dane dotyczące polskich sportowców. Pod koniec igrzysk olimpijskich w Paryżu doszło do włamania na stronę internetową POLADA, a na jednym z kanałów na Telegramie, powiązanym z grupą UNC1151, opublikowano wykradzione dane. Grupa wykorzystała to wydarzenie do dystrybucji treści dezinformacyjnych, dotyczących zażywania środków dopingujących przez polskich sportowców.

W ubiegłym roku grupa wielokrotnie wiązana była z dystrybucją treści dezinformacyjnych, które dotyczyły m.in. sytuacji w Ukrainie, ćwiczeń wojskowych Steadfast Defender 2024 i Dragon-24, a także wielu innych wydarzeń społeczno-politycznych.



Rysunek 4. Treść propagandowa zamieszczona przez grupę UNC1151 na stronie Polskiej Agencji Antydopingowej

3.3.8.2 APT28/FANCY BEAR/FOREST BLIZZARD

W 2024 r. CERT Polska zaobserwował znaczący wzrost aktywności grupy APT28, która jest wiązana z Głównym Zarządem Wywiadowczym Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). Działania grupy skupiły się głównie na dystrybucji szkodliwego oprogramowania oraz próbach kradzieży danych dostępowych do systemów pocztowych Microsoft Outlook.

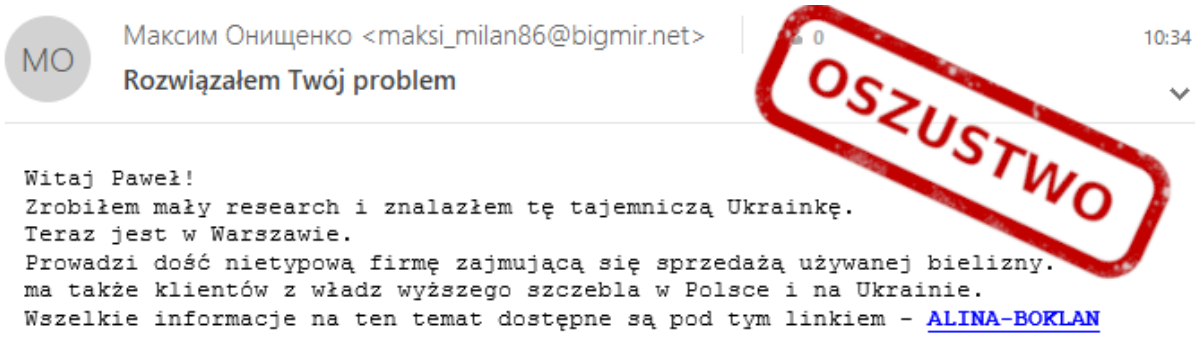
Rysunek 5. Przykład treści dezinformacyjnej w serwisie Telegram

W maju 2024 r. CSIRT NASK, we współpracy z CSIRT MON i CSIRT GOV, zaobserwował kolejną z wielu prób infekcji szkodliwym oprogramowaniem użytkowników w polskich instytucjach i podmiotach publicznych. Treść rozsyłanych wiadomości e-mail miała na celu wzbudzenie zainteresowania potencjalnych ofiar i skłonienie ich do kliknięcia w link zamieszczony w treści wiadomości.

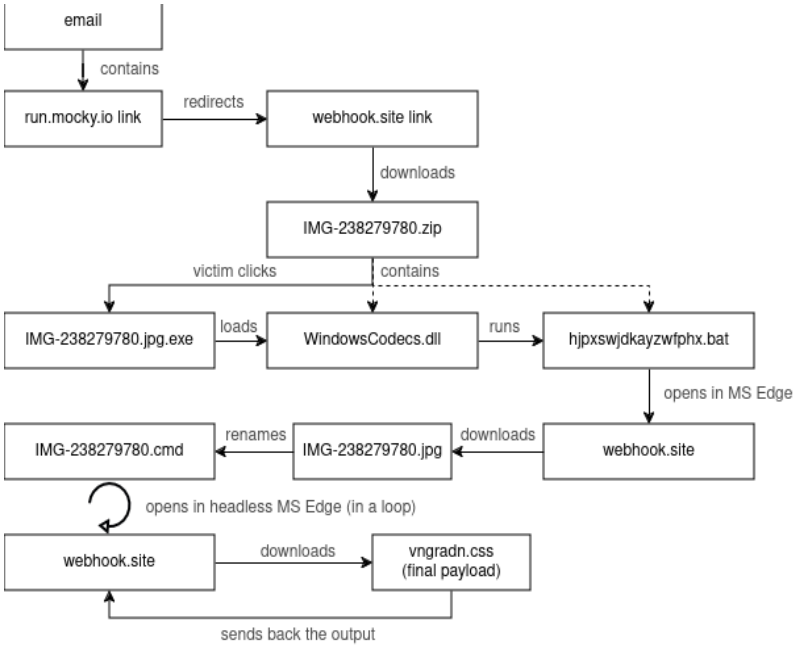
Po kliknięciu w link użytkownik przenoszony był najpierw do serwisu run.mocky[.]io, a następnie webhook[.]site, skąd pobierane było archiwum ZIP. Serwisy te są darmowe i popularne wśród osób związanych z IT. Warto podkreślić, że wykorzystanie darmowych, powszechnie używanych usług zamiast własnych domen pozwala adwersarzom znacznie ograniczyć wykrycie złośliwych linków i jednocześnie obniża koszt prowadzonej przez nich operacji. Jest to trend, który obserwujemy u wielu grup APT.

Archiwum ZIP zawierało trzy pliki: kalkulator windowsowy ze zmienioną nazwą, np. IMG-238279780.jpg.exe, który udaje zdjęcie i zachęca ofiarę do kliknięcia, skrypt .bat (plik ukryty), fałszywą bibliotekę WindowsCodecs.dll (plik ukryty).

Rysunek 6. Przykład wiadomości użytej przez grupę APT28 do dystrybucji szkodliwego oprogramowania



Rysunek 7. Diagram przedstawiający poszczególne etapy infekcji



Jeśli ofiara uruchomiła plik IMG-238279780.jpg.exe (będący nieszkodliwym kalkulatorem), podczas startu próbował on załadować bibliotekę WindowsCodecs.dll, która została podstawiona przez atakujących. Jest to technika znana jako DLL Side-Loading. Głównym celem biblioteki DLL było uruchomienie dołączonego skryptu BAT. Po przejściu przez kolejne etapy infekcji użytkownik infekowany był szkodliwym oprogramowaniem HEADLACE. Pełna analiza kampanii została opisana na stronie internetowej CERT Polska[8].

Oprócz działań związanych ze szkodliwym oprogramowaniem grupa APT28 prowadziła intensywne kampanie phishingowe wymierzone w polskie instytucje rządowe. Celem tych działań było wyłudzanie danych uwierzytelniających do kont Microsoft Outlook, co mogłoby umożliwić atakującym dostęp do wrażliwych informacji. Uzyskanie takiego dostępu pozwoliłoby na kradzież korespondencji służbowej, co niosłoby ze sobą poważne zagrożenie dla bezpieczeństwa informacji w tych instytucjach. Dodatkowo dostęp do konta mógłby umożliwić grupie APT28 pozyskanie danych o pracownikach z książki adresowej, co stanowiłoby cenną bazę informacji do dalszych działań. Taki scenariusz mógłby również umożliwić grupie dystrybucję szkodliwego oprogramowania poprzez wykorzystanie zaufania do nadawców wiadomości.

3.3.9 WSPÓŁPRACA KRAJOWA I MIĘDZYNARODOWA ORAZ UDZIAŁ W PROJEKCIE FETTA

W 2024 r. CSIRT NASK w ramach działań związanych z obserwacją aktywności grup APT kontynuował bliską współpracę z CSIRT-ami poziomu krajowego (CSIRT MON i CSIRT GOV) oraz z zespołami polskich służb specjalnych, z którymi regularnie wymieniał informacje o zagrożeniach oraz przeprowadzał analizy kampanii.

Współpraca międzynarodowa w ramach CSIRTs Network oraz z partnerami komercyjnymi pozwoliła wymieniać się informacjami na temat ataków prowadzonych równocześnie w innych krajach europejskich, co przyczyniło się do skutecznej ochrony obywateli oraz instytucji przed zagrożeniami.

W 2024 r. zespół CERT Polska zaangażował się również w projekt FETTA[9] (Federated European Team for Threat Analysis, Europejski Zespół Analizy Zagrożeń), którego głównym zadaniem jest ułatwienie współpracy i wymiana wiedzy w obszarze CTI, w tym m.in. o zagrożeniach związanych z grupami APT, o wykorzystywanych podatnościach oraz o nowych metodykach stosowanych przez atakujących.

[8] https://cert.pl/posts/2024/05/apt28-kampania
[9] https://cert.pl/posts/2024/01/fetta

3.3.10 OPIS NAJWAŻNIEJSZYCH REALIZOWANYCH DZIAŁAŃ W OBSZARZE CYBERBEZPIECZEŃSTWA

W 2024 r. CSIRT NASK w celu wzmocnienia krajowego systemu cyberbezpieczeństwa kontynuował wdrażanie rozwiązań zgodnych z zapisami ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, a także rozwijał narzędzia już funkcjonujące. Działania te obejmowały m.in.:

- Uruchomienie systemu teleinformatycznego (telegraf.cert.pl) służącego do wymiany informacji o wzorcach szkodliwych wiadomości SMS oraz zawierającego wykaz nadpisów wiadomości SMS zarezerwowanych dla podmiotów publicznych. CSIRT NASK tworzy wzorce szkodliwych wiadomości na podstawie zgłoszeń wysłanych przez odbiorców tych wiadomości oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów. CSIRT NASK zapewnia dostęp do informacji zawartych w systemie Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi UKE i przedsiębiorcom telekomunikacyjnym. Przedsiębiorcy telekomunikacyjni mają obowiązek blokowania fałszywych SMS-ów zgodnie ze wzorcami oraz wiadomości SMS zawierające fałszywe nadpisy.
- Udostępnienie na stronie incydent.cert.pl/nadpis formularza umożliwiającego podmiotom publicznym zgłaszanie nadpisów wiadomości SMS.
- Prowadzenie i aktualizowanie **Listy Ostrzeżeń**, która funkcjonuje od 2020 r. Wpisywane są na nią domeny wprowadzające użytkowników w błąd i wyłudzające od nich dane. Celem listy jest chronienie użytkowników końcowych przed wejściem na niebezpieczną domenę poprzez zablokowanie jej na poziomie DNS.
- Rozwój serwisu **bezpiecznapoczta.cert.pl** – serwis powstał, by chronić użytkowników poczty elektronicznej i ułatwić instytucjom sprawdzanie poprawności konfiguracji mechanizmów zapewniających jej bezpieczeństwo.

Innym działaniem mającym przyczynić się do poprawy cyberbezpieczeństwa obywateli było uruchomienie w sierpniu 2024 r. usługi **Bezpiecznie w sieci w aplikacji mObywatel**, za pomocą której użytkownicy mogą w łatwy sposób zgłaszać niepokojące zjawiska w sieci, takie jak szkodliwe strony internetowe czy oszustwa. Tego typu zgłoszenia trafiają do CERT Polska. Można także zgłosić nielegalne treści związane z nieodpowiednimi zachowaniami wobec dzieci – takie zgłoszenia są analizowane przez ekspertów z zespołu Dyżurnet.pl. W ramach usługi Bezpiecznie w sieci dostępna jest także **Baza wiedzy**, gdzie są zamieszczane artykuły na temat zagrożeń w internecie oraz o bezpiecznym korzystaniu z sieci przygotowywane przez ekspertów z CERT Polska. Dodatkowo użytkownicy mogą otrzymywać powiadomienia o aktualnych cyberzagrożeniach. Nowa usługa to efekt współpracy Ministerstwa Cyfryzacji, CERT Polska oraz Centralnego Ośrodka Informatyki.

CERT Polska ma przyznany **status CNA** (ang. *CVE Numbering Authority*), dzięki temu jako jedyna instytucja w Polsce i jeden z 7 CERT-ów w Europie może nadawać numery CVE (ang. *Common Vulnerabilities and Exposures*) służące do identyfikacji i katalogowania publicznie ujawnionych podatności. Baza CVE jest dostępna za darmo dla każdego. W okresie od stycznia do grudnia 2024 r. Dział CERT Polska nadał **88** takich identyfikatorów podatnościom, także tym odkrytym w ramach badań własnych.

W związku z rosnącą liczbą cyberzagrożeń CSIRT NASK rozwijał narzędzie Artemis, służące do wykrywania najczęściej występujących podatności i błędów konfiguracyjnych obecnych w ramach usług sieciowych, a także przekazywał osobom odpowiedzialnym za dany system informacje o znalezionych podatnościach i błędnych konfiguracjach.

W 2024 r. w ramach projektu **Artemis** łącznie przeskanowano ok. **249,8 tys.** domen i adresów IP i ok. **795,5 tys.** subdomen. W sumie wykryto ok. **331,6 tys.** podatności lub błędnych konfiguracji, w tym ok. **20 tys. stanowiących wysokie** zagrożenie. W analizowanym okresie wykryto przynajmniej jedną podatność/błędną konfigurację w ok. **104,1 tys.** przeskanowanych domenach/subdomenach. W analizowanym okresie CSIRT NASK wysłał **88,9 tys.** powiadomień o wykrytych nieprawidłowościach. Ostrzeżenia zostały przekazane m.in. do placówek oświatowych, uczelni, jednostek samorządu terytorialnego, osób odpowiedzialnych za bezpieczeństwo systemów w domenie gov.pl, placówek medycznych, producentów automatyki przemysłowej, mediów lokalnych, a także operatorów usług kluczowych. Dzięki temu, że znalezione podatności i błędne konfiguracje są zgłaszane osobom odpowiedzialnym za dany system, CSIRT NASK zwiększa bezpieczeństwo polskiego internetu.

W 2024 r. CSIRT NASK w dalszym ciągu rozwijał platformę **n6** (system agregacji i udostępniania informacji o zagrożeniach wspierający instytucje w monitorowaniu aktualnych trendów w cyberbezpieczeństwie oraz dzieleniu się informacjami o zdarzeniach sieciowych), który jest udostępniany na licencji z otwartym kodem źródłowym.

Podobnie jak w poprzednich latach CSIRT NASK w ramach wzmacniania współpracy międzysektorowej rozwijał program Partnerstwo dla Cyberbezpieczeństwa (PdC). Jest to istotny kanał wymiany informacji pomiędzy podmiotami KSC. Celem PdC jest wymiana dobrych praktyk i zacieśnianie współpracy w ramach krajowego systemu cyberbezpieczeństwa. W 2024 r. odbyły się spotkania i szkolenia, podczas których eksperci dzielili się wiedzą m.in. na temat najważniejszych krajowych i unijnych regulacji prawnych w obszarze cyberbezpieczeństwa, występujących cyberzagrożeń i metod ochrony przed nimi, a także na tematy związane z nowymi technologiami i innowacyjnymi rozwiązaniami w cyberbezpieczeństwie. W trakcie spotkań poruszano też kwestie związane z budowaniem świadomości w zakresie cyberbezpieczeństwa. Regularnie przygotowywano także i rozsyłano materiały informacyjno-edukacyjne dla uczestników programu PdC.

Istotnym elementem działalności CSIRT NASK w roku 2024 była kontynuacja prac nad realizacją projektu Centrum Cyberbezpieczeństwa NASK (CCN), którego głównym celem jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Projekt stanowi odpowiedź na szereg wyzwań i potrzeb w związku z rosnącą liczbą zagrożeń w cyberprzestrzeni. W ramach CCN powstaną m.in.: Krajowe Centrum Odzyskiwania Danych, Krajowe Centrum Operacyjne Cyberbezpieczeństwa, Laboratorium Bezpieczeństwa AI, Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania, Ośrodek Modelowania Certyfikacji Cyberbezpieczeństwa. Prace nad realizacją projektu rozpoczęły się w trzecim kwartale 2023 r., a planowany termin ich zakończenia to 2029 r.

W celu zapewnienia ochrony przed atakami DDoS (*Distributed Denial of Service*) dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP w dalszym ciągu realizowano usługę AntyDDoS.

Wskazane powyżej działania w istotny sposób przełożyły się na funkcjonowanie krajowego systemu cyberbezpieczeństwa i rozwijanie współpracy pomiędzy podmiotami go tworzącymi.

3.3.11 ANALIZA I OCENA FUNKCJONOWANIA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

W 2024 r. CSIRT NASK – w ramach monitorowania zmian w obszarze *constituency* CSIRT NASK związanych z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, a także z rozwojem krajowego i europejskiego prawa w obszarze cyberbezpieczeństwa – opracował analizy:

- „Dostawcy usług zaufania w dyrektywie NIS 2 a dotychczasowe regulacje”,
- „Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze zmiany dla podmiotów”,
- „Wdrożenie DSA w Polsce”,
- broszura informacyjna „Zakazane systemy AI” (opracowana przez ekspertów z NASK-PIB we współpracy z Ministerstwem Cyfryzacji),
- Raport „Krajobraz europejskich ISAC-ów w 2023 roku”.

3.3.12 ZIDENTYFIKOWANE NAJPOWAŻNIEJSZE ZAGROŻENIA TECHNICZNE DLA SYSTEMÓW TELEINFORMATYCZNYCH:

Najpoważniejszym zagrożeniem technicznym są coraz liczniejsze podatności w urządzeniach brzegowych i oprogramowaniu dostępnym z internetu. Często podatności dotyczą np. koncentratorów VPN. Rośnie również liczba przypadków, gdzie luka była wykorzystywana przez atakujących jeszcze przed opublikowaniem aktualizacji naprawiającej błąd, są to tzw. podatności 0day. W takich sytuacjach nawet jeśli organizacja dba o bezpieczeństwo i dokonuje aktualizacji, może paść ofiarą ataku. Wymusza to podejście, w którym należy zakładać, że do ataku już doszło, i przenieść ciężar monitorowania bezpieczeństwa oraz segmentacji wewnątrz organizacji. Będzie to duże wyzwanie w najbliższych latach.

3.3.13 ZIDENTYFIKOWANE NAJPOWAŻNIEJSZE ZAGROŻENIA SYSTEMOWE DLA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA:

Największym systemowym zagrożeniem napotykanym podczas obsługi incydentów przez CSIRT NASK jest trudność w ustaleniu właściciela adresacji IP. Częste są przypadki, w których CSIRT NASK posiada informację o podatności, ale nie może z nią dotrzeć na czas do administratora przez brak kontaktu. Dużym systemowym wyzwaniem będzie również zapewnienie kadr dla planowanych sektorowych zespołów cyberbezpieczeństwa. W krótkim czasie znacząco wzrośnie zapotrzebowanie na specjalistów cyberbezpieczeństwa pracujących dla sektora publicznego.

3.3.14 WNIOSKI I REKOMENDACJE

CSIRT NASK obserwuje ciągły wzrost zagrożeń zarówno w obszarze przestępczości zorganizowanej (ransomware), jak i grup sponsorowanych przez obce państwa (APT). Żeby skutecznie walczyć z tymi zagrożeniami, niezbędna jest jeszcze bliższa współpraca w ramach krajowego systemu cyberbezpieczeństwa oraz ze służbami specjalnymi. Częste są przypadki, że atak widziany przez jeden z CSIRT-ów jest tylko małym wycinkiem obrazu i nie da się go przeanalizować w całości bez współpracy. CSIRT NASK rekomenduje łączenie już istniejących systemów klasy TIP (Threat Intelligence Platform) w różnych organizacjach, celem jeszcze szybszej analizy zagrożeń.

CSIRT NASK rekomenduje rozpoczęcie prac legislacyjnych mających na celu wypracowanie skuteczniejszych metod dotarcia do właścicieli adresacji IP w przypadku stwierdzenia występowania podatności lub konfiguracji pozwalającej na atak.

CSIRT NASK widzi potrzebę promocji Listy Ostrzeżeń wśród mniejszych dostawców usług internetowych oraz wśród firm korzystających z własnych systemów DNS. Korzystanie z Listy Ostrzeżeń jest dobrowolne i tylko dzięki edukacji będziemy zwiększali jej skuteczność.

3.3.15 PLANOWANE DZIAŁANIA W 2025 R.

- CSIRT NASK będzie uczestniczył w działaniach związanych z polską prezydencją w Radzie Unii Europejskiej.
- CSIRT NASK planuje kontynuować dotychczas prowadzoną współpracę krajową i międzynarodową w zakresie monitorowania działań grup APT, w szczególności z CSIRT-ami poziomu krajowego (CSIRT GOV i CSIRT MON) oraz z zespołami odpowiednich polskich służb specjalnych, a także w ramach CSIRTs Network oraz z partnerami komercyjnymi.
- Artemis – rozwój skanera wykrywającego najczęściej występujące podatności i błędy konfiguracyjne obecne w ramach usług sieciowych. Narzędzie przeznaczone jest do weryfikacji przede wszystkim podmiotów z *constituency* CSIRT NASK, czyli np. szkół, szpitali, instytutów badawczych, uczelni, jednostek samorządu terytorialnego. Znalezione podatności i błędne konfiguracje są i będą zgłaszane osobom odpowiedzialnym za dany system.
- Rozwój platformy n6 służącej do zbierania informacji o wykrytych zagrożeniach i podatnościach.
- CSIRT NASK planuje w 2025 r. uruchomienie nowej usługi (moje.cert.pl) pozwalającej na zlecanie skanowania systemem Artemis każdemu obywatelowi posiadającemu stronę internetową. W systemie będą również informacje o zagrożeniach dla adresacji IP pochodzące z systemu n6 oraz informacje o wyciekach dla kont e-mailowych w zweryfikowanych domenach podanych przez obywatela.
- W odpowiedzi na rosnącą skalę zagrożeń w sieci, a także skokową zmienność liczby zgłoszeń prowadzone będą prace podnoszące efektywność obsługi oraz zwiększające szybkość udzielania informacji zwrotnej dla zgłaszających podejrzane wiadomości. W 2025 r. planowane są znaczne prace rozwojowe mające na celu automatyzację klasyfikacji zgłaszanych incydentów, w tym z wykorzystaniem uczenia maszynowego.
- CERT Polska/CSIRT NASK pełniący funkcję CNA (ang. *CVE Numbering Authority*) w dalszym ciągu będzie współtworzyć bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności.
- Dalsze monitorowanie kampanii wykorzystujących jako kanał dystrybucji wiadomości SMS (smishing) oraz tworzenie nowych wzorców wiadomości, które pozwalają zatrzymać tego typu

wiadomości na poziomie operatora komórkowego. CSIRT NASK nadal będzie obsługiwał system wymiany informacji o smishingu i prowadził wykaz zastrzeżonych nadpisów dla podmiotów publicznych.
- CSIRT NASK będzie w dalszym ciągu opracowywał rekomendacje oraz zalecenia dotyczące występujących podatności.
- CSIRT NASK planuje kontynuować działania informacyjno-edukacyjne, w szczególności mające na celu podnoszenie świadomości obywateli w zakresie cyberzagrożeń i cyberhigieny.
- W związku z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa CSIRT NASK będzie koordynował współpracę CSIRT-ów sektorowych i wspierał rozwój ich kompetencji.
- CSIRT NASK planuje monitorować oszustwa związane z fałszywymi reklamami na platformach społecznościowych i komunikować oczekiwania wobec firm, które tymi platformami zarządzają. W szczególności w 2025 r. zostanie sprawdzone, czy firma Meta wdraża zmiany zarekomendowane w 2024 r. przez CERT Polska.
- CSIRT NASK będzie rozwijał system ostrzeżeń dostępnych dla obywateli, takich jak np. powiadomienie o cyberzagrożeniach w aplikacji mObywatel.
- W ramach inwestycji realizowanej ze środków Krajowego Planu Odbudowy CSIRT NASK, w roli lidera, rozpocznie we współpracy z Komendą Główną Policji projekt pod akronimem CROPT. Celem przedsięwzięcia jest modernizacja i profesjonalizacja działań operacyjnych prowadzonych w siedzibie podmiotu KSC, u którego wystąpił incydent. W projekcie szczególny nacisk zostanie położony na analizę incydentów z wykorzystaniem szkodliwego oprogramowania szyfrującego. W 2024 r. CSIRT NASK zarejestrował i obsłużył 147 incydentów tego typu, z czego 25 w podmiotach publicznych.

3.3.16 PRZEWIDYWANIA DOTYCZĄCE SYTUACJI W CYBERPRZESTRZENI NA LATA 2025–2026

- Wzrost liczby ataków powiązanych z obcymi państwami (grupy APT).
- Dalszy wzrost wykorzystania w atakach na firmy podatności w oprogramowaniu i urządzeniach brzegowych. Można przewidywać, że coraz mocniej ten wektor będzie wypierał złośliwe oprogramowanie dystrybuowane pocztą elektroniczną oraz klasyczne phishingi.
- Dalszy wzrost wykorzystania socjotechniki w oszustwach wymierzonych w obywateli. Ataki będą coraz prostsze technicznie, ale trudniejsze do oceny pod kątem wiarygodności.
- Większa liczba kampanii, w których oszuści będą wykorzystywać sztuczną inteligencję do wygenerowania fałszywego głosu i wizerunku.

4 ORGANY WŁAŚCIWE DO SPRAW CYBERBEZPIECZEŃSTWA I SEKTOROWE ZESPOŁY CYBERBEZPIECZEŃSTWA

Organy właściwe i ich zadania zdefiniowane są w art. 41 UKSC. Przepisy te przewidują istnienie następujących sektorów i odpowiedzialnych za nich organów:

1) sektor energii – minister właściwy do spraw energii (Minister Klimatu i Środowiska);
2) sektor transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu (Minister Infrastruktury);
3) podsektor transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej (Minister Infrastruktury);
4) sektor bankowy i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;
5) sektor ochrony zdrowia **(z wyłączeniem podmiotów podległych MON)** – minister właściwy do spraw zdrowia (Minister Zdrowia);
6) sektor ochrony zdrowia obejmujący podmioty podległe MON - Minister Obrony Narodowej;
7) sektor zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej (Minister Infrastruktury);
8) sektor infrastruktury cyfrowej **(z wyłączeniem podmiotów podległych MON)** – minister właściwy do spraw informatyzacji (Minister Cyfryzacji);
9) sektor infrastruktury cyfrowej obejmujący podmioty podległe **MON** - Minister Obrony Narodowej;
10) dostawcy usług cyfrowych (z wyłączeniem podmiotów podległych MON) - minister właściwy do spraw informatyzacji (Minister Cyfryzacji);
11) dostawcy usług cyfrowych obejmujący podmioty podległe MON - Minister Obrony Narodowej.

4.1 SEKTOR ENERGII (MKIŚ)

Ministerstwo Klimatu i Środowiska

4.1.1 DZIAŁANIA ZREALIZOWANE W 2024 R.

4.1.1.1 IDENTYFIKACJA ORAZ PROWADZENIE POSTĘPOWAŃ ADMINISTRACYJNYCH WOBEC OPERATORÓW USŁUG KLUCZOWYCH Z SEKTORA ENERGII

W 2024 r. w związku wnioskiem spółki o ponowne rozpatrzenie sprawy dot. wydania decyzji uznającej ją za operatora usługi kluczowej, organ właściwy prowadził postępowanie w zakresie tego wniosku.

Ponadto, Minister Klimatu i Środowiska (MKiŚ), jako organ właściwy ds. cyberbezpieczeństwa sektora energii, wszczął dwa postępowania administracyjne mające na celu nałożenie kary na operatorów usług kluczowych, którzy nie wywiązali się terminowo z obowiązku ustanowionego w art. 15 UKSC.

Dodatkowo, na bieżąco następowała aktualizacja danych osób do kontaktów wyznaczonych przez operatorów usług kluczowych (zgodnie z obowiązkiem wskazanym w UKSC) oraz weryfikacja danych spółek wyznaczonych jako operatorzy usług kluczowych w związku z przejęciami/fuzjami.

Na bieżąco była prowadzona także analiza sektora pod kątem identyfikacji podmiotów do uznania za OUK.

4.1.1.2 NADZÓR NAD PODMIOTAMI KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

W 2024 r. miała miejsce kolejna tura audytów bezpieczeństwa systemów informacyjnych operatorów usług kluczowych w sektorze energii na gruncie przepisów UKSC. W związku z powyższym, prowadzony był szereg działań nadzorczych względem operatorów usług kluczowych, polegających m.in. na weryfikacji realizacji obowiązku przeprowadzania przez nich okresowych audytów bezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej, analizie sprawozdań z przeprowadzonych audytów pod kątem wykrytych niezgodności, terminowości ich przeprowadzenia czy weryfikacji obowiązku zgłaszania incydentów poważnych do odpowiednich jednostek (właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego - CSIRT).

W 2024 r. przeanalizowano łącznie 35 sprawozdań z audytów przeprowadzonych u poszczególnych operatorów usług kluczowych. Zbiorcza informacja pozyskana z analizy przytoczonych powyżej raportów, pozwala skutecznie realizować działania nadzorcze względem podmiotów z sektora oraz określić poziom dojrzałości, a także cyberodporności wśród operatorów usług kluczowych z sektora energia. Analiza sprawozdań z przeprowadzonych przez OUK audytów bezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej, pod kątem weryfikacji realizowania przez nich ustawowych obowiązków określonych w UKSC, zostanie także wykorzystana do zaplanowania czynności kontrolnych organu właściwego względem OUK na rok 2025. Rozpoczęto pracę nad przygotowaniem dokumentacji kontrolnej, w tym przygotowania programu kontroli, która zostanie zrealizowana w 2025 r.

Wśród innych czynności nadzorczych w 2024 r. znalazła się również weryfikacja realizacji Zaleceń Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. *w sprawie cyberbezpieczeństwa w sektorze energetycznym* (notyfikowana jako dokument nr C(2019) 2400)[10]. MKiŚ zebrało odpowiedzi od OUK i na tej podstawie w 2025 r. zostanie sporządzone stosowne podsumowanie.

[10] Zalecenia cyberbezpieczeństwa w sektorze energetycznym są poddawane ewaluacji w okresach 2-letnich.

W 2024 r. żaden z CSIRT poziomu krajowego nie przekazał do Ministerstwa Klimatu i Środowiska wniosku o wezwanie operatorów usług kluczowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego.

4.1.1.3 PROWADZENIE AKCJI PODNOSZĄCYCH ŚWIADOMOŚĆ W OBSZARZE CYBERBEZPIECZEŃSTWA SEKTORA ENERGII

Przykładem działań podnoszących świadomość w obszarze cyberbezpieczeństwa sektora energii jest m.in.:

- opracowywanie i dystrybucja tygodniowego biuletynu dotyczącego cyberbezpieczeństwa w ramach Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii,
- dystrybucja raportów OSINT ENISA do OUK,
- w przypadku dostrzeżenia ważnych podatności lub krytycznych zagrożeń, MKiŚ w sposób doraźny rozsyła do operatorów usług kluczowych z sektora energii ostrzeżenia, dobre praktyki czy komunikaty Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Ponadto, na stronie internetowej Ministerstwa Klimatu i Środowiska funkcjonuje zakładka nt. cyberbezpieczeństwa w sektorze energii. Są w niej umieszczone podstawowe informacje m.in. o tym kim jest operator usługi kluczowej i jakie ma zadania i obowiązki, o organie właściwym, a także liczne publikacje w języku polskim i angielskim oraz akty prawne krajowe i międzynarodowe dotyczące cyberbezpieczeństwa.

4.1.1.4 UDZIAŁ W ĆWICZENIACH CYBERBEZPIECZEŃSTWA POZIOMU KRAJOWEGO I MIĘDZYNARODOWEGO

W 2024 r. odbyło się kilka ważnych wydarzeń:

- W lutym 2024 r. przedstawiciele MKiŚ i kilku operatorów usług kluczowych z sektora energii wzięli udział w drugiej edycji ćwiczeń cyberbezpieczeństwa zorganizowanych dla sektora energii przez Departamentem Energii USA i Ministerstwo Cyfryzacji, które miały miejsce Warszawie.
- W czerwcu 2024 r. odbyły się ogólnoeuropejskie ćwiczenia w zakresie cyberbezpieczeństwa sektora energii „CyberEurope 2024". Głównym koordynatorem ćwiczeń był NASK-PIB we współpracy z Ministerstwem Klimatu i Środowiska. Ta edycja ćwiczeń była dedykowana sektorowi energii – podsektorowi energii elektrycznej i gazu. W wydarzeniu wzięli udział przedstawiciele MKiŚ, spółek z podsektora gazu i energii elektrycznej, CSIRT poziomu krajowego i innych podmiotów krajowego systemu cyberbezpieczeństwa.
- W listopadzie przedstawiciele MKiŚ wzięli udział w ćwiczeniach cyberbezpieczeństwa KSC-EXE 2024 organizowanych przez Ministerstwo Cyfryzacji.

4.1.1.5 ZESPÓŁ DS. MONITOROWANIA CYBERBEZPIECZEŃSTWA SEKTORA ENERGII

Przy Ministrze Klimatu i Środowiska od 2020 r. funkcjonuje Zespół ds. monitorowania cyberbezpieczeństwa sektora energii. Zespół jest organem opiniodawczo-doradczym Ministra Klimatu i Środowiska, współorganizowanym z Polskimi Sieciami Elektroenergetycznymi S.A. Formuła pracy zespołu posiada elementy funkcjonowania ISAC[11].

W 2024 r. odbyło się 12 spotkań Zespołu (raz w miesiącu), a od początku działania Zespołu było ich 97. Podczas spotkań następuje wymiana wiedzy eksperckiej na tematy związane z aktualnymi zagrożeniami, wyzwaniami technicznymi, legislacyjnymi lub jakiejkolwiek innej natury. Na spotkaniach często poruszane są m.in. kwestie implementacji międzynarodowych norm i standardów, legislacji krajowej i europejskiej, rozwiązań technologicznych itp. Do udziału w spotkaniach zapraszani są również przedstawiciele CSIRT GOV i CSIRT NASK.

[11] ISAC - ang. Information Sharing and Analysis Center - Centrum Analizy i Wymiany Informacji.

W ramach prac Zespołu dystrybuowany jest tygodniowy biuletyn zawierający informacje dotyczące szeroko pojętego cyberbezpieczeństwa.

Powołane zostały również grupy zadaniowe m.in. grupa zadaniowa ds. implementacji dyrektywy NIS 2. Powołana grupa ma na celu wsparcie procesu implementacji dyrektywy NIS 2 do polskiego porządku prawnego, poprzez m.in. koordynację kontaktów organu właściwego sektora energii z nadzorowanym sektorem, wypracowywanie opinii, dokonywanie analiz jakościowych oraz ilościowych.

4.1.1.6 WSPÓŁPRACA MIĘDZYNARODOWA

W lutym 2024 r. Ministerstwo Cyfryzacji przekazało informację o rozpoczęciu prac związanych ze wsparciem ENISA[12] w podnoszeniu cyberbezpieczeństwa w UE – projekt ENISA Support Action. W celu omówienia szczegółów programu z operatorami usług kluczowych, MKiŚ zorganizowało spotkanie z przedstawicielem ENISA. Wzięli w nim udział przedstawiciele 22 operatorów usług kluczowych, a formalne zapotrzebowanie przekazało 9 OUK. MKiŚ również zgłosiło do Ministerstwa Cyfryzacji zapotrzebowanie wsparcie w ramach projektu. ENISA przekazała informację, że realizacja wsparcia w ramach programu będzie możliwa po zakończeniu procesu wyłonienia nowego wykonawcy oraz jego weryfikacji.

Przedstawiciele MKiŚ uczestniczą w pracach Grupy Roboczej WS8 funkcjonującej w ramach Grupy Współpracy NIS. Grupa Robocza 8 (*Work Stream 8 on Energy Sector*) zajmuje się kwestią cyberbezpieczeństwa w sektorze energii, a zwłaszcza opracowaniem dokumentów wspierających implementację dyrektywy NIS 2, NCCS, realizację wymagań bezpieczeństwa w sektorze, jak i dokumentów służących zarządzaniu ryzykiem. W 2024 r. MKiŚ wzięło aktywny udział w posiedzeniu plenarnym oraz w warsztatach ENISA '101' training dot. zarządzania bezpieczeństwem informacji w cyberbezpieczeństwie zgodnie z dyrektywą NIS2 dedykowanych organom właściwym ds. cyberbezpieczeństwa, które odbyły się w Brukseli.

W marcu 2024 r. odbyły się 2 spotkania grupy WS8 dotyczące NCCS oraz nadchodzącej współpracy z ACER w zakresie wdrażania obowiązków wynikających z Kodeksu.

W kwietniu 2024 r. przedstawiciele MKiŚ wzięli udział w dwustronnym spotkaniu z przedstawicielami Komisji Europejskiej na temat sposobów komunikacji najważniejszych kwestii ustanawianych przez Kodeks sieci dotyczący cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej [13] (NCCS). Ponadto, przedstawiciele MKiŚ zgłosili potrzebę poprawienia tłumaczenia projektu NCCS na język polski ze względu na to, że wiele sformułowań nie zostało poprawnie przełożonych. MKiŚ opracowało i przekazało do Komisji Europejskiej uwagi do polskiego tłumaczenia NCCS. Uwagi te zostały uwzględnione i polskie tłumaczenie NCCS zostało poprawione.

We wrześniu 2024 r. pracownicy MKiŚ odbyli spotkanie z przedstawicielami ENISA w ich siedzibie. Głównym tematem spotkania było omówienie współpracy pomiędzy MKiŚ i operatorami usług kluczowych z sektora energii a ENISA w zakresie programu „Support Action", Dodatkowo, przedyskutowano inne możliwe formy wzmocnienia współpracy pomiędzy MKiŚ a ENISA w zakresie podnoszenia świadomości sytuacyjnej w zakresie cyberbezpieczeństwa w sektorze energii, co przyczyni się do podniesienia poziomu cyberbezpieczeństwa sektora na poziomie krajowym. Ustalono możliwość przekazywania raportów OSINT dot. zagrożeń cyberbezpieczeństwa do OUK nadzorowanych przez MKiŚ.

W 2024 r. jeden z pracowników MKiŚ został delegowany na kolejne 2 lata jako ekspert krajowy do ENISA.

[12] Agencja UE ds. Cyberbezpieczeństwa.

[13] Rozporządzenie Delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

Ponadto przedstawiciele MKiŚ brali udział w licznych konferencjach i warsztatach dot. cyberbezpieczeństwa sektora energii celem podnoszenia kompetencji.

4.1.2 INNE ZADANIA

- Aktywny udział w pracach legislacyjnych nad projektami ustaw o krajowym systemie cyberbezpieczeństwa implementującej założenia dyrektywy NIS 2, o krajowym systemie certyfikacji implementującej założenia Aktu o cyberbezpieczeństwie oraz o zarządzaniu kryzysowym implementującej założenia dyrektywy CER, celem uwzględnienia specyfiki sektora energii.
- Aktywny udział w pracach nad przygotowaniem wykazu inicjalnego podmiotów kluczowych i ważnych w sektorze energii i gospodarowania odpadami, poprzez bliską współpracę z przedstawicielami NASK-PIB oraz Ministerstwa Cyfryzacji.
- Realizacja zadań związanych z dostosowaniem prawa krajowego do przyjętego rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (NCCS), w tym opracowanie dostosowujących przepisów prawnych w ramach procedowanej ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa.
- Organizacja spotkań z interesariuszami (np. URE, PTPiREE, PSE) w sprawie wdrożenia zapisów NCCS do polskiego porządku prawnego.
- MKiŚ aktywnie uczestniczyło i brało udział w dyskusjach podczas organizowanych Forach Organów Właściwych. Jedno ze spotkań zorganizowało w swojej siedzibie Ministerstwo Klimatu i Środowiska.
- W grudniu 2024 r. MKiŚ rozpoczęło prace nad przygotowaniem wniosku o dofinansowanie na uruchomienie CSIRT sektorowego w sektorze energia w ramach naboru wniosków KPO. Została nawiązana w tym zakresie współpraca z NASK-PIB oraz innymi organami właściwymi.
- MKiŚ współpracuje z NASK-PIB w zakresie opracowania formularza dojrzałości, który następnie ma zostać zaimplementowany do systemu S46. Tym samym ma on wspierać przyszłe działania nadzorcze organów właściwych ds. cyberbezpieczeństwa nad podmiotami kluczowymi i ważnymi na gruncie dyrektywy NIS2. Współpraca ta jest kontynuowana w 2025 r.
- Udział w konsultacjach prac nad nowymi funkcjonalnościami systemu S46, które planowane są do wdrożenia wraz z wejściem w życie nowelizacji UKSC oraz przedstawienie potrzeb organu właściwego ds. cyberbezpieczeństwa w tym kontekście.

4.1.3 ANALIZA I OCENA FUNKCJONOWANIA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Minister właściwy ds. energii od 2018 r. pełni rolę organu właściwego ds. cyberbezpieczeństwa dla sektora energii. W tym czasie realizował zadania wskazane w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Na podstawie dotychczasowych doświadczeń należy stwierdzić, że system ten spełnia swój cel jakim jest zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. W sektorze energii podmioty uznane za operatorów usług kluczowych od momentu wejścia w życie UKSC podniosły swój poziom dojrzałości o czym świadczy m.in. mniejsza ilość niezgodności w sprawozdaniach z przeprowadzonych audytów czy ogólna ocena poziomu dojrzałości, którą OUK przeprowadzili na początku 2022 r.

Należy również zwrócić uwagę na dobrą współpracę pomiędzy organami właściwymi, a także organami właściwymi a CSIRT poziomu krajowego. Jest to bardzo ważny aspekt, ponieważ organy właściwe odpowiedzialne są za nadzór nad operatorami usług kluczowych, a CSIRT poziomu krajowego stanowią

podmioty operacyjne mające za zadanie wspierać OUK podczas wystąpienia incydentów poważnych. W związku z przyjęciem dyrektywy NIS2, konieczny był wysoki stopień zaangażowania organu właściwego ds. cyberbezpieczeństwa dla sektora energii w prace legislacyjne dotyczące projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Jednocześnie, procedowano również projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym, który ma implementować do polskiego prawa zapisy dyrektywy CER. Stworzenie odpowiedniej spójności pomiędzy tymi regulacjami jest kluczowe dla zbudowania efektywnego systemu cyberbezpieczeństwa i zarządzania kryzysowego. Wynika to przede wszystkim z faktu, że zagrożenia cyberbezpieczeństwa mają wpływ na cały proces technologiczny i infrastrukturę danego podmiotu. Z racji tego, działania z zakresu cyberbezpieczeństwa i zarządzania kryzysowego powinny zostać skorelowane, co pozwoli podmiotom na efektywniejsze wykorzystanie zasobów.

W ramach bieżącej działalności Wydziału ds. Cyberbezpieczeństwa Sektora Energii MKiŚ co miesiąc przygotowywany jest raport dotyczący stanu cyberbezpieczeństwa sektora energii, który przekazywany jest do Ministra Klimatu i Środowiska. Dokument ten zawiera informacje ze wszystkich dostępnych Wydziałowi ds. Cyberbezpieczeństwa Sektora Energii źródeł (m.in. raport dzienny CSIRT NASK, biuletyn tygodniowy CSIRT GOV, raport OSINT ENISA, informacje ze spółek, informacje z systemu S46, informacje z ENISA Situational Awareness Report i innych), co stanowi ważne uzupełnienie świadomości sytuacyjnej organizacji. W ramach otrzymywanych raportów, Ministerstwo Klimatu i Środowiska, jako członek grupy roboczej Work Stream 8, było odbiorcą dwumiesięcznych raportów sytuacyjnych dotyczących sektora energii (ENISA Situational Awareness Report. Energy Sector, TLP: GREEN) opracowanych przez ENISA. W 2024 r. ENISA oceniła poziom zagrożeń w unijnym sektorze energii na SUBSTANTIAL (3 stopień w 5ciostopniowej skali). Nota ta oznacza, że jest prawdopodobieństwo wystąpienia bezpośrednich ataków na wiele podmiotów z sektora energii w tym samym czasie, a zakłócenie w sektorze energii jest uważane za możliwe. W tym okresie, stwierdzono trochę niższy poziom zagrożeń dla sektora energii globalnie (MODERATE – 2 stopień). Oznacza to, że istnieje potencjalne ryzyko bezpośredniej działalności cyberprzestępców, jednakże jest to uznawane za mało prawdopodobne. Ewentualna działalność cyberprzestępców może spowodować drobne zakłócenia w działaniu sektora energii.

4.1.4 WNIOSKI I REKOMENDACJE.

Na podstawie dotychczasowych doświadczeń, Ministerstwo Klimatu i Środowiska chciałoby zarekomendować następujące działania:

1. organizacja kolejnej edycji ćwiczeń KSC EXE – do tej pory tego typu ćwiczenia odbyły się 2 razy - w 2020 r. i 2024 r. W związku ze zmieniająca się sytuacją geopolityczną i krajobrazem zagrożeń, uważamy, że powinno się dokonywać regularnych ćwiczeń z zakresu cyberbezpieczeństwa, aby w sytuacji zmaterializowania się różnych ryzyk podmioty wchodzące w zakres krajowego systemu cyberbezpieczeństwa wiedziały co dokładnie należy robić, z kim się kontaktować i jakie informacje przekazywać. Ponadto, zeszłoroczne ćwiczenia rozpoczęły proces wzmacniania współpracy pomiędzy różnymi instytucjami, co będzie miało znaczący wpływ na efektywność współpracy pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa w sytuacji realnego zagrożenia;
2. organizacja w ramach cyklów szkoleń realizowanych przez Ministerstwo Cyfryzacji, szkoleń technicznych na poziomie zaawansowanym – wynika to z faktu, że wśród operatorów usług kluczowych osoby zajmujące się kwestiami cyberbezpieczeństwa systemów często są pracownikami z długoletnim stażem i dużym doświadczeniem w bezpieczeństwie systemów IT i OT, więc nie uczestniczą w szkoleniach dedykowanych dla każdego. Tego rodzaju szkolenia przyczyniłyby się do jeszcze wyższego poziomu cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, ponieważ mogliby w nich wziąć udział również przedstawiciele OUK z innych sektorów czy podmiotów publicznych;
3. po wejściu w życie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, organizacja pilotażowych szkoleń realizowanych przez Ministerstwo Cyfryzacji, dot. obowiązków wynikających z nowelizacji ustawy. Szkolenia dedykowane dla nowych podmiotów kluczowych i ważnych;

4. organizacja ćwiczeń typu cyberpoligon dla OUK – tego typu ćwiczenia przyczyniają się do możliwości zastosowania wiedzy w praktyce. Często są to drogie wydarzenia i dużej liczby podmiotów nie stać na to, aby regularnie wysyłać swoich pracowników do udziału w tego typu ćwiczeniach, więc możliwość wzięcia udziału w takim przedsięwzięciu raz w roku przyniosłaby wymierne skutki w postaci podniesienia poziomu cyberbezpieczeństwa poprzez lepsze przygotowanie pracowników komórek odpowiedzialnych za cyberbezpieczeństwo;
5. kontunuowanie organizacji spotkań w formie Forum Organów Właściwych. Jest to dobre miejsce do wymiany doświadczeń i dobrych praktyk. W ramach nadchodzących zmian krajowego systemu cyberbezpieczeństwa, konieczna jest jeszcze mocniejsza współpraca organów właściwych ds. cyberbezpieczeństwa. Ponadto, pojawią się nowe organy właściwe, które dzięki bieżącej kooperacji z dotychczasowymi organami będą mogły szybciej osiągnąć zdolność operacyjną, a także otrzymać wsparcie w różnych kwestiach. Ważne jest, aby w tych spotkaniach brali udział również przedstawiciele CSIRT poziomu krajowego i CSIRT sektorowe oraz inne instytucje publiczne zaangażowane w krajowy system cyberbezpieczeństwa.

4.1.5 PLANOWANE DZIAŁANIA W 2025 R.

1. Dalszy aktywny udział w pracach legislacyjnych nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.
2. Dalszy udział w pracach grupy zadaniowej Work Stream 8, działającej w ramach Grupy Współpracy NIS, która zajmuje się kwestią cyberbezpieczeństwa w sektorze energii.
3. Dalsze zaangażowanie w sprawy międzynarodowe dot. cyberbezpieczeństwa, jak chociażby współpraca z ENISA, udział w pracach P-TECC czy współpraca na poziomie Unii Europejskiej.
4. Kontynuacja współpracy z CSIRT GOV i CSIRT NASK, Ministerstwem Cyfryzacji i innymi organami Właściwymi do spraw cyberbezpieczeństwa.
5. Rozpoczęcie procesu ustanowienia CSIRT sektorowego w sektorze energii oraz jedoczesna realizacja projektu KPO, z którego zostaną przyznane środki na ten cel.
6. Kontynuacja procesu analizy audytów cyberbezpieczeństwa oraz prowadzenie kontroli operatorów usług kluczowych. Ewentualne wszczęcie postępowań o nałożenie administracyjnych kar pieniężnych.
7. Rozpoczęcie procesu weryfikacji realizacji obowiązków nowych podmiotów kluczowych i ważnych, po wejściu w życie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, w tym: weryfikacja kompletności procesu samoidentyfikacji, terminowości realizacji obowiązków bazowych, takich jak zgłaszanie osób kontaktowych.
8. Dostosowanie funkcjonowania Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii do nowych okoliczności związanych z nowelizacją ustawy, w tym dołączenie przedstawicieli podmiotów kluczowych i ważnych do Zespołu.
9. Prace nad utworzeniem ISAC w nadzorowanych sektorach.
10. Analiza poziomu dojrzałości nowych spółek, które będą nadzorowane przez MKiŚ.
11. Analiza potrzeb szkoleniowych nowych podmiotów kluczowych i ważnych z nadzorowanych sektorów.
12. Po wejściu w życie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, MKiŚ zacznie pełnić rolę organu właściwego z NCCS. Podjęte zostaną działania organizacyjne, mające na celu wyznaczanie podmiotów objętych tą regulacją oraz inne działania nadzorcze.
13. Po wejściu w życie nowelizacji UKSC, rozpoczęcie działań mających na celu osiągnięcie operacyjności przez organ właściwy ds. cyberbezpieczeństwa dla sektora gospodarowania odpadami.

4.2 DZIAŁANIA MINISTRA OBRONY NARODOWEJ JAKO ORGANU WŁAŚCIWEGO DO SPRAW CYBERBEZPIECZEŃSTWA

Ministerstwo Obrony Narodowej

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa Ministerstwo Obrony Narodowej (MON) realizował zadania organu właściwego do spraw cyberbezpieczeństwa w sektorze zdrowia w odniesieniu do jednostek wojskowej służby zdrowia, będących operatorami usług kluczowych (OUK).

Ministerstwo Obrony Narodowej prowadziło również bieżącą analizę pod kątem identyfikacji nowych, potencjalnych podmiotów spełniających kryteria uznania za operatora usługi kluczowej w sektorach zdrowie i infrastruktura cyfrowa oraz ustalenia, czy nadal spełnione są przesłanki przyjęte za podstawę do wydania decyzji o uznaniu za operatora usługi kluczowej. W oparciu o powyższe analizy nie wydano żadnej decyzji o uznaniu podmiotu za operatora usługi kluczowej, ani decyzji stwierdzającej wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej.

Ministerstwo Obrony Narodowej monitorowało operatorów usług kluczowych pod kątem realizacji obowiązków nałożonych na nich przepisami ustawy.

Więcej informacji nt. przedsięwzięć realizowanych przez MON w zakresie cyberbezpieczeństwa w zakładkach CSIRT MON oraz Ministerstwo Obrony Narodowej.

4.3 SEKTOR BANKOWY I INFRASTRUKTURY RYNKÓW FINANSOWYCH (KNF)

4.3.1 ZADANIA

4.3.1.1 ANALIZA PODMIOTÓW RYNKU FINANSOWEGO W ZAKRESIE SPEŁNIENIA KRYTERIÓW

W ramach realizacji zadań organu właściwego prowadzono systematyczne czynności analityczne obejmujące bieżącą weryfikację podmiotów w sektorze bankowym i infrastruktury rynków finansowych. Analiza ta była ukierunkowana na dwa kluczowe aspekty:

- ocenę spełnienia kryteriów kwalifikujących do uznania za operatora usługi kluczowej,
- weryfikację utrzymywania warunków kwalifikujących podmiot jako operatora usługi kluczowej.

4.3.1.2 BIEŻĄCY NADZÓR, W TYM PRZEKAZYWANIE INFORMACJI ORAZ KONTROLE OPERATORÓW USŁUG KLUCZOWYCH

W ramach sprawowanego nadzoru nad operatorami usług kluczowych w sektorze bankowym i infrastruktury rynków finansowych w 2024 r. przeprowadzono 3 kontrole. W ich trakcie dokonano szczegółowej analizy wybranych obszarów działalności operatorów usług kluczowych w kontekście wypełniania obowiązków przewidzianych w UKSC.

Równolegle prowadzono działania doskonalące procesy kontrolne w ramach Urzędu KNF. W 2024 r. opracowano wewnętrzne metodyki dotyczące kontroli operatorów usług kluczowych, co przyczyniło się do standaryzacji procesu kontrolnego.

Działalność nadzorcza KNF koncentrowała się na monitorowaniu przestrzegania przepisów UKSC przez operatorów usług kluczowych sektora bankowego i infrastruktury rynków finansowych.

W 2024 r. Komisja Nadzoru Finansowego, działając jako Organ Właściwy, przekazywała Operatorom Usług Kluczowych szereg istotnych informacji dotyczących cyberzagrożeń zidentyfikowanych na polskim rynku finansowym. W tym zakresie KNF kierowała do operatorów usług kluczowych m.in. pisemne stanowiska nadzorcze i pisma sygnalizacyjne, a także wnioski o wyjaśnienia bądź przekazanie dodatkowych informacji na temat realizacji określonych obowiązków wynikających z przepisów UKSC.

4.3.1.3 DZIAŁANIA EDUKACYJNE

W roku 2024 CSIRT KNF zintensyfikował działania w obszarze prewencji i edukacji, opracowując 254 ostrzeżenia dotyczące najnowszych wektorów ataków oraz metod działania cyberprzestępców. Materiały przygotowane przez CSIRT KNF zostały wykorzystane jako źródło w 2814 publikacjach mediów o zasięgu ogólnokrajowym, co świadczy o wysokiej wartości merytorycznej i aktualności przekazywanych informacji.

Szczególnie istotnym elementem działań edukacyjnych był projekt CEDUR, w ramach którego przeprowadzono 13 webinariów. Tematyka szkoleń obejmowała krytyczne aspekty cyberbezpieczeństwa, mechanizmy ochrony aktywów finansowych klientów oraz dogłębną analizę funkcjonowania złośliwego oprogramowania. Dodatkowo, zorganizowano serię dedykowanych webinariów poświęconych Rozporządzeniu DORA, podczas których szczegółowo omówiono nowe wymogi regulacyjne dla podmiotów finansowych i dostawców usług ICT. Przedstawiciele Urzędu KNF aktywnie uczestniczyli w inicjatywach edukacyjnych o zasięgu krajowym i międzynarodowym, wnosząc istotny wkład w rozwój wiedzy o cyberbezpieczeństwie sektora finansowego.

4.3.1.4 DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

W 2024 roku KNF zrealizował szereg strategicznych inicjatyw mających na celu efektywne wdrożenie wymogów DORA w Polsce. Działania te obejmowały organizację specjalistycznych szkoleń i webinariów, a także intensywną współpracę z organami nadzoru na poziomie krajowym i unijnym w celu harmonizacji regulacji i praktyk nadzorczych.

Rozporządzenie DORA stanowi przełomową regulację unijną, której celem jest harmonizacja i wzmocnienie operacyjnej odporności cyfrowej instytucji finansowych w Unii Europejskiej. Regulacja ta jest strategiczną odpowiedzią na wzrastającą złożoność zagrożeń w cyberprzestrzeni oraz rosnące uzależnienie sektora finansowego od technologii informacyjno-komunikacyjnych. DORA wprowadza kompleksowe wymogi w zakresie zarządzania ryzykiem technologicznym, koncentrując się na pięciu kluczowych filarach:

- Systematyczne i ustrukturyzowane zarządzanie ryzykiem ICT,
- Zaawansowane testowanie odporności cyfrowej, ze szczególnym uwzględnieniem testów TLPT,
- Kompleksowe zarządzanie ryzykiem w relacjach z dostawcami usług ICT,
- Implementacja zintegrowanych ram nadzoru nad kluczowymi dostawcami usług ICT oraz łańcuchem dostaw,
- Standaryzacja i centralizacja procesu raportowania znaczących incydentów ICT na poziomie krajowym i unijnym.

4.3.1.5 EU-SCICF – KOORDYNACJA CYBERINCYDENTÓW CHARAKTERZE SYSTEMOWYM

KNF pełni rolę punktu kontaktowego wynikającą z Zalecenia Europejskiej Rady Ds. Ryzyka Systemowego w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (ESRB/2021/17). W ramach tej funkcji KNF uczestniczy w rozwoju frameworku EU-SCICF, który ustanawia ramy koordynacji w zakresie cyberincydentów o charakterze systemowym.

4.3.2 DZIAŁALNOŚĆ SEKTOROWA ZESPOŁU CYBERBEZPIECZEŃSTWA CSIRT KNF

4.3.2.1 PRZECIWDZIAŁANIE ATAKOM RANSOMWARE

W odpowiedzi na eskalację zagrożeń związanych z atakami ransomware, CSIRT KNF opracował kompleksowy dokument "Dobre praktyki w zakresie zapobiegania i reagowania na ataki ransomware". Publikacja ta zawiera zaawansowane wytyczne dotyczące wzmacniania cyberbezpieczeństwa organizacji oraz szczegółowe rekomendacje w zakresie minimalizacji skutków potencjalnych incydentów.

Ataki ransomware zostały zidentyfikowane jako jedno z najbardziej krytycznych zagrożeń dla ciągłości działania organizacji. W związku z tym, CSIRT KNF rekomenduje przeprowadzenie pogłębionej analizy ryzyka w kontekście specyficznych zagrożeń ransomware dla infrastruktury teleinformatycznej. Na podstawie tej analizy organizacje powinny wypracować dedykowane procesy i procedury oraz wdrożyć adekwatne rozwiązania techniczne minimalizujące ryzyko skutecznego ataku.

4.3.2.2 BEZPIECZEŃSTWO INFRASTRUKTURY PODMIOTÓW NADZOROWANYCH

W 2024 roku CSIRT KNF zintensyfikował działania w zakresie proaktywnej identyfikacji i neutralizacji cyberzagrożeń w sektorze finansowym. W ramach tych działań:

- Dystrybuowano informacje o zidentyfikowanych podatnościach i nieprawidłowościach,
- **Przygotowano i przekazano 698 specjalistycznych ostrzeżeń zawierających szczegółowe charakterystyki zagrożeń oraz rekomendowane działania mitygacyjne.**

CSIRT KNF, we współpracy z CSIRT NASK, przeprowadził zaawansowane testy bezpieczeństwa infrastruktury podmiotów finansowych z wykorzystaniem platformy Artemis. W ramach tej inicjatywy zrealizowano 312 zgłoszeń do podmiotów nadzorowanych zawierających szczegółowe informacje o wykrytych podatnościach i zagrożeniach.

4.3.2.3 WYMIANA INFORMACJI O CYBERZAGROŻENIACH

CSIRT KNF wdrożył zaawansowane narzędzia umożliwiające efektywną komunikację i wymianę informacji o cyberzagrożeniach z podmiotami rynku finansowego, w tym operatorami usług kluczowych. Sprawna wymiana informacji stanowi fundamentalny element budowania cyberodporności sektora finansowego, umożliwiając szybką identyfikację i neutralizację zagrożeń oraz skuteczną prewencję przyszłych incydentów.

W 2024 roku kontynuowano organizację cyklicznych, miesięcznych spotkań z przedstawicielami sektora finansowego, podczas których analizowano bieżące cyberzagrożenia oraz nowe techniki stosowane przez cyberprzestępców.

4.3.2.4 OCHRONA NIEPROFESJONALNYCH UCZESTNIKÓW RYNKU

CSIRT KNF prowadzi systematyczny monitoring i analizę zagrożeń w obszarze cyberbezpieczeństwa sektora finansowego. Zgromadzona wiedza ekspercka jest wykorzystywana do minimalizacji ryzyk oraz realizacji ukierunkowanych działań edukacyjnych dla użytkowników bankowości elektronicznej.

Tabela 24. Dane zidentyfikowane przez CSIRT KNF w 2024 r.

Obiekt:	Liczba:
Strony phishingowe	51 241
Fałszywe reklamy inwestycyjne w mediach społecznościowych	10 951

Zidentyfikowane złośliwe domeny zostały zgłoszone do blokady przez CSIRT NASK poprzez mechanizmy „Listy ostrzeżeń przed niebezpiecznymi stronami".

4.3.3 PLANOWANE DZIAŁANIA W 2025 R.

W 2025 r. KNF planuje realizację następujących działań w obszarze cyberbezpieczeństwa:

- kontynuowanie realizacji zadań organu właściwego oraz sektorowego zespołu CSIRT,
- realizowanie nowych obowiązków wynikających z regulacji DORA,
- rozwój współpracy w ramach EU-SCICF,
- intensyfikację działań na rzecz wzmacniania cyberodporności sektora finansowego.

4.4 SEKTOR OCHRONY ZDROWIA (Z WYŁĄCZENIEM PODMIOTÓW PODLEGŁYCH MON) (MZ)

Minister Zdrowia, jako organ właściwy dla sektora ochrony zdrowia w rozumieniu przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „UKSC"), w roku 2024 prowadził wielkokierunkowe działania związane z wykonywaniem przez niego obowiązków nałożonych UKSC.

4.4.1 PODJĘTE PRZEDSIĘWZIĘCIA

W 2024 r. Minister Zdrowia sprawując nadzór nad operatorami usług kluczowych (dalej: „Operatorzy") ustanowionymi w sektorze ochrony zdrowia:

- prowadził bieżącą analizę podmiotów pod kątem uznania ich za Operatora lub niespełnienia warunków pozostania Operatorem;
- **przeprowadził postępowanie administracyjne, na podstawie którego wydał 1 decyzję stwierdzającą wygaśnięcie decyzji o uznaniu podmiotu Operatorem; obecnie w sektorze ochrony zdrowia jest 238 Operatorów;**
- ustawicznie monitorował – na podstawie art. 42 ust. 1 pkt 6 UKSC – Operatorów pod kątem realizacji obowiązków nałożonych na nich przepisami ustawy;
- przeprowadzał analizy przekazywanych przez Operatorów sprawozdań z audytów zgodności z wymogami UKSC, o których mowa w art. 15 ust. 1;
- przeprowadził kontrolę Operatora, w ramach której wykonano szczegółową analizę objętych kontrolą obszarów działalności w kontekście obowiązków przewidzianych w UKSC. W oparciu o wyniki kontroli wydane zostały zalecenia oraz podjęto czynności związane z monitorowaniem ich realizacji.
- wydawał rekomendacje dla Operatorów w zakresie wdrażania rozwiązań mających na celu wzmocnienie cyberodporności, w tym poprzez usuwanie podatności w systemie cyberbezpieczeństwa Operatorów;
- koordynował prace nad projektem dofinansowania podmiotów leczniczych podejmujących działania mające na celu podniesienie poziomu cyberbezpieczeństwa;
- współpracował z NASK Państwowym Instytutem Badawczym (NASK-PIB) i Operatorami w ramach projektu podłączania Operatorów do zintegrowanego systemu zarządzania cyberbezpieczeństwem – S46 (narzędzia rozwijanego przez NASK-PIB na zlecenie Ministra Cyfryzacji); na dzień 31.12.2024 r. status podłączeń do S46 przedstawiał się następująco:
  - 129 podłączonych Operatorów,
  - 11 Operatorów w trakcie podłączenia,
  - 6 Operatorów w trakcie podpisywania umowy z NASK-PIB,
  - 14 Operatorów w trakcie podpisywania porozumienia z Ministrem Cyfryzacji;
- współpracował z NASK-PIB:
  - w ramach rozwoju nowych funkcjonalności systemu S46;
  - w procesie tworzenia ankiet dedykowanych samoocenie Operatorów pod kątem spełniania wymogów Dyrektywy NIS2.

4.4.2 POZOSTAŁE ZADANIA

Do innych zadań realizowanych przez Ministerstwo Zdrowia należy zaliczyć:

- współpracę z utworzonym sektorowym zespołem cyberbezpieczeństwa dla sektora ochrony zdrowia – CSIRT CeZ, który rozpoczął funkcjonowanie we wrześniu 2023 r.;
- udzielanie wsparcia podmiotom sektora ochrony zdrowia przy usuwaniu skutków incydentów bezpieczeństwa w cyberprzestrzeni; wyżej wymienione zadanie realizuje z ramienia Ministerstwa Zdrowia podległa mu, wyspecjalizowana i doświadczona jednostka Centrum e- Zdrowia (CeZ);
- udzielanie pomocy w odbudowie zaplecza teleinformatycznego Operatorów, którzy ucierpieli podczas wrześniowej powodzi;
- uczestnictwo w cyklicznych spotkaniach w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa;
- uczestnictwo w cyklicznych posiedzeniach Forum Organów Właściwych;
- przystąpienie i uczestnictwo w programie Partnerstwo dla Cyberbezpieczeństwa, powstałym z inicjatywy NASK-PIB i Ministerstwa Cyfryzacji;
- udział wraz z przedstawicielami CSIRT CeZ w organizowanych przez Ministerstwo Cyfryzacji jednodniowych ćwiczeniach cyberbezpieczeństwa w ramach krajowego systemu cyberbezpieczeństwa (KSC-EXE 2024).

4.4.3 PLANOWANE DZIAŁANIA W 2025 R.

W 2025 r. Minister Zdrowia planuje realizację następujących działań w obszarze odpowiedzialności ustanowionej przepisami UKSC:

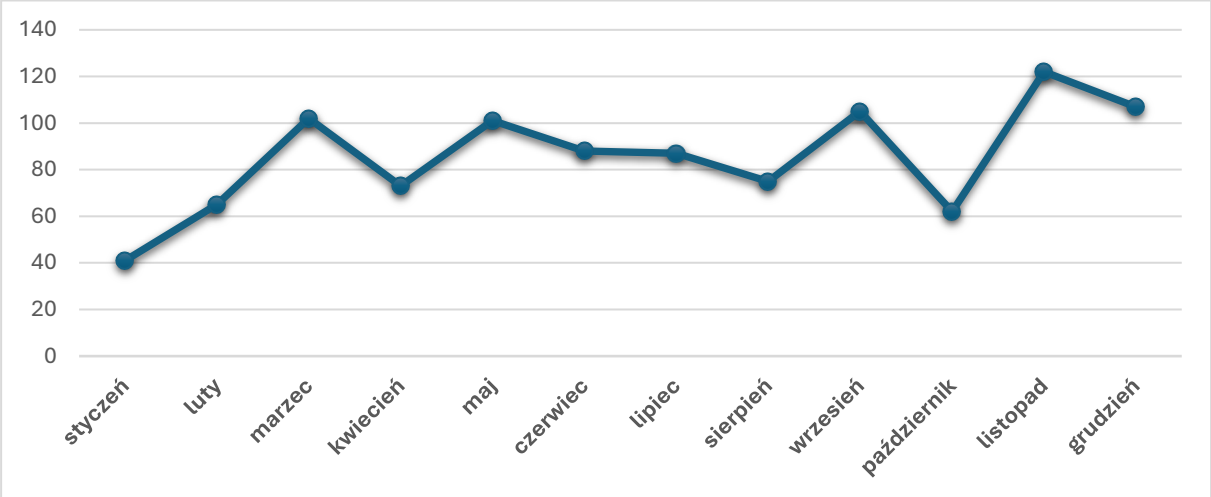
- kontynuowanie współpracy z NASK-PIB w ramach procesu podłączania Operatorów do S46;
- prowadzenie kontroli Operatorów;
- przygotowanie do realizacji zadań wynikających z procedowanej nowelizacji UKSC, implementującej dyrektywę NIS2 do polskiego porządku prawnego;
- uruchomienie naboru wniosków na dofinansowanie działań zwiększających poziom cyberbezpieczeństwa szpitali w ramach środków z Krajowego Planu Odbudowy;
- współpraca z ENISA w zakresie założeń planu działania Unii Europejskiej mającego na celu zwiększenie cyberodporności sektora ochrony zdrowia;
- aktualizacja, opracowanego we współpracy z ENISA, podręcznika reagowania na incydenty cyberbezpieczeństwa w jednostkach leczniczych;
- zapewnienie, we współpracy z NASK-PIB, redundantnego podłączenia CSIRT CEZ i Ministerstwa Zdrowia do systemu S46.

4.4.4 CENTRUM E- ZDROWIA (CEZ) – CSIRT CEZ

4.4.4.1 STATYSTYKI OBSŁUŻONYCH INCYDENTÓW

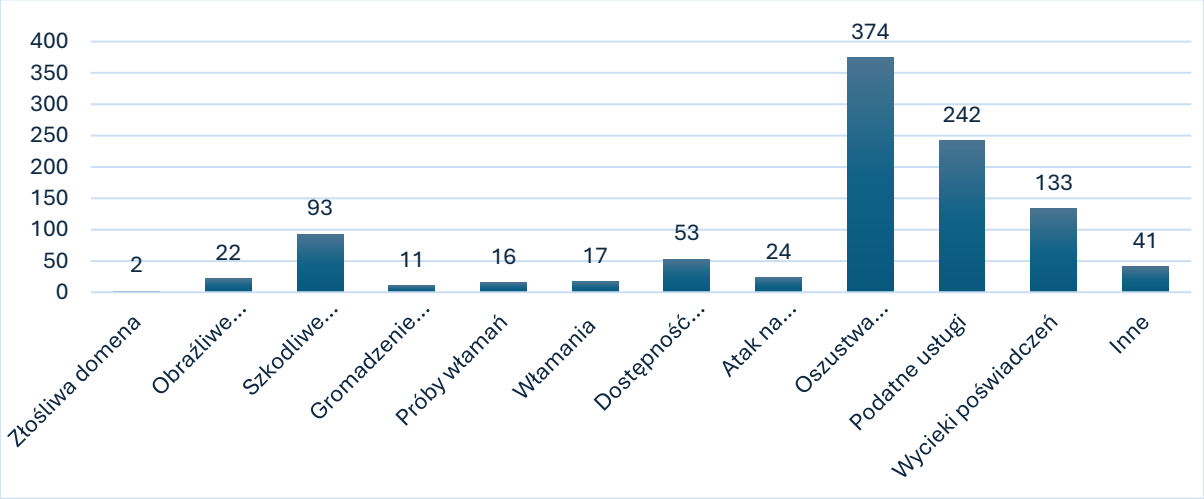
Zespół CSIRT CeZ w roku 2024 zarejestrował łącznie 1028 incydentów różnego typu w sektorze ochrony zdrowia.

Tabela 25. Incydenty obsłużone przez CSIRT CeZ w 2024r.



Incydenty, sklasyfikowane według kategorii:

Tabela 26. Podział incydentów ze względu na typ w 2024r.



Ponadto w roku 2024 wykryto pięć ataków typu ransomware, z czego jeden z nich był incydentem poważnym.

4.4.4.2 OPIS NAJWAŻNIEJSZYCH INCYDENTÓW

W 2024 roku zespół CSIRT CeZ koordynował proces reagowania, analizy oraz mitygacji szeregu incydentów bezpieczeństwa w podmiotach sektora ochrony zdrowia.

Wskazany powyżej incydent poważny (atak typu ransomware) doprowadził do zakłócenia działania infrastruktury teleinformatycznej w podmiocie medycznym. W odpowiedzi na zgłoszenie zespół CSIRT CeZ przekazał zalecenia dotyczące wstępnej mitygacji skutków ataku.

Po zabezpieczeniu materiałów przeprowadzono analizę zebranych próbek i logów, na podstawie której opracowano kolejne rekomendacje. Obejmowały one konieczność wprowadzenia zmian konfiguracyjnych w infrastrukturze oraz wdrożenie dodatkowych mechanizmów bezpieczeństwa, umożliwiających skuteczniejsze wykrywanie i reagowanie na zagrożenia.

W trakcie trwania incydentu oraz po jego zakończeniu zapewniono wsparcie w zakresie działań mających na celu odbudowę i zabezpieczenie środowiska teleinformatycznego.

Równolegle odnotowano znaczną liczbę kampanii phishingowych wymierzonych w podmioty sektora ochrony zdrowia oraz ataków typu DDoS. W odpowiedzi na te zagrożenia CSIRT CeZ prowadził działania analityczne, wspierał podmioty w zakresie wdrażania środków ochronnych oraz przekazywał rekomendacje dotyczące zabezpieczeń.

4.4.4.3 LICZBA PRZESKANOWANYCH PODMIOTÓW I WYKRYTYCH PODATNOŚCI

W analizowanym okresie przeprowadzono skanowanie czterech podmiotów z sektora ochrony zdrowia na ich zlecenie. Celem tego procesu była identyfikacja potencjalnych podatności oraz błędów konfiguracyjnych, które mogłyby stanowić zagrożenie dla bezpieczeństwa infrastruktury teleinformatycznej. Wszystkie działania zostały przeprowadzone zgodnie z ustalonym zakresem i za zgodą zleceniodawców.
W wyniku skanowania czterech podmiotów zidentyfikowano:

Tabela 27. Zestawienie liczby wykrytych podatności

Klasa podatności:	Liczba:
Krytyczne (CVSS > 9	4
Wysokie (CVSS 7–9)	12
Średnie (CVSS 4–7)	83
Niskie (CVSS < 4):	14

4.4.4.4 NAJCZĘŚCIEJ WYSTĘPUJĄCE PODATNOŚCI I BŁĘDY KONFIGURACYJNE:

- Brak w aktualizacji oprogramowania:
- Systemy operacyjne bez wsparcia producenta
- Brak stosowania nagłówków typu Security-Headers, które skutecznie przeciwdziałają m.in. atakom typu XSS, w tym ładowaniu treści stron internetowych z potencjalnie niebezpiecznych źródeł.
- Brak stosowania nagłówków SPF, DKIM, DMARC w przypadku korzystania z usług pocztowych.
- Występowanie usług zapewniających szyfrowaną komunikację przy użyciu przestarzałych protokołów TLSv1.0 i/lub TLSv1.1.
- Wygasłe certyfikaty SSL/TLS.

4.4.4.5 PODSUMOWANIE

W 2024 roku przeprowadzono skanowanie czterech podmiotów z sektora ochrony zdrowia w celu identyfikacji podatności i błędów konfiguracyjnych zagrażających bezpieczeństwu ich infrastruktury teleinformatycznej. **Wykryto łącznie 113 podatności w tym: 4 krytyczne, 12 wysokich, 83 średnich i 14 niskich.** Najczęstsze problemy obejmowały brak aktualizacji oprogramowania, niestosowanie nagłówków Security-Headers, SPF, DKIM, DMARC, protokoły TLSv1.0/1.1 oraz wygasłe certyfikaty SSL/TLS.

Rysunek 8. Liczba wykrytych podatności z klasyfikacją

Rodzaj podatności:	Liczba
Krytyczne	4
Wysokie	12
Średnie	83
Niskie	14
Łącznie	**113**

4.4.4.6 STATYSTYKI BŁĘDÓW KONFIGURACYJNYCH I PODATNOŚCI

W 2024 r. wykryto znaczną ilość błędów konfiguracyjnych i podatności, będącą wynikiem analiz pasywnych, raportów generowanych przez system n6, rozwiązania Artemis, a także z innych źródeł, w tym od osób prywatnych.

4.4.4.6.1 ZAKRES DANYCH

1. Analiza pasywna infrastruktury teleinformatycznej:
    - Pasywna enumeracja subdomen oraz wykorzystanie otwartych narzędzi do analizy bezpieczeństwa infrastruktury. Analiza obejmowała m.in. publicznie dostępne zasoby, takie jak konfiguracje sieciowe, otwarte porty, czy panele logowania.
2. Dane z systemu n6:
    - Monitorowanie i analiza podatności wykrytych w ramach infrastruktury sieciowej obejmującej krytyczne usługi i zasoby teleinformatyczne.
    - Dane obejmowały zarówno luki bezpieczeństwa, jak i błędy konfiguracji, które mogły stanowić potencjalne wektory ataku.
3. Rozwiązanie Artemis oraz zgłoszenia z innych źródeł, w tym od osób prywatnych:
    - Skany wykonane za pomocą rozwiązania Artemis oraz zgłoszenia dotyczące nieprawidłowości w systemach publicznie dostępnych, takich jak błędne konfiguracje DNS, otwarte porty, niezabezpieczone panele logowania oraz inne potencjalne zagrożenia.

4.4.4.7 NAJCZĘŚCIEJ WYSTĘPUJĄCE BŁĘDY KONFIGURACYJNE

Publicznie dostępne panele logowania:

- W trakcie analizy wykryto publicznie dostępne panele administracyjne do usług pocztowych, wymiany plików itp.

Publicznie dostępne otwarte porty:

- W analizowanym okresie wykryto obecność otwartych portów, takich jak SSH, RDP, SMB, DICOM, VNC, Telnet.

4.4.4.8 WYNIKI I STATYSTYKI

Łączna liczba zidentyfikowanych błędów i podatności: 388

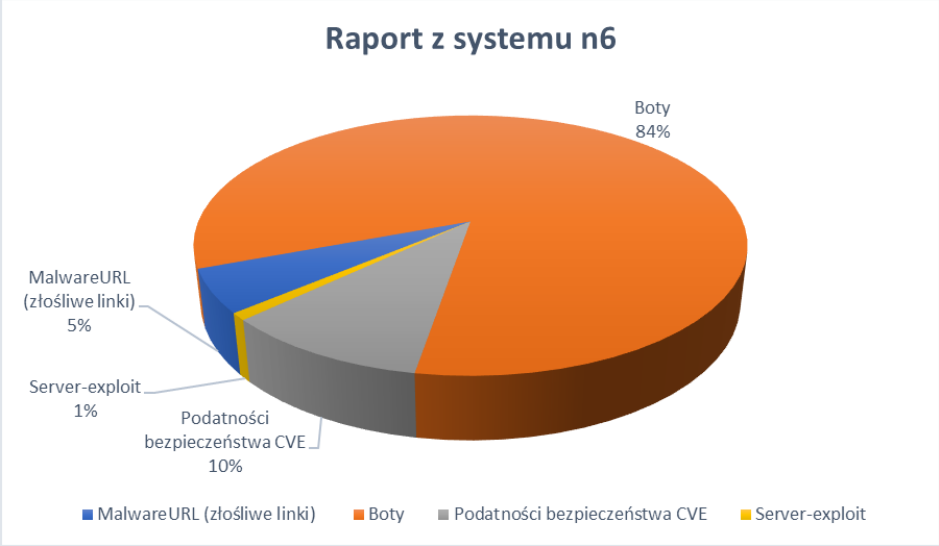
I. Błędy konfiguracyjne: 77
II. Dane z systemu n6:

1) Monitorowane adresacje IP: 272,
2) Wykryte podatności: 223 (tab. poniżej),

Tabela 28. Zestawienie wykrytych podatności

Typ wykrytej podatności	Liczba wykrytych podatności:
Malware URL (złośliwe linki)	12
Boty	186
Podatności bezpieczeństwa CVE	23
Server-exploit	2
Łącznie	**223**

Tabela 29. Raport z systemu N6



4.4.4.9 DANE Z INNYCH ŹRÓDEŁ, W TYM OD OSÓB PRYWATNYCH

Łącznie zgłoszono 88 potencjalnych zagrożeń, z których:

1) Zgłoszone przez osoby nie związane z podmiotem: 29:
   a) 26 zostało potwierdzonych jako realne podatności;
   b) 3 dotyczyło błędów konfiguracyjnych systemów publicznie dostępnych.
2) Znalezione za pomocą skanów rozwiązania Artemis: 59:
   a) 37 zostało potwierdzonych jako realne podatności;
   b) 22 dotyczyło błędów konfiguracyjnych systemów publicznie dostępnych.

4.4.4.10 PODSUMOWANIE

Rysunek 9. Wykryte podatności w 2024 r.

Rodzaj podatności	Liczba
Błędy konfiguracyjnych	77
Podatności z systemu n6 (m.in. boty i luki CVE)	223
Podatności pochodzących z innych źródeł (w tym Artemis)	88
Łącznie:	**388**

4.4.4.10.1 WSPÓŁPRACA Z INNYMI ZESPOŁAMI CYBERBEZPIECZEŃSTWA

Podczas wykonywania codziennych zadań CSIRT CeZ blisko współpracuje z CSIRT-ami poziomu krajowego oraz odpowiednimi zespołami do zwalczania cyberprzestępczości w kraju.

Współpraca z CSIRT NASK umożliwia błyskawiczną wymianę informacji o incydentach i zagrożeniach, co pozwala na szybką reakcję na incydenty oraz wpływa na ograniczenie występowania nowych. Poprzez wymianę wiedzy o nowych technikach ataków, podatnościach i najlepszych praktykach, skuteczniej rozwijamy metody obrony.

Szybka wymiana informacji na temat zagrożeń oraz w ramach obsługi incydentu jest bardzo ważna. W związku z tym zawarte zostało porozumie na mocy, którego nawiązano współpracę z Centralnym Biurem Zwalczania Cyberprzestępczości – CBZC oraz nawiązano również współpracę z Dowództwem Komponentu Wojsk Obrony Cyberprzestrzeni – DKWOC.

W związku z coraz nowszymi technikami i taktykami ataków od początku istnienia zespołu CSIRT CeZ wykorzystuje różne dostępne narzędzia w walce z zagrożeniami. W tym celu dzięki współpracy z CSIRT

NASK oraz informacjami uzyskiwanymi z systemu Artemis, możliwe jest w sposób ciągły zwiększanie poziom bezpieczeństwa w sektorze ochrony zdrowia. Na podstawie otrzymywanych informacji ostrzegamy podmioty o podatnościach i błędnych konfiguracjach występujących w ich infrastrukturze, co przekłada się na poprawę poziomu bezpieczeństwa.

Zespół CSIRT CeZ korzysta także z platformy n6 stworzonej przez zespół CSIRT NASK. Dzięki tej usłudze możemy pomóc wykryć problemy związane z poziomem bezpieczeństwa infrastruktury danego podmiotu. Po wykryciu anomalii w danej sieci lub podatności aplikacji dostępnych z poziomu internetu, niezwłocznie o tym fakcie informujemy podległy nam podmiot.

Zespół CSIRT CeZ jest również uczestnikiem różnego rodzaju wydarzeń związanych z cyberbezpieczeństwem. Jednym z nich jest uczestnictwo w Programie Partnerstwo dla Cyberbezpieczeństwa (PdC).

W zakresie wymiany informacji na poziomie międzynarodowym, zespół CSIRT CeZ jest częścią The Trusted Introducer Service z oznaczeniem Listed Team.

4.4.4.10.2 PODNOSZENIE ŚWIADOMOŚCI O CYBERZAGROŻENIACH

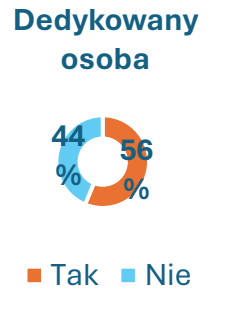
Zespół CSIRT CeZ wspólnie z Akademią CeZ przeprowadził w drugiej połowie roku 6 szkoleń dedykowanych dla kadry kierowniczej podmiotów wykonujących działalność leczniczą. Przeszkolono ponad 430 osób. Szkolenia te w roku bieżącym są kontynuowane. Szkolenia te w sposób przekrojowy przybliżały uczestnikom liczne zagadnienia związane z cyber zagrożeniami oraz budową w świetle obowiązujących przepisów kompleksową obroną przed cyberzagrożeniami.

4.4.4.10.3 ANALIZA SEKTORA

Centrum e-Zdrowia wraz z zespołem CSIRT CeZ cyklicznie od 2021 bada poziom dojrzałości podmiotów szpitalnych w obszarze cyberbezpieczeństwa. Przeprowadzona na koniec ubiegłego roku kolejna ankieta badająca poziom dojrzałości cyberbezpieczeństwa w podmiotach, pokazuje pewną poprawę w niektórych obszarach. Poprawa następuje jednak bardzo powoli.

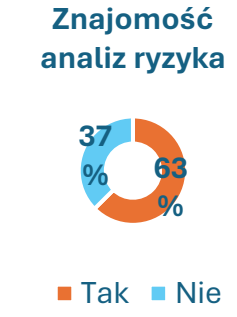
Jedno z pytań ankiety, na które warto zwrócić uwagę dotyczy tego czy podmiot posiada dedykowany etat do spraw cyberbezpieczeństwa. Niestety pomimo pewnej poprawy, nadal w prawie połowie ankietowanych podmiotów brakuje dedykowanej kadry. Wykres przedstawia liczę podmiotów, która w danym roku zadeklarowała, że posiada etat ds. cyberbezpieczeństwa.
Z wyników ankiety wynika także, pomimo poprawy, iż liczba dyrektorów placówek, którzy zostali przeszkoleni w zakresie podstaw cyberbezpieczeństwa nadal jest daleka od dostatecznej. To szkolenie, które ma przede wszystkim podnieść świadomość zagrożeń jakie występują w sieci, tak aby świadomie podejmować decyzje kierując podmiotem. Widać tu znaczą poprawę. Jednak nadal ponad 60% managerów nie miało takich szkoleń, pomimo, że prowadzi je m.in. CSIRT CeZ – nieodpłatnie i online.

Pomimo drobnej poprawy w 2024 roku prawie 40% dyrektorów nie zapoznaje się z analizami ryzyka w obszarze cyberbezpieczeństwa. Nie wiedzą więc czy i czego brakuje aby dopełnić obowiązków

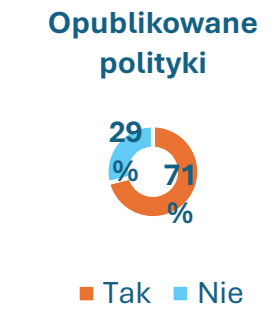


Rysunek 10. Wyniki ankiety

Rysunek 13. Wyniki ankiety



Rysunek 12. Wyniki ankiety



Rysunek 11. Wyniki ankiety

ustawowych oraz

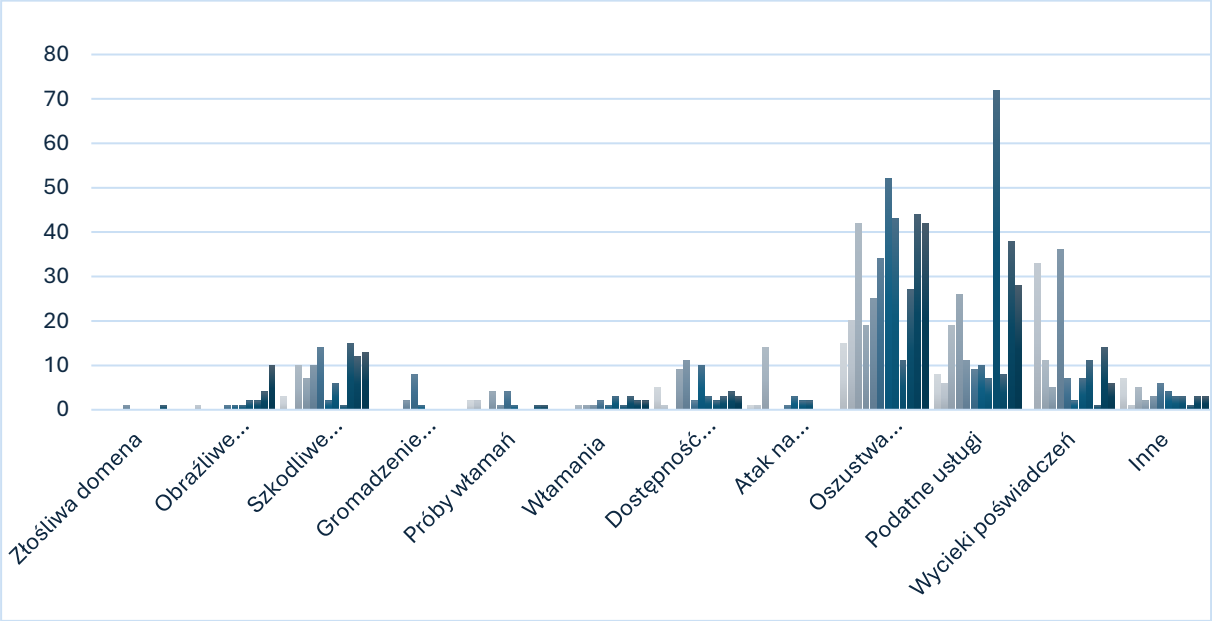
żeby zabezpieczyć dane. 29% podmiotów nigdy nie opublikowała lub nie zaktualizowała polityki bezpieczeństwa informacji o zakres cyberbezpieczeństwa. Z przeprowadzonej ankiety wynika także, iż 26% placówek nie ma zabezpieczenia tak podstawowego jak firewall, a 39% nie ma rozwiązania klasy EDR.

4.4.4.11 WNIOSKI

Analiza statystyczna incydentów wskazuje, że najpowszechniejszymi wektorami ataku są kategorie:

- Oszustwa komputerowe
- Podatne usługi
- Wycieki poświadczeń

Tabela 30. Występowanie poszczególnych typów incydentów z podziałem na miesiące w 2024r.



Prawidłowo podjęte działania zaradcze, poza innymi działaniami, mogłyby istotnie wpłynąć na podniesie poziomu cyberodporności w sektorze.

Analiza zidentyfikowanych wektorów ataku oraz przypisanie im odpowiednich metod mitygacji pozwala na uzyskanie następujących wyników:

Oszustwa komputerowe:

- Podnoszenie świadomości użytkowników na temat cyberzagrożeń.
- Prawidłowa konfiguracja systemu korespondencji elektronicznej.
- Prawidłowo wdrożone narzędzi bezpieczeństwa i ochrony poczty.

Podatne usługi:

- Instalowanie możliwe szybko i w sposób bezpieczny najnowszych. Stabilnych wersji stosowanego oprogramowania.
- Wdrożenie procesu cyklicznego monitorowania infrastruktura także pod względem występowania podatności.
- Monitorowanie ostrzeżeń oraz doniesień o nowych podatnościach i wersjach w celu szybkiego łatania.

Wycieki poświadczeń:

- Podnoszenie świadomości użytkowników na temat cyberzagrożeń.
- Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji uwzględniającym silne polityki haseł oraz odpowiednie zasady przetwarzania informacji.
- Wdrożenie adekwatnych narzędzi bezpieczeństwa oraz monitorowania wyników z tych urządzeń.

Ze względu na niedostatek etatów oraz środków finansowych podmioty te mają poważny problem z kadrą IT. Zespoły zwykle są nieliczne, zbyt obciążone i poświęcają zdecydowaną większość czasu na zapewnienie ciągłości działania. Braki finansów przekładają się też na problem z podnoszeniem kompetencji zespołu – brak szkoleń.

Zbyt małe zespoły przekładają się niestety na brak zintegrowanej architektury bezpieczeństwa. Z braku czasu i ludzi, narzędzia bezpieczeństwa często uruchamiane są punktowo, wybiórczo. Wdrażany jest Firewall i antywirus jako minimum, ale nie są analizowane wszystkie słabości, wszystkie tzw. powierzchnie ataku, nie sprawdza się czy zmitygowano wszystkie słabości oraz wektory ataku. W takim środowisku narzędzia nie działają jako jeden system bezpieczeństwa.

4.4.5 PLANOWANE DZIAŁANIA

- Rozwój narzędzi i systemów – planowane są zakupy sprzętu oraz narzędzi wykorzystywanych do monitorowania i analizy incydentów bezpieczeństwa w sektorze.
- Zwiększenie możliwości wczesnego wykrywania podatności – planowane jest pozyskanie narzędzi, które pomogą cyklicznie wyszukiwać podatności w sektorze.
- Rozwój zespołu – kontynuowane będą działania mające na celu zwiększenie kompetencji zespołu poprzez szkolenia oraz rekrutację nowych ekspertów w obszarze cyberbezpieczeństwa.
- Zwiększenie efektywności obsługi zgłoszeń – prowadzone będą prace nad usprawnieniem procesów analizy i reakcji na incydenty.
- Rozwój działań edukacyjnych i podnoszenie świadomości – kontynuowane będą działania informacyjno-edukacyjne, mające na celu zwiększenie świadomości pracowników sektora ochrony zdrowia w zakresie cyberbezpieczeństwa oraz promowanie najlepszych praktyk w obszarze ochrony danych i systemów IT.
- Opracowanie rekomendacji i zaleceń – opracowywane i publikowane będą zalecenia oraz dobre praktyki dla podmiotów z sektora ochrony zdrowia.
- Udział w projektach mających na celu podnoszenie cyberodporności sektora.

4.5 DZIAŁANIA MINISTRA INFRASTRUKTURY JAKO ORGANU WŁAŚCIWEGO DO SPRAW CYBEBRZPIECZEŃSTWA (MI)

Minister Infrastruktury jest organem właściwym ds. cyberbezpieczeństwa dla dwóch sektorów: transportu (w ramach którego wyróżnia się cztery podsektory: kolejowy, lotniczy, wodny oraz drogowy) oraz zaopatrzenia w wodę pitną i jej dystrybucji.

4.5.1 ZADANIA I DZIAŁANIA STATUTOWE, JAKO ORGANU WŁAŚCIWEGO

Ministerstwo Infrastruktury realizowało zadania organu właściwego dla sektora transportu i sektora zaopatrzenia w wodę pitną i jej dystrybucję, poprzez:

- prowadzenie bieżącej analizy podmiotów w sektorach transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji pod kątem uznania za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
- monitorowanie stosowania przepisów UKSC przez operatorów usług kluczowych, poprzez działania nadzorcze, pozyskując sprawozdania z audytów bezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej, następnie przeprowadzając analizę wyników audytów pod kątem nieprawidłowości, ale również wypracowywania oceny bezpieczeństwa operatora. W Ministerstwie Infrastruktury prowadzone jest elektroniczne zestawienie dotyczące realizacji wymagań nałożonych przez UKSC na operatorów usług kluczowych.
- prowadzenie kontroli operatorów usług kluczowych w zakresie bezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej, przy czym przedmiotowa kontrola następuje po analizie sprawozdań z przeprowadzonych audytów pod kątem wykrytych niezgodności oraz terminowości ich przeprowadzenia (w 2024 r. przeprowadzono jedną kontrolę doraźną).
- stałą współpracę z operatorami usług kluczowych z zakresu realizacji przepisów UKSC, doradztwo w przypadku wątpliwości stwierdzonych przez operatorów usług kluczowych.
- współpracę z CSIRT GOV, CSIRT NASK i CSIRT MON w zakresie powiadamiania o cyberzagrożeniach, w tym dystrybucję rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa;

4.5.2 PRACE NAD NOWELIZACJĄ USTAWY O KSC

Ministerstwo Infrastruktury aktywnie angażowało się w prace poświęcone projektowi ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32).

4.5.3 CSIRT SEKTOROWY

W związku z przewidywanym utworzeniem sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT sektorowego) dla sektora transportu i sektora zaopatrzenia w wodę pitną i dystrybucję, Ministerstwo Infrastruktury podejmowało szereg działań związanych przygotowaniem do projektu, w tym:

- dokonano analizy potrzeb i oczekiwań wobec CSIRT sektorowego wśród podmiotów wyznaczonych na operatorów usług kluczowych w nadzorowanych sektorach, podmiotów przewidywanych do wyznaczenia na podmioty kluczowe i ważne, świadczących usługi w nadzorowanych sektorach oraz ISAC-Kolej i Aviation-ISAC.

- w celu oszacowania skali funkcjonowania CSIRT sektorowego, dokonano analizy incydentów, jakie miały miejsce na przestrzeni lat w nadzorowanych podmiotach oraz na podstawie innych zestawień;
- rozpoczęto przygotowania do złożenia wniosku o objęcie przedsięwzięcia wsparciem w ramach inwestycji Krajowego Planu Odbudowy i Zwiększenia Odporności pn. *C3.1.1. Cyberbezpieczeńwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo*;
- nawiązano ścisłą współpracę z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK-PIB) w zakresie wsparcia merytorycznego w przygotowaniu do utworzenia CSIRT sektorowego, obejmującą szereg działań podejmowanych przez obydwie strony.

4.5.4 ZAKŁÓCENIA SYGNAŁU GNSS

Z uwagi na znaczący wzrost liczby przypadków zakłóceń sygnałów GNSS, tj. zagłuszania sygnału GNSS (jamming) i fałszowania sygnału GNSS (spoofing), podjęto szereg działań związanych m.in. z oceną skali zagrożenia, oceną ryzyk związanych z zakłóceniami, możliwości przeciwdziałania zakłóceniom, podejmowania działań wyprzedzających oraz mitygacji skutków wystąpienia zakłóceń przede wszystkim dla operacji lotniczych i morskich.

4.5.5 CENTRA WYMIANY INFORMACJI I ANALIZ (ISAC)

Na bazie doświadczeń funkcjonujących w podsektorze kolejowym i lotniczym Centrów Wymiany Informacji i Analiz (ISAC), tj. ISAC-Kolej oraz Aviation-ISAC oraz biorąc pod uwagę korzyści wynikające z uczestnictwa w tej formie współpracy publiczno-prywatnej, Ministerstwo Infrastruktury czynnie włączało się w dalsze promowanie tej inicjatywy, poprzez:

- bezpośrednią współpracę z podmiotami z sektora zaopatrzenia w wodę pitną i jej dystrybucję oraz podsektora transportu wodnego do ustanowienia takich struktur;
- wsparcie w wymianie wiedzy i najlepszych praktyk związanych z tworzeniem ISAC m.in. poprzez budowanie przestrzeni do współpracy, spotkania z przedstawicielami istniejących już w sektorze transportu Centrami Wymiany Informacji i Analiz, czy współdzielenie i omawianie dokumentów.

4.5.6 DOJRZAŁOŚĆ PODMIOTÓW Z NADZOROWANYCH SEKTORÓW W OBSZARZE CYBERBEZPIECZEŃSTWA I ICH GOTOWOŚĆ DO WEJŚCIA W ŻYCIE DYREKTYWY NIS2

W ramach projektu realizowanego wspólnie z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa oraz firmą Deloitte pn. *Cybersecurity Support Action* opracowano raport: *Dojrzałość w obszarze cyberbezpieczeństwa – sektor zaopatrzenia w wodę pitną i jej dystrybucji*. W 2024 r. został on rozdystrybuowany do podmiotów uczestniczących w badaniu. Projekt ten był szczególnie istotny, ponieważ swoim zasięgiem obejmował nie tylko bieżących operatorów usług kluczowych, ale także podmioty przewidywane jako podmioty kluczowe i podmioty ważne w rozumieniu Dyrektywy NIS2. Głównymi celami tego badania było określenie obecnego stanu cyberbezpieczeństwa sektora zaopatrzenia w wodę pitną i jej dystrybucji oraz kierunku działań mających na celu poprawę odporności i bezpieczeństwa sektora, a także określenie gotowości podmiotów działających w sektorze zaopatrzenia w wodę pitną i jej dystrybucji na wdrożenie wymagań Dyrektywy NIS2.

4.5.7 WSPÓŁPRACA Z URZĘDEM LOTNICTWA CYWILNEGO

Ministerstwo Infrastruktury wraz z Urzędem Lotnictwa Cywilnego stworzyło w ubiegłym roku przestrzeń wymiany informacji skupiającą się na wymaganiach stawianych wobec podsektora transportu lotniczego w ramach tzw. pakietu rozporządzeń Part-IS. Dialog nad prawidłowym przygotowaniem się podmiotów oraz o możliwościach ujednolicenia wymagań wynikających z wdrożenia rozporządzenia Part-IS jest istotny, ponieważ w pewnych zidentyfikowanych obszarach będzie wymagał powielenia zadań już realizowane na bazie Dyrektywy NIS2.

4.5.8 SYSTEM S46

Ministerstwo Infrastruktury aktywnie promowało System S46 wśród nadzorowanych operatorów usług kluczowych, który służy m.in. do wspierania szacowania ryzyka na poziomie krajowym. W ramach działań operacyjnych w 2024 r. podejmowano comiesięczne spotkania z przedstawicielami NASK, których celem był rozwój systemu oraz narzędzi będących wsparciem dla operatorów usług kluczowych. To działanie jest istotne z punktu widzenia planowanych zmian w polskim prawodawstwie spowodowanych zapisami Dyrektywy NIS2 oraz gwałtownym wzrostem zagrożeń w cyberprzestrzeni. W celu zapewnienia wsparcia podmiotom w nadzorowanych sektorach w zakresie spełnienia wymogów Dyrektywy NIS2 przewiduje się podjęcie działań promujących System S46 także wśród podmiotów kluczowych i podmiotów ważnych.

4.5.9 UDZIAŁ W WYDARZENIACH

Przedstawiciele Ministerstwa Infrastruktury aktywnie uczestniczyli w licznych wydarzeniach i inicjatywach z obszaru KSC i cyberbezpieczeństwa, a także udzielano patronatów honorowych, w tym:

- udział w organizowanych przez Ministerstwo Cyfryzacji spotkaniach w ramach Forum organów właściwych, czy Połączonego Centrum Operacyjnym Cyberbezpieczeństwa;
- udział w ćwiczeniach KSC-EXE 2024, mających na celu weryfikację zdolności operacyjnych podmiotów krajowego systemu cyberbezpieczeństwa odpowiedzialnych za zapewnienie ochrony przed zagrożeniami w cyberprzestrzeni, gdzie studium przypadku obejmowało swoim zakresem właściwość Ministra Infrastruktury;
- udział w programie Partnerstwo dla Cyberbezpieczeństwa, opartym na wielosektorowej współpracy na rzecz cyberbezpieczeństwa.

4.5.10 POZOSTAŁE ZAGADNIENIA

Ministerstwo Infrastruktury podejmowało także szereg innych działań, jak:

- współpraca z wybranymi operatorami usług kluczowych z sektorów będących we właściwości Ministra Infrastruktury, w tym w postaci nadzoru, w celu zapewnienia odpowiedniego poziomu dojrzałości podmiotu w obszarze cyberbezpieczeństwa i mitygacji zagrożeń;
- budowano relacje z podmiotami, które wraz z nowelizacją UKSC prawdopodobnie staną się podmiotami kluczowymi i ważnymi;
- dystrybucja rekomendacji wydawanych przez Pełnomocnika ds. cyberbezpieczeństwa;
- udział w pracach nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa;

4.5.11 WNIOSKI I REKOMENDACJE

Wielkie wyzwanie przed jakim obecnie stoi Ministerstwo Infrastruktury to znaczne zwiększenie podmiotów pozostających we właściwości Ministra Infrastruktury jako organu właściwego ds. cyberbezpieczeństwa w ramach nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa. Wiąże się to także ze wzrostem posiadanych kompetencji oraz zadań jakie organ właściwy powinien wykonać, ponieważ nowa perspektywa prawna ukazuje rolę Ministerstwa Infrastruktury nie tylko jako organu nadzorującego, ale również podmiotu wykonawczego do obowiązków ujętych projektem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

Znaczny wzrost podmiotów pozostających w nadzorze czy rozszerzenie katalogu zadań dla podmiotów nadzorujących bezpośrednio wpływają na zwiększenie zakresu obowiązków realizowanych przez organ właściwy, co przekłada się na konieczność zapewnienia odpowiednich zasobów kadrowych i zdolności operacyjnych. Należy przy tym zauważyć, że Minister Infrastruktury jest organem właściwym ds. cyberbezpieczeństwa dla dwóch sektorów: transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji, dlatego jednym z najistotniejszych wyzwań będzie utworzenie CSIRTu sektorowego odpowiadającego potrzebom obu tych sektorów. Jest to niezwykle istotne w kontekście występowania zróżnicowanych systemów informacyjnych wykorzystywanych do świadczenia usług nie tylko w poszczególnych

dziedzinach transportu (w ramach którego wyróżnia się cztery podsektory: kolejowy, lotniczy, wodny oraz drogowy), jak i w podmiotach odpowiadających za dostawę i dystrybucję wody oraz przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe lub przemysłowe.

Pomocne w realizacji tego zadania niewątpliwie okazały się działania podjęte w ubiegłym roku przez Ministerstwo Infrastruktury, na podstawie których: badano oczekiwania nadzorowanych sektorów co do najbardziej istotnych w ich ocenie zadań, jakie taki zespół powinien wykonywać, zbadano skalę historycznie występujących incydentów bezpieczeństwa informacji w nadzorowanych podmiotach, przeanalizowano istotne aspekty jakie powinien posiadać taki zespół – od kompetencji, poprzez procesy, schematy postępowania, aż po kwestie formalne czy techniczne.

4.5.12 PLANOWANE DZIAŁANIA W 2025 R.

1. Realizacja zadań statutowych jako organu właściwego ds. cyberbezpieczeństwa, w tym kontrole operatorów usług kluczowych.
2. Szczegółowa weryfikacja podmiotów, które po wejściu w życie nowelizacji UKSC na podstawie samoidentyfikacji powinny ocenić czy kwalifikują się jako podmiot kluczowy lub podmiot ważny, dla których organem właściwym ds. cyberbezpieczeństwa jest Minister Infrastruktury. W przypadku braku dokonania samodzielnie wpisu do rejestru przez podmiot kwalifikujący się w ramach znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa, na podstawie posiadanych kompetencji Ministerstwo Infrastruktury będzie analizowało nadzorowane sektory oraz dokonywało wpisu z urzędu wobec podmiotów, które powinny znaleźć się w ramach krajowego systemu cyberbezpieczeństwa i nie dokonały takiego zgłoszenia z własnej inicjatywy.
3. Wzmacnianie zdolności operacyjnych organu właściwego w związku ze skokowym wzrostem liczby nadzorowanych podmiotów oraz zwiększonym zakresem wymaganych do spełnienia obowiązków. Zadanie będzie realizowane po wejściu w życie nowelizacji UKSC, adekwatnie do potrzeb i możliwości.
4. Kontynuacja prac związanych utworzeniem CSIRTu sektorowego, którego zakres obejmie dwa sektory pozostające we właściwości Ministra Infrastruktury: transportu oraz zaopatrzenia w wodę pitną i jej dystrybucję.
5. Zacieśnianie współpracy z podmiotami KSC z sektorów będących we właściwości Ministra Infrastruktury, w tym w szczególności w zakresie cyberbezpieczeństwa oraz przygotowania się do wdrożenia i spełnienia wymogów ustawowych.
6. Kontynuacja starań mających na celu ustanowienie ISAC w podsektorze transportu wodnego oraz w sektorze zaopatrzenia w wodę pitną i jej dystrybucji.
7. Dalsze działania ukierunkowane na promowanie KSC oraz budowanie świadomości w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa.

4.6 DZIAŁANIA MINISTRA CYFRYZACJI JAKO ORGANU WŁAŚCIWEGO DO SPRAW CYBEBRZPIECZEŃSTWA (MC)

4.6.1 REALIZOWANE ZADANIA

Minister właściwy do spraw informatyzacji, w roli organu właściwego do spraw cyberbezpieczeństwa w 2024 r. (tj. Minister Cyfryzacji):

1. Prowadził bieżącą analizę podmiotów w sektorze infrastruktura cyfrowa pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej. W efekcie powyższego, nie wydał żadnej decyzje o uznaniu podmiotu za operatora usługi kluczowej oraz decyzji stwierdzającej wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej;
2. Monitorował stosowanie przepisów UKSC przez operatorów usług kluczowych;
3. W ramach działań nadzorczych w zakresie wykonywania przez operatorów usług kluczowych wynikających z UKSC obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych, przeprowadził 3 kontrole operatorów usług kluczowych oraz nałożył 4 administracyjne kary pieniężne;

Ponadto:

1. Poddano analizie kolejne, przekazane przez operatorów usług kluczowych, sprawozdania z audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Na jej podstawie podejmowano dalsze czynności nadzorcze.
2. Przedstawiciele organu właściwego uczestniczyli w pracach nad projektem ustawy o zmianie UKSC oraz niektórych innych ustaw, implementującej do krajowego porządku prawnego Dyrektywę NIS 2.

4.6.2 FORUM ORGANÓW WŁAŚCIWYCH

W 2024 r. odbyły się trzy fora organów właściwych krajowego systemu cyberbezpieczeństwa (inicjatywa została zapoczątkowana pod koniec 2022 r. przez resort cyfryzacji w celu stworzenia, pomiędzy organami właściwymi do spraw cyberbezpieczeństwa, wspólnej przestrzeni do wymiany doświadczeń, wiedzy, nawiązania współpracy, wypracowywania wspólnych stanowisk oraz diagnozowania aktualnych potrzeb). W głównej mierze tematem spotkań była implementacja Dyrektywy NIS 2 i założenia projektu ustawy o zmianie UKSC i innych ustaw.

4.6.3 SYSTEM S46

Ministerstwo Cyfryzacji we współpracy z NASK-PIB kontynuowało rozwój i utrzymanie Systemu S46, o którym mowa w art. 46 ust. 1 UKSC. System wdrożono 1 stycznia 2021 r., zgodnie z art. 89 tej ustawy. S46 wspiera zgłaszanie i obsługę incydentów, wymianę informacji i współpracę pomiędzy podmiotami KSC, a także szacowanie ryzyka na poziomie krajowym.

Na zakończenie 2024 r. z Systemu S46 korzystało 248 podmiotów, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, takie jak Jednostki Samorządu Terytorialnego. W obszarze utrzymania zapewniono sprawność systemu na poziomie nie mniejszym niż 99% w skali roku. W obszarze rozwoju prowadzono prace związane z dostosowaniem systemu do wymagań nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. W ramach prac związanych z dostosowaniem do tych wymagań wykonany został rejestr podmiotów KSC, który umożliwi samorejestrację.

Na podstawie rejestru jednostek gospodarki narodowej REGON przeprowadzone zostały wstępne szacunki ilości podmiotów, które obejmie znowelizowana ustawa. Z uwagi na uzyskane wskaźniki z tego szacowania, wskazujące na potrzebę podłączenia do systemu S46 ponad 60 tys. podmiotów, opracowana została metoda bezpiecznego podłączania tych podmiotów poprzez internet. Na potrzeby Urzędu Ochrony Danych Osobowych opracowana została usługa systemu S46 pozwalająca składać informacje o incydentach naruszeniu ochrony danych osobowych.

4.6.4 BUDOWA SEKTOROWEGO ZESPOŁU CYBERBEZPIECZEŃSTWA CSIRT-CYFRA

W Ministerstwie Cyfryzacji podjęto decyzję o rozpoczęciu budowy sektorowego zespołu cyberbezpieczeństwa o roboczej nazwie CSIRT-Cyfra, który po uchwaleniu nowelizacji UKSC stanie się sektorowym CSIRTem. Zespół ten obsługiwać ma podmioty z sektora infrastruktury cyfrowej. Uruchomienie pierwszych usług planowane jest na przełomie 2025/2026 roku. Budowa zespołu w latach 2025-2026 finansowana ma być ze środków KPO w ramach Inwestycji C3.1.1. „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo” KPO (Nabór nr KPOD.05.10-IW.06-003/24).

Inne działania realizowane przez Ministerstwo Cyfryzacji, nie związane bezpośrednio z pełnieniem funkcji organu właściwego, przedstawione są w rozdziale.

5 SŁUŻBY SPECJALNE

Jednym z kluczowych elementów KSC są służby specjalne. Służby specjalne w Polsce możemy podzielić na te o charakterze kontrwywiadowczym, czyli Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Służba Kontrwywiadu Wojskowego (SKW), jak i wywiadowczym, do których zaliczają się Agencja Wywiadu (AW) oraz Służba Wywiadu Wojskowego (SWW). Ponadto status służby specjalnej posiada także Centralne Biuro Antykorupcyjne (CBA), które realizuje zadania o *stricte* charakterze policyjnym, dlatego też działania Biura zostały opisane w części Sprawozdania dotyczącej zwalczania cyberprzestępczości.

Służby specjalne realizują zadania w zakresie cyberbezpieczeństwa zarówno w ramach obowiązków wynikających z UKSC (szczególnie ABW w prowadzonym przez siebie CSIRTcie poziomu krajowego tj. CSIRT GOV), jak i innych ustaw określających zakres działania i kompetencje służb specjalnych.

Należy zaznaczyć, że rola służb specjalnych w zapewnianiu bezpieczeństwa teleinformatycznego na poziomie krajowym jest szczególna - zarówno w zakresie liczby, specyfiki, jak i charakteru realizowanych zadań oraz podejmowanych przedsięwzięć. Większość działań Służb pozostaje w sferze działań objętych klauzulą tajności, dlatego też szczegóły dot. działalności ww. zakresie zostały zawarte w niejawnym załączniku do niniejszego Sprawozdania.

Ponadto zgodnie z art. 34 ust. 1 UKSC – CSIRTy poziomu krajowego oraz sektorowe zespoły cyberbezpieczeństwa, jak i podmioty świadczące usługi z zakresu cyberbezpieczeństwa zobowiązane są współpracować nie tylko z organami ścigania i wymiaru sprawiedliwości, ale także ze służbami specjalnymi przy realizacji ich ustawowych zadań.

Działalność krajowych służb specjalnych w zakresie cyberbezpieczeństwa skupiają się w zakresach obejmujących m.in.: aktywną obronę systemów teleinformatycznych, zadań dot. zabezpieczenia kontrwywiadowczego w środowisku cyfrowym oraz pozyskiwaniu informacji wywiadowczych przy użyciu technologii komputerowych, a także identyfikowaniu zagrożeń oraz zbieraniu i analizowaniu informacji, celem dostarczania kluczowych informacji dla najważniejszych osób w państwie.

Poza tym służby specjalne biorą aktywny udział w działaniach PCOC, co ma szczególne znaczenie dla koordynowania działań najważniejszych instytucji i sprawnego działania w odpowiedzi na pojawiające się zagrożenia. Ponadto Służby te biorą czynny udział w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa.

5.1 AGENCJA WYWIADU (AW)

5.1.1 ROZWÓJ KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

5.1.1.1 WDROŻENIE I OCENA FUNKCJONOWANIA PRZEPISÓW O KSC

Funkcjonariusze Agencji Wywiadu w roku 2024 aktywnie uczestniczyli w spotkaniach PCOC. W ich ramach, aspekt wdrożenia i oceny funkcjonowania przepisów o krajowym systemie cyberbezpieczeństwa jest jednym z analizowanych zagadnień, wynikającym z praktycznego ich zastosowania w bieżącej działalności AW, jak i współpracy z pozostałymi aktorami krajowego systemu cyberbezpieczeństwa.

Ponadto, Służba śledzi proces legislacyjny dot. nowelizacji Ustawy o krajowym systemie cyberbezpieczeństwa, ze szczególnym uwzględnieniem form zacieśniania współpracy w ramach PCOC.

Agencja Wywiadu aktywnie uczestniczy również w formułowaniu nowej Strategii Cyberbezpieczeństwa RP na lata 2025-2029 poprzez sformułowanie propozycji znaczących zmian dot. m.in. obszaru Cyber Threat Intelligence, dezinformacji, czy też podnoszenia świadomości w obszarze cyberbezpieczeństwa, w tym na drodze testów socjotechicznych.

5.1.1.2 PODNIESIENIE EFEKTYWNOŚCI FUNKCJONOWANIA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Agencja Wywiadu aktywnie korzysta z inicjatyw podejmowanych w ramach funkcjonowania krajowego systemu cyberbezpieczeństwa, np. ze stanowiska komputerowego wykorzystywanego do komunikacji niejawnej MILNET-Z uruchomionego w ramach PCOC, a także komunikatora Threema wykorzystywanego do komunikacji jawnej podczas wymiany informacji o cyberzagrożeniach. Inicjatywy te, w ocenie AW, znacznie polepszyły możliwości kontaktu z różnymi aktorami krajowymi partycypującymi w procesie doskonalenia zabezpieczeń cyberprzestrzeni RP. Prowadzone z ich wykorzystaniem rozmowy przyczyniają się do pozyskiwania i wymiany informacji o zagrożeniach dla bezpieczeństwa cyberprzestrzeni RP, co podnosi efektywność realizowanych zadań w zakresie cyberobrony.

AW wspierało w 2024 r. zarówno krajowe zespoły bezpieczeństwa (min. CSIRT MON, KNF, CBZC, SKW) jak również inne zespoły państw sojuszniczych (wchodzących w skład NATO) w ramach prowadzonych przez nie działań.

Działania AW w zakresie ochrony cyberprzestrzeni wynikają bezpośrednio z ustawy o ABW oraz AW. Agencja Wywiadu prowadząc czynności z zakresu rozpoznania elektronicznego polegającego min. na monitorowaniu środków komunikacji wykorzystywanych za granicami RP rozpoznaje również zagrożenia związane z atakami cybernetycznymi. Szczególną rolę w rozpoznawaniu wrogiej aktywności w cyberprzestrzeni odgrywa powstały w połowie 2024 r. zespół CTI, którego głównym zadaniem jest identyfikacja, analiza oraz dystrybucja informacji dot. wrogiej aktywności w sieciach teleinformatycznych mogącej uderzać w bezpieczeństwo infrastruktury teleinformatycznej RP oraz krajów sojuszniczych.

5.1.1.3 ROZBUDOWA SYSTEMU WYMIANY INFORMACJI NA POTRZEBY KIEROWANIA BEZPIECZEŃSTWEM NARODOWYM

AW sukcesywnie rozbudowuje liczbę stanowisk dostępowych do systemu MILNET-Z, wykorzystywanego m.in. do zdalnych spotkań Połączonego Centrum Operacyjnego Cyberbezpieczeństwa.

Ponadto, Służba rozbudowuje własne, kluczowe systemy ochrony i wymiany danych o charakterze niejawnym.

5.1.1.4 ZWIĘKSZENIE CYBERBEZPIECZEŃSTWA USŁUG KLUCZOWYCH I CYFROWYCH ORAZ INFRASTRUKTURY KRYTYCZNEJ

AW w zakresie swoich kierunkowych działań ustawowych, dostarcza informacji, które pomagają zabezpieczać przedmiotowe zasoby lub mitygować zagrożenia, które już wystąpiły.

Ponadto, funkcjonariusze AW uczestniczyli również w spotkaniach Zespołu ds. Incydentów Krytycznych, które są zwoływane w przypadku zakłócenia poufności, integralności lub dostępności krytycznych zasobów lub kluczowych usług na terenie RP.

W Służbie za usługę kluczową uznać należy szybką i bezpieczną wymianę danych operacyjnych, która jest sukcesywnie udoskonalana w zakresie zabezpieczeń w cyberprzestrzeni. Użytkowane systemy podlegają stałemu nadzorowi pod kątem bezpieczeństwa oraz wykrywanych podatności.

5.1.1.5 WYPRACOWANIE I WDROŻENIE METODYKI SZACOWANIA RYZYKA NA POZIOMIE KRAJOWYM

Funkcjonariusze Agencji Wywiadu odpowiedzialni za proces zapewniania cyberbezpieczeństwa uczestniczyli w sposób pośredni w szacowaniu ryzyka na poziomie krajowym poprzez dostarczanie ważnych informacji dot. cyberataków do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, z którym pozostają w bieżącym kontakcie.

Jednocześnie, otrzymywane informacje zwrotne w postaci raportów o zagrożeniach cyberbezpieczeństwa, zawierających często szczegółowe informacje o atakach, w tym adresy IP, domeny, hashe plików, są bezzwłocznie wykorzystywane do uniemożliwienia połączenia z nimi z sieci internetowych Agencji Wywiadu, minimalizując tym samym ryzyko wystąpienia związanych z nimi zagrożeń.

5.1.1.6 ZWIĘKSZANIE ZDOLNOŚCI DO ZWALCZANIA CYBERPRZESTĘPCZOŚCI, W TYM CYBERSZPIEGOSTWA I ZDARZEŃ O CHARAKTERZE TERRORYSTYCZNYM

Agencja Wywiadu, z uwagi na specyfikę służby, posiada szeroki zakres możliwości współpracy z partnerami międzynarodowymi, z którymi utrzymuje kontakt w zakresie przeciwdziałania zagrożeniom cyberbezpieczeństwa, w szczególności wymieniając informacje przydatne z punktu widzenia działań cyberdefensywnych, jak Indicators of Compromise - IOC.

Informacje, które są istotne w odniesieniu do cyberprzestrzeni RP, są następnie przekazywane do Zespołu CSIRT GOV. Agencja Wywiadu realizuje również zadania z zakresu aktywnej cyberobrony, które wpływają na zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa.

Ponadto, podejmuje czynności mające na celu pozyskiwanie i przetwarzanie informacji ważnych z punktu widzenia bezpieczeństwa Państwa. W ich wyniku Agencja Wywiadu przekazuje odbiorcom zewnętrznym informacje wywiadu odnoszące się do tematyki cyberzagrożeń.

5.1.1.7 OPRACOWANIE I WDROŻENIE NARODOWYCH STANDARDÓW CYBERBEZPIECZEŃSTWA ORAZ PROMOWANIE DOBRYCH PRAKTYK I ZALECEŃ

Podczas projektowania, wdrażania, a następnie w fazie eksploatacji systemów teleinformatycznych w Agencji Wywiadu, na bieżąco brane są pod uwagę Narodowe Standardy Cyberbezpieczeństwa, a także zalecenia i dobre praktyki opisane w Polskich Normach PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, a także ISO 31000, ze szczególnym uwzględnieniem modernizacji sieci internet w oparciu o model „zero zaufania".

5.1.1.8 BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW

Agencja Wywiadu dysponuje procedurami wewnętrznymi, mającymi na celu zapewnienie bezpieczeństwa łańcucha dostaw w postaci wymuszenia określonych zapisów w umowach z dostawcami

produktów i usług, w szczególności w zapisach SLA uwzględnia się dodatkowo kwestie podatności bezpieczeństwa produktów i usług, a nie jedynie ich dostępności.

Ponadto, podmioty dostarczające usługi dla Agencji Wywiadu są kompleksowo sprawdzane m.in. w zakresie ich wiarygodności, a także powiązań z innymi instytucjami i przedsiębiorstwami.

Agencja Wywiadu zobowiązuje je również do podpisania właściwych deklaracji w ramach umów o zachowaniu poufności wszelkich informacji pozyskanych podczas realizacji usług.

5.1.1.9 TESTY I AUDYTY CYBERBEZPIECZEŃSTWA

Agencji Wywiadu przeprowadza okresowo testy bezpieczeństwa środowisk hostingowych, w tym m.in. strony internetowej Agencji Wywiadu. Ponadto, w umowach zawartych z dostawcami usług z sektora prywatnego, Agencja Wywiadu zobowiązała strony umów do przeprowadzania tego typu testów dla świadczonych na jej rzecz usług.

5.1.2 ZWIĘKSZENIE POTENCJAŁU - PODMIOT REALIZUJACY ZADANIA STRATEGII

5.1.2.1 ROZBUDOWA ZASOBÓW PRZEMYSŁOWYCH I TECHNOLOGICZNYCH NA POTRZEBY CYBERBEZPIECZEŃSTWA

Oficerowie Agencji Wywiadu w ramach wspierania kompetencji wyższych uczelni w obszarze cyberbezpieczeństwa, w roku 2024 prowadzili liczne wykłady na uczelniach, dzieląc się jawną wiedzą, wynikającą z ich doświadczenia praktycznego podczas służby w komórce organizacyjnej, której zadaniem jest cyberobrona Agencji Wywiadu. Prowadzone wykłady spotykały się każdorazowo z dużym zainteresowaniem, o czym świadczyła liczba ich uczestników, jak i pytania zadawane przez studentów. Prowadzone wykłady przyczyniały się nie tylko do zwiększania świadomości dot. cyberzagrożeń wśród studentów, a tym samym przyszłych pracowników przemysłu i branży usług, ale miały również charakter naborowy, tj. związany z zachęcaniem do służby w AW. Ponadto, opisywane wydarzenia przyczyniały się do budowania rozpoznawalności marki, jaką jest Agencja Wywiadu.

5.1.2.2 NASTAWIENIE NA ROZWÓJ WSPÓŁPRACY MIĘDZY SEKTOREM PUBLICZNYM I PRYWATNYM

Agencja Wywiadu współpracuje z sektorem prywatnym w dziedzinie cyberbezpieczeństwa usług internetowych, z których aktywnie korzysta. W tym celu realizowane są umowy m.in. z NASK S.A. dotyczące bezpiecznego hostingu poczty elektronicznej Agencji Wywiadu, strony internetowej, zapewnienia usług z zakresu wirtualnych sieci prywatnych, zarządzania obsługą incydentów, czy rozbudowy infrastruktury światłowodowej.

5.1.3 ZWIĘKSZANIE KOMPETENCJI KADRY PODMIOTÓW ISTOTNYCH DLA CYBERBEZPIECZEŃSTWA RP

Agencja Wywiadu w roku 2024 kontynuowała współpracę z Naukową i Akademicką Siecią Komputerową - Państwowym Instytutem Badawczym, w ramach zadania pt. "działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla kluczowych osób w państwie", w ramach której wytypowani oficerowie przeszkolili łącznie kilkadziesiąt osób piastujących najwyższe stanowiska w RP, w tym posłów, ministrów i wiceministrów oraz dyrektorów biur w ministerstwach.

Agencja Wywiadu przykłada również dużą uwagę do szkolenia własnych kadr z zakresu cyberbezpieczeństwa. Tematyka cyberobrony stanowi element szkolenia funkcjonariuszy na każdym jego etapie.

Realizowano również działania mające na celu utrzymanie przez funkcjonariuszy i pracowników AW aktualnej wiedzy z zakresu cyberobrony poprzez bieżące monitorowanie prasy i przygotowywanie skrótu najważniejszych informacji z tego obszaru.

5.1.3.1 ROZWIJANIE ŚWIADOMOŚCI SPOŁECZNEJ W KIERUNKU BEZPIECZNEGO KORZYSTANIA Z CYBERPRZESTRZENI

W ramach poszerzania wiedzy z zakresu cyberzagrożeń Agencja Wywiadu, w roku 2024, prowadziła tematyczne wykłady na uczelniach, a także organizowała szkolenia online, na które zapisać mógł się każdy internauta, po uprzednim zgłoszeniu. Wykłady w Internecie, organizowane przez Służbę spotkały się z dużym zainteresowaniem i dobrymi ocenami.

5.1.3.2 AKTYWNA WSPÓŁPRACA MIĘDZYNARODOWA NA POZIOMIE OPERACYJNYM I TECHNICZNYM

Agencja Wywiadu prowadzi bieżącą współpracę z partnerami zagranicznymi mającą na celu nie tylko wymianę informacji z zakresu cyberbezpieczeństwa, ale również zaznaczenie obecności Agencji Wywiadu, jako istotnego aktora w procesie zapewniania cyberbezpieczeństwa. Efektem podejmowanych inicjatyw, wymiany informacji i odbytych spotkań roboczych są zapytania ze strony partnerów zagranicznych o dodatkowe informacje z zakresu cyberataków, którymi Agencja Wywiadu dysponuje i jest w stanie je udostępnić.

Ponadto, Agencja Wywiadu na poziomie technicznym współpracuje z partnerami w ramach Unii Europejskiej i NATO, wdrażając w ścisłej współpracy z tymi podmiotami metody oraz środki mające zapewnić bezpieczną łączność międzynarodową, zarówno bilateralną, jak i multilateralną. Dzięki tej kooperacji jest możliwa wymiana informacji istotnych z punktu widzenia bezpieczeństwa Państwa.

Szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej Sprawozdania.

5.2 AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO (ABW)

Jawne informacje dot. działalności ABW w cyberprzestrzeni zawarte zostały w rozdziale CSIRT GOV. Natomiast **szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej niniejszego Sprawozdania.**

5.3 SŁUŻBA WYWIADU WOJSKOWEGO (SWW)

Szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej Sprawozdania.

5.4 SŁUŻBA KONTRWYWIADU WOJSKOWEGO (SKW)

5.4.1 DZIAŁANIA SKW MAJĄCE NA CELU PRZECIWDZIAŁANIE AKTYWNOŚCI ROSYJSKICH SŁUŻB SPECJALNYCH (RSS)

5.4.1.1 OCENA SKUTECZNOŚCI I EFEKTÓW PRZECIWDZIAŁANIA AKTYWNOŚCI SVR UKIERUNKOWANEJ NA SYSTEMY INFORMATYCZNE AMBASAD ORAZ OPROGRAMOWANIA „TEAMCITY"

W grudniu 2023r., SKW brała udział w międzynarodowych działaniach, w które zaangażowane były służby specjalne polski (SKW), USA (NSA, FBI) oraz Wielkiej Brytanii (GCHQ). Działania te miały na celu zakłócenie oraz wyeliminowanie zagrożenia płynącego z aktywności Służby Wywiadu Zagranicznego Rosji (SVR – zbiór aktywności nazywany w przestrzeni publicznej najczęściej jako APT29).

5.4.1.2 OPERACJA DYINGEMBER

W styczniu 2024 r., SKW brała udział w międzynarodowej operacji pk. DYINGEMBER, mającej na celu wyeliminowanie infrastruktury operacyjnej wykorzystywanej przez GRU (JW26165 – zbiór aktywności najczęściej nazywanych nazywany jako APT28) do anonimowego realizowania działań wywiadowczych, ataków w cyberprzestrzeni oraz przełamywania zabezpieczeń.
W toku operacji SKW oraz partnerskie służby z kilkunastu krajów, w skoordynowany sposób usunęły narzędzia GRU z kilkuset urządzeń, zabezpieczając je jednocześnie przed ponownym wykorzystywaniem przez GRU.

Wyeliminowana infrastruktura była używana w szeregu działań o charakterze wywiadowczym, m.in.:

- Do zarządzania złośliwym oprogramowaniem GRU wykorzystywała w działaniach wywiadowczych – m.in. przeciwko celom na Ukrainie oraz w próbach uzyskania dostępu do systemów informatycznych RON;
- Do kradzieży danych uwierzytelniających poprzez wiadomości phishingowej oraz poprzez przejęcie kontroli i modyfikację paneli logowania do kont pocztowych m.in. w Polsce, na Ukrainie oraz innych państwach NATO i UE;
- Jako platformy na których tymczasowo *hostowano* (umieszczano) wykradzione dane oraz narzędzia operacyjne;
- Do zestawienia „tuneli" – połączeń do wnętrza sieci – do skompromitowanych systemów informatycznych;
- Do anonimizacji przeglądania stron internetowych i pobieranych z sieci internet danych.

5.4.2 INNE ZIDENTYFIKOWANE ZAGROŻENIEA W KTÓRYCH ROZPOZNANIU BRAŁO UDZIAŁ SKW - MANIPULACJA SYSTEMAI STEROANIA STSEMÓW OCZYSZCZANIA WODY

W dniu 17.01.2024 r. na kanale w komunikatorze *Telegram* i nazwie „*CyberArmyofRussia_Reborn*" umieszczone zostało nagranie wideo ukazujące rzekomy cyberatak na systemy oczyszczania wody zlokalizowane w Polsce. Na nagraniu widać jak nieustalona osoba zmienia parametry procesu przemysłowego oczyszczania ścieków (m.in. parametry techniczne i chemiczne). Na nagraniu widać następujące nazwy: „Oczyszczalnia Ścieków Wydmin", „Oczyszczalnia Ścieków Biogest Przerość", „Oczyszczalnia Ścieków Systemu Biogest Sidra", „Oczyszczalnia Ścieków w Kątach".

Dodatkowo na drugim umieszczonym w zbliżonym czasie na tym samym kanale nagraniu, widoczna jest modyfikacja parametrów pracy systemów oczyszczania wody w miastach w USA: „City of Abernathy", „City of Muleshoe". Na nagraniu widać, że atakujący posiada poprawne dane uwierzytelniające do panelu sterowania procesem przemysłowym. Atakujący modyfikuje parametry przemysłowe funkcjonowania systemu oczyszczania wody (m.in. prędkość działania oraz układ pomp tłoczących wodę do wieży ciśnień) oraz wyłącza systemy automatycznej kontroli.

Atakujący uzyskał też dostęp do okna pozwalającego na zmiany wartości chlorowania wody. Nagranie kończy się komunikatem o utracie połączenia systemu sterowania ze sterownikami przemysłowymi. CERT.PL, po otrzymaniu informacji od SKW, potwierdził zdarzenie. Operator systemu zdawał sobie sprawę ze zdarzenia, ale traktował je jako „samoistną losową zmianę".

5.4.3 PROGNOZY I PRZEWIDYWANIA

5.4.3.1 WYKORZYTSANBE URZĄDZEŃ SOHO DO PROWADZENIA BUDOWY INFRASTRUKTURY OPERACYJENJ

W ocenie SKW obce służby specjalne będą kontynuowały wykorzystywanie cywilnych, należących do małych firm i osób prywatnych, urządzeń sieciowych klasy SOHO. Urządzenia te zazwyczaj są stare, nie posiadają wsparcia od producentów. Na wiele z nich można znaleźć w sieci internet gotowe skrypty służące do przełamywania zabezpieczeń. W sieci internet znajdują się dziesiątki tysięcy dostępnych urządzeń. Wszystko to sprawia, ze klasa SOHO jest idealna do budowania taniej w utrzymaniu i zarządzaniu, anonimowej, rozproszonej infrastruktury operacyjnej.

5.4.3.2 ZAGROŻENIA DLA SYSTEMÓW PRZEMYSŁOWYCH

W 2024 r, SKW obserwowała rozpoznawanie systemów przemysłowych infrastruktury krytycznej ze strony zarówno (prawdopodobnie) pro-rosyjskich aktywistów, jak i (prawdopodobnie) służb specjalnych. Jest prawdopodobne, że w 2025 r. zaobserwowane zostaną kolejne próby pozyskiwania informacji o/lub modyfikacjach działania systemów przemysłowych.

Dotychczasowe doświadczenia pokazują, że praktycznie w ostatnich latach, co roku upubliczniane jest przynajmniej jedno zdarzenie związane z kompromitacją łańcuch dostaw oprogramowania lub usług (odkrycie XZ backdoor w 2024 r., aktywność SVR przeciwko TeamCity w 2023 r. kompromitacja Viasat przez GRU w 2022 r.) o krytycznym znaczeniu. Jest możliwe, że podobne zdarzenie będzie miało miejsce również w 2025 r.

Innym wariantem zagrożenia dla łańcucha dostaw jest zagrożenie możliwość uzyskania przez RSS dostęp do firmy informatycznej (np. ISP. Outsourcingowej), a następnie wykorzystanie danych dostępowych i infrastruktury firmy do skrytej kompromitacji jej klientów. Podmioty szczególnie narażone na działania RSS powinny wdrożyć mechanizmy ograniczające te zagrożenia (przykładowo - nadzór nad sesjami, umożliwienie logowania tylko w zgłoszonych wcześniej oknach administracyjnych, nagrywanie sesji).

Szczegóły podejmowanych przedsięwzięć zamieszczono w części niejawnej Sprawozdania.

6 ZWALCZANIE CYBERPRZESTĘPCZOŚCI

Cyberprzestępczość jest jednym z największych i najszybciej rozwijających się zagrożeń dla społeczeństwa. Cyberprzestępcy działają z wykorzystaniem nowoczesnych technologii, wyspecjalizowanych narzędzi i form ataku na systemy teleinformatyczne, a swoje usługi oferują w tzw. ciemnym Internecie (Darknet). Zauważalny jest wzrost wykorzystywania sztucznej inteligencji oraz zagrożeń związanych z działaniami w tzw. świecie wirtualnym (Metaverse). Cyberprzestępczość to w zdecydowanej większości działalność o charakterze międzynarodowym. Infrastruktura przestępcza i dane umożliwiające wykrycie sprawców rozproszone są poza granicami kraju.

Skuteczna walka z zagrożeniami płynącymi z sieci internet i cyberprzestępcami możliwa jest wyłącznie w warunkach, w których organy ścigania nie ustępują cyberprzestępcom zarówno w technologii, jak i w umiejętnościach.

6.1 MINISTERSTWO SPRAWIEDLIWOŚCI (MS)

6.1.1 PODJĘTE PRZEDSIĘWZIĘCIA

do najważniejszych działań realizowanych w obszarze cyberbezpieczeństwa na poziomie krajowym i sektorowym, należy zaliczyć wystąpienie Biura Cyberbezpieczeństwa w dniu 5 czerwca 2024 r. do Dyrektorów Sądów Apelacyjnych z rekomendacją podjęcia współpracy z Departamentem Bezpieczeństwa Teleinformatycznego ABW w celu zainstalowania systemu ARAKIS GOV. Krok ten ma na celu zwiększenie bezpieczeństwa cybernetycznego sądów powszechnych, ale także – poprzez centralizację informacji z sond ARAKIS w ABW – bezpieczeństwa kraju. Biuro Cyberbezpieczeństwa koordynuje powyższy proces. Biuro Cyberbezpieczeństwa koordynuje również ustanawianie i wdrażanie standardów zabezpieczeń oraz rozwiązań informatycznych z zakresu cyberbezpieczeństwa w sądach powszechnych.

Z zagrożeń systemowych, widocznych z poziomu Biura Cyberbezpieczeństwa, należałoby wymienić fakt niewystarczającego zabezpieczenia cybernetycznego części z instytucji wymienionych w art. 4 pkt. 7 UKSC, które jednocześnie wymienione zostały w Obwieszczeniu Ministra Sprawiedliwości z dnia 4 grudnia 2024 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Sprawiedliwości lub przez niego nadzorowanych (M.P. 2024 poz. 1040).

Jest to ponad 700 instytucji, wobec których, na podstawie §29 Regulaminu Organizacyjnego Ministerstwa Sprawiedliwości z dnia 25 czerwca 2024 roku, za wykonywanie zadań zapewniających prawidłowe funkcjonowanie systemu ochrony cyberbezpieczeństwa odpowiada Biuro Cyberbezpieczeństwa, które na dzień przygotowywania przedmiotowej odpowiedzi liczy tylko 11,05 etatu (łącznie z dyrektorem i jego zastępcą). Koordynacja prawidłowego zabezpieczenia cyberprzestrzeni we wszystkich wyżej wymienionych instytucjach stanowi bardzo duże wyzwanie przy obecnej obsadzie etatowej, co wymusiło ustalenie priorytetów (skupienie się w pierwszej kolejności na sądownictwie powszechnym).

6.1.2 WNIOSKI I REKOMENDACJE

Biuro Cyberbezpieczeństwa pragnie zasugerować utworzenie na poziomie CSIRT MON, CSIRT NASK i CSIRT GOV wspólnego centrum wymiany informacji o zagrożeniach dla podmiotów wymienionych w art. 4 ustawy o Krajowym Systemie Cyberbezpieczeństwa. Rozwiązanie takie (np. https://www.mispproject. org/) znacznie usprawniłoby sposób zarządzania powiadomieniami o zagrożeniach, umożliwiając integrację z posiadanymi systemami bezpieczeństwa.

Tabela 31. Osądzeni, skazani za wybrane przestępstwa w I instancji sądów rejonowych

Rodzaje przestępstw	OSĄDZENI ogółem	OSĄDZENI, SKAZANI ZA WYBRANE PRZESTĘPSTWA W I INSTANCJI SĄDÓW REJONOWYCH									
		ogółem (liczba osób)	z tego		z tego orzeczono karę:						
			kobiety	mężczyzni	Pozbawienie wolności razem	w tym z warunkowym zawieszeniem	Ograniczenie wolności	Kara mieszana	Grzywna samoistna	Środki poprawczo - wychowawcze	Środki karne orzeczone samoistnie
2023											
Ogółem	295 921	252 627	27 309	225 318	95 633	39 651	69 284	2 274	85 219	34	183
w tym:											
Art. 200a § 1 kk	40	36	1	35	24	10	6	1	5	0	0
Art. 200a § 2 kk	120	108	1	107	55	31	26	1	25	0	1
Art. 267 § 1 kk	159	98	24	74	14	6	12	0	71	0	1
Art. 268a kk	45	32	7	25	12	8	2	0	17	0	1
Art. 269 kk	3	3	1	2	2	2	1	0	0	0	0
Art. 269a kk	4	2	0	2	1	1	0	0	1	0	0
Art. 269b kk	21	5	0	5	2	1	0	0	3	0	0
Art. 287 kk	189	159	29	130	61	38	53	0	45	0	0
2024											
	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023
Ogółem	274 129 -7%	229 162 -9%	25 753 -6%	203 409 -10%	88 549 -7%	36 046 -9%	62 553 -10%	1 969 -13%	75 881 -11%	31 3%	179 -2%
w tym:											
Art. 200a § 1 kk	23 -43%	22 -39%	0 -100%	22 -37%	16 -33%	9 -10%	3 -50%	0 -100%	3 -40%	0 0%	0 0%
Art. 200a § 2 kk	116 -3%	103 -5%	0 -100%	103 -4%	51 -7%	37 19%	30 15%	1 0%	18 -28%	0 0%	3 200%
Art. 267 § 1 kk	163 3%	88 -10%	22 -8%	66 -11%	13 -7%	9 50%	12 0%	0 0%	63 -11%	0 0%	0 0%
Art. 268a kk	9 -80%	5 -84%	0 -100%	5 -80%	4 -67%	1 -88%	0 -100%	0 0%	1 -99%	0 0%	0 0%
Art. 269 kk	2 -33%	1 -67%	0 -100%	1 -50%	0 -100%	0 -100%	0 -100%	0 0%	1 0%	0 0%	0 0%
Art. 269a kk	3 -25%	2 0%	0 0%	2 0%	2 100%	2 100%	0 0%	0 0%	0 -100%	0 0%	0 0%
Art. 269b kk	35 67%	17 240%	4 400%	13 160%	2 0%	2 100%	4 0%	0 0%	11 267%	0 0%	1 100%
Art. 287 kk	200 6%	165 4%	41 41%	124 -5%	61 0%	27 -29%	46 -13%	0 0%	58 29%	0 0%	0 0%

Tabela 32. dane dot. osądzonych i skazanych za przestępstwo z art. 165 § 1 i 3 kk w I instancji sądów okręgowych za lata 2023 i 2024 r.

Rodzaje przestępstw	OSĄDZENI ogółem	OSĄDZENI, SKAZANI ZA WYBRANE PRZESTĘPSTWA W I INSTANCJI SĄDÓW OKRĘGOWYCH							
		ogółem (liczba osób)	z tego		z tego orzeczono karę:				
			kobiety	mężczyzni	Pozbawienie wolności razem	w tym z warunkowym zawieszeniem	Dożywotnie pozbawienie wolności	Kara mieszana	Inne skazania
2023									
Ogółem	8 466	7 631	1 066	6 565	6 980	2 639	25	99	527
w tym:									
Art. 165 § 1 i 3 kk	33	31	6	25	28	22	0	0	3
2024									
	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023	2024 Zmiana do 2023
Ogółem	8 759 3%	7 824 3%	1 091 2%	6 733 3%	7 196 3%	2 656 1%	15 -40%	74 -25%	539 2%
w tym:									
Art. 165 § 1 i 3 kk	49 48%	44 42%	22 267%	22 -12%	40 43%	23 5%	0 0%	0 0%	4 0%

6.2 PROKURATURA KRAJOWA

6.2.1 PODJĘTE DZIAŁANIA

Najważniejsze realizowane przez Prokuraturę Krajową działania w obszarze zwalczania cyberprzestępczości w 2024 r.:

- nadzorowanie przez prokuratorów Departamentu do Spraw Cyberprzestępczości i Informatyzacji najpoważniejszych postępowań dotyczących cyberprzestępczości — łącznie w Prokuraturze Krajowej w 2024 r. **nadzorowano 172 najpoważniejsza śledztwa w kraju, dotyczące cyberprzestępczości** (rejestr Dsn),
- organizacja powszechnych szkoleń online w zakresie tematyki zwalczania cyberprzestępczości prowadzonych przez prokuratorów Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej oraz podmioty współdziałające - w 2024 r. zorganizowano szkolenia w których udział wzięło łącznie 13 tysięcy osób,
- koordynacja postępowań w zakresie cyberprzestępczości w celu zmniejszenia ilości prowadzonych spraw o ten sam czyn, poprzez ich łączenie w postępowania zbiorcze, np: w zakresie fałszywych sklepów internetowych czy kaskadowych alarmów bombowych (art. 224a kk),
- rozwój narzędzi informatycznych i budowa nowych funkcjonalności mających na celu ułatwienie i przyspieszenie pozyskiwania informacji niezbędnych w postępowaniach czy lepsze zarządzanie zasobem informacyjnym, w szczególności prowadzone prace wspólnie z Policją nad budową modułu do wymiany danych pomiędzy systemami PROK- a sys. ERCDŚ, podłączenie do systemu prokuratury PROK-SYS rejestru zewnętrznego - Systemu Informacji Finansowej (SInF).

6.2.2 DZIAŁANIA PLANOWANE DO RELAIZACJI W LATACH 2025 — 2027

- zapewnienie kompleksowego ekosystemu regulacji odnoszących się do zwalczania cyberprzestępczości, zabezpieczenia elektronicznego materiału dowodowego oraz przeciwdziałanie kradzieży tożsamości,
- wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości w prokuraturze,
- informatyzacja postępowania karnego,
- podnoszenie zdolności analitycznych organów ścigania i wymiaru sprawiedliwości przy wykorzystaniu nowych technologii,
- wymiana wiedzy i doświadczeń zakresu cyberbezpieczeństwa oraz metod wykorzystywanych przez sprawców cyberprzestępstw w celu podniesienia skuteczności organów ścigania oraz cyberodporności.

6.2.3 DANE STATYSTYCZNE DOT. DZIAŁALNOŚCI

Tabela 33. Dane statystyczne dot. działalności Prokuratury Krajowej w zakresie zwalczania cyberprzestępczości

1. Przepis	2. Zarejestrowany spraw	3. Odmowy wszczęcia	4. Umorzenie NN (niewykrycie sprawcy przestępstwa)	5. Umorzenie pozostałe (art. 17 § 1 pkt 1 do 11 kpk, warunkowe umorzenie postępowania, wniosek o umorzenie – art. 342 kpk)	6. Akt oskarżenia (oraz winsoki o wyrok skazujący art. 335 § 1kpk)
Art. 287kk (oszustwo komputerowe	171558	2490	12586	1172	645
art. 267 kk (bezprawne uzyskanie informacji)	21039	6600	10971	2426	662
art. 268 kk (utrudnianie zapoznania się z informacją)	658	188	273	128	43
art. 268a kk (niszczenie danych informatycznych)	2688	901	1540	188	36
art. 269 kk (uszkodzenie danych informatycznego)	36	6	16	3	5
art. 269a kk (uszkodzenie systemu informatycznego)	112	16	69	11	7
art. 269b kk (wytwarzanie oprogramowania i narzędzi do popełnienia przestępstwa)	162	14	93	18	32
art. 200a kk (uwodzenie małoletniego w sieci)	939	123	196	233	286
art. 202 § 3 kk (rozpowszechnianie twardej pornografii)	598	46	81	120	232
art. 202 § 4 kk (utrwalanie pornografii z udziałem małoletniego)	166	13	23	48	103
art. 202 § 4a kk (posiadanie pornografii dziecięcej)	689	24	58	199	420
art. 286 kk (oszustwo, na podstawie danych Policji, można szacować, iż 50% spraw z zakresu 286 kk dotyczy cyberprzestępczości, w zestawieniu są wszystkie sprawy z art. 286 kk)	163854	33113	65509	27563	19749
art. 190a § 2kk (kradzież tożsamości)	7777	2871	2271	1117	668
art. 29, 30, 31, 32 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (generowanie sztucznego ruchu, smishing, CLI Spoofing, niezgodną z prawem modyfikację informacji adresowej)	1461	139	1080	29	4

6.3 CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI (CBZC)

6.3.1 ZADANIA CBZC

Z dniem 12 stycznia 2022 r. zostało powołane Centralne Biuro Zwalczania Cyberprzestępczości jako jednostka Policji służby zwalczania cyberprzestępczości, do zadań której należy:

- rozpoznawanie i zwalczanie przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobieganie tym przestępstwom, a także wykrywanie i ściganie sprawców tych przestępstw;
- wspieranie w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw, o których mowa w pkt 1, a także wykrywaniu i ściganiu sprawców tych przestępstw.

Centralne Biuro Zwalczania Cyberprzestępczości w ramach swojej działalności prowadzi działania:

- o charakterze ogólnym w zakresie:
  - zapobiegania cyberprzestępczości poprzez budowanie bezpieczeństwa w cyberprzestrzeni w oparciu o właściwą komunikację ze społeczeństwem,
  - działań profilaktycznych, w tym spotkania, kampanie uświadamiające, spoty i inne we współpracy z NASK i innymi instytucjami zajmującymi się problematyką cyberbezpieczeństwa,
  - organizacji wspólnie z NASK szkoleń, m.in. dla pracowników sektora bankowego, samorządowego oraz grup szczególnie narażonych na wiktymizację, np. seniorów,
  - zacieśnienia współpracy z krajowymi podmiotami publicznymi i prywatnymi oraz instytucjami międzynarodowymi,
  - wdrażania i rozwijania nowoczesnych technologii i innowacji,
  - współpracy i uczestnictwa w międzynarodowych szkoleniach i konferencjach o tematyce związanej z cyberprzestępczością.

- O charakterze szczególnym:
  - rozpoznawanie, eliminowanie i redukowanie prawdopodobieństwa wystąpienia cyberprzestępstw,
  - współpraca z krajowymi i zagranicznymi podmiotami oraz organami ścigania w zakresie podnoszenia poziomu wiedzy w zakresie cyberbezpieczeństwa oraz zwalczania cyberprzestępczości,
  - organizowanie specjalistycznych szkoleń dla funkcjonariuszy i pracowników CBZC oraz innych jednostek organizacyjnych Policji,
  - współpraca z Prokuraturą w zakresie wymiany informacji oraz pogłębiania wiedzy na temat metod i narzędzi używanych przez sprawców, istniejących zagrożeń i sposobów ich rozpoznawania, prawnych i faktycznych możliwości pozyskiwania i zabezpieczania dowodów, metod identyfikacji i przeciwdziałania zagrożeniom związanych z atakami cybernetycznymi,
  - gromadzenia danych dotyczących cyberprzestępczości i analizowanie jej trendów w Polsce i na świecie,
  - diagnozowanie i analizowanie trendów technologicznych w celu rozwijania strategii i metodyki ich wykorzystania dla potrzeb zwalczania cybeprzestępczości.

6.3.2 DZIAŁANIA PODJĘTE W 2024 R.

CBZC w roku 2024 podejmowało działania m.in. w następujących obszarach:

- oszustwa i pranie pieniędzy,
- CSAM,
- złośliwe oprogramowanie, hacking,
- inne, w tym handel w sieci internet narkotykami, bronią, lekami.

6.3.3 Dane dotyczące wyników w zwalczaniu cyberprzestępczości w kategoriach będących w szczególnym zainteresowaniu CBZC za rok 2024

przedstawiają się następująco:

Tabela 34. Dane CBZC w zakresie realizacji zadań

Zadanie	Wynik
Wszczęte postępowania przygotowawcze:	438
Zakończone postępowania przygotowawcze:	447
Łącznie funkcjonariusze CBZC prowadzili postępowań w liczbie:	1253
Wykrywalność wyniosła:	84%
Przedstawiono zarzuty osobom w liczbie:	1073
Zostało zatrzymanych osób w liczbie:	848
Zastosowano środek zapobiegawczy w postaci tymczasowego aresztowania osobom w liczbie:	312
Na poczet przyszłych kar, grzywien, zadośćuczynienia pokrzywdzonym itp. zabezpieczono mienie o łącznej wartości:	72,7 mln. zł,
Odzyskano mienie o wartości:	49,7 mln. zł

6.3.4 REKOMENDACJE

CBZC rekomenduje w zakresie zwalczania zaawansowanych form cyberprzestępczości następujące czynności:

- rozwijanie szerokiej współpracy organów ścigania w kontekście międzynarodowym, w szczególności na forum takich organizacji jak Agencja Unii Europejskiej Europol oraz Międzynarodowa Organizacja Policji Kryminalnych INTERPOL,
- rozwijanie skutecznych kanałów komunikacji i współpracy z dostawcami usług elektronicznych,
- podnoszenie kompetencji funkcjonariuszy Policji w zakresie najnowszych technologii,
- rozwijanie i wdrażanie narzędzi inteligentnego przetwarzania dużych wolumenów danych (w szczególności z zabezpieczonych nośników danych),
- stałe monitorowanie najnowszych trendów technologicznych i związanych z nimi zagrożeń, w celu identyfikacji nowych rodzajów cyberprzestępstw,
- wdrażanie najnowszych rozwiązań (np. z obszaru sztucznej inteligencji) dla potrzeb skutecznego zwalczania i zapobiegania cyberprzestępczości,
- prowadzenie działań i kampanii prewencyjnych skierowanych do społeczeństwa.

Więcej informacji dot. działalności Policji w cyberprzestrzeni zostało zawarte w rozdziale dot. KGP.

6.4 KOMENDA GŁÓWNA POLCJI (KGP)

6.4.1 ZADANIA I ROLA KGP

Policja zajmuje się kompleksowym projektowaniem, realizowaniem, wdrażaniem, utrzymaniem i rozwojem systemów teleinformatycznych, teletransmisyjnych, telekomutacyjnych i radiokomunikacyjnych, które stanowią kluczowe wsparcie dla działalności wielu organów i instytucji państwowych. Powyższe obejmuje systemy międzynarodowe, krajowe, policyjne, niejawne oraz systemy infrastruktury krytycznej. Odbiorcami usług są m.in.: Kancelaria Prezydenta RP, Kancelaria Sejmu RP, Kancelaria Senatu RP, Kancelaria Prezesa Rady Ministrów, urzędy wojewódzkie, ABW, Biuro Bezpieczeństwa Narodowego, Centra Powiadamiania Ratunkowego, administracja rządowa, Urząd ds. Cudzoziemców, sądy, prokuratury, Straż Graniczna.

Na wszystkich etapach budowy rozwiązań szczególna uwaga przywiązywana jest do obszaru zapewniającego cyberbezpieczeństwo zasobów informacyjnych administrowanych przez Policję. W celu wymiany informacji o incydentach i zagrożeniach, a także wspólnego reagowania na zagrożenia w cyberprzestrzeni oraz pomocy w likwidacji skutków incydentów Policja współpracuje z CSIRT GOV, prowadzonym przez Szefa ABW. Realizując zadania związane z zapewnianiem bezpieczeństwa w cyberprzestrzeni na poziomie krajowym, Policja współpracuje z wiodącymi podmiotami w zakresie cyberbezpieczeństwa (w oparciu o zawierane umowy i porozumienia), a także z operatorami usług kluczowych oraz dostawcami usług cyfrowych (w celu zapewnienia ochrony infrastruktury krytycznej).

W ramach zadań związanych z zapewnieniem cyberbezpieczeństwa realizowane są działania w obszarze zagwarantowania zgodności systemu zarządzania bezpieczeństwem informacji w obszarze systemów teleinformatycznych eksploatowanych w zakresie Krajowego Systemu Informatycznego (KSI) z normą PN-ISO/IEC 27001:2023-08, w tym w szczególności szacowanie ryzyka oraz projektowanie i koordynowanie bezpieczeństwa informacji i zapewnienie ciągłości działania procesów informacyjnych. Przedstawiciele MSWiA oraz organy, a także jednostki organizacyjne podległe lub nadzorowane przez Ministra SWiA uczestniczą w cotygodniowych posiedzeniach Zespołu ds. Koordynacji Cyberbezpieczeństwa organizowanym przez RCB.

Jednocześnie wśród funkcjonariuszy i pracowników Policji budowana jest świadomość istnienia zagrożeń w cyberprzestrzeni poprzez udział w szkoleniach poświęconych przedmiotowemu zagadnieniu. Podobne działania realizowane są przez inne organy, a także jednostki organizacyjne podległe lub nadzorowane przez Ministra SWiA. Dodatkowo należy wskazać, że Policja prowadzi, w tym zakresie, szkolenia dla uczniów, nauczycieli i rodziców dzieci szkół podstawowych i ponadpodstawowych.

Ponadto policja pełni istotną rolę w zakresie zapewniania bezpieczeństwa w cyberprzestrzeni, ochronę infrastruktury krytycznej i danych wrażliwych pozostających w zakresie jej odpowiedzialności. W dobie cyfryzacji i rosnącej liczby zagrożeń w sieci, działania KGP w tym obszarze mają kluczowe znaczenie zarówno dla Policji, jak i społeczeństwa.

Policji zostały powierzone obowiązki tzw. Centralnego Organu Technicznego KSI (COT KSI), w ramach których realizowany jest:

- dostęp do Narodowej Kopii tego systemu wszystkim uprawnionym instytucjom w kraju.
- Komendant Główny Policji jest operatorem OST 112, tj. Ogólnopolskiej Sieci Teleinformatycznej na potrzeby obsługi numeru alarmowego 112, integrującej Systemy Informatyczne Centrów Powiadamiania Ratunkowego, Systemy Wspomagania Dowodzenia Policji i Państwowej Straży Pożarnej oraz PLI CBD (Platformę Lokalizacyjno-Informacyjną z Centralną Bazą Danych Urzędu Komunikacji Elektronicznej).
- Komendant Główny Policji jest administratorem Systemu Łączności Rządowej, zapewniając bezpieczny dostęp do usług telekomunikacyjnych dla najważniejszych osób w państwie oraz

Szefem Krajowego Centrum Informacji Kryminalnych, w którym są gromadzone i udostępniane uprawnionym użytkownikom informacje kryminalne, dot. osób, przestępstw, podmiotów, przedmiotów, rachunków bankowych i rachunków papierów wartościowych.

Ponadto KGP:

- wyznacza strategie i kierunki działania jednostek Policji zajmujących się cyberprzestępczością, takich jak Centralne Biuro Zwalczania Cyberprzestępczości,
- koordynuje współpracę między jednostkami terenowymi Policji w przypadku wystąpienia incydentów cyberbezpieczeństwa o charakterze lokalnym i krajowym,
- odpowiada za opracowywanie procedur ochrony danych oraz reagowania na incydenty zagrażające bezpieczeństwu kluczowych systemów informatycznych administrowanych przez Policję,
- opracowuje plany ciągłości działania oraz przeprowadza analizy ryzyka w obszarze cyberbezpieczeństwa,
- utrzymuje i rozwija istotne dla funkcjonowania Policji systemy informacyjne,
- poszukuje podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych,
- prowadzi zaawansowane działania z zakresu aktywnej obrony systemów informacyjnych.
- Biuro Łączności i Informatyki KGP, jako wyspecjalizowana jednostka organizacyjna, zapewnia uprawnionym podmiotom dostęp do systemów informatycznych Policji - przykładem takiego systemu jest Krajowy System Informacyjny Policji, z którego korzystają takie służby jak m.in. Straż Graniczna czy Agencja Bezpieczeństwa Wewnętrznego,
- prowadzi również działania edukacyjne, podnoszące świadomość w obszarze cyberbezpieczeństwa, organizując wykłady i szkolenia zarówno wewnętrzne w samej formacji, jak i zewnętrzne dla instytucji, a także dla szkół podstawowych i ponadpodstawowych.

6.4.2 Rekomendacje:

- utrzymanie/pozyskanie wyspecjalizowanych zespołów/specjalistów do obsługi incydentów bezpieczeństwa, monitorowania sytuacji w cyberprzestrzeni Policji,
- zapewnienie/modernizacja narzędzi do aktywnej obrony cyberprzestrzeni Policji, w której funkcjonują jedna z najrozleglejszych infrastruktur telekomunikacyjnych i wielkoskalowe systemy informatyczne,
- niezbędna jest międzyresortowa/międzyinstytucjonalna wymiana informacji/doświadczeń z zakresu ochrony cyberprzestrzeni,
- efektywna współpraca z rynkiem prywatnym dostawców sprzętu informatycznego i oprogramowania, w celu zapewnienia sektorowi administracji publicznej dostępu do najnowszych rozwiązań technologicznych,
- stałe podnoszenie kwalifikacji zespołów zajmujących się poszczególnymi dziedzinami cyberbezpieczeństwa,
- nieustanne podnoszenie świadomości cyberbezpieczeństwa wśród pracowników i funkcjonariuszy,
- skuteczne eliminowanie zjawiska Shadow IT poprzez zapewnienie pracownikom i funkcjonariuszom wydajnych narzędzi niezbędnych do wykonywania ich obowiązków.

Więcej informacji dot. działalności Policji w cyberprzestrzeni zostało zawarte w rozdziale dot. CBZC.

6.5 CENTRALNE BIURO ANTYKORUPCYJNE (CBA)

6.5.1 ZADANIA

Centralne Biuro Antykorupcyjne (CBA) w 2024 r. realizowało szereg przedsięwzięć analityczno-informacyjnych oraz kontrolnych obejmujących swoim zakresem szerokorozumianą branżę IT, w tym działania związane z przeciwdziałaniem zagrożeniom o charakterze cyberprzestępczym.

Ponadto w minionym roku CBA brało czynny udział:

- w posiedzeniach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC);
- w realizacji ścisłej współpracy CSIRT GOV przy wykorzystaniu CSIRT CBA. W zakres współrealizowanych przedsięwzięć zaliczyć można— m.in. wymianę IOC (*ang. Indicator of Compromise*) w zakresie ataków teleinformatycznych skierowanych wobec CBA oraz wdrażanie zaleceń CSIRT GOV;
- w przeprowadzaniu szkoleń z zagadnień dot. cyberbezpieczeństwa dla osób pełniących szczególnie ważne funkcje publiczne koordynowanych przez NASK PIB (program *SecureV*).

7 MINISTERSTWO OBRONY NARODOWEJ (MON)

7.1 DZIAŁANIA REALIZOWANE PRZEZ RESORT OBRONY NARODOWEJ W ZAKRESIE CYBERBEZPIECZEŃSTWA, W SZCZEGÓLNOŚCI SŁUŻĄCE REALIZACJI STRATEGII CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2019-2024

7.1.1 WDROŻENIE I OCENA FUNKCJONOWANIA PRZEPISÓW O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Ministerstwo Obrony Narodowej koordynowało w ramach resortu obrony narodowej uzgodnienia projektu *ustawy zmianującą ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.* MON we współpracy z DKWOC/CSIRT MON brały udział w opracowywaniu przepisów, w szczególności dotyczących zakresu zadań Ministra Obrony Narodowej oraz CSIRT poziomu krajowego.

Ponadto dokonano analizy wpływu projektowanych zmian na resortowy system cyberbezpieczeństwa i rozpoczęto przygotowania do ich implementacji w ramach resortu.

7.1.2 PODNIESIENIE EFEKTYWNOŚCI FUNKCJONOWANIA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Powyższe było realizowane poprzez:

- DKWOC/CSIRT MON organizowali cotygodniowe spotkania przedstawicieli CSIRT poziomu krajowego oraz CSIRT KNF, PSE, UKE umożliwiające wymianę bieżących informacji o cyberzagrożeniach i incydentach.
- Przedstawiciele Ministerstwa Obrony Narodowej brali udział w Forum Organów Właściwych.
- Minister Obrony Narodowej (lub jego przedstawiciel) uczestniczył w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa.
- Przedstawiciele resortu, w tym CSIRT MON, brali udział w spotkaniach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa.
- Przedstawiciele DKWOC/CSIRT MON brali udział w pracach grupy roboczej zajmującej się implementacją oraz utrzymaniem i rozwijaniem systemu teleinformatycznego S46 wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa zgodnie z UKSC
- DKWOC/CSIRT MON wdrożył oraz zapewnił ciągłość funkcjonowania i rozwoju dedykowanego systemu teleinformatycznego wraz z systemami informatycznymi budowanymi na potrzeby wykrywania, rozpoznania i zwalczania zagrożeń cyberbezpieczeństwa.
- DKWOC/CSIRT MON rozpoczął pracę wsparcia i automatyzacji procesu obsługi incydentów oraz PWC (Proaktywnego Wykrywania Cyberzagrożeń).
- DKWOC/CSIRT MON ukompletował wyposażenie przewidziane dla Zespołów Zadaniowych oraz personelu DKWOC/CSIRT MON zabezpieczające pracę w ramach Proaktywnego Wykrywania Cyberzagrożeń oraz wsparcia w obsłudze incydentów.
- DKWOC/CSIRT MON informował o nowo publikowanych podatnościach sprzętu oraz oprogramowania użytkowanego w RON oraz podmiotach nadzorowanych (PN) i współpracujących, przygotowywał zalecenia, ostrzeżenia oraz komunikaty dla użytkowników systemów RON oraz podmiotów we właściwości CSIRT MON, dystrybuował biuletyny i raporty dotyczących zidentyfikowanych podatności.
- DKWOC/CSIRT MON prowadził bieżącą analizę podatności oraz zagrożeń w nadzorowanych systemach informatycznych poprzez cykliczne skanowania.
- DKWOC/CSIRT MON prowadził ocenę wpływu incydentów na system obronny państwa.

- DKWOC/CSIRT MON prowadził wymianę informacji z pozostałymi zespołami CSIRT poziomu krajowego oraz pozostałymi podmiotami KSC.

7.1.3 ZWIĘKSZENIE CYBERBEZPIECZEŃSTWA USŁUG KLUCZOWYCH I CYFROWYCH ORAZ INFRASTRUKTURY KRYTYCZNEJ

MON we współpracy z Morskim Centrum Cyberbezpieczeństwa Akademii Marynarki Wojennej w Gdyni (MCC), celem podniesienia poziomu wiedzy personelu wojskowych placówek ochrony zdrowia odpowiedzialnych za cyberbezpieczeństwo, zorganizował w marcu 2024 konferencję „Zimowa Szkoła Cyberbezpieczeństwa". Tematem wiodącym konferencji była tematyka bezpieczeństwa systemów i sieci teleinformatycznych wykorzystywanych w ochronie zdrowia jednostek RON.

7.1.4 ZWIĘKSZANIE ZDOLNOŚCI DO ZWALCZANIA CYBERPRZESTĘPCZOŚCI,W TYM CYBERSZPIEGOSTWA I ZDARZEŃ O CHARAKTERZE TERRORYSTYCZNYM

DKWOC/CSIRT MON:

- Monitorował stan bezpieczeństwa zasobów, usług i aplikacji podłączonych do internetu w ramach RON oraz podmiotów nadzorowanych (PN) i współpracujących (External Attack Surface Management).
- Współpracował z CBZC Policji w ramach działań mających na celu identyfikowanie fałszywych zbiórek pieniędzy na rzecz powodzian.

MCC AMW:

- Zorganizowało w maju 2024 r. konferencję pt. „Przestępczość teleinformatyczna XXI-6". Tematem wiodącym konferencji była tematyka zwalczania cyberprzestępczości ze szczególnym uwzględnieniem sektora e-commerce i bankowości. W ramach konferencji przeprowadzono warsztaty dla zespołów bezpieczeństwa wybranych banków z wykorzystaniem środowiska cyberpoligonu.

7.1.5 OPRACOWANIE I WDROŻENIE NARODOWYCH STANDARDÓW CYBERBEZPIECZEŃSTWA ORAZ PROMOWANIE DOBRYCH PRAKTYK I ZALECEŃ

DKWOC/CSIRT MON opracował:

- „Lokalne plany reagowania na incydenty komputerowe", opisujące zasady postępowania w obszarze reagowania na incydenty komputerowe, w systemach teleinformatycznych lub rozwiązaniach informatycznych resortu obrony narodowej.

Ministerstwo Obrony Narodowej opracowało:

- „Politykę etykietowania danych w systemach teleinformatycznych resortu obrony narodowej" – dokument określa zasady etykietowania danych w systemach teleinformatycznych RON, celem wdrożenia polityki jest zwiększenie bezpieczeństwa danych (w szczególności prawnie chronionych) przetwarzanych w systemach oraz zapewnienie efektywnej i kontrolowanej wymiany informacji pomiędzy systemami o różnych poziomach bezpieczeństwa oraz pomiędzy systemami narodowymi i służącymi do przetwarzania informacji międzynarodowych.

7.1.6 BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW ORAZ TESTY I AUDYTY BEZPIECZEŃSTWA

- Ministerstwo Obrony Narodowej rozpoczęło prace nad „Polityką bezpieczeństwa resortu obrony narodowej w zakresie przeciwdziałania cyberzagrożeniom łańcucha dostaw".
- DKWOC/CSIRT MON prowadził testy bezpieczeństwa systemów teleinformatycznych wprowadzanych do użytku lub eksploatowanych w Siłach Zbrojnych RP .

7.1.7 STYMULOWANIE BADAŃ I ROZWOJU W OBSZARZE CYBERBEZPIECZEŃSTWA

DKWOC prowadził nadzór nad realizacją badań pk. MIKOK, OptoKrypt i APQ, finansowanych przez NCBR. Głównymi celami realizacji tych przedsięwzięć są:

- Budowa modułowej infrastruktury komputera kwantowego (MIKOK);
- Budowa urządzenia realizującego kwantową wymianę klucza i generatora kwantowego oraz kodowania fazowego do ochrony transmisji (OptoKrypt);
- Opracowanie algorytmów postkwantowych szyfrowania, podpisu cyfrowego i uzgadniania klucza (APQ).

Wymienione przedsięwzięcia uruchomiono w celu opracowania nowych metod zabezpieczenia danych z uwzględnieniem zagrożeń związanych z perspektywą powstania komputerów kwantowych oraz rozwoju technologicznego w zakresie budowy komputera kwantowego.

Resort obrony narodowej realizował także projekty odnoszących się do łączności:

- Opracowanie metodyki testów i oceny radiolinii IV pasma, udział w testach urządzeń producentów krajowych i zagranicznych oraz opracowanie raportu z testów zgodnie z metodyką;
- Opracowanie koncepcji architektury militarnej instalacji testowej 5G.

Wojskowy Instytut Łączności im. prof. dr hab. Janusza Groszkowskiego – Państwowy Instytut Badawczy, w 2024 r. realizował nw. projekty finansowane w ramach dotacji Ministra ON:

- Opracowanie bazowego zestawu szkolno-treningowego posterunku monitorowania widma częstotliwości radiowych oraz namierzania źródeł zakłóceń;
- Przeprowadzenie badania podatności radiostacji na ofensywne działania w cyberprzestrzeni;
- Zrealizowanie projektu dot. aktywnego przeciwdziałania atakom na układy FPGA.

Efekty tych projektów zostały przyjęte i wykorzystane przez zaineresowane podmioty RON.

7.1.8 ZWIĘKSZANIE KOMPETENCJI INSTYTUCJONALNYCH ORAZ REALIZACJA WSPÓŁPRACY MIĘDZY SEKTOREM PUBLINCZYM I PRYWATNYM

Rozwój współpracy między sektorem publicznym i prywatnym realizowano poprzez:

- Organizację i/lub uczestnictwo w spotkaniach technicznych z udziałem przedstawicieli przemysłu i sektora publicznego na arenie krajowej i międzynarodowej oraz wsparcie realizacji badań naukowych w obszarze cyberbezpieczeństwa.

Ponadto,

- Pozyskiwano i rozwijano narzędzia służące budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej (SZ RP) oraz opracowano szkolenia dla zdefiniowanych ścieżek szkoleniowych kluczowych ról zawodowych cyberbezpieczeństwa w oparciu o Standard NIST 800-181 (NICE Framework) i ECSC rozpoczęło proces szkolenia w celu podnoszenia kompetencji kadr resortu do prowadzenia pełnego spektrum działań w cyberprzestrzeni oraz ćwiczenia z wykorzystaniem cyberpoligonu.
- Prowadzono działania w zakresie rozwoju zdolności SZ RP do realizacji działań w cyberprzestrzeni układzie krajowym, sojuszniczym i koalicyjnym, w tym poprzez udział w ćwiczeniach międzynarodowych z obszaru cyber. W 2024 uczestniczono m.in. w ćwiczeniach:
  - Locked Shields 24 – zorganizowanym przez NATO CCDCOE, podczas którego DKWOC tworzyło wspólny polsko-fiński zespół Blue Team, zajmując czołowe miejsce wśród zwycięzców ćwiczenia. W ćwiczeniu poza DKWOC, brali też udział żołnierze z ZDC WOT;
  - DEFENDER 24 – zorganizowanym przez Stany Zjednoczone we współpracy z Polską i Estonią. W DKWOC zlokalizowano elementy kierownictwa ćwiczenia oraz międzynarodowy zespół ds. Defensive Cyberspace Operations. W Estonii działał zespół DKWOC symulujący działania przeciwnika w cyberprzestrzeni. W ćwiczeniach brali też udział żołnierze z ZDC WOT;
  - Cyber Coalition 24 – w ramach, którego specjaliści DKWOC pełnili funkcje jednego z kluczowych elementów – Dowództwa Komponentu Operacji Specjalnych (SOCC), realizowaną w obszarze jego funkcjonalności do prowadzenia działań w cyberprzestrzeni. POL SOCC dowodził zespołami z innych państw;

- Cyber Flag 24 – zorganizowanym przez Stany Zjednoczone dla najbliższych sojuszników, mającym zwiększyć interoperacyjność działań w cyberprzestrzeni. Ze strony DKWOC uczestniczyło 14 przedstawicieli;
- DEFNET 24 – zorganizowanym przez francuskie dowództwo COMCYBER, mającym na celu skonsolidowanie przygotowania pod kątem defensywnej technologii informacyjnej, m.in. poprzez sprawdzenie spójności działań poszczególnych uczestników wydarzenia;
- CAX CyberNet – zorganizowanym przez Niderlandy, skupiającym się na aspektach strategicznych, operacyjnych i technicznych domeny cyber;
- Cyber Spartan – międzynarodowym ćwiczeniu typu Live Fire, zorganizowanym przez UK, mającym na celu doskonalenie umiejętności identyfikacji, wykrywania, ochrony i reagowania na zagrożenia cybernetyczne poprzez realistyczne scenariusze i współpracę zespołową;
- CYBER SHIELD – największym ćwiczeniu IIIinois National Guard, w ramach którego polscy specjaliści ćwiczyli cyberobronę z USA oraz innymi państwami;
- CWIX (JFTC Bydgoszcz) i Crossed Swords (CCDCOE, Estonia) – ćwiczeniu przyczyniającym się do podnoszenia poziomu interoperacyjności sojuszniczej oraz zwiększania zdolności do kolektywnej obrony;
- CyberBaltic – międzynarodowym ćwiczeniu, w których uczestniczyli żołnierze z ZDC WOT.

7.1.9 ZWIĘKSZENIE KOMPETENCJI KADRY PODMIOTÓW ISTOTNYCH DLA CYBERBEZPIECZEŃSTWA RP

Eksperckie Centrum Szkolenia Cyberbepieczeństwa (ECSC):

- Zorganizowało specjalistyczne szkolenia w dziedzinie IT, cyberbezpieczeństwa, oraz kryptologii na potrzeby RON. Centrum prowadzi szkolenia na wszystkich poziomach zaawansowania od podstawowego, poprzez zaawansowany po ekspercki. Oferta szkoleniowa ECSC jest tworzona w ścisłej koordynacji z jednostką ekspercką w obszarze IT, cyber oraz krypto - DKWOC i zabezpiecza bieżące i przyszłe potrzeby w tym zakresie. Szkolenia prowadzone są w dwóch trybach: stacjonarnym w oddziałach ECSC oraz zdalnym z wykorzystaniem dedykowanej platformy szkolenia na odległość (elearning). Obecne portfolio szkoleń ECSC jest sukcesywnie poszerzane i obejmuje obecnie: 34 z szkolenia zakresu IT oraz 30 szkoleń z zakresu cyber. Łącznie, w 2024 r., w 506 zrealizowanych przez ECSC szkoleniach (w tym 36 zdalnie) uczestniczyło przeszło 8,3 tys osób (w tym 3180 zdalnie).
- Zorganizowano szereg seminariów, warsztatów i konferencji m.in.: CyberBEZPIECZNI, CyberEXPERT, CyberEXPERT GAME.
- ECSC kontynuowało działania w obszarze certyfikacji osób w obszarze cyberbezpieczeństwa. W roku 2024 wysiłki Centrum skupiały się na utrzymaniu i rozszerzeniu akredytacji udzielonej ECSC przez Polskie Centrum Akredytacji o kolejne programy.

DKWOC prowadził szkolenia z zakresu cyberbezpieczeństwa dla pracowników i żołnierzy Resortu Obrony Narodowej. Szkolenia i warsztaty odbywały się w formie stacjonarnej i uzupełniane były kursami e-learningowymi.

Morskie Centrum Cyberbezpieczeństwa Akademii Marynarki Wojennej w Gdyni:

- Zorganizowało w października 2024 r. konferencję pt. „Dezinformacja wojskowa". Tematem wiodącym konferencji były działania dezinformacyjne i propagandowe oraz przeciwdziałanie im w RON.
- Kontynuowało prowadzenie:
  - Studiów podyplomowych „Cyberbezpieczeństwo" - obejmujących kwestie z zakresu cyberbezpieczeństwa w obszarze technicznym, prawnym i zarządczym;
  - Studiów podyplomowych EMBA „Zrządzania cyberbezpieczeństwem i usługami cyfrowymi" – obejmujących kwestie w zakresie zarządzania cyberbezpieczeństwem i usługami cyfrowymi. Studia były prowadzone we współpracy z DKWOC Fundacją Bezpieczna Cyberprzestrzeń oraz stowarzyszeniem ISSA Polska;
  - Studiów podyplomowych DBA „Zrządzania cyberbezpieczeństwem i usługami cyfrowymi"

Wojskowa Akademia Techniczna (WAT) kontynuowała prowadzenie:

- Studiów magisterskich na kierunku kryptologia i cyberbezpieczeństwo, zarówno w ramach studiów wojskowych jak i cywilnych;
- Studiów MBA w zakresie cyberbezpieczeństwa.

7.1.10 STWORZENIE WARUNKÓW DO BEZPIECZNEGO KORZYSTANIA Z CYBERPRZESTRZENI PRZEZ OBYWATELI

- MON współpracy z jednostkami resortu realizowało cykliczny projekt pn. Akademia_CYBER.MIL, którego celem jest budowanie świadomości i wiedzy w zakresie cyberbezpieczeństwa oraz przygotowanie studentów do wyzwań związanych z ochroną cyberprzestrzeni. II edycja Projektu w roku akademickim 2023/2024 realizowana była w szesnastu uczelniach publicznych prowadzących kierunki studiów związane z szeroko rozumianym cyberbezpieczeństwem i informatyką, natomiast III edycja, w roku akademickim 2024/2025 realizowana jest w szesnastu politechnikach i uczelniach technicznych na obszarze całego kraju. W ramach projektu studenci mają okazję wziąć udział w wykładach prowadzonych przez specjalistów z zakresu cyberbezpieczeństwa, kursach e-learningowych, warsztatach i zawodach typu Capture The Flag.
- Centralne Wojskowe Centrum Rekrutacji we współpracy z DKWOC, WAT i MCC kontynuowano program CYBER.MIL z klasą polegający na utworzeniu i prowadzeniu w szkołach ponadpodstawowych klas o profilu "Cyberbezpieczeństwo i nowoczesne technologie informatyczne". Głównym celem programu jest wykształcenie potencjalnych kandydatów do korpusów osobowych kadry zawodowej i naukowej Sił Zbrojnych RP, w tym szczególnie do Wojsk Obrony Cyberprzestrzeni. W ramach kształcenia realizowano zarówno zajęcia teoretyczne jak i praktyczne dot. podstaw kryptografii, algorytmiki, cyberbezpieczeństwa oraz zarządzanie bezpieczeństwem danych i informacji.
- MCC i MON zorganizowały we wrześniu 2024 r. kolejna edycję Letniej Szkoła Cyberbezpieczeństwa. Konferencja była skierowana przede wszystkim do pracowników szeroko rozumianych mediów oraz działów informacyjnych/rzeczników prasowych podmiotów administracji publicznej i dotyczyła kwestii zagrożeń w środowisku informacyjnym, metod manipulacji społeczeństwem i mediami, operacji informacyjnych i psychologicznych, wiarygodności źródeł informacji oraz bezpieczeństwa informacyjnego wojska i żołnierzy.
- MON po raz kolejny zorganizował Konkursu o nagrodę im. Mariana Rejewskiego na najlepszą pracę naukową poświęconą cyberbezpieczeństwu i kryptologii (VI edycja). Celem konkursu jest m.in. promowanie polskiej myśli intelektualnej i wykorzystania potencjału naukowego dla potrzeb wzmocnienia obronności kraju.

7.1.11 AKTYWNA WSPÓŁPRACA MIĘDZYNARODOWA NA POZIOMIE STRATEGICZNO-POLITYCZNYM

Ministerstwo Obrony Narodowej :

- Zorganizowało, w październiku 2024 r. w Rzymie, we współpracy z Biurem Attache Obrony RP w Rzymie, konferencję bilateralną pt. „Sharing Cyber 2024 Warsaw – Rome”. Inicjatywa była kontynuacją formuły zapoczątkowanej w 2023 r. w Ambasadzie RP w Paryżu. W konferencji wzięli udział polscy i włoscy reprezentanci SZ, administracji publicznej, środowisk naukowych oraz podmiotów sektora prywatnego.
- Zorganizowało w kwietniu 2024 r. w Poznaniu, we współpracy z Grupą MTP, I Międzynarodowy Kongres Cyberbezpieczeństwa – IN.SE.CON. W wydarzeniu wzięło udział blisko 1.500 uczestników z kraju i zagranicy, w tym najwyżsi urzędnicy państwowi kształtujący obszar bezpieczeństwa w cyberprzestrzeni w Polsce, przedstawiciele SZ RP, czołowi eksperci krajowi oraz partnerzy zagraniczni z NATO i UE oraz państw sojuszniczych (przedstawiciele Europejskiego Kolegium Bezpieczeństwa i Obrony UE, Kwatery Głównej NATO, Departamentu Obrony USA oraz resortów obrony: Republiki Korei, Niemiec, Włoch, Gruzji i Rwandy). Wydarzenie miało na celu upowszechnienie w społeczeństwie tematyki bezpieczeństwa w cyberprzestrzeni, stworzenie forum wymiany wiedzy eksperckiej i doświadczeń i budowania współpracy podmiotów krajowych i zagranicznych w obszarze cyberbezpieczeństwa, inicjowanie i wspieranie projektów służących modernizacji wyposażenia i rozwiązań używanych w SZ RP

w obszarze zapewnienia bezpieczeństwa w cyberprzestrzeni, kreowanie społecznego zaplecza SZ m.in. poprzez pozyskanie partnerów do działalności na rzecz bezpieczeństwa i obronności państwa – nawiązywanie relacji z podmiotami sektora prywatnego z dziedziny nowych technologii i bezpieczeństwa w cyberprzestrzeni.

7.1.12 AKTYWNA WSPÓŁPRACA MIĘDZYNARODOWA NA POZIOMIE OPERACYJNYM I TECHNICZNYM Z PODMIOTAMI ZEWNĘTRZNYMI

- CSIRT MON dołączył do FIRST (The Forum of Incident Response and Security Teams) - lidera w reagowaniu na incydenty. Członkostwo w FIRST umożliwia zespołom reagowania na incydenty skuteczniejsze reagowanie na incydenty bezpieczeństwa — zarówno reaktywne, jak i proaktywne.
- DKWOC/CSIRT MON w zakresie współpracy w ramach UE uczestniczył w nw. projektach:
  - PESCO – Cyber Rapid Response Teams (CRRTs),
  - PESCO – Cyber and Information Domain Coordination Center (CIDCC),
  - MICNET – Military Computer Emergency Response Oprational Network.
- DKWOC/CSIRT MON kontynuował współpracę z NATO Cyber Operations Centre (CyOC) w zakresie wymiany informacji o zagrożeniach i incydentach w cyberprzestrzeni.
- DKWOC rozwijało funkcjonowanie Narodowego Punktu Kontaktowego do współpracy z NATO.
- ZDC DWOT kontynuowało współpracę z Estonian Defence League's Cyber Unit.

ECSC rozwijało współpracę z European Security And Defence College[14] (ESDC) Network i jest jedną z czterech polskich instytucji, które uczestniczą w tej inicjatywie. Przygotowane przez ECSC szkolenia adresowane były do personelu technicznego średniego szczebla państw UE (krajów członkowskich oraz instytucji i organów UE), którzy w ramach swoich obowiązków odpowiadają za kwestie związane z cyberbezpieczeństwem.

Ponadto, odbywało się szkolenie ukraińskich żołnierzy w Polsce w ramach międzynarodowej misji EUMAM Ukraine (UE Millitary Assistance Mission in support of Ukraine). Przygotowane przez ECSC szkolenia adresowane były do personelu technicznego średniego szczebla, którzy w ramach swoich obowiązków odpowiadają za kwestie związane z cyberbezpieczeństwem, w tym w szczególności zapewnieniem bezpieczeństwa, utrzymaniem i zarządzaniem systemami operacyjnymi. W raportowanym okresie łącznie przeszkolono 24 żołnierzy Sił Zbrojnych Ukrainy.

7.2 WNIOSKI I REKOMENDACJE

- Biorąc pod uwagę osiągnięte do tej pory rezultaty, a także mając na względzie planowane cele oraz specyfikę realizowanych przedsięwzięć, należy dążyć do kontynuowania programów takich jak CYBER.MIL i Akademia_CYBER.MIL w kolejnych latach, co pozwoli na pozyskanie w przyszłości przez ron personelu specjalistycznego w obszarze cyberbezpieczeństwa.
- Realizacja przez WIŁ-PIB zadań zleconych z zakresu kryptologii i cyberbezpieczeństwa stanowi dużą wartość dla rozwoju zdolności w obszarze zwiększania bezpieczeństwa cyberprzestrzeni w resorcie obrony narodowej. Zasadne jest kontynuowanie przedmiotowych zadań w kolejnych latach.
- Rekomendowane jest stymulowanie na poziomie krajowym rozwoju badań naukowych w obszarze cyberbezpieczeństwa i upowszechnianie ich wyników na rzecz podmiotów KSC.
- Konieczne jest kontynuowanie współpracy pomiędzy podmiotami KSC i wdrażanie mechanizmów ułatwiających wymianę informacji pomiędzy nimi, tworzenie forum wymiany wiedzy eksperckiej i doświadczeń.
- Zasadne jest kontynuowanie zaangażowania na arenie międzynarodowej, w tym w ramach UE i NATO. Powyższe przyczynia się do ugruntowania pozycji i skutecznie buduje wizerunek Polski jako rzetelnego i stałego partnera na arenie międzynarodowej. W sferze wojskowej, należy

[14] Europejskie Kolegium Bezpieczeństwa i Obrony

angażować się w inicjatywy UE celem uzupełnienia dotychczasowych działań podejmowanych w ramach NATO i formatach bilateralnych. Analizując całokształt dotychczasowego dorobku aktywności międzynarodowej w obszarze bezpieczeństwa cyberprzestrzeni dostrzegalny jest potencjał do wzmocnienia wymiaru europejskiego, co pozwoli na bardziej zrównoważone podejście do kwestii budowania odporności. Potencjalnymi obszarami polskiego zaangażowania może być aktywne uczestnictwo w pracach ENISA, organizacja ćwiczeń w formacie unijnym czy zwiększenie wysiłku szkoleniowego. Należy również kontynuować organizację wydarzeń skierowanych do partnerów (lub potencjalnych partnerów), co umożliwi budowanie i zacieśnianie relacji, tworzenie platformy wymiany doświadczeń i wiedzy oraz inicjowanie wspólnych inicjatyw zarówno na poziomie strategiczno-politycznym jak również techniczno-operacyjnym.

- Rekomendowane jest wykorzystanie sprawowania w pierwszym półroczu 2025 r. przewodnictwa Polski w Radzie UE w celu pozycjonowania naszego kraju w roli lidera rozwoju zdolności obszaru cyberbezpieczeństwa w ramach UE. Na tym gruncie dążenie do osiągniecia kluczowych celów Prezydencji określonych przez KPRM tj. działań na rzecz wsparcia Ukrainy, pogłębiania relacji transatlantyckich czy promowania polskiego przemysłu obszaru cyber i IT.
- Konieczne jest wdrażanie i rozwijanie kompleksowej strategii cyberbezpieczeństwa, obejmującej:
  - Podnoszenie poziomu bezpieczeństwa systemów teleinformatycznych;
  - Podnoszenie poziomu bezpieczeństwa infrastruktury sieciowej;
  - Podnoszenie świadomości i edukacja użytkowników o zagrożeniach cybernetycznych;
  - Współpracę i wymianę informacji o zagrożeniach na poziomie krajowym i międzynarodowym; z sojusznikami, partnerami, środowiskiem naukowo-badawczym oraz komercyjnymi firmami zajmującymi się bezpieczeństwem w cyberprzestrzeni;
  - Wdrażanie nowoczesnych technologii i rozwiązań chroniących systemy teleinformatyczne oraz regularne testy i audyty bezpieczeństwa.
- Zapewnienie odpowiedniego budżetu dla właściwej realizacji zadań z zakresu cyberbezpieczeństwa, w tym utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji przez podmioty KSC, wdrażania odpowiednich, adekwatnych do zagrożeń, środków zarządzania ryzykiem w cyberbezpieczeństwie i budowania wysokokwalifikowanych kadr/ rozwoju potencjału kadr realizujących zadania z zakresu cyberbezpieczeństwa.
- Rekomendowane jest wsparcie podmiotów administracji publicznej w zakresie budowy, utrzymania i doskonalenia systemów zarzadzania ciągłości działania, w tym przygotowywanie planów ciągłości działania, procedur awaryjnych i przywracania sprawności/odtworzenia po awarii oraz ich testowania.
- Wskazane jest kontynuowanie prac związanych z certyfikacją osób w obszarze cyberbezpieczeństwa. Certyfikacja osób pozwala na wyznaczanie na stanowiska związane z cyberbezpieczeństwem osób kompetentnych, posiadających odpowiednią wiedzę i doświadczenie potwierdzoną właściwym certyfikatem.
- Rekomendowane jest wdrożenie modeli i programów zarządzania kompetencjami dedykowanych dla personelu zajmującego się cyberbezpieczeństwem. Powyższe porządkuje proces szkolenia i zwiększa efektywny rozwój kompetencji personelu, umożliwiając osiągnięcie zdolności do prowadzenia kompleksowych działań w domenie cyberprzestrzeni. W związku z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, zgodnie z którą wszystkie podmioty administracji publicznej będą podmiotami kluczowymi, rekomenduje się podjęcie działań w powyższym zakresie na poziomie szefa służby cywilnej w odniesieniu do pracowników służby cywilnej.
- W obszarze posiadanych kadr eksperckich niezmiennie największym wyzwaniem pozostaje pozyskanie i utrzymanie specjalistów z zakresu cyberbezpieczeństwa w szczególności w związku z ich ograniczoną dostępnością na krajowym rynku pracy. Konieczne jest zwiększenie efektywności zarządzania Funduszem Cyberbezpieczeństwa i kształtowanie mechanizmów umożliwiających niwelację różnic w płacach pomiędzy sektorem publicznym i prywatnym.
- W dalszym ciągu należy konsekwentnie rozwijać zakres i zwiększać potencjał RON oraz krajowe zdolności szkoleniowe w obszarze cyberbezpieczeństwa.

7.3 PREDYKCJE DOTYCZĄCE SYTUACJI W CYBERPRZESTRZENI NA LATA 2025-2026.

- Działania kognitywne w cyberprzestrzeni, w tym zwiększenie ilości i jakości cyfrowych materiałów dezinformacyjnych i propagandowych.
- Intensyfikacja wykorzystania AI do cyberataków.
- Zwiększenie skali cyberataków na elementy infrastruktury przemysłowej dostępnych z sieci, urządzeniami IoT i urządzenia autonomiczne.
- Wykorzystywanie małych sieci typu SOHO do budowania rozproszonej infrastruktury pośredniczącej w prowadzeniu działań w cyberprzestrzeni.
- Ataki z wykorzystaniem podatności w łańcuchach dostaw umożliwiających przejęcie dostępu do serwerów, lub oprogramowania służącego do automatycznej dystrybucji oprogramowania, lub jego aktualizacji.
- Ataki prowadzone za pośrednictwem przejętych zasobów zewnętrznych dostawców usług, posiadających uprzywilejowany dostęp do sieci będącej właściwym celem ataku.

7.4 PLANOWANE DZIAŁANIA W 2025 R.

- Aktualizacja „Modelu Zagrożeń dla systemów teleinformatycznych RON na 2025 rok".
- Wzmocnienie współpracy z krajowymi i zagranicznymi podmiotami w zakresie wymiany informacji w zakresie obsługi incydentów oraz o cyberzagrożeniach.
- Budowanie świadomości sytuacyjnej o zagrożeniach w cyberprzestrzeni poprzez szkolenia dla personelu RON oraz podmiotów nadzorowanych.
- Podnoszenie kwalifikacji personelu RON w obszarze cyberbezpieczeństwa poprzez cykliczne szkolenia oraz ćwiczenia.
- Dostosowanie struktur do właściwej i efektywnej realizacji zadań wynikających z nowelizacji UKSC.
- Rozwój programu szkoleń oraz narzędzi do praktycznej weryfikacji odporności na zagrożenia phishingowe w RON.
- Kontynuowanie prac mających na celu wykorzystanie certyfikacji w procesie doboru i oceny kadr w obszarze cyberbezpieczeństwa.
- Kontynuacja działań w zakresie organizacji konferencji, szkoleń i warsztatów z zakresu cyberbezpieczeństwa zarówno dla jednostek ron, podmiotów współpracujących z RON i innych podmiotów KSC.
- Kontynuacja programów Akademia_CYBER.MIL i CYBER.MIL z klasą.
- Kontynuacja realizacji studiów na kierunkach związanych z cyberbezpieczeństwem na uczelniach wojskowych.
- Wdrożenie polityki etykietowania danych w RON.
- Wdrożenie polityki bezpieczeństwa RON dot. przeciwdziałania cyberzagrożeniom w łańcuchu dostaw na rzecz Sił Zbrojnych.
- Kontynuacja testów bezpieczeństwa systemów teleinformatycznych (ST) eksploatowanych w SZ RP, w tym aktywne testowanie systemów celem weryfikacji procedur reagowania na incydenty komputerowe oraz sposobów przeciwdziałania atakom na ST RON. Wypracowanie zasad podstawowej weryfikacji źródła i jakości pozyskiwanej informacji cyfrowej z uwzględnieniem wykorzystania AI.

8 INNE INSTYTUCJE WSPÓŁTWORZĄCE KSC

8.1 MINISTERSTWO EDUKACJI NARODOWEJ (MEN)

8.1.1 POLITYKA CYFROWEJ TRANSFORMACJI EDUKACJI (PCTE)

12 września br. Rada Ministrów przyjęła uchwałę w sprawie przyjęcia Polityki Cyfrowej Transformacji Edukacji (PCTE)[15], która ma charakter programu i dokumentu strategicznego, wyznaczającego ramy polityki państwa i działań podejmowanych w obszarze cyfryzacji edukacji w perspektywie krótko, średnio oraz długoterminowej.

PCTE stwierdza jednoznacznie, że bezpieczne korzystanie z mediów i informacji, przeciwdziałanie dezinformacji oraz znajomość zasad bezpieczeństwa, odpowiedzialnego i bezpiecznego korzystania z zasobów edukacyjnych i urządzeń cyfrowych są kluczowymi zagadnieniami nie tylko w odniesieniu do uczniów, ale również w przypadku nauczycieli i innych pracowników szkół.

Dlatego specjalnym programem, w szczególności w zakresie przeciwdziałania dezinformacji, powinni zostać objęci wszyscy członkowie społeczności szkolnej oraz rodzice. Wiedza, jak zabezpieczyć dane, odróżnić informacje celowo fałszywe i szkodzące od wprowadzających w błąd w wyniku nieświadomości, że rozpowszechniane informacje są nieprawdziwe, jak postępować z treściami nieprawdziwymi lub wprowadzającymi w błąd, jest niezbędna do prawidłowego funkcjonowania dzieci i młodzieży we współczesnym świecie.

Celem zaproponowanych w PTCE działań jest podniesienie świadomości, wiedzy i umiejętności całej społeczności szkolnej, w tym rodziców.

Cyfrowe bezpieczeństwo związane ze zdolnością do rozumienia treści i ich weryfikowania jest silnie umocowane w ogólnej strategii rozwoju alfabetyzacji i kompetencji komunikacyjnych. Ważnym aspektem cyberbezpieczeństwa jest profilaktyka cyberprzemocy, uzależnień, świadomość zagrożeń i konsekwencji prawnych prowadzonej aktywności w Internecie.

PCTE wskazuje, iż należy opracować i upowszechnić standard reagowania na incydenty w Internecie i katalog zagadnień do poruszenia w pracy z uczniami. Standard ten musi podlegać ciągłej rewizji, zgodnej z rekomendacjami i badaniami międzynarodowymi. Istotne jest zachęcanie do realizowania wspólnych projektów szkolnych poświęconych cyberbezpieczeństwu, jak również brania udziału w wydarzeniach o tej tematyce.

8.1.2 INNE ZADNIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

W kwestii bezpieczeństwa teleinformatycznego systemów wewnętrznych Ministerstwa Edukacji Narodowej, jak i systemów publicznie dostępnych (w tym Systemu Informacji Oświatowej i Krajowego Systemu Danych Oświatowych), i dla części systemów Ośrodka Rozwoju Edukacji oraz Centralnej Komisji Egzaminacyjnej Centrum Informatyczne Edukacji zrealizowało 1246 zadań związanych z cyberbezpeczeństwem. Zadania te dotyczyły bieżącego zapewnienia bezpieczeństwa oraz podniesienia poziomu cyberbezpieczeństwa w systemach utrzymywanych i nadzorowanych przez CIE. Nadzór nad

[15] Uchwała nr 98 Rady Ministrów w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji" z dnia 12 września 2024 r. (M.P. z 2024 r. poz. 812)

realizacją zadań realizowany był w sposób ciągły. W 2024 roku organizacja utworzyła także plan szkoleń pracowników celem stałego podnoszenia kwalifikacji kadry pracowniczej.

8.1.3 WNIOSKI I REKOMENDACJE

Konieczne jest opracowanie i realizacja programu powszechnych szkoleń koordynowanych i stworzonych cyfrowo przez odpowiednie instytucje, np. NASK i dostępnych dla wszystkich z koniecznością periodycznej aktualizacji mikropoświadczeń, dotyczących następujących tematów:

1. Bezpieczne korzystanie z informacji: uzyskiwanie dostępu do różnego rodzaju mediów, udostępnianie treści medialnych, tworzenie komunikacji w różnych kontekstach, świadomość znaczenia komunikatów niewerbalnych.
2. Reagowanie na treści szkodliwe i stosowanie narzędzi zapobiegających dostępowi do nich.
3. Przeciwdziałanie dezinformacji: rozróżnianie informacji celowo fałszywych i szkodzących od wprowadzających w błąd w wyniku nieświadomego rozpowszechniania, postępowanie z treściami nieprawdziwymi lub wprowadzającymi w błąd, znajomość sposobów prostowania i wyjaśniania już przedstawionych informacji.
4. Ochrona danych osobowych: zwiększenie świadomości dotyczącej zbierania i przetwarzania danych osobowych, w tym danych szczególnych kategorii i danych behawioralnych, profilowania, przez aplikacje w Internecie i na telefonach komórkowych, rozpoznawania phishingu.
5. Znajomość metod oceny i wiarygodności informacji przez porównywanie niezależnych źródeł, ocenę aktualności informacji, ocenę intencji autora. Znajomość zasad działania trolli i innych zjawisk modyfikowania informacji w mediach np. cheapfake, deepfake.
6. Przepisy prawa i zasady bezpieczeństwa dotyczące zasobów edukacyjnych i urządzeń cyfrowych: wiedza o ochronie produktów i usług prawami autorskimi, prawo autorskie i regulacje prawne dotyczące ochrony własności intelektualnej, normy etyczne dotyczące korzystania z cudzych i własnych materiałów elektronicznych i aplikacji, zasady działania oprogramowania ransomware, podstawowe możliwości zabezpieczania systemu operacyjnego i pracy w sieci przed niepożądanymi działaniami osób trzecich, możliwości szyfrowania informacji i stosowania podpisu elektronicznego, korzystanie z VPN.

8.2 MINISTERSTWO SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (MSWIA)

8.2.1 OPIS NAJWAŻNIEJSZYCH REALIZOWANYCH DZIAŁAŃ DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W OBSZARZE ODPOWIEDZIALNOŚCI MINISTRA SWIA

Kluczowym elementem zapewnienia sprawnego funkcjonowania organów władzy i administracji publicznej oraz bezpieczeństwa państwa i jego obywateli są systemy teleinformatyczne, stanowiące integralną część infrastruktury krytycznej. Poprzez odpowiednie ich działanie możliwe jest skuteczne wykonywanie zadań, gwarantowanie bezpieczeństwa życia i zdrowia obywateli oraz ochrona wszelkich dóbr środowiskowych i finansowych. Należy również pamiętać, że bezpieczeństwo infrastruktury krytycznej państwa zależy nie tylko od prawidłowego funkcjonowania systemów teleinformatycznych, ale także od zasobów ludzkich i kadrowych. Sprawność działania całej infrastruktury opiera się bowiem na pracy odpowiednio wykwalifikowanych pracowników, którzy rozumieją swoje obowiązki i są właściwie przeszkoleni do wykonywania swoich zadań. Z uwagi na powyższe niezwykle istotne jest zapewnienie, aby wykonawcy oraz użytkownicy systemów teleinformatycznych posiadali niezbędne kwalifikacje oraz rozumieli swoje obowiązki. Ponadto, ważne jest zminimalizowanie ryzyka kradzieży, naruszenia oraz niewłaściwego użytkowania urządzeń teleinformatycznych, co stanowi kluczowy element zapewnienia integralności i bezpieczeństwa infrastruktury krytycznej.

Ministerstwo Spraw Wewnętrznych i Administracji oraz organy, a także jednostki organizacyjne podległe lub nadzorowane przez Ministra SWiA sukcesywnie rozwijają się w zakresie transformacji cyfrowej i informatycznej wysoko stawiając zagadnienia dotyczące cyberbezpieczeństwa, w tym cyberodporności oraz zapewniania ciągłości działania usług. W ramach podstawowych aktywów resortu MSWiA w obszarze zasobów teleinformatycznych znajdują się różnorodne technologicznie systemy informacyjne, systemy użytkowane przez inne organy władzy i administracji publicznej, systemy teletransmisyjne, umożliwiające wymianę informacji oraz systemy telekomutacyjne i łączności bezprzewodowej. Powyższe aktywa odgrywają istotną rolę w realizacji zadań zarówno przez MSWiA, jak i przez podległe mu służby odpowiedzialne za bezpieczeństwo obywateli i utrzymanie porządku publicznego. Wskazane systemy te stanowią nieodłączną część infrastruktury krytycznej w obszarze ochrony bezpieczeństwa publicznego, granic, ochrony przeciwpożarowej oraz bezpieczeństwa państwa.

Ministerstwo Spraw Wewnętrznych i Administracji oraz służby podległe Ministrowi SWiA, w ramach swoich struktur, utworzyły zespoły monitorujące wykorzystywaną infrastrukturę teleinformatyczną, a także, realizują zadania wynikające UKSC, dotyczące m.in.: zarządzania incydentami cyberbezpieczeństwa, zgłaszania zidentyfikowanych incydentów do właściwego zespołu CSIRT oraz zapewnienia obsługi incydentów we współpracy z właściwym zespołem CSIRT.

8.2.1.1 DZIAŁANIA REALIZOWANE PRZEZ MSWIA

Infrastruktura teleinformatyczna MSWiA podlega ochronie realizowanej przez CSIRT GOV. Ministerstwo Spraw Wewnętrznych i Administracji nie posiada własnego SOC (Zespół Security Operations Center). Za bezpieczeństwo elementów infrastruktury krytycznej w MSWiA (GovNet, OST 112[16], TESTA-ng[17]) odpowiada Departament Teleinformatyki w MSWiA. W ramach stałej współpracy z CSIRT GOV, MSWiA aktywnie korzysta z ostrzeżeń generowanych przez utrzymywany przez ABW system ARAKIS-GOV[18] .

Dodatkowo, wdrażane są otrzymywane na bieżąco rekomendacje i zalecenia w zakresie zagadnień organizacyjnych i technicznych z obszaru cyberbezpieczeństwa. Tematyka ww. ostrzeżeń obejmuje zarówno informacje o podatnościach w oprogramowaniu, konieczności blokowania szkodliwych adresów IP, analizie aktywności sieciowej, jak i kampanie phishingowe. Ministerstwo Spraw Wewnętrznych i Administracji korzysta również z wykonywanej przez ABW oceny bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa, realizowanej na podstawie art. 32a ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Ponadto, przedstawiciele MSWiA biorą udział w cyklicznych spotkaniach organizowanych przez RCB przy wykorzystaniu systemu PCOC.

Ciągła dostępność procesów w obszarze sprawy wewnętrzne i administracja publiczna obecnie w coraz większym stopniu zależy od wsparcia IT (Information Technology). Wymaga to odpowiednich środków bezpieczeństwa i odporności w celu zapewnienia wsparcia cyklu życia systemów IT. W MSWiA obowiązują procedury cyberbezpieczeństwa opisane w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Zapewniona jest ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Istnieją mechanizmy zabezpieczania informacji w sposób uniemożliwiający osobie nieuprawnionej ujawnienie, modyfikacje, usunięcie lub zniszczenie ww. informacji. Zapisy w zawieranych umowach serwisowych ze stronami trzecimi (m.in.: dostawcami sprzętu i oprogramowania na potrzeby realizacji projektów wdrożeniowych), gwarantują odpowiedni poziom bezpieczeństwa informacji. Ustalone zostały również zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. Okresowo zapewniany jest audyt wewnętrzny w zakresie bezpieczeństwa informacji, w tym dotyczący nowo wdrażanych systemów/sieci.

W MSWiA powołany został Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni MSWiA odpowiadający m.in. za monitorowanie stanu bezpieczeństwa sieci i systemów teleinformatycznych, monitorowanie i gromadzenie dostępnych informacji o zagrożeniach cybernetycznych, szacowanie ryzyka w obszarze bezpieczeństwa informacji i cyberbezpieczeństwa, opiniowanie procedur reagowania na incydenty, inicjowanie i koordynowanie zadań w zakresie cyberbezpieczeństwa, w tym inicjowanie szkoleń i upowszechnianie wiedzy z zakresu bezpieczeństwa cyberprzestrzeni, oraz współpracę z organami, a także jednostkami organizacyjnymi podległymi lub nadzorowanymi przez Ministra SWiA.

Ministerstwo Spraw Wewnętrznych i Administracji odpowiada za cyberbezpieczeństwo infrastruktury telekomunikacyjnej, zapewniającej niezawodną i bezpieczną transmisję danych (fizyczna separacja od internetu) i wykorzystywanej na potrzeby świadczenia usług dla klientów wchodzących w skład administracji rządowej (GovNet); ogólnopolską platformę teletransmisyjną wykorzystywaną przez służby bezpieczeństwa i porządku publicznego oraz ratownictwa (OST 112); a także infrastrukturę umożliwiającą przesyłanie danych i realizację usług między interesariuszami europejskimi, tj. Komisją Europejską, agencjami i instytucjami europejskimi oraz administracjami Państw Członkowskich UE (TESTA-ng). W MSWiA umiejscowiony jest *Crisis Manager*, który w nagłych przypadkach może podejmować decyzje na poziomie operacyjnym w kwestiach bezpieczeństwa ww. sieci na poziomie

[16] Ogólnopolska Sieć Teleinformatyczna.

[17] Trans-European Services for Telematics between Administrations – New Generation.

[18] System powstał we współpracy Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz NASK. Wspiera ochronę zasobów teleinformatycznych administracji publicznej i stanowi uzupełnienie standardowych systemów ochrony sieci takich jak firewall, antywirus czy IDS/IPS

krajowym. Obszar ten objęty jest także zainteresowaniem w ramach Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (JHA). Rada JHA, której członkami są unijni ministrowie spraw wewnętrznych, czuwa nad współpracą i wspólną polityką w kwestiach transgranicznych, rozwijając unijną przestrzeń wolności, bezpieczeństwa i sprawiedliwości. W Radzie JHA Polskę reprezentuje Minister SWiA.

W kompetencji ministra właściwego do spraw wewnętrznych pozostaje wykonywanie działalności telekomunikacyjnej w odniesieniu do sieci telekomunikacyjnej eksploatowanej przez MSWiA na potrzeby Kancelarii Prezydenta RP, Kancelarii Sejmu RP, Kancelarii Senatu RP i administracji rządowej poprzez zapewnienie bezpiecznej łączności rządowej. Do ww. celu wykorzystuje Sieć Łączności Rządowej (SŁR), zarządzaną i administrowaną przez Ministra SWiA, w porozumieniu z Szefem ABW. W przedmiotowej sieci świadczone są, dla osób funkcyjnych oraz organów terenowych na poziomie województw, usługi telekomunikacyjne SŁR-J (jawna), a także SŁR-N (niejawna). Wspomniane usługi są pomocne w bieżącej pracy oraz we wszystkich stanach gotowości państwa, w tym sytuacjach kryzysowych.

Stały rozwój sieci GovNet oraz zwiększająca się jej rola w zaspokajaniu potrzeb sektora rządowego w obszarze zagwarantowania dostępu do usług teleinformatycznych ma kluczowe znaczenie dla zapewnienia bezpieczeństwa państwa oraz skutecznej realizacji statutowych zadań administracji publicznej. Potrzeby sektora rządowego obejmują nie tylko kwestie komunikacyjne, ale także wymagania dotyczące bezpieczeństwa, wydajności i niezawodności. Wraz z rosnącą rolą sieci GovNet, konieczne było zapewnienie odpowiedniego poziomu skalowalności. Obecnie GovNet posiada 345 węzłów powiatowych oraz 17 węzłów szkieletowych (agregacyjnych). Umożliwia to dostęp urzędów publicznych obsługujących obywateli do kluczowych usług udostępnianych przez sieć GovNet m.in. Systemu Rejestrów Państwowych (SRP), Centralnej Ewidencji Pojazdów i Kierowców (CEPiK), wideokonferencji, telefonii tradycyjnej i VoIP (*Voice over Internet Protocol*). W celu nadzoru nad siecią wdrożony został dedykowany system do zarządzania i monitorowania sieci oraz system do paszportyzacji sieci. Ze względu na krytyczny charakter sieci oraz jej znaczenie dla bezpieczeństwa zarówno pod względem infrastruktury, jak i świadczonych za jej pośrednictwem usług, w ramach projektu przygotowane zostały plany ciągłości działania. Na arenie krajowej sieć GovNet pełni rolę transportową dla TESTA-ng, co oznacza, że jej nieprawidłowe działanie może zakłócić współpracę między państwami członkowskimi. Dla zapewnienia maksymalnego bezpieczeństwa wykorzystuje solidne szyfrowanie przy użyciu certyfikowanych urządzeń szyfrujących. W celu ochrony przed zagrożeniami oraz zapewnienia cyberbezpieczeństwa, w tym również bezpieczeństwa danych wymienianych przy jej użyciu, jest ona odpowiednio zarządzana i podlega kontroli. Stały monitoring cyberbezpieczeństwa zasobów odbywa się z wykorzystaniem posiadanych systemów monitorowania.

Ogólnopolska Sieć Teleinformatyczna (OST 112) stanowi jednolitą, ogólnopolską infrastrukturę teletransmisyjną, która została zaprojektowana w oparciu o technologię MPLS. Sieć ta jest wykorzystywana przez służby bezpieczeństwa i porządku publicznego oraz służby ratownictwa, a także inne organy administracji państwowej do komunikacji głosowej, transmisji danych i wideo. Sieć OST 112 działająca na potrzeby obsługi numeru alarmowego 112, to infrastruktura komunikacyjna, niezbędna do sprawnej obsługi wywołań na numer 112 i inne połączenia alarmowe oraz komunikacji pomiędzy służbami odpowiedzialnymi za ratownictwo i bezpieczeństwo publiczne. OST 112 obejmuje ponad 900 lokalizacji istotnych z punktu widzenia funkcjonowania Systemu Powiadamiania Ratunkowego, takich jak: komendy policji, jednostki straży pożarnej, urzędy wojewódzkie. Infrastruktura ta, pomimo że działa na protokołach internetowych, jest jednak całkowicie odizolowana od publicznego internetu. OST112 to infrastruktura, z której korzystają najważniejsze systemy odpowiadające za bezpieczeństwo Polaków, m.in. numer alarmowy 112, System Rejestrów Państwowych (zawiera kluczowe dane polskich obywateli) czy Centralna Ewidencja Pojazdów i Kierowców (CEPiK).

W Polsce działają końcówki krajowe systemów teleinformatycznych administracji publicznej obejmujących całą Strefę Schengen. Nazywane są one wielkoskalowymi systemami informacyjnymi Unii Europejskiej (WSIUE). Infrastruktura komunikacyjna WSIUE wykorzystuje sieć TESTA-ng, która zapewnia sieć szkieletową oddzieloną od publicznego internetu. TESTA-ng jest preferowanym rozwiązaniem dla paneuropejskiej wymiany informacji między administracjami. W ramach tej sieci istnieje komunikacja pomiędzy ministerstwami, jednostkami organizacyjnymi Policji, Straży Granicznej, Państwowej Straży Pożarnej, agencji wywiadowczych i bezpieczeństwa oraz wojska. Wymiana danych przez interfejs komunikacyjny systemów teleinformatycznych sieci TESTA-ng umożliwia dostęp do danych

udostępnianych przez inne kraje członkowskie UE oraz kraje stowarzyszone. Infrastruktura TESTA-ng umożliwia wymianę informacji niejawnych UE do poziomu „RESTREINT UE/EU Restricted".

8.2.1.2 DZIAŁANIA REALIZOWANE PRZEZ POLICJĘ

Informacje dot. działalności policji w cyberprzestrzeni, w tym działań Komendy Głównej Policji oraz Centralnego Biura Zwalczania Cyberprzestępczości zostały zawarte w rozdziałach KGP oraz CBZC.

8.2.1.3 DZIAŁANIA REALIZOWANE PRZEZ STRAŻ GRANICZNĄ

Straż Graniczna wykorzystuje szereg systemów teleinformatycznych do kontroli ruchu granicznego, wsparcia procesu dowodzenia, zarządzania procedurami administracyjnymi wobec cudzoziemców oraz przeciwdziałania poważnym przestępstwom i terroryzmowi. Powyższe obejmuje w większości autorskie rozwiązania stworzone przez funkcjonariuszy i pracowników SG, bez udziału firm trzecich. Spośród zasobów osobowych SG został stworzony zespół inżynierów, którego członkowie własnymi siłami projektują, tworzą, wdrażają i utrzymują kluczowe systemy SG. Przyjęta koncepcja pozwala na znaczne zmniejszenie kosztów budowy i rozwoju systemów, elastyczne i szybkie dostosowywanie do zmieniającego się otoczenia prawnego, wkomponowanie mechanizmów bezpieczeństwa już na etapie tworzenia aplikacji.

W celu realizacji powyższych zamierzeń Biuro Łączności i Informatyki Komendy Głównej SG [19] koncentruje się na dążeniu do utrzymania wysokiej sprawności systemów teleinformatycznych, umożliwiających nieprzerwany dostęp do baz danych, wykorzystywanych przy realizacji zadań ustawowych przez funkcjonariuszy na terenie całego kraju w warunkach operacyjnych. Utrzymanie wysokiej dostępności systemów w dobie zagrożeń z cyberprzestrzeni wymaga zapewnienia ich odporności. Powyższe ma istotne znacznie, gdyż systemy SG muszą spełniać paradygmaty, które podnoszą ryzyko ataku z cyberprzestrzeni:

- Mobilność i dostęp do baz danych w tym do informacji z baz niejawnych musi być zapewniony m.in. przez sieci telefonii komórkowej;
- otwartość na podmioty komercyjne - systemy SG muszą w celu właściwego funkcjonowania posiadać dostęp do zasobów dostępnych poprzez sieć internet, takich jak np. dane z systemów rezerwacyjnych na potrzeby systemu KSI PNR (krajowy system informacji o pasażerach), a jednocześnie komunikować się z niejawnymi systemami służb bezpieczeństwa i porządku publicznego;
- atrakcyjność informacji dla potencjalnych cyberprzestępców – SG gromadzi oraz udostępnia służbom bezpieczeństwa i porządku publicznego dane w tym dane biometryczne ze zbiorów liczone w setek milionów rekordów;
- cyfrowe usługi dla obywateli krajów trzecich – w ramach systemu ETIAS [20] oraz narzędzi interoperacyjności konieczne będzie zapewnienie dostępu dla cudzoziemców do usług związanych z ich obsługą.

Obszar cyberbezpieczeństwa SG objęty został kompleksowym systemem o nazwie KORUND. Przedmiotowy system obejmuje strukturę monitorowania, reagowania i ochrony przez cyberzagrożeniami. System wkomponował się w „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022"[21] , a następnie w działania na rzecz wdrożenia „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024"[8]. System cyberbezpieczeństwa KORUND stanowi zewnętrzną barierę ochronną dla strategicznych aplikacji budowanych samodzielnie przez SG w ramach Centralnych Systemów Informatycznych SG (CSI SG), które zgodnie z przyjętą

[19] Dalej: „BŁiI"

[20] Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) – warunek wjazdu wprowadzony przez UE dla obywateli zwolnionych z obowiązku wizowego, podróżujących do strefy Schengen oraz Bułgarii, Cypru i Rumunii.

[21] https://www.gov.pl/web/cyfryzacja/krajowe-ramy-polityki-cyberbezpieczenstwa
http://www.dziennikustaw.gov.pl/MP/rok/2019/pozycja/1037 [9] Dz. Urz. KGSG 2015.96.

koncepcją tzw. *security by design* (bezpieczeństwo na etapie projektowania), są zabezpieczane na każdym etapie od koncepcji do wdrożenia. Przedmiotowa kwestia ma kluczowe znaczenie w kontekście budowanych systemów wielkoskalowych takich jak Entry/Exit, ETIAS czy narzędzia interoperacyjności oraz KSI PNR, gdyż SG, przetwarzając duże ilości danych sensytywnych, jak np. dane biometryczne, staje się coraz częściej celem ataków. Dodatkowo, w ramach ww. przedsięwzięcia, w celu zapewnienia metodycznego podejścia do cyberbezpieczeństwa, został wdrożony System Zarządzania Bezpieczeństwem Informacji i Usługami IT, w ramach którego są implementowane i aktualizowane na bieżąco polityki, procedury i instrukcje, mające na celu poprawę bezpieczeństwa informacji w SG.

Uwzględniając fakt, że wektory ataków ewoluują, dalsze działania będą się opierały na rozwoju i utrzymaniu funkcjonujących usług cyberbezpieczeństwa systemu KORUND oraz utrzymaniu niezbędnej kadry technicznej. Konieczne będzie również dalsze zapewnianie redundancji kluczowych elementów infrastruktury teleinformatycznej i uruchamianie zapasowych ośrodków przetwarzania danych, a także wykorzystanie rozwiązań opartych o sztuczną inteligencję do wykrywania cyberataków opartych na analizie przepływów sieciowych, tzw. poligon doświadczalny symulujący cyberataki w warunkach zbliżonych do rzeczywistych czy mechanizmy przeszukiwania sieci anonimowych, celem pozyskania informacji o planowanych atakach na infrastrukturę.

Mając na względzie wyzwania stojące przed SG w zakresie zapewnienia odporności systemów, jak również doświadczenia wynikające z aneksji Krymu, polegające na destabilizacji infrastruktury krytycznej cyberatakami towarzyszącymi działaniom zbrojnym, Decyzją Komendanta Głównego SG (KG SG), z 22 grudnia 2015 r.[9] powołany został Komitet do spraw Bezpieczeństwa Teleinformatycznego SG oraz Zespół Security Operations Center SG (SOC SG), który realizuje zadania wskazane w regulacjach ustawowych. Do zadań SOC SG, poza obsługą incydentów i zarządzaniem nimi, należy również wymiana informacji z CSIRT-ami oraz odpowiednie reagowanie w sytuacji potencjalnego lub zaistniałego zagrożenia.

Zespół działa na terenie całego kraju i jest nadzorowany przez dyrektora BŁiI. Współpraca MSWiA oraz SG koncentruje się na kwestiach związanych ze strategią cyberbepieczeństwa oraz wymianą doświadczeń w realizowanych projektach.

8.2.1.4 DZIAŁANIA REALIZOWANE PRZEZ PAŃSTWOWĄ STRAŻ POŻARNĄ

Państwowa Straż Pożarna (PSP) pełni istotną funkcję w systemie bezpieczeństwa Państwa. W celu zwiększenia cyberbezpieczeństwa w zakresie usług i infrastruktury krytycznej oraz bezpieczeństwa informacji przetwarzanych w ramach posiadanych systemów, w Komendzie Głównej PSP (KG PSP) przygotowano projekt wdrożenia Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji. W tym celu został powołany zespół do opracowania założeń i dostosowania istniejących dokumentów w KG PSP do obowiązujących przepisów prawa oraz normy PN-ISO 27001.

Komenda Główna Państwowej Straży Pożarnej prowadzi działania, mające na celu bezpieczne użytkowanie środowiska teleinformatycznego. Powyższe realizowane jest poprzez wykorzystanie nowoczesnych systemów bezpieczeństwa oraz bieżącą współpracę z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. Biuro Informatyki i Łączności KG PSP na bieżąco wymienia informacje w zakresie rozpoznawania, zapobiegania i wykrywania zagrożeń godzących w bezpieczeństwo, istotnych dla bezpiecznego korzystania z cyberprzestrzeni. Jednocześnie KG PSP bierze czynny udział w ramach systemu wczesnego ostrzegania o zagrożeniach w Internecie pn. ARAKIS-GOV.

Zespół CERT KG PSP regularnie prowadzi akcje informacyjne wśród pracowników oraz podległych jednostek. Ponadto, w KG PSP w intranecie aktualizowane są artykuły związane z cyberbezpieczeństwem.

Wszystkie umowy świadczone na rzecz KG PSP, realizowane w 2023 r. przez podmioty zewnętrzne, które odnosiły się do infrastruktury krytycznej, posiadały Instrukcję Bezpieczeństwa, stanowiącą zbiór wymagań organizacyjnych i technicznych, jakie muszą być spełnione podczas realizacji przedmiotowych umów.

W KG PSP wykonywane były okresowo audyty i skanowanie sieci narzędziami wykrywającymi potencjalne luki w zabezpieczeniach oraz wykrywającymi podatności i błędy konfiguracji. Wybiórczo

audytom poddawana była konfiguracja systemów teleinformatycznych funkcjonujących w KG PSP. Przeprowadzona została również weryfikacja realizacji zadań w związku z wprowadzeniem stopni alarmowych i stopni alarmowych CRP, w ramach ustawy z dnia 10 czerwca 2016 r. o działaniach antyterorrystyczych[22] w zakresie kompetencji KG PSP. Ponadto, została przeprowadzona kontrola wewnętrzna „Sprawdzenie realizacji zaleceń i wniosków z kontroli nt. Działania systemów teleinformatycznych używanych do realizacji zadań publicznych".

8.2.1.5 DZIAŁANIA REALIZOWANE PRZEZ SŁUŻBĘ OCHRONY PAŃSTWA

Służba Ochrony Państwa (SOP) sukcesywnie rozwija swoje systemy teleinformatyczne, w tym niejawne. Powyższe wiąże się nie tylko z kwestiami technicznymi i infrastrukturalnymi, ale także przeszkoleniem pracowników i zapewnieniem odpowiedniej kadry administrującej nimi.

8.2.2 WNIOSKI I REKOMENDACJE

W opinii MSWiA, w zakresie cyberbezpieczeństwa istotne są trzy główne wyzwania. Po pierwsze, ochrona infrastruktury krytycznej, gdzie kluczowe elementy, takie jak elektrownie, sieci energetyczne, systemy transportowe i usługi zdrowotne, są narażone na cyberataki, które mogą zakłócić dostawy energii, komunikację czy opiekę zdrowotną. Po drugie, obrona cyberprzestrzeni, aby chronić zdolność państwa do zapewnienia bezpieczeństwa narodowego przed wrogimi działaniami w cyberprzestrzeni. Po trzecie, konieczność radzenia sobie zarówno z zagrożeniami zewnętrznymi, wynikającymi z działań państw obcych, jak i zagrożeniami wewnętrznymi, czyli atakami przeprowadzanymi przez grupy przestępcze lub osoby prywatne. W obliczu tych wyzwań, należy skoncentrować się na rozwijaniu skutecznych strategii cyberbezpieczeństwa. Wprowadzenie nowoczesnych technologii, takich jak sztuczna inteligencja i analiza big data, może umożliwić szybkie wykrywanie i reagowanie na zagrożenia. Współpraca międzyinstytucjonalna oraz partnerstwo z sektorem prywatnym i instytucjami badawczymi są kluczowe dla wymiany wiedzy i doświadczeń w dziedzinie cyberbezpieczeństwa. Ponadto, kontynuacja inwestycji w szkolenia pracowników w zakresie cyberbezpieczeństwa jest niezbędna, aby podnosić poziom świadomości i umiejętności w tym obszarze.

8.2.2.1 ZAPEWNIENIE ODPOWIEDNICH ZASOBÓW DLA CYBERBEZPIECZEŃSTWA

W sektorze publicznym gromadzi się znaczne ilości danych wrażliwych, takich jak dane osobowe obywateli, informacje rządowe i związane z bezpieczeństwem narodowym. Ataki cybernetyczne, które prowadzą do wycieku lub utraty takich danych, mogą wywołać poważne konsekwencje, takie jak naruszenie prywatności, oszustwa finansowe i inne przestępstwa związane z danymi osobowymi. Kwestią kluczową jest zapewnienie odpowiednich zasobów kadrowych, w aspekcie ilościowym i jakościowym, dla podmiotów publicznych. Obserwowane są również stale rosnące, niekiedy wyjątkowo dynamicznie, koszty zakupu, utrzymania i rozbudowy infrastruktury bezpieczeństwa, co stanowi istotne obciążenie dla budżetu instytucji państwowych.

Dotychczas obserwowane problemy z zatrudnianiem do Ministerstwa wykwalifikowanej kadry na kluczowych dla bezpieczeństwa zasobów stanowiskach, a także znaczące obciążenie licznymi obowiązkami dotychczasowej kadry może doprowadzić do przełamania przyjętej linii obrony cybernetycznej. Niestabilna sytuacja geopolityczna, w szczególności związana z konfliktem za wschodnią granicą kraju, stale rosnąca liczba systemów obsługiwana przez coraz mniejszą liczbę administratorów IT oraz nieadekwatne do potrzeb zasoby finansowe na zakup i modernizację kluczowych narzędzi informatycznych służących bezpieczeństwu mogą mieć poważne konsekwencje nie tylko w zakresie bezpieczeństwa aktywów MSWiA, ale również w wymiarze narodowym. Stale rosnące, niekiedy wyjątkowo dynamicznie, koszty zakupu, utrzymania i rozbudowy infrastruktury bezpieczeństwa są trudne do udźwignięcia przez poszczególne jednostki sektora finansów publicznych, w tym przez Ministerstwo, znacząco obciążając tym samym budżet Skarbu Państwa. Zasadnym zatem w ocenie

[22] Dz.U. z 2024 r. poz. 92.

MSWiA wydaje się podjęcie na forum międzyresortowym dyskusji w zakresie oceny możliwości zminimalizowania powyższych ryzyk i wypracowania kompleksowych rozwiązań, które długofalowo zapewnią rozwiązanie powyższych problemów oraz podjęcia ewentualnych decyzji w zakresie wydzielenia przez podmioty wchodzące w skład KSC osobnego budżetu przeznaczonego na cele związane z cyberbezpieczeństwem.

W odniesieniu do ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, proponuje się zwrócić uwagę, że ustawa ograniczyła odpływ specjalistów ds. cyberbezpieczeństwa z sektora publicznego, natomiast nie przyczyniła się w istotny sposób do wzrostu zatrudnienia specjalistów cyberbezpieczeństwa w sektorze publicznym. W opinii MSWiA, obecne zatrudnienie osób realizujących zadania z zakresu cyberbezpieczeństwa, zwłaszcza w zakresie wysokokwalifikowanych specjalistów w sektorze publicznym, jest niewystarczające co było sygnalizowane w wielu raportach. Należy zatem tak zmodyfikować powyższą ustawę (lub stworzyć nowe rozwiązania) aby umożliwiła realne konkurowanie na rynku pracy podmiotów z sektora publicznego z sektorem prywatnym. Obecnie ustawa nie gwarantuje otrzymania dodatku przez podmiot w kolejnych latach co pośrednio utrudnia złożenie konkurencyjnej oferty pracy przez podmiot publiczny. Niedobór wysoko wykwalifikowanych specjalistów w sektorze publicznym ma duży niekorzystny wpływ na realne bezpieczeństwo.

8.2.2.2 OCHRONA INFORMACJI O INFRASTRUKTURZE KRYTYCZNEJ

UKE, w związku z implementacją w Polskim prawie postanowień dyrektywy Parlamentu Europejskiego i Rady, nr 2014/61/UE z dnia 15 maja 2014 r. w sprawie środków mających na celu zmniejszenie kosztów realizacji szybkich sieci łączności elektronicznej [23] realizuje tzw. „*Punkt informacyjny do spraw telekomunikacji*" (PIT), będący system informatycznym działającym w sieci internet. System ten, współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, polega na prezentacji w sieci internet, interaktywnego serwisu mapowego zawierającego komplet danych zebranych podczas opisanych powyżej inwentaryzacji. W efekcie, publicznie prezentowana może być kompletna informacja dotycząca uzbrojenia teletechnicznego (infrastruktura techniczna i kanały technologiczne) wszystkich obiektów, w tym także obiektów kwalifikujących się do kategorii infrastruktury krytycznej (IK)[24].

Prezentacja szczegółowych informacji, takich jak sieci telekomunikacyjne czy kanały techniczne, a dotyczących obiektów IK w serwisach mapowych, może ułatwić identyfikację takich obiektów i sprzyjać potencjalnym zagrożeniom, w tym ułatwiać planowanie ataków terrorystycznych lub działań sabotażowych agentom obcych państw. Posiadając takie informacje, mogą oni potencjalnie zidentyfikować najbardziej krytyczne punkty i wykorzystać je w celu destabilizacji kraju. Może to także sprzyjać atakom cybernetycznym, ponieważ przestępcy mogą wykorzystać te informacje do celowanego ataku na ważne węzły komunikacyjne lub infrastrukturę sieciową.

Wydaje się, że najprostszym rozwiązaniem problemu jest zastosowanie podejścia opartego na klasyfikacji obiektów IK oraz reglamentacji informacji na ich temat, w taki sposób, by to tylko uprawnione osoby lub instytucje/organy mogły mieć dostęp do pełnych danych w celu zapewnienia bezpieczeństwa narodowego i ochrony infrastruktury. Rozwiązaniem może być powołanie międzyresortowego zespołu mającego na celu dokonanie klasyfikacji takich obiektów pod kątem identyfikacji obiektów kluczowych, które wymagają szczególnej ochrony oraz opracowywanie zasad identyfikacji krytyczności takich obiektów.

[23] https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=celex:32014L0061

[24] Przykład mapy dla okolic ul. Batorego w serwisie mapowym UKE Punkt Informacyjny ds. Telekomunikacji

8.2.2.3 BRAK UMOCOWAŃ DLA USŁUG CHMUROWYCH W ZAKRESIE INFORMACJI KLAUZULOWANYCH

Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. *w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”*[25] wprowadziła do obiegu pojęcia korzystania z usług przetwarzania w Rządowej Chmurze Obliczeniowej (RChO) lub w Publicznych Chmurach Obliczeniowych (PChO).

Wątpliwość budzą plany związane z zastosowaniem chmury do przetwarzania informacji niejawnych. Należy zauważyć, iż pomimo tego, że ustawa o ochronie informacji niejawnych[26] nie wyklucza wprost zastosowania rozwiązań chmurowych, to już spełnienie wymagań określonych w aktach wykonawczych mi.in. w zakresie oznaczania informatycznych nośników danych, konieczności zorganizowania stref ochronnych lub wymagań określonych w zaleceniach wydanych ma mocy art. 52 ww. ustawy m.in. w zakresie ochrony elektromagnetycznej, mogą utrudniać lub w niektórych przypadkach uniemożliwiać takie działanie. Obawy także dotyczą następujących kwestii: ryzyka braku dostępu do zasobów w przypadku awarii systemów lub infrastruktury, możliwości nieuprawnionego dostępu do systemów przez osoby trzecie na skutek błędów programistycznych czy także trudności związanych z lokalizacją fizyczną tych systemów. We wszystkich powyższych wątpliwościach zwracam uwagę na fakt, że rozwiązania chmurowe do przetwarzania informacji niejawnych nie gwarantują bezpieczeństwa tych informacji, a tym samym zwiększa się ryzyko wystąpienia incydentów bezpieczeństwa związanych z niekontrolowanym wypływem informacji niejawnych.

8.2.2.4 POWSZECHNE WYKORZYSTYWANIE ROZWIĄZAŃ CHMUROWYCH (CLOUD)

W ostatnich kilku latach zauważalne stało się szybkie przechodzenie podmiotów z lokalnej infrastruktury na rozwiązania oparte na chmurze. Podmioty coraz częściej dostrzegają zalety związane z chmurą obliczeniową: poprawę skalowalności i efektywności kosztowej, optymalizację procesów biznesowych, zwiększenie operacyjności biznesowej i automatyzacji zadań. Rozwiązania chmurowe zapewniają uniwersalny, wygodny i szybki dostęp do wspólnych zasobów IT (m.in. dostęp do różnych sieci, baz danych, aplikacji i usług), wymagający tylko minimalnego poziomu zarządzania czy interakcji z dostawcą.

Niezależnie od niewątpliwych korzyści wynikających z wykorzystania rozwiązań cloud’owych, dynamiczny proces migracji danych do chmury niesie ze sobą nowe wyzwania w obszarze cyberbezpieczeństwa. Niekwestionowanym priorytetem musi stać się bezpieczeństwo zasobów lokowanych w chmurze. Wybór niewłaściwego lub niewiarygodnego dostawcy może doprowadzić do wycieku danych, a niekiedy może stać się powodem ich całkowitej utraty. Rozwiązania chmurowe w perspektywie długotrwałego wykorzystania są dość kosztowne. Pomimo stałego postępu w dziedzinie bezpieczeństwa, istnieje dość wysokie ryzyko ataków hakerskich na duże centra przetwarzania danych. Przechowywanie danych, w szczególności danych osobowych rodzi dodatkowe obawy w zakresie prywatności i zgodności z przepisami, chociażby rozporządzenia RODO.

Analizując zagrożenia związane z wykorzystywaniem chmur nie można pominąć jeszcze jednej kwestii: dostawcy różnego oprogramowania, w tym specjalistycznego oprogramowania do prowadzenia analiz bezpieczeństwa infrastruktury informatycznej, coraz częściej udostępniają systemy oparte wyłącznie na chmurze lub wykorzystujące elementy takich rozwiązań. Prowadzi do niepokojącego spostrzeżenia, że korzystanie chociażby przez właścicieli elementów infrastruktury krytycznej państwa lub operatorów usług kluczowych może doprowadzić do ujawnienia informacji o podatnościach tej istotnej dla bezpieczeństwa państwa infrastruktury podmiotom nieuprawnionym np. dostawcom rozwiązań IT.

Dodatkowym zagadnieniem jest lokalizacja przechowywania danych. Globalni dostawcy chmury często przechowują informacje na serwerach zlokalizowanych poza granicami kraju użytkownika. Może to

[25] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190000862
[26] Dz.U. 2010 nr 182 poz. 1228

oznaczać podleganie obcym przepisom. Np. amerykański *CLOUD Act*[27] pozwala rządowi USA żądać dostępu do danych przechowywanych przez amerykańskie firmy, nawet jeśli znajdują się one w Europie. Jak podkreśla Europejski Inspektor Ochrony Danych[28] podmioty z UE mogą podlegać amerykańskiej ustawie *CLOUD Act*, jeżeli korzystają z usług takich jak usługi internetowe, które mają związek z USA lub mają siedzibę na przykład w USA.

8.2.2.5 WPROWADZENIE SYSTEMÓW AI DO INFRASTRUKTURY BEZPIECZEŃSTWA

Wprowadzenie systemów AI do infrastruktury bezpieczeństwa informatycznego umożliwia szybsze wykrywanie i reagowanie na potencjalne zagrożenia. Przede wszystkim, narzędzia oparte na AI mogą analizować duże ilości danych w czasie rzeczywistym, identyfikując wzorce i anomalie, które mogą wskazywać na ataki lub niebezpieczne zachowania. Dodatkowo, systemy oparte na sztucznej inteligencji mogą dostosowywać się do zmieniających się warunków i nowych rodzajów zagrożeń, co czyni je bardziej elastycznymi i efektywnymi w porównaniu do tradycyjnych metod. Mogą również automatycznie aktualizować strategie obronne w zależności od ewolucji zagrożeń. Inteligentne systemy są również zdolne do szybkiego reagowania na incydenty, ograniczając szkody i minimalizując czas, w jakim złośliwe działania mogą wpływać na systemy informatyczne. Wykorzystanie algorytmów uczenia maszynowego pozwala na budowanie modeli predykcyjnych, które potrafią antycypować potencjalne ataki na podstawie wcześniejszych wzorców. Należy wzmocnić i wspierać prace nad zastosowaniem takich systemów w administracji.

8.2.2.6 URUCHOMIENIE SYSTEMU BEZPIECZNEJ ŁĄCZNOŚCI PAŃSTWOWEJ (SBŁP)

Systemy bezpiecznej wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym konieczne są nie tylko dla zapewnienia cyberbezpieczeństwa w kraju, ale także dla kompleksowego systemu bezpieczeństwa narodowego. Zgodne to jest z zaleceniami odporności NATO, w szczególności z obszarem odporności nr 6 „Odporne Systemy Łączności Cywilnej", którego celem jest zapewnienie stałej dostępności i gwarantowanego dostępu do niezawodnych, bezpiecznych i solidnych usług komunikacyjnych w czasie pokoju, kryzysu i konfliktu, z uwzględnieniem potencjalnych zagrożeń (cybernetycznych, fizycznych, personalnych, hybrydowych, zagrożeń spowodowanych przez człowieka lub naturalnych, pandemii/epidemii, zmian klimatu) przy użyciu nowych technologii.

W roku 2025 realizowane będą prace nad utworzeniem Systemu Bezpiecznej Łączności Państwowej (SBŁP) zapewniającego wymianę informacji pomiędzy organami odpowiedzialnymi za realizację zadań z zakresu zarządzania kryzysowego, bezpieczeństwa państwa, ochrony porządku publicznego, ratownictwa, ochrony ludności i obrony cywilnej. Powstanie SBŁP realizuje zapisy *Rozdziału 8 Wykrywanie zagrożeń, ostrzeganie, powiadamianie i alarmowanie o zagrożeniach oraz System Bezpiecznej Łączności Państwowej* ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej[29], ustanawiającej Ministra właściwego do spraw wewnętrznych operatorem. SBŁP swym zakresem obejmuje jawną (SBŁP-J) i niejawną (SBŁP-N) łączność stacjonarną; infrastrukturę wideokonferencyjną (SBŁP-V); bezpieczną łączność mobilną (SBŁP-M), w tym niejawną łączność komórkową (SBŁP-MN), łączność trankingową (SBŁP-T), łączność radiową (SBŁP-KF) oraz bezpieczną łączność satelitarną (SBŁP-S). Infrastruktura techniczna będąca podstawą SBŁP jest infrastrukturą pozostającą w gestii resortu SWiA. Obejmuje MSWiA oraz organy i jednostki organizacyjne podległe Ministrowi SWiA lub przez niego nadzorowane, w tym KGP, KGPSP, KGSG, SOP, UdSC, CPD MSWiA, ZER MSWiA służby zapewniające bezpieczeństwo wewnętrzne oraz zewnętrzne państwa (ABW, SKW, SWW, MON), oddziałuje także na zapewnienie ciągłości funkcjonowania obiektów wchodzących w skład systemu kierowania bezpieczeństwem narodowym.

[27] Ustawa CLOUD Act (Clifying Lawful Overseas Use of Data Act) została przyjęta przez Kongres Stanów Zjednoczonych Ameryki (USA) 23 marca 2018 r. w celu usprawnienia procedur zarówno dla władz USA, jak i zagranicznych w zakresie uzyskiwania dostępu do danych przechowywanych przez dostawców usług w kontekście dochodzeń karnych.
[28] (https://www.edps.europa.eu/press-publications/publications/newsletters/newsletter96_en#cloud
[29] Dz.U.2024.1907

Bazą SBŁP-J będzie infrastruktura sieci teletransmisyjnej GovNet jako medium zapewniające niezawodną i bezpieczną transmisję danych (fizyczna separacja od internetu). GovNet łączący ministerstwa, urzędy centralne, wojewódzkie pełni rolę transportową w zakresie transmisji danych, ochrony przesyłanych i przetwarzanych danych, w tym danych osobowych, a także umożliwia udostępnianie kluczowych usług, w tym usług działających w dedykowanych sieciach VPN/LAN. Nastąpi rozbudowa infrastruktury sieci GovNet do jednostek/organów administracji rządowej na poziomie gminnym. Bezpośrednimi użytkownikami SBŁP-J będą organy administracji publicznej, urzędy obsługujące te organy oraz jednostki organizacyjne podległe tym organom lub przez nie nadzorowane wykonujące zadania z zakresu bezpieczeństwa państwa, ochrony porządku publicznego, ratownictwa, ochrony ludności i obrony cywilnej oraz zarządzania kryzysowego, powiadamiania, ostrzegania i alarmowania ludności; szpitale resortu SWiA, Zapasowe Miejsca Pracy Wojewodów (w tym Zapasowe Stanowiska Kierowania.

Poprzez rozbudowę sieci GovNet liczba jej węzłów wzrośnie o blisko 2800, co znacznie zwiększy zasięg ustandaryzowanej sieci transportowej na terenie RP oraz dostęp urzędów publicznych obsługujących obywateli do usług udostępnianych przez sieć GovNet. Utworzenie nowych węzłów sieci GovNet pozwoli na połączenie administracji rządowej oraz samorządowej za pomocą jednolitej, i co najważniejsze bezpiecznej, wydzielonej sieci teletransmisyjnej opartej na technologii MPLS. Po zrealizowaniu projektu do rozbudowanej sieci GovNet będą mogły się podłączyć inne instytucje rządowe, pozarządowe oraz samorządowe, jak również będzie możliwość integracji systemów ostrzegania ludności cywilnej o zagrożeniach, co znacząco podniesie bezpieczeństwo obywateli.

GovNet MPLS jako sieć operatorska jest wykorzystywana do zapewnienia komunikacji z zasobami teleinformatycznymi Unii Europejskiej w ramach sieci TESTA-ng. W ramach tej sieci nastąpi uruchomienie usług dla podmiotów administracji krajowej korzystających z systemu wymiany informacji na rynku krajowym IMI[30] Komisji Europejskiej. SBŁP-J pozwoli na połączenie administracji rządowej za pomocą jednolitej i co najważniejsze bezpiecznej, wydzielonej sieci teletransmisyjnej opartej na technologii MPLS. Możliwa będzie integracja systemów ostrzegania ludności cywilnej o zagrożeniach, co znacząco podniesie bezpieczeństwo obywateli.

Sieć Łączności Rządowej (SŁR), będąca elementem infrastruktury krytycznej państwa (na podstawie decyzji Dyrektora Rządowego Centrum Bezpieczeństwa RCB-Z-446/2017) wykorzystywana jest do zapewnienia łączności specjalnej pomiędzy najważniejszymi osobami w państwie (m.in. KPRM, Kancelaria Prezydenta RP, Kancelaria Sejmu RP, Kancelaria Senatu RP, ministerstwa, urzędy obsługujące organy administracji rządowej wykonujące zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności, ochrony granicy, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania infrastruktury krytycznej, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony weterynaryjnej, ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sądownictwa i prokuratury). Sieć ta rozbudowywana będzie jako SBŁP-N. Powstaną komponenty infrastruktury wideokonferencyjnej (SBŁP-V); bezpieczna łączność mobilna (SBŁP-M). Uruchomiony zostanie system telekonferencji dla zarządzania kryzysowego z możliwością użycia mostków dla łączności niejawnej. System umożliwi szyfrowanie „*end-to-end*", zapewniając ochronę przesyłanych danych.

Zbudowany zostanie system niejawnej łączności mobilnej (SBŁP-MN) jako niezawodna, bezpieczna platforma komunikacyjna, dostosowana do specyficznych wymogów operacyjnych i gotowa do pracy w wymagających warunkach. SBŁP-MN stworzy zdolność przekazywania informacji, w tym niejawnych w ramach administracji publicznej. Nastąpi integracja istniejących resortowych, cywilnych i wojskowych, jawnych i niejawnych systemów teleinformatycznych, wspierających zarządzanie kryzysowe oraz wyznaczenie podmiotu wiodącego w tym obszarze. Zapewniona zostanie synergia dla uniknięcia braku kompatybilności wprowadzanych rozwiązań.

[30] Internal Market Information System

Do zasięgu krajowego rozbudowany zostanie system łączności radiowej (SBŁP-T) w oparciu o technologię cyfrową w standardzie TETRA, z szyfrowaniem interfejsu radiowego w standardzie TEA2, z uwzględnieniem szyfrowania „*end-to-end*" z możliwością rozszerzania o rozwiązania hybrydowe, które docelowo pozwolą korzystać także z usług w standardach szerokopasmowych LTE/5G. Rozwiązanie takie zgodnie jest kierunkiem rozwoju wąskopasmowych sieci działających w większości krajów europejskich. Uzupełnieniem będą kanały komunikacyjne zakresu częstotliwości radiowych umożliwiające wymianę wiadomości wykorzystujące propagację fal elektromagnetycznych w kanałach radiowych z wykorzystaniem środków urządzeń radiowych (SBŁP-KF). Medium dopełniającym będzie bezpieczna łączność satelitarna (SBŁP-S) postrzegana jako niezawodne narzędzie komunikacji w zakresie obrony, pomocy humanitarnej i reagowania w sytuacjach kryzysowych, a także jako odporne na zakłócenia medium komunikacyjne.

8.2.2.7 REALIZACJA CELU ODPORNOŚCI NATO „ODPORNE SYSTEMY ŁĄCZNOŚCI CYWILNEJ"

MSWiA analizując zakres podmiotowy ustawy z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej [31], w szczególności w zakresie opisanym w rozdziale 8 dotyczącym Systemu Bezpiecznej Łączności Państwowej (SBŁP) widzi możliwość skorelowania działań związanych z budową SBŁP w oparciu o systemy teleinformatyczne posiadane lub wykorzystywane przez MSWiA oraz służby i organy podległe lub nadzorowane przez Ministra SWiA. Celem Obszaru odporności NATO nr 6 jest zapewnienie stałej dostępności i gwarantowanego dostępu do niezawodnych, bezpiecznych i solidnych usług komunikacyjnych w czasie pokoju, kryzysu i konfliktu, z uwzględnieniem potencjalnych zagrożeń (cybernetycznych, fizycznych, personalnych, hybrydowych, zagrożeń spowodowanych przez człowieka lub naturalnych, pandemii/epidemii, zmian klimatu) przy użyciu nowych technologii. Podobnemu celowi służy SBŁP, który zgodnie z art. 74 ust 1 wspominanej ustawy, powstaje w celu zapewnienia ciągłości i bezpieczeństwa funkcjonowania administracji państwowej oraz ochrony ludności i obrony cywilnej, a Minister właściwy do spraw wewnętrznych nazywany jest „operatorem SBŁP". MSWiA będąc koordynatorem tego obszaru rozpocznie działania mające na celu wkomponowanie zakresu SBŁP do zaleceń odporności.

8.2.2.8 MODERNIZACJA INFRASTRUKTURY TESTA-NG

W kolejnych latach MSWiA planuje sukcesywny rozwój infrastruktury TESTA-ng w celu dalszego zapewniania działania w bezpiecznym i zabezpieczonym środowisku oraz zapewniania adekwatnych poziomów ochrony aktywów i informacji współmiernie do zidentyfikowanych ryzyk. Zaplanowane jest umożliwienie dynamicznego zwiększania ilości użytkowników sieci TESTA-ng oraz zaspokojenie potrzeb sektora rządowego w obszarze zagwarantowania dostępu do usług teleinformatycznych UE przy zapewnieniu najwyższego poziomu zgodności z ramami regulacyjnymi UE i wymogami bezpieczeństwa, a także wzmocnienie cyberobrony i zwiększenie zdolności do szybkiego wykrywania i reagowania na operacje cybernetyczne. W II połowie 2025 nastąpi rozbudowa węzłów o nowe moduły technologiczne, rozbudowa Polskiej Domeny Lokalnej (PDL) o nowe urządzenia agregujące ruch sieciowy oraz zakup urządzeń dostępowych\końcowych dla nowych użytkowników.

8.2.2.9 URUCHOMIENIE BEZPIECZNEJ ŁĄCZNOŚCI SATELITARNEJ *SECURE CONNECTIVITY*

MSWiA planuje rozpoczęcie działań związanych z możliwościami przełączanie systemów tworzących SBŁP z sieciami satelitarnymi udostępnianymi za pomocą programu GOVSATCOM. W obszarze zapewnienia warunków do budowy takiej łączności w ramach unijnej inicjatywy mającej na celu rozwój bezpiecznej łączności satelitarnej GOVSATCOM i *Secure Connectivity*, Polskę reprezentuje minister właściwy do spraw wewnętrznych. Działanie obejmuje także udział w inicjatywie Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych (DG Home) mającej na celu ustanowienie unijnego Systemu Komunikacji

[31] https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240001907/T/D20241907L.pdf

Krytycznej (EUCCS). Ponieważ kraje UE w większości opierają swoje systemy łączności kryzysowej na sieci w standardzie TETRA, bądź też TETRAPOL, MSWiA podjęła krajowe działania w tym zakresie (w ramach tworzonego SBŁP) rozbudowując system łączności radiowej (SBŁP-T). Planowane są dalsze działania mające na celu rozwijanie programu komunikacji satelitarnej GOVSATCOM jako wspomagającego działanie EUCCS, w tym także wykorzystanie łączności radiowej (TETRA) i satelitarnej (GOVSATCOM) wraz usługą precyzyjnej i szyfrowanej nawigacji (PRS). Realizowane w tym celu będą działania na bazie platformy kontaktowej dla wewnętrznych usług (POC-IS).

Planowane jest zapewnienie warunków do korzystania z hybrydowej infrastruktury telekomunikacyjnej przez użytkowników zarządzania kryzysowego za pomocą mobilnych terminali terenowych umożliwiających komunikację w miejscach, gdzie brakuje dostępu do tradycyjnych sieci. Zapewniony zostanie dostęp do usług satelitarnych MEO/GEO umożliwiający dostęp do szerokopasmowych usług telekomunikacyjnych w tymczasowych centrach zarządzania. Z informacji uzyskanych w DG Home wynika, że KE przyjmie wniosek dotyczący rozporządzenia w sprawie „ustanowienia europejskiego systemu łączności krytycznej" w I kwartale 2026 r.

8.2.2.10 BUDOWA CENTRÓW KOMPETENCYJNYCH ODPOWIEDZIALNYCH ZA ZAPEWNIENIE CYBERBEZPIECZEŃSTWA DLA KOMUNIKACJI KRYTYCZNEJ

MSWiA planuje budowę wojewódzkich centrów kompetencyjnych zarządzanych centralnie przez powstałe w tym celu resortowe centrum kompetencyjne MSWiA.

Uruchomione zostanie centrum kompetencyjne MSWiA pełniące rolę Security Operations Center (SOC) dla powstałych centrów wojewódzkich. Do zadań resortowego centrum kompetencyjne MSWiA należeć będzie monitorowanie stanu bezpieczeństwa systemów i sieci teleinformatycznych, za obsługę których odpowiada MSWIA, w których nie są przetwarzane informacje niejawne. Zadania dotyczyć będą monitorowania i gromadzenie informacji o zagrożeniach i potencjalnych ryzykach; prowadzenie analiz infrastruktury teleinformatycznej SBŁP; inicjowanie działań mających na celu zapewnienie bezpieczeństwa cyberprzestrzeni w obszarach SBŁP. Resortowe centrum kompetencyjne MSWiA współpracować będzie z zespołami działającymi na poziomie wojewódzkim w szczególności poprzez wydawanie zaleceń i rekomendacji oraz udzielanie głosu doradczego w kwestach cyberbezpieczeństwa.

Dla zwiększenia poziomu bezpieczeństwa informacji w jednostkach administracji rządowej szczebla wojewódzkiego, na poziomie wojewódzkim zostaną zbudowane wyspecjalizowane zespoły SOC oraz działy analizy zagrożeń i zespoły reagowania na incydenty zarządzane centralnie przez resortowe SOC. Nastąpi rozbudowa infrastruktury teleinformatycznej (serwery i oprogramowanie) i jej integracja z SBŁP. Każdy zespół wojewódzki będzie dysponować odpowiednimi narzędziami technologicznymi.

8.2.3 PRZEWIDYWANIA DOTYCZĄCE SYTUACJI W CYBERPRZESTRZENI NA LATA 2025-2026

Na postawie systemów bezpieczeństwa i wczesnego ostrzegania takich jak system Arakis 2.0 oraz systemów monitorowania MSWiA zwrócono uwagę na znaczący wzrost złośliwego ruchu sieciowego na adresy publiczne Ministerstwa. W ocenie MSWiA jest to związane z rosnącym zjawiskiem cyberprzestępczości, jak również rosnącym zagrożeniem ze strony grup haktywistycznych oraz grup APT powiązanych ze służbami państw-adwersarzy. W szczególności to ostatnie zagrożenie ma szczególny wymiar wobec trwającej wojny Rosji z Ukrainą, w której Polska pełni rolę hubu wsparcia dla Ukrainy oraz sama udziela wielkoskalowej pomocy, jak również działań hybrydowych ze strony Rosji, Białorusi i innych aktorów wymierzonych w Zachód, w tym w Polskę. MSWiA na podstawie danych z systemów monitorowania poziomu bezpieczeństwa sieci i systemów teleinformatycznych odnotowuje systematyczny wzrost ilości ataków i prób przełamania zabezpieczeń. Spektrum działań grup APT obejmuje różnorodne czynności – od systematycznie realizowanego rozpoznania infrastruktury teleinformatycznej, poprzez cyberszpiegostwo, zakłócanie działania systemów IT i sieci. Do najpoważniejszych zagrożeń ze strony grup APT można zaliczyć: ataki *spear-phishingowe* mające na celu wykradanie poświadczeń logowania lub infekcji urządzenia złośliwym oprogramowaniem, skompromitowanie komercyjnych dostawców usług i rozwiązań IT, wykorzystywanie przez grupy APT podatności typu *zero-day*, ataki typu *brute-force* w celu uzyskania dostępu do zasobów sieciowych i skrzynek pocztowych. Z informacji prezentowanych m.in. w ramach spotkań PCOC wynika, że

w licznych atakach grupy APT wykorzystywały skompromitowane prywatne urządzenia sieciowe (m.in. zlokalizowane w Polsce) oraz posługiwały się infrastrukturą animizującą typu VPN/proxy w celu ukrycia złośliwej aktywności.

Istnieje realne zagrożenie, że technologie oparte o AI są lub wkrótce zostaną wykorzystane do przeprowadzania precyzyjnych i ukierunkowanych o dużym nasileniu i zautomatyzowaniu ataków cybernetycznych. Celem minimalizowana ryzyk konieczne wydaje się budowanie przemyślanej strategii działania w zakresie ochrony i obrony zasobów informacyjnych państwa.

8.3 RZĄDOWE CENTRUM BEZPIECZEŃSTWA (RCB)

8.3.1 ZREALIZOWANE PRZEDSIĘWZIĘCIA

RCB w 2024 r. zrealizowało następujące przedsięwzięcia w obszarze rozwoju krajowego systemu cyberbezpieczeństwa:

- odbyło się 6 posiedzeń PCOC w formule stacjonarnej,
- odbyło się 26 posiedzeń PCOC w formule zdalnej,
- odbyło się 2 posiedzenia Zespołu Incydentów Krytycznych,
- trwały prace nad implementacją Dyrektywy CER w zakresie opracowania Krajowej Oceny Ryzyka obejmującej między innymi istotne zagrożeń cyberbezpieczeństwa,
- trwały prace nad implementacją Dyrektywy CER w zakresie opracowania Strategii Odporności Podmiotów Krytycznych dotyczącej zwiększenie odporności podmiotów krytycznych poprzez zapewnienie niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej,
- trwały prace nad dostosowaniem Systemu S46 do prowadzenia wykazu podmiotów krytycznych.

W obszarze podniesienie poziomu odporności systemów informacyjnych:

- prowadzenie ćwiczeń i stress testów w obszarze operatorów infrastruktury krytycznej mających na celu wzmocnienie odporności operatorów infrastruktury krytycznej na zagrożenia antagonistyczne w szczególności w obszarze cyberbezpieczeństwa,
- stosowanie przez operatorów infrastruktury krytycznej minimalnych standardów w zakresie cyberbezpieczeństwa – opracowanie dokumentu minimalne wymagania dla operatorów infrastruktury krytycznej m. in. w zakresie cyberbezpieczeństwa, mających na celu wdrażanie adekwatnych do wyników przeprowadzonej analizy zagrożeń rozwiązań,
- organizacja cyklicznych seminariów cyberbezpieczeństwa dla operatorów infrastruktury krytycznej, urzędów centralnych i szczebla wojewódzkiego. oraz organizacja corocznych krajowych forów ochrony infrastruktury krytycznej.

W obszarze budowanie świadomości, wiedzy i kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz obywateli:

- przeciwdziałanie cyberzagrożeniom i wzmocnienie systemu cyberbezpieczeństwa przez Zespół Zagrożeń Hybrydowych powołany przy Rządowym Zespole Zarządzania Kryzysowego, którego celem m.in. jest wczesna identyfikacja zagrożeń hybrydowych oraz wsparcie koordynacji działań w obszarze cyberbezpieczeństwa,
- koordynacja wymiany informacji pomiędzy administracją, służbami i operatorami infrastruktury krytycznej,
- tworzenie cyklicznych raportów o stanie realizacji zadań wynikających z wprowadzonych stopni CRP. Tworzenie raportów o zdarzeniach i incydentach mających miejsce podczas obowiązywania stopni alarmowych CRP,
- komunikacja na stronach internetowych i publikowanie na profilach mediów społecznościowych kampanii informacyjnych na temat cyberbezpieczeństwa – wzrost świadomości obywateli.

W obszarze wzmocnienia silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa udział w międzynarodowych ćwiczeniach .

8.4 RADA DO SPRAW CYFRYZACJI (RDSC)

8.4.1 O RADZIE

Zgodnie z art. 17 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[32] przy ministrze właściwym do spraw informatyzacji działa Rada do Spraw Cyfryzacji, która jest organem opiniodawczo-doradczym ministra.

Rada do Spraw Cyfryzacji jest „think-tankiem", którego członkowie wspierają swoją wiedzą i doświadczeniem Ministra Cyfryzacji oraz Komitet Rady Ministrów do Spraw Cyfryzacji. Rada opiniuje dokumenty strategiczne (projekty i programy rozwoju) oraz inne dokumenty związane z działalnością resortu cyfryzacji. Rada składa się z minimum 15 członków, którzy reprezentują administrację publiczną, organizacje pozarządowe, sektor gospodarki cyfrowej oraz środowiska naukowe i eksperckie. Istotnym elementem w działaniach Rady jest praca zespołowa i dobre relacje z szerokim gronem interesariuszy, w tym m.in. współpraca z organizacjami pozarządowymi. W ramach działań Rady przedstawiciele organizacji pozarządowych mogą być zapraszani do przedstawienia swoich opinii na forum Rady – jest to możliwe na podstawie zaproszenia skierowanego przez ministra właściwego do spraw informatyzacji lub Przewodniczącego Rady.

Podczas posiedzeń Rady uczestnicy prezentują swoje poglądy niezależnie od stanowiska instytucji, w której pracują. Działalność Rady jest wartością dodaną do działań podejmowanych w zakresie cyfryzacji kraju zarówno w Ministerstwie Cyfryzacji, jak również w innych resortach. Głównym nurtem działań Rady jest generowanie nowych pomysłów, które mogą być realizowane przez Ministerstwo Cyfryzacji. Prowadzone przez Radę prace mają przede wszystkim wymiar projektowy, dzięki czemu Rada zajmuje się rozwiązywaniem konkretnych problemów oraz przedstawianiem rozwiązań wdrożeniowych. Wielosektorowy i wielopodmiotowy potencjał Rady, a także otwarta na współpracę z interesariuszami formuła pracy pozwala agregować wiedzę i trendy z różnych środowisk.

8.4.2 ZREALIZOWANE PRZEDSIĘWZIĘCIA

W 2024 roku Rada V kadencji zebrała się na szesnastu posiedzeniach. Podczas pięciu posiedzeń Rady, których tematyka koncentrowała się na kwestiach z zakresu cyberbezpieczeństwa zostały omówione poniższe zagadnienia:

- Cyberbezpieczeństwo – przedstawienie aktualnych działań Ministerstwa Cyfryzacji oraz omówienie propozycji tematów współpracy Rady ds. Cyfryzacji z Ministerstwem;
- Informacja w sprawie zmiany maksymalnych limitów wydatków określonych w art. 27 ust. 1 pkt 3–10 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa;
- Cyberbezpieczeństwo w sektorze zdrowia:
  - Wnioski Zakładu Ubezpieczeń Społecznych płynące z obserwacji aktualnych incydentów;
  - Propozycje działań mających na celu zwiększenie bezpieczeństwa danych pacjentów wobec obserwowanych zagrożeń.
- Projekt Strategii Cyberbezpieczeństwa oraz projekt ustawy o Krajowym Systemie Cyberbezpieczeństwa;
- Projekt ustawy o Krajowym Systemie Certyfikacji Cyberbezpieczeństwa oraz certyfikacja w zakresie cyberbezpieczeństwa z perspektywy małych i średnich przedsiębiorstw.

[32] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2024, poz. 1557)

8.4.3 PODJĘTE STANOWISKA

Rada do Spraw Cyfryzacji w 2024 r. wydała następujące stanowiska obejmujące tematykę cyberbezpieczeństwa:

- Stanowisko Rady do Spraw Cyfryzacji w sprawie Funduszu Cyberbezpieczeństwa z dnia 30 września 2024 r. skierowane do Ministra Finansów.
- Stanowisko Rady do Spraw Cyfryzacji w sprawie projektu strategii cyfryzacji – wersja projektu z dnia 4 października 2024 r. z dnia 14 października 2024 r. skierowane do Ministra Cyfryzacji.
- Stanowisko Rady do Spraw Cyfryzacji w sprawie rządowego projektu ustawy o zmianie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz innych regulacji i instrumentów mających na celu wzmocnienie cyberbezpieczeństwa w Polsce z dnia 15 grudnia 2024 r. skierowane do Prezesa Rady Ministrów.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/rada-do-spraw-cyfryzacji

8.5 MINISTERSTWO ROZWOJU I TECHNOLOGII (MRIT)

8.5.1 PODJĘTE PRZEDSIĘWZIĘCIA – „BIZNES.GOV.PL”

MRiT przygotowało projekt pn. „Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa firm poprzez udostępnienie usług cyfrowych w ramach Biznes.gov.pl”, którego realizacja planowana jest do końca 2026 r. Projekt jest realizowany przez Ministerstwo Rozwoju i Technologii we współpracy z Naukową i Akademicką Siecią Badawczą – Państwowym Instytutem Badawczym.

Celem projektu jest znaczące wzmocnienie cyberodporności sektora małych i średnich przedsiębiorstw (MŚP) poprzez wdrożenie nowoczesnych e-usług, które będą wspierać poprawę jakości usług cyfrowych oraz zwiększenie poziomu cyberbezpieczeństwa.

Projekt jest integralnym elementem dostosowania polskiej gospodarki do wymagań wynikających z Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2) oraz rozporządzenia Cyber Resilience Act (CRA), mając na celu kompleksowe wsparcie zgodności z regulacjami unijnymi. Stanowi on rozszerzenie programu pilotażowego "Firma Bezpieczna Cyfrowo" realizowanego przez Ministerstwo Rozwoju i Technologii we współpracy z NASK.

W ramach projektu rozwinięty zostanie system Biznes.gov.pl poprzez utworzenie modułu "Bezpieczna Firma". Nowy moduł zapewni firmom dostęp do zestawu narzędzi umożliwiających:

- diagnozę dojrzałości cyfrowej przedsiębiorstwa oraz ocenę poziomu cyberbezpieczeństwa;
- analizę zgodności z wymogami Cyber Resilience Act, w tym generowanie dokumentacji potwierdzającej zgodność z przepisami;
- weryfikację obowiązków wynikających z dyrektywy NIS2 oraz wsparcie w procesie dostosowawczym.

Projektowane rozwiązania pozwolą przedsiębiorcom korzystać z zaawansowanych narzędzi analitycznych i rekomendacyjnych, które będą dostosowane do indywidualnych potrzeb użytkownika. System automatycznie wygeneruje raporty z diagnozy, spersonalizowane zalecenia oraz szablony deklaracji zgodności, co ułatwi spełnienie skomplikowanych wymogów regulacyjnych.

Dostęp do usług będzie zapewniony za pośrednictwem Konta Przedsiębiorcy na platformie Biznes.gov.pl, będącej również łącznikiem do programów oceny zgodności i certyfikacji cyberbezpieczeństwa. Dodatkowe wsparcie zapewni call center, oferujące ekspercką pomoc w zakresie regulacji prawnych, certyfikacji oraz najlepszych praktyk w dziedzinie zarządzania bezpieczeństwem cyfrowym.

Realizacja projektu znacząco zwiększy odporność sektora MŚP na zagrożenia cyfrowe, przyczyniając się do podniesienia poziomu bezpieczeństwa całej gospodarki. Inicjatywa ta wspiera również rozwój zrównoważonego ekosystemu cyfrowego, sprzyjając bezpiecznej transformacji cyfrowej w Polsce.

8.6 MINISTERSTWO FINANSÓW (MF)

8.6.1 OPIS NAJWAŻNIEJSZYCH REALIZOWANYCH DZIAŁAŃ W OBSZARZE CYBERBEZPIECZEŃSTWA.

1. Opiniowanie projektów przepisów w obszarze krajowego systemu Cyberbezpieczeństwa w szczególności:

   1) W obszarze sektora bankowość i infrastruktura rynków finansowych, realizacja zadania dotyczącego zapewnienia stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 oraz implementacji dyrektywy Parlamentu Europejskiego i Rady 2022/2556 z dnia 14 grudnia 2022 r. w sprawie zmiany dyrektyw 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego. W celu realizacji ww. zadań, opracowany został projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji. Projekt ten był przedmiotem uzgodnień i konsultacji w 2024 r. W dniu 13 grudnia 2024 r. ww. projekt został przyjęty przez Komitet do Spraw Europejskich. Planowane jest rozpatrzenie przez Stały Komitet Rady Ministrów przedmiotowego projektu, w dniu 6 lutego br.

   2) W zakresie projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa, która służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjnokomunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15) i zmienia się ustawę z dnia 30 kwietnia 2010 r. o instytutach badawczych oraz ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

   3) Projektu nowej Strategii Cyberbezpieczeństwa RP na lata 2025-2029.

   4) Projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa,

2. Analiza wymagań oraz realizacja działań dostosowujących do wymogów dyrektywy NIS 2 (przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS 2)), w tym ocena zgodności, opracowanie harmonogramu i koncepcji dostosowania RF do nowych wymogów.
3. Przeprowadzono ocenę obecnego stopnia dojrzałości Resortu Finansów (RF) w zakresie NIS2, zidentyfikowano obszary w RF wymagające naprawy i wskazano rekomendowane działania do podjęcia w celu podniesienia poziomu cyberbezpieczeństwa oraz uzgodniono priorytety i sposób wdrożenia rekomendacji.
4. Rozbudowa i aktualizacja kanałów informacyjnych do współpracy RCB oraz CSIRT GOV.
5. Współdziałanie z zespołami CSIRT GOV oraz CSIRT NASK, w zakresie wystąpienia incydentów, mających wpływ na bezpieczeństwo informacji infrastruktury,

6. Rozwój struktur odpowiedzialnych za reagowanie na incydenty cyberbezpieczeństwa, w tym utworzenie w strukturze CIRF Wydziału SOC.
7. Rozwój systemów teleinformatycznych, w tym niejawnych. Bieżące monitorowanie procesów zachodzących w systemach informatycznych w obszarze cyberbezpieczeństwa pozwala na właściwe reagowanie na odporność systemów informacyjnych.
8. W ramach Programu Współdziałania w obszarze audytów IT przeprowadza badanie poziomu zabezpieczeń systemów teleinformatycznych kluczowych podmiotów w Polsce.
9. Departament Audyt Środków Publicznych, pełniący funkcję Instytucji Audytowej w Polsce realizował w 2024 r. audyty w zakresie kluczowego wymogu 6, kryterium oceny 6.41. Powyższe kryterium jest badane w odniesieniu do centralnych i lokalnych systemów informatycznych, których właścicielami są instytucje zaangażowane w dystrybucję środków pochodzących z budżetu UE. Powyższe systemy wykorzystywane są do agregacji danych niezbędnych do rozliczania projektów realizowanych ze środków UE. Celem osiemnastu audytów było potwierdzenie stanu realizacji wydanych zaleceń w latach wcześniejszych. W obszarze audytów IT przeprowadza badanie poziomu zabezpieczeń systemów teleinformatycznych kluczowych podmiotów w Polsce. W ramach ww. audytów wydawane są rekomendacje mające na celu podniesienie poziomu bezpieczeństwa, w tym cyberbezpieczeństwa.

8.6.2 ZIDENTYFIKOWANE NAJPOWAŻNIEJSZE ZAGROŻENIA SYSTEMOWE DLA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA:

Tabela 35. Zidentyfikowane kampanie

Kampania	Link do materiałów:
Ostrzeżenie przed fałszywymi SMS-ami dotyczącymi płatności w e-TOLL (20.03.2024)	https://www.gov.pl/web/kas/ostrzezenie-przed-falszywymisms-ami-dotyczacymi-platnosci-w-e-toll
Uwaga! Przestępcy podszywają się pod pracowników urzędów skarbowych (09.07.2024)	https://www.gov.pl/web/kas/uwaga-przestepcypodszywaja-sie-pod-pracownikow-urzedow-skarbowych
Fałszywe wiadomości SMS (26.09.2024)	https://www.gov.pl/web/kas/falszywe-wiadomosci-sms
Próby podszywania się pod KAS za pomocą e-maili (03.10.2024)	https://www.gov.pl/web/kas/proby-podszywania-sie-pod-kas-za-pomoca-emaili
Fałszywe wezwania do zapłaty (05.12.2024)	https://www.gov.pl/web/kas/falszywe-wezwania-do-zaplaty
Dodatkowo, każda z tych informacji była również dystrybuowana poprzez social media MF/KAS	-

8.6.3 PLANOWANE DZIAŁANIA W 2025 R.

1. Kontynuacja prac nad wdrażaniem nowych rozwiązań i opracowywaniem działań w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem NIS2 i KSC.
2. Integracje zakupionego rozwiązania Cyber Threat Intelligence z systemami wewnętrznymi miedzy innymi SIEM w celu wczesnego wykrywania i przewidywania cyber ataków na infrastrukturę resortu finansów. System CTI ma zapewnić nam proaktywne zarządzanie bezpieczeństwem IT.
3. Kontynuacja współpracy właściwymi zespołami w zakresie zadań dotyczących zapobiegania i reagowania na incydenty.

8.7 URZĄD KOMUNIKACJI ELEKTRONICZNEJ (UKE)

8.7.1 NAJWAŻNIEJSZE DZIAŁANIA W OBSZARZE CYBERBEZPIECZEŃSTWA

8.7.1.1 WDROŻENIE USTAWY O ZWALCZANIU NADUŻYĆ W KOMUNIKACJI ELEKTRONICZNEJ

- w lutym 2024 r. zawarto porozumienie z czterema największymi operatorami, określające szczegółowe środki organizacyjne i techniczne w zakresie zapobiegania CLI spoofing. Dokument ten stał się podstawą do wdrożenia rozwiązania pn. „Bezpieczna zatoka".
- w kwietniu 2024 r. uczestniczono w uruchomieniu rozwiązań antysmishingowych.
- w lipcu 2024 r. opublikowano rekomendacje Prezesa UKE dla przedsiębiorców komunikacji elektronicznej, dotyczące działań w obszarze zwalczania CLI spoofing.
- we wrześniu 2024 r. włączono się w proces wdrożenia rozwiązań anty-CLI spoofing.

8.7.1.2 BUDOWA ŚWIADOMOŚCI W OBSZARZE CYBERBEZPIECZEŃSTWA

Zrealizowano szereg inicjatyw, w tym szkolenia online, ukierunkowanych na zwiększenie świadomości użytkowników urządzeń telekomunikacyjnych i internetu w obszarze bezpiecznego poruszania się w cyberprzestrzeni. Działania te, skierowane zwłaszcza do osób starszych, młodzieży oraz osób z niepełnosprawnościami, objęły łącznie ponad 75 tysięcy uczestników.

8.7.2 FUNKCJONOWANIE KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa (KSC) ocenia się pozytywnie, jednak brak istotnego elementu jakim są sektorowe CSIRT - odpowiedzialne za koordynację wymiany informacji o bezpieczeństwie wewnątrz i pomiędzy poszczególnymi sektorami, ogranicza możliwość szybkiego i skutecznego reagowania w przypadku incydentów obejmujących kilka podmiotów bądź wpływających na inne obszary. Podczas spotkań z przedstawicielami izb gospodarczych sektora wskazywano na potrzebę koordynacji lub wsparcia, zwłaszcza dla mniejszych podmiotów niemających wystarczających kompetencji do utrzymania akceptowalnego poziomu bezpieczeństwa w cyberprzestrzeni.

8.7.3 ZAGROŻENIA DLA SEKTORA KOMUNIKACJI ELEKTRONICZNEJ I KRAJU

- Niewystarczająco szybkie dostosowywanie regulacji do rosnącej skali i tempa ewolucji zagrożeń oraz nadużyć w komunikacji elektronicznej, jak również do błyskawicznie zmieniających się technologii, co przekłada się na opóźnienia w skutecznym reagowaniu na nowe wektory ataków;
- Wykorzystanie sztucznej inteligencji i technologii kwantowych przez cyberprzestępców i inne podmioty o wrogich zamiarach;
- Eksploatacja podatności w łańcuchach dostaw stanowiących podstawę dla prawidłowego funkcjonowania systemów teleinformatycznych;
- Zakłócenia transmisji sygnałów, ograniczanie dostępności usług oraz fizyczne uszkodzenia infrastruktury telekomunikacyjnej;
- Utrata lub nieprawidłowa kontrola dostępu do zasobów, skutkująca ryzykiem nieuprawnionej ingerencji lub ujawnienia danych;
- Przejęcie tożsamości użytkownika cyberprzestrzeni, prowadzące do nadużyć i dalszych ataków.

8.7.4 WNIOSKI I REKOMENDACJE

1. Brak nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa rodzi niepewność prawną dla przedsiębiorców komunikacji elektronicznej w odniesieniu do wdrażania wymogów NIS2

oraz zbieżności podejmowanych działań z obowiązkami wynikającymi z innych przepisów (m.in. DORA, CER);

2. Utworzenie CSIRT dedykowanego sektorowi komunikacji elektronicznej i usług pocztowych pozwoli znacząco usprawnić wymianę informacji o incydentach, zagrożeniach i podatnościach charakterystycznych dla tego sektora, a także ograniczać skutki ewentualnych incydentów;
3. Podmioty sektora telekomunikacyjnego pozytywnie oceniają możliwość wymiany informacji i doświadczeń w obszarze cyberbezpieczeństwa podczas spotkań i warsztatów organizowanych w formule ISAC przez UKE;
4. Dynamiczne zmiany technologiczne skutkują pojawianiem się nowych mechanizmów nadużyć oraz udoskonaleniem istniejących (m.in. wykorzystanie AI, wangiri), co wskazuje na potrzebę regularnego przeglądu i aktualizacji ustawy o zwalczaniu nadużyć w komunikacji elektronicznej.

8.7.5 ZASADNICZE PRZEDSIĘWZIĘCIA PLANOWANE DO REALIZACJI W 2025 ROKU: OWERED BY TCPDF (WWW.TCPDF.ORG)

1. Kontynuacja współpracy z przedsiębiorcami komunikacji elektronicznej i pocztowymi w procesie wdrażania dyrektywy NIS2 oraz planowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.
2. Rozszerzanie i umacnianie współpracy z dotychczasowymi oraz nowymi podmiotami KSC na podstawie zawieranych porozumień dwustronnych.
3. Monitorowanie realizacji zadań wynikających z ustawy o zwalczaniu nadużyć w komunikacji elektronicznej przez podmioty sektora telekomunikacyjnego.
4. Zacieśnianie współdziałania z przedsiębiorcami telekomunikacyjnymi i izbami gospodarczymi sektora, ukierunkowane na wymianę informacji o nadużyciach w komunikacji elektronicznej oraz wdrażanie rozwiązań technicznych podnoszących poziom bezpieczeństwa.
5. Udział w szkoleniach i konferencjach z zakresu cyberbezpieczeństwa.

8.7.6 PRZEWIDYWANIA DOTYCZĄCE SYTUACJI W CYBERPRZESTRZENI W LATACH 2025–2026:

1. Dalszy wzrost liczby zagrożeń skutkujących zakłócaniem dostępności usług, ściśle powiązany z aktualnym otoczeniem bezpieczeństwa państwa.
2. Systematyczne poszerzanie zastosowań nowoczesnych technologii w tworzeniu nowych wektorów ataków na użytkowników cyberprzestrzeni.
3. Rosnąca rola sztucznej inteligencji jako jednego z kluczowych filarów bezpieczeństwa cyfrowego.

8.8 URZĄD OCHRONY DANYCH OSOBOWYCH (UODO)

8.8.1 PODJĘTE PRZEDSIĘWZIĘCIA

UODO w 2024 r. w obszarze cyberbezpieczeństwa przede wszystkim prowadził akcje podnoszące świadomość oraz działania prewencyjne.

Wśród wartych uwagi działań warto wskazać XIV. edycję programu „Twoje dane -Twoja sprawa", w który zaangażowanych było 1.796 nauczycieli, a 48.651 uczniów wzięło udział łącznie w 3.164 lekcjach na temat ochrony danych osobowych. Nauczyciele i uczniowie podjęli 1.355 działań edukacyjnych, w tym 443 z okazji Dnia Ochrony Danych Osobowych. Koordynatorzy Programu kontynuowali *cykl #ODOlekcji* – zajęć w formie online, w trakcie których starano się podejmować szczególnie bliskie uczniom tematy. Wśród nich znalazły się zagadnienia dotyczące m.in. tożsamości cyfrowej oraz technologii *deepfake*. Ogromnym zainteresowaniem cieszył się cykl zajęć pt. *Deepfake: fałszywa rzeczywistość w sieci – czy jesteś na to gotowy?*

Na poziomie krajowym i sektorowym Urząd współpracował również z organami właściwymi do spraw cyberbezpieczeństwa, zgodnie z art. 34 ust. 2 i art. 39 ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077).

W 2024 r. podjęto wspólnie z MC i NASK-PIB inicjatywę rozszerzenia funkcjonalności systemu teleinformatycznego S46, aby umożliwić dokonywanie zgłoszeń naruszeń ochrony danych osobowych, o których mowa w art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[33].

8.8.2 OCENA FUNKCJONOWANIA KSC

Odnośnie do analizy i oceny funkcjonowania krajowego systemu cyberbezpieczeństwa oraz wniosków i rekomendacji UODO podtrzymuje dotychczasowe stanowiska przedstawiane w toku prac legislacyjnych.

Z perspektywy UODO w 2024 r. najpoważniejsze zagrożenia wynikały z niewdrożenia przez administratorów odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku. W toku przeprowadzonych postępowań niejednokrotnie ustalano, że stosowane środki nie uwzględniały stanu wiedzy technicznej oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych, co skutkowało nałożeniem przez Prezesa Urzędu Ochrony Danych Osobowych administracyjnych kar pieniężnych. Mając powyższe na uwadze rekomendowane jest zintensyfikowanie działań w celu uwzględnienia ochrony danych w fazie projektowania systemów teleinformatycznych, jak też zapewnienia domyślnej ochrony danych. Szczególną uwagę należy też zwrócić na obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

[33] Dz. Urz. UE L 119 z 04.05.2026, str. 1, z późn. zm.

8.8.3 PLANOWANE DZIAŁANIA W 2025 R.

W 2025 r. UODO planuje kontynuację dotychczasowych działań, w tym inicjatyw skierowanych w szczególności do dzieci. Przewidziano m.in. XV. edycję ogólnopolskiego programu edukacyjnego „Twoje dane -Twoja sprawa", w ramach którego zdefiniowane zostaną zadania konkursowe adekwatne do wieku i doświadczenia uczestników. Nadto, Prezes UODO będzie kontynuować ogólnopolskie spotkania z mieszkańcami oraz władzami wojewódzkimi i samorządowymi oraz inspektorami ochrony danych osobowych jednostek samorządu terytorialnego.

Celem nowej inicjatywy Urzędu Ochrony Danych Osobowych pn. „UODO rusza w kraj" jest lepsze zrozumienie lokalnych problemów ochrony danych osobowych. Podczas wydarzenia Prezes UODO wraz ze swoimi współpracownikami będzie kontynuował kolejne spotkania z wójtami, burmistrzami oraz prezydentami miast. Rozmowy mają skupiać się na problematyce ochrony danych osobowych w jednostkach samorządu terytorialnego. UODO przeprowadzi również szkolenia dla inspektorów ochrony danych z JST.

Planowane jest również zaktualizowanie poradników tematycznych UODO oraz rewizja dotychczasowych stanowisk Urzędu, w tym w szczególności odnoszących się do przetwarzania danych osobowych w obszarze zatrudnienia, działalności związków zawodowych, edukacji oraz monitoringu wizyjnego, przy uwzględnieniu interesów i obowiązków administratorów oraz praw osób, których dane dotyczą.

8.8.4 PROGNOZA SYTUACJI W CYBERPRZESTRZENI NA LATA 2025-2026

Podejmując próbę predykcji sytuacji cyberprzestrzeni w latach 2025-2026 można założyć, że największe wyzwania w obszarze cyberbezpieczeństwa będą wynikały z nasilenia ataków ukierunkowanych na usługi chmurowe, których celem będzie przede wszystkim pozyskanie danych osobowych. Mimo, że urządzenia brzegowe nadal będą częstym celem cyberprzestępców, istnieje znaczące prawdopodobieństwo, że wykrywane będzie coraz więcej luk w zabezpieczeniach specyficznych dla środowiska chmurowego. Należy również założyć tendencję wzrostową naruszeń w obszarze rozwiązań opartych na AI. Zagrożenia będą wynikały nie tylko ze złośliwego wykorzystania AI, ale również z uwagi na znaczące ilości danych przetwarzanych przez takie systemy, jak też ich upowszechnienie.

Wysoce prawdopodobne jest również, że pojawią się nowe sposoby wykorzystania AI przez adwersarzy, w tym oparte na inżynierii społecznej oraz mechanizmach socjotechnicznych. Wykorzystanie sztucznej inteligencji do tworzenia oferty Crime-as-a-service (CaaS) jest w zasadzie pewne przy uwzględnieniu kierunku rozwoju zestawów phishingowych, DDoS-as-a-Service czy Ransomware-as-a-Service. Spodziewać można się również ataków ukierunkowanych na wpływanie na proces identyfikacji i autentykacji użytkowników systemów teleinformatycznych.

9 REALIZOWANE DZIAŁANIA W ZAKRESIE ZAPEWNIENIA CYBERBEZPIECZEŃSTWA NA POZIOMIE KRAJOWYM

9.1 ROZWÓJ KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

9.1.1 CENTRUM CYBERBEZPIECZEŃSTWA NASK (CCN)

Celem strategicznym projektu CCN jest wzmocnienie krajowego systemu cyberbezpieczeństwa poprzez utworzenie Centrum Cyberbezpieczeństwa, na które złożą się jakościowo nowe tematyczne specjalistyczne centra, ośrodki i laboratoria istotne z punktu widzenia wzmocnienia krajowego systemu cyberbezpieczeństwa. Na projekt ten to składają się 3 następujące powiązane ze sobą podzadania:

1. Utworzenie obiektu CCN;
2. Utworzenie 7 specjalistycznych centrów, ośrodków i laboratoriów, tj.:
   - Krajowego Centrum Odzyskiwania Danych;
   - Krajowego Centrum Operacyjnego Cyberbezpieczeństwa;
   - Modelowego Ośrodka Treningowo-Szkoleniowego w obszarze Cyberbezpieczeństwa;
   - Laboratorium Bezpieczeństwa AI;
   - Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania;
   - Krajowego Centrum Wsparcia Security dla JST;
   - Ośrodka Modelowania Certyfikacji Cyberbezpieczeństwa;
3. Rozbudowa infrastruktury NASK PIB działającej na rzecz CSIRT NASK.

Jest to inwestycja o łącznej wysokości 310 mln zł, w zdolność i gotowość państwa do reagowania na obecne i przyszłe zagrożenia z cyberprzestrzeni.

W dniu 10 grudnia 2024 r. został podpisany akt notarialny dotyczący oddania w użytkowanie wieczyste NASK-PIB gruntu skarbu państwa pod budowę Centrum Cyberbezpieczeństwa w Warszawie. Równolegle toczyły się prace projektowe w poszczególnych zespołach dedykowanych związane z utworzeniem ww. centrów, laboratoriów i ośrodków, w tym sukcesywnie rozstrzygane były postępowania przetargowe na wyposażenie Centrum oraz usługi związane z prowadzeniem inwestycji budowlanej. W 2025 r. kontynuowane będą przygotowania do budowy siedziby Centrum.

Więcej informacji pod adresem: https://www.gov.pl/web/cppc/centrum-cyberbezpieczenstwa-nask-akronim-ccn

9.1.2 NOWELIZACJA ROZPORZĄDZENIA RADY MINISTRÓW W SPRAWIE ZAKRESU DZIAŁANIA ORAZ TRYBU PRACY KOLEGIUM DO SPRAW CYBERBEZPIECZEŃSTWA

W 2024 r. przygotowana została nowelizacja rozporządzenia Rady Ministrów w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa. Dotychczasowe doświadczenia związane z obsługą prac Kolegium wskazywały na konieczność dokonania zmian w tym zakresie, mających na celu podniesienie efektywności obsługi Kolegium oraz uproszczenie procesu przygotowywania dokumentów związanych z jego pracami. W szczególności zostały wyeliminowane wątpliwości powstające przy sporządzaniu protokołów z posiedzeń w przedmiocie zgłaszania wniosków przez uczestników posiedzenia, usunięto nadmiarowe obowiązki, które stanowiły ryzyko z punktu widzenia ochrony informacji niejawnych, czy wprowadzono procedurę wyznaczania zastępcy sekretarza Kolegium. Procedura ta ma istotne znaczenie z uwagi na to, że pozwala na zapewnienie ciągłości prac Kolegium do spraw Cyberbezpieczeństwa. Nowelizacja weszła w życie 15 maja 2024 r.

9.1.3 PROJEKTY W RAMACH KRAJOWEGO PLANU ODBUDOWY (KPO)

Istotnym wsparciem dla rozwoju cyberbezpieczeństwa Polski są projekty przewidziane do realizacji w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (Inwestycja C3.1.1 Cyber). W 2024 roku prowadzone były intensywne prace zmierzające do wdrożenia czterech przedsięwzięć o łącznej wartości 864,6 mln zł (192,5 mln euro). Były to:

1. Ustanowienie sieci 5 sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) – Celem tego przedsięwzięcia jest utworzenie lub rozwój 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) w sektorach kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Nabór wniosków do tego przedsięwzięcia rozpoczął się w dniu 13.11.2024 r. Sektorowe zespoły cyberbezpieczeństwa, o których mowa w art. 44 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077,1222), będą budowane lub rozwijane dla sektorów: energii, transportu, ochrony zdrowia, bankowości i infrastruktury rynków finansowych, infrastruktury cyfrowej, oraz zaopatrzenia w wodę pitną i jej dystrybucji.
2. Podłączenie 385 podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem – W dniu 3.09.2024 r. podpisana została umowa pomiędzy Centrum Projektów Polska Cyfrowa i NASK-PIB na jego dofinansowanie. Projekt będzie wdrażany do 30.06.2026 roku.
3. Udzielenie 500 podmiotom wsparcia na rzecz modernizacji i rozbudowania infrastruktur cyberbezpieczeństwa przy wykorzystaniu technologii informacyjnej i technologii operacyjnej – przedsięwzięcie to zostało podzielone na 2 nabory, tj.:
    - **I nabór pn. „Cyberbezpieczny Rząd" – celem tego naboru jest udzielenie wsparcia grantowego centralnym i naczelnym organom administracji rządowej oraz wojewodom w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Uruchomienie naboru wniosków o granty zaplanowane zostało w lutym 2025 roku.**
    - **II nabór pn. „Cyberbezpieczne wodociągi" – celem tego naboru jest udzielenie wsparcia grantowego dla przedsiębiorstw wodociągowo-kanalizacyjnych, wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS) w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Uruchomienie naboru wniosków o granty zaplanowane zostało w II kw. 2025 roku.**
4. Utworzenie sieci specjalistów w dziedzinie cyberbezpieczeństwa na szczeblu wojewódzkim, aby wesprzeć organy publiczne w radzeniu sobie z incydentami i odzyskiwaniu danych oraz podejmowanie działań służących podnoszeniu świadomości w zakresie cyberbezpieczeństwa – Celem tego przedsięwzięcia jest modernizacja i profesjonalizacji zespołów Policji, które będą wspierać zaatakowane podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych. Nabór wniosków do tego przedsięwzięcia rozpoczął się w dniu 19.12.2024 r. Zadanie realizowane będzie do 30.06.2026 roku.

Ponadto Ministerstwo Cyfryzacji rozpoczęło pracę nad rozporządzeniem Ministra Cyfryzacji w sprawie udzielania pomocy *de minimis* na wsparcie przedsiębiorstw wodociągowo-kanalizacyjnych objętych krajowym systemem cyberbezpieczeństwa w ramach Krajowego Planu Odbudowy i Zwiększania Odporności. Głównym celem projektowanego rozporządzenia jest udzielenie pomocy *de minimis* przedsiębiorstwom wodociągowo-kanalizacyjnych objętych KSC na:

1. wdrożenie środków organizacyjnych służących zapewnianiu cyberbezpieczeństwa;
2. zakup lub modernizację środków technicznych służących zapewnianiu cyberbezpieczeństwa;
3. rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

9.1.4 PLANY DZIAŁANIA PRZEDSIĘBIORCÓW TELEKOMUNIKACYJNYCH W SYTUACJACH SZCZEGÓLNYCH ZAGROŻEŃ

Ministerstwo Cyfryzacji w 2024 r. realizowało stałe zadanie w zakresie uzgadniania planów działania przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń. Obowiązek sporządzenia planu i zakres uzgodnień wynikał z art. 176a ust. 2 ustawy Prawo telekomunikacyjne, a następnie z art. 39 ust. 2 ustawy Prawo komunikacji elektronicznej oraz rozporządzenia Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych. Posiadanie planu działań jest istotne z punktu widzenia potrzeby efektywnego reagowania na przypadki

wystąpienia sytuacji kryzysowych, stanów nadzwyczajnych i bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej[34]. Zadanie to będzie kontynuowane w 2025 r.

W 2024 r. Ministerstwo Cyfryzacji wszczęło prace legislacyjne nad projektem rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, które ma dostosować istniejące przepisy do uchwalonej w 2024 r. ustawy - Prawo komunikacji elektronicznej.

9.1.5 WDROŻENIE DYREKTYWY NIS 2

Ministerstwo Cyfryzacji prowadzi prace nad implementacją do krajowego porządku prawnego przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2). W 2024 r. opracowano projekt ustawy implementującej ww. dyrektywę – projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32), który został zaprezentowany w kwietniu 2024 r. Do 24 maja 2024 r. trwały konsultacje publiczne, w ramach których do projektu zgłoszono 1567 uwag. Na podstawie przedstawionych propozycji przygotowano nową wersję projektu, która została skierowana na Komitet do spraw Europejskich.

9.1.6 USTAWA O KRYPTOAKTYWACH

Pod koniec 2023 r. Ministerstwo Finansów zaczęło prace nad sporządzeniem projektu ustawy o kryptoaktywach, która ma za zadanie zapewnienie stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (tzw. Rozporządzenie MiCA). Rozporządzenie zostało opublikowane dnia 9 czerwca 2023 r. oraz wprowadza ramy regulacyjne w zakresie rynku kryptoaktywów zapewniające m.in. bezpieczeństwo uczestników tego rynku oraz systemu finansowego. Biorąc pod uwagę cyfrową naturę regulowanych instrumentów rozporządzenie to ma wpływ na cyberbezpieczeństwo kraju. Ww. projekt ustawy został 10 grudnia 2024 r. przyjęty przez Komitet do spraw Europejskich, a następnie został przekazany pod obrady Stałego Komitetu Rady Ministrów.

9.1.7 STANDARDY I REKOMENDACJE CYBERBEZPIECZEŃSTWA

W 2024 r. Ministerstwo Cyfryzacji opracowało i zamieściło w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl (Standardy i rekomendacje - Baza wiedzy - Portal Gov.pl) pięć rekomendacji, dobrych praktyk i zaleceń konfiguracyjnych związanych z cyberbezpieczeństwem dotyczących stosowania zalecanych środków bezpieczeństwa i ochrony prywatności w ramach skutecznego zarządzania ryzykiem, osiągania bezpieczeństwa w systemach informacyjnych oraz przetwarzania w chmurze. Dotychczas opublikowano 44 publikacje w zakresie wymagań organizacyjno-technicznych rekomendujących rozwiązania bezpieczeństwa informacji.
W 2025 planowane jest opracowanie kolejnych 5 publikacji rekomendujących dobre praktyki i zalecenia konfiguracyjne podnoszące poziom cyberbezpieczeństwa.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyberbezpieczenstwa2

[34] Z tego względu plan powinien zawierać, m.in. zasady współpracy z innymi przedsiębiorcami telekomunikacyjnymi, z podmiotami i służbami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy ludności, a także zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego; wykaz przygotowanych technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; opis sposobów utrzymania ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej oraz ich odtworzenia w przypadku utraty możliwości świadczenia tych usług (ważne, w sytuacji świadczenia usług dla służb ratowniczych oraz wykonujących zadania na rzecz bezpieczeństwa i obronności państwa).

9.1.8 PROJEKT „PIONIER-Q W RAMACH EUROPEAN QUANTUM COMMUNICATION INFRASTRUCTURE"

Projekt PIONIER-Q jest oficjalnym wkładem Polski do europejskiej inicjatywy - European Quantum Communication Infrastructure (EuroQCI10) uruchomionej w 2019 roku. EuroQCI będzie bezpieczną infrastrukturą łączności kwantowej obejmującą całą UE. Komisja Europejska współpracuje ze wszystkimi 27 państwami członkowskimi UE oraz Europejską Agencją Kosmiczną (ESA) w celu zaprojektowania, opracowania i wdrożenia EuroQCI, który będzie składał się z segmentu naziemnego opartego na sieciach łączności światłowodowej, łączących strategiczne obiekty na poziomie krajowym i transgranicznym oraz segmentu kosmicznego opartego na satelitach. Będzie ona integralną częścią IRIS²11, nowego unijnego systemu bezpiecznej komunikacji opartej na przestrzeni kosmicznej. EuroQCI będzie chronić wrażliwe dane i infrastrukturę krytyczną poprzez integrację systemów kwantowych z istniejącą infrastrukturą komunikacyjną, zapewniając dodatkową warstwę bezpieczeństwa opartą na fizyce kwantowej. Wzmocni ochronę europejskich instytucji rządowych, ich centrów danych, szpitali, sieci energetycznych i innych. Realizacja projektu PIONIER-Q jest kluczowym elementem dla efektywnego udziału Polski w tej inicjatywie.

W ramach Projektu zostanie uruchomiona infrastruktura oraz usługi związane z generowaniem oraz przesyłaniem kluczy w technologii kwantowej dystrybucji kluczy (QKD – Quantum Key Distribution). Jest to metoda bezpiecznego generowania oraz dystrybucji kluczy oparta na zasadach mechaniki kwantowej, które następnie mogą zostać wykorzystane np. do szyfrowania danych lub uwierzytelniania usług i użytkowników. Technologia QKD może zostać wykorzystana w aktualnych algorytmach do symetrycznego szyfrowania danych lub do przyszłych rozwiązań algorytmów szyfrowania danych typu post quantum, będących aktualnie przedmiotem standaryzacji. Sieci komunikacji kwantowej są potencjalnym elementem do łączenia oraz skalowania infrastruktur obliczeń kwantowych. Długofalowym celem projektu jest wypracowanie rozwiązań oraz zbudowanie fundamentów pod sieci bezpiecznej komunikacji między innymi dla jednostek administracji lokalnej, centralnej oraz na poziomie transgranicznym (pomiędzy państwami członkowskimi i instytucjami UE). Dotyczy to zarówno komunikacji w segmencie naziemnym, jak i satelitarnym.

W grudniu 2023 r. Prezes Rady Ministrów powierzył Konsorcjum PIONIER-Q realizację zadania z zakresu informatyzacji sektora publicznego oraz innowacji cyfrowych, polegającego na utrzymaniu zdolności zleceniobiorców do realizacji projektu pn. „PIONIER-Q: Ogólnopolska Kwantowa Infrastruktura Komunikacyjna", będącego wkładem Polski do inicjatywy EuroQCI – budowy europejskiej infrastruktury komunikacji kwantowej. Po stronie rządowej działania w tym zakresie realizowane są przez Ministerstwo Cyfryzacji.

W skład Konsorcjum PIONIER-Q wchodzą:

- Poznańskie Centrum Superkomputerowo-Sieciowe,
- Akademickie Centrum Komputerowe Cyfronet AGH,
- Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego,
- Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy,
- Centrum Informatyczne TASK,
- Wrocławskie Centrum Sieciowo-Superkomputerowe.

Od 2023 r. Ministerstwo Cyfryzacji współfinansuje projekt PIONIER-Q w wysokości 25%. Zaangażowanie Ministerstwa Cyfryzacji było realizowane również w 2024 r. i będzie kontynuowane w 2025 r.

9.2 PODNIESIENIE POZIOMU ODPORNOŚCI SYSTEMÓW INFORMACYJNYCH ADMINISTRACJI PUBLICZNEJ I SEKTORA PRYWATNEGO ORAZ OSIĄGNIĘCIE ZDOLNOŚCI DO SKUTECZNEGO ZAPOBIEGANIA I REAGOWANIA NA INCYDENTY

9.2.1 SYSTEM KOMUNIKACJI RZĄDOWEJ – NIEJAWNEJ (SKR-Z)

Resort Cyfryzacji, w 2021 r. zlecił NASK-PIB realizację zadania publicznego p.n. „Budowa systemu łączności mobilnej umożliwiającej przetwarzanie informacji niejawnych do klauzuli „zastrzeżone" (SKR-Z) w oparciu o system CATEL". Zadanie było kontynuowane w 2024 roku na podstawie zleconej umowy dotacji celowej i zakończyło się uruchomieniem produkcyjnym systemu SKR-Z.

W 2024 roku zakres przedmiotowy zadania obejmował realizację czynności utrzymaniowych, wymaganych do operacyjnego działania systemu oraz wdrażania go na szerszą skalę w 2025 roku. Ze względu na potrzeby związane z zapewnieniem bezpiecznej komunikacji pomiędzy przedstawicielami administracji publicznej, Zadanie obejmuje również obszar rozbudowy systemu.

Obecnie liczba aktywnych użytkowników wynosi około **1050** użytkowników w ponad **100** podmiotach i ich liczba stale rośnie.

9.2.2 PROJEKT „BEZPIECZNY KOMUNIKATOR" - THREEMA ONPREM

Resort Cyfryzacji w celu zapewnienia bezpiecznej szyfrowanej komunikacji jednostkom administracji publicznej od 2022 roku wdraża w ramach realizowanej umowy bezpieczny komunikator Threema OnPrem. Komunikator ten zapewnia bezpieczną wymianę informacji w zakresie przesyła danych i komunikacji głosowej.

Obecnie Komunikator posiada liczbę **5 345** aktywnych użytkowników spośród wszystkich użytkowników w liczbie **543**. Liczba użytkowników systematycznie rośnie.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/komunikator

9.2.3 USŁUGA „ZASTRZEŻ PESEL"

W styczniu 2024 r. do aplikacji mObywatel została dodana funkcja „Zastrzeż PESEL". Jest to usługa, która pozwala swobodnie zarządzać własnym numerem PESEL. Oznacza to, że obywatel może zmienić jego status na zastrzeżony i w ten sposób zablokować jego wykorzystywanie przez banki i inne instytucje. Od 1 czerwca 2024 te instytucje są zobowiązane do sprawdzania statusu numeru PESEL swoich klientów. Jeśli okaże się, że PESEL jest zastrzeżony, nie będzie można za jego pomocą wziąć kredytu, kupić czegoś na raty, wnioskować o duplikat karty SIM czy załatwić niektórych spraw notarialnych.

Zastrzeżenie numeru PESEL zabezpieczy obywatela przed jego nieuprawnionym użyciem. Z poziomu aplikacji możliwe szybkie zastrzeżenie numeru PESEL, jak również stałe lub czasowe jego zastrzeżenie. Przy pomocy usługi obywatel może również sprawdzić, kto weryfikował jego PESEL.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja-badania-i-projektowanie-mobywatel20/zastrzez-pesel

9.2.4 USŁUGA „BEZPIECZNIE W SIECI"

W dniu 14.08.2024 r. w aplikacji mObywatel uruchomiono ww. usługę. która umożliwia zgłaszanie incydentów z następujących kategorii:

- złośliwa strona internetowa (próba wyłudzenia danych osobowych lub pieniędzy),
- podejrzany SMS (niepokojąca treść lub nadawca),
- podejrzany e-mail (niepokojące załączniki, szantaż lub phishing),
- oszustwo (fałszywe sklepy internetowe i inne próby podszywania się pod firmy lub instytucje),
- inny (pozostałe zdarzenia, które nie pasują do poprzednich rodzajów incydentów).

Każda z wymienionych wyżej kategorii ma odrębną ścieżkę w aplikacji – tak, aby proces zgłaszania był jak najbardziej intuicyjny i dostosowany do danej sytuacji. Zgłoszenia są następnie przekazywane do

zespołu specjalistów z CERT Polska, którzy na co dzień zajmują się reagowaniem na zagrożenia dotyczące cyberbezpieczeństwa. Usługa umożliwia włączenie alerty z ostrzeżeniami o zagrożeniach w Internecie. Dzięki nim użytkownicy usługi mogą otrzymywać bieżące informacje o atakach cyberprzestępców.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/bezpiecznie-w-sieci--nowa-usluga-do-walki-z-cyberzagrozeniami-od-dzis-dostepna-w-mobywatelu

9.2.5 PROGRAM „CYBERBEZPIECZNY SAMORZĄD"

W 2024 roku Ministerstwo Cyfryzacji wspólnie z Centrum Projektów Polska Cyfrowa oraz NASK PIB kontynuowało wdrażanie największego projektu grantowego w programie FERC ukierunkowanego na zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego. Celem podejmowanych działań jest wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Grupą docelową projektu były jednostki samorządu terytorialnego w kraju (2807 JST = 100%) wraz z jednostkami podległymi.

W 2024 r. w ramach projektu podpisane zostały wszystkie umowy z 2495 samorządami które złożyły poprawne wnioski o grant na łączną kwotę blisko 1,5 mld zł. Środki otrzymało niemal 90% wszystkich jednostek samorządowych w kraju. Do końca 2024 roku samorządy otrzymały 700 mln zł. Gminy, powiaty jak i samorządy województw wydatkują środki na trzy kluczowe obszary wsparcia:

Rysunek 14. Logo Cyberbezpieczny Samorząd

- **organizacyjny** – związany z procedurami obowiązującymi w obszarze cyberbezpieczeństwa (w szczególności wdrożenie i audyt Systemu Zarządzania Bezpieczeństwem Informacji);
- **kompetencyjny** – obejmujący szkolenia pracowników JST, w tym zarówno zaawansowanych szkoleń dla personelu informatycznego jak i szkoleń podstawowych związanych z budowaniem świadomości cyberzagrożeń i umiejętności reagowania na nie;
- **techniczny** – w ramach którego możliwy jest szeroki wachlarz działań: począwszy od zakupu sprzętu informatycznego, poprzez licencje, oprogramowanie oraz usługi wspierające cyberbezpieczeństwo.

Zgodnie z zapisami regulaminu konkursu środki pozyskane z grantów samorządy będą mogły wykorzystać maksymalnie do połowy 2026 r.

Więcej informacji pod adresem: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

9.2.6 PROJEKT „OSŁONA INFORMACYJNA KAMPANII WYBORCZEJ 2024 R."

W 2024 r. Ministerstwo Cyfryzacji udzieliło Naukowej i Akademickiej Sieci Komputerowej – Państwowy Instytut Badawczy (NASK-PIB) dotacji celowej na realizację zadania publicznego pn. „Osłona informacyjna kampanii wyborczej 2024 r." z terminem realizacji: 01.04-31.12.2024 r.

9.3 REALIZOWANE ZADANIA NASK-PIB W RAMACH UDZIELONEJ DOTACJI:

1. Utrzymanie i rozbudowa przez NASK-PIB serwisu www.bezpiecznewybory.pl dedykowanego treściom szkodliwym. Serwis to wiarygodne źródło informacji w tematyce wykrywania oraz przeciwdziałania dezinformacji w trakcie wyborów. Serwis dedykowany jest obywatelom RP oraz podmiotom realizującym zadania publiczne. Dzięki udostępnieniu danych z monitoringu, analizom oraz tekstom eksperckim, wyborcy oraz instytucje mogą znaleźć informacje będące w ich zainteresowaniu. W ramach funkcjonalności serwisu przewidziano możliwość transparentnego zgłaszania treści szkodliwych do właścicieli mediów społecznościowych. Serwis jest miejscem, w którym można znaleźć zweryfikowane treści, potwierdzone u źródła informacje na temat procesu wyborczego oraz poradniki i wskazówki uzyskane od partnerów z Big Techów.
2. Obsługa, tj. weryfikacja treści przesłanych od użytkowników serwisu i obywateli – research i analiza informacji, przesyłanie informacji odpowiednim podmiotom, opisywanie zgłoszenia, udzielenie oficjalnej odpowiedzi przez zespół serwisu www.bezpiecznewybory.pl na zgłoszenia wpływające w trakcie procesu wyborczego przez:
   - formularz w serwisie www.bezpiecznewybory.pl;
   - wiadomości e-mail przesyłane na adres e-mail: bezpiecznewybory@nask.pl;
   - wiadomości do Działu Przeciwdziałania Dezinformacji (DPD) NASK-PIB – e-mail na adres informacje@nask.pl, dezinformacja@nask.pl, oznaczenia profilu @włączweryfikację w serwisie Facebook oraz X (niegdyś Twitter); 4) inne kanały.
3. Ciągły monitoring mediów społecznościowych w języku polskim w kontekście wyborczym, w tym tematyki wyborów samorządowych w Polsce, jak i treści związanych z wyborami do Parlamentu Europejskiego. Celem jest/było wykrycie głównych linii narracyjnych dotyczących bezpieczeństwa wyborczego, podmiotów (tzw. aktorów) biorących aktywny udział w procesie dezinformacji w polskich mediach społecznościowych.
4. Przygotowanie dwóch raportów badawczych obejmujących analizę ilościową i jakościową oraz kluczowe statystyki na temat:
   - dezinformacji na temat wyborów samorządowych odnotowanej w okresie 01 - 22.04.2024;
   - dezinformacji w trakcie kampanii wyborczej do Parlamentu Europejskiego.
5. Organizacja spotkań edukacyjnych, w tym dla podmiotów zaangażowanych w wybory samorządowe w Polsce w 2024 r. oraz w zakresie ochrony referendów przed dezinformacją na poziomie lokalnym w aspekcie dezinformacji dla pracowników JST i mediów.
6. Organizacja lub udział w konferencjach dedykowanych dezinformacji i cyberbezpieczeństwu, w tym organizacja panelu/i dotyczących dezinformacji wyborczej w ramach Forum Ekonomicznego w Karpaczu. Przewidziana jest prezentacja raportu zawierającego analizę trendów i tematów związanych z wyborami oraz prezentacja wniosków i rekomendacji przed wyborami prezydenckimi.
7. Przygotowanie raportów dotyczących wpływu dezinformacji na proces wyborczy oraz analiza dezinformacji na podstawie danych dotyczących kampanii dezinformacyjnych w 2024 roku w Europie oraz analiza dezinformacji na podstawie danych dotyczących kampanii dezinformacyjnych w 2024 roku w Europie przy współpracy z ekspertami zagranicznymi oraz predykcje technik dezinformujących, narracji i metod w perspektywie nadchodzących wyborów prezydenckich.
8. Opracowanie przewodnika dotyczącego reagowania w sytuacjach kryzysowych związanych z dezinformacją, między innymi wyborczą.

9.3.1 SYSTEM „ANTYDDOS”

W ramach prac Ministerstwa Cyfryzacji w 2024 r. kontynuowano realizację zleconego NASK-PIB zadania pn. „**Zapewnienie usługi chmurowej ochrony przed atakami DDoS – Distributed Denial of Service dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP**”. Celem zadania jest zapewnienie na możliwie najwyższym poziomie ochrony przed atakami DDoS – Distributed Denial of Service dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP. Ochrona przed atakami DDoS polega na

przekierowaniu całego ruchu skierowanego do serwisu objętego ochroną do centrum oczyszczania (tzw. Scrubbing Center, dalej: SC), celem oddzielenia ruchu pożądanego od niepożądanego. W celu maksymalizacji efektu SC powinno być zlokalizowane poza siecią atakowanego, możliwie blisko źródła ataków. W wyniku realizacji zadania, oczyszczony ruch zostaje przekierowywany z SC do NASK-PIB, a następnie przygotowanym kanałem komunikacyjnym do serwisu podmiotu objętego ochroną.

Rysunek 15. Logo programu AntyDDoS

W ramach realizacji przedmiotowego zadania w latach 2022 – 2024 objętych ochroną zostało 75 podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP, w tym m.in. Siły Zbrojne RP, służby specjalne oraz urzędy centralne.

Zadanie jest nieprzerwanie realizowane od 2022 r. i będzie realizowane do 31 grudnia 2025 r.

9.3.2 FUNDUSZ CYBERBEZPIECZEŃSTWA – ŚWIADCZENIE TELEINFORMATYCZNE

Fundusz Cyberbezpieczeństwa, którego dysponentem jest minister właściwy do spraw informatyzacji, został powołany ustawą z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Głównym zadaniem Funduszu, jako państwowego funduszu celowego, jest wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami poprzez finansowanie świadczenia teleinformatycznego, tj. dodatku do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenia pieniężnego.

Świadczenie teleinformatyczne może zostać przyznane osobom realizującym zadania z zakresu cyberbezpieczeństwa na rzecz podmiotów wymienionych w ustawie, m.in. w CSIRT poziomu krajowego, służbach odpowiedzialnych za bezpieczeństwo państwa oraz bezpieczeństwo powszechne, a także w niektórych urzędach administracji publicznej.

Warunkiem ubiegania się o wsparcie ze środków Funduszu jest złożenie przez uprawniony podmiot wniosku do ministra właściwego do spraw informatyzacji. Wnioski spełniające wymagania formalne przekazywane są do Kolegium do Spraw Cyberbezpieczeństwa, które wydaje opinię w zakresie wnioskowanych kwot.

W 2024 r. Minister Cyfryzacji zawarł 112 umów o udzielenie wsparcia ze środków Funduszu Cyberbezpieczeństwa na łączną kwotę 331 503 782,00 zł. Świadczenie teleinformatyczne otrzymało blisko 6 500 osób realizujących zadania w zakresie zapewnienia cyberbezpieczeństwa w kluczowych instytucjach w kraju.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/przypominamy-zasady-ubiegania-sie-o-srodki-z-funduszu-cyberbezpieczenstwa

9.3.3 STOPNIE ALARMOWE CRP

Od 21 lutego 2022 r. na terytorium Rzeczypospolitej Polskiej obowiązywał trzeci stopień alarmowy CHARLIE-CRP. Zgodnie z *ustawą o działaniach antyterrorystycznych* stopnie alarmowe CRP są wprowadzane przez Prezesa Rady Ministrów w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia.

Zarządzeniem nr 17 dnia 29 lutego 2024 r. Prezes Rady Ministrów zarządził obniżenie stopnia alarmowego dla polskiej cyberprzestrzeni na stopień BRAVO-CRP, który jest drugim z czterech stopni alarmowych określonych w ustawie.

Obecnie stopień BRAVO CRP obowiązuje na terytorium Rzeczypospolitej Polskiej **do 28 lutego 2025 roku**.

9.4 ZWIĘKSZENIE POTENCJAŁU NARODOWEGO W ZAKRESIE TECHNOLOGII CYBERBEZPIECZEŃSTWA

9.4.1 PROGRAM WSPÓŁPRACY W CYBERBEZPIECZEŃSTWIE (PWCYBER)

W 2024 r. Ministerstwo Cyfryzacji kontynuowało współpracę o charakterze partnerstwa publiczno-prywatnego w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber) uruchomionego w 2019 r. Kluczowym obszarem współpracy w ramach partnerstwa jest podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatycznych.

Rysunek 16. Logo PWCyber

W 2024 r. do PWCyber dołączyło 12 nowych partnerów, tym samym na koniec roku 2024 w ramach Programu współpracowało łącznie 50 firm technologicznych (polskich i zagranicznych) oraz organizacji.

Rok 2024 r. był rokiem jubileuszowym funkcjonowania Programu. Po 5 latach od powstania, Program PWCyber przechodzi ewaluację. Utworzona została specjalna ankieta oceny dla nowych kandydatów, a w opracowaniu jest regulamin Programu.

W ramach obchodów, podczas 16. Edycji Europejskiego Kongresu Gospodarczego w Katowicach w dniu 8 maja 2024 r. zorganizowano panel dyskusyjny pt. „Bezpieczeństwo łańcucha dostaw (nie tylko) w świetle Dyrektywy NIS2".

Głównym wydarzeniem podsumowującym 5-lecie PWCyber było uroczyste spotkanie z partnerami, które odbyło się 22 października br. w Warszawie. W wydarzeniu uczestniczyli przedstawiciele 40 partnerów (łącznie 81 osób). Z okazji rocznicy Programu wydano także raport podsumowujący dotychczasową współpracę pt. *5 lat PWCyber - publikacja jubileuszowa.*

Spotkanie było okazją do podsumowania 5 lat funkcjonowania Programu oraz dyskusji o dalszych kierunkach jego rozwoju.

W 2024 r. powstała również pierwsza grupa robocza w ramach PWCyber, której celem jest wypracowanie rekomendacji dotyczących zmian w ustawie Prawo zamówień publicznych, a także opracowanie rekomendacji dot. bezpiecznych zakupów rozwiązań IT.

W ramach dotychczasowej współpracy odbyły się m.in. wspólnie organizowane szkolenia dla administracji publicznej, jednostek samorządu terytorialnego, Polskiej Akademii Nauk, podmiotów publicznych wykonujących działalność leczniczą, Operatorów Usług Kluczowych, a także warsztaty techniczne. W bazie wiedzy o cyberbezpieczeństwie na stronie: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo zamieszczane są rekomendacje i poradniki partnerów Programu

W 2024 r. dzięki współpracy z ekspertami partnerów technologicznych PWCyber odbyły się 34 szkolenia online w których uczestniczyło ponad 21 tys. osób.

Rysunek 17. Uczestnicy konferencji podsumowującej pięciolecie programu PWCyber

W ramach współpracy przeprowadzono także warsztaty techniczne z partnerami Programu:

- W dniu 28.05.2024 r. pracownicy Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji uczestniczyli w międzynarodowych zawodach DDoS Game Day w Monachium organizowanych przez firmę Amazon Web Services.
- Warsztat z Fortinet w dniu 3.07.2024 r. – prezentacja zasady działania Supportu oraz PSIRT Fortinet w kontekście badania urządzeń narażonych na cyberatak.
- Warsztaty z Yubico w dniach 31.07.2024 oraz 24.09.2024 dot. ochrony kluczowych dostępów za pomocą uwierzytelniania wieloskładnikowego odpornego na phishing.
- W dniu 17.12.2024 r. w siedzibie Amazon Web Services (AWS) odbył się finał AWS DDoS Game Day. Wydarzenie, podczas którego uczestnicy rywalizowali w symulacji rzeczywistych scenariuszy ataków typu DDoS. Każdy zespół otrzymał środowisko IT, które należało zabezpieczyć przed falami ataków, korzystając z zaawansowanych narzędzi AWS, takich jak AWS Shield, AWS WAF (Web Application Firewall) czy Amazon CloudFront. Zespoły musiały w czasie rzeczywistym analizować sytuację, identyfikować zagrożenia i implementować skuteczne rozwiązania obronne. W finale udział wzięły przedstawiciele instytucji odpowiedzialnych za cyberbieczeństwo na poziomie krajowym. Najlepsza okazała się drużyna ZagubieniwAkcji złożona z przedstawicieli Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni. Wydarzenie było doskonałą okazją do poznania nowoczesnych rozwiązań w zakresie ochrony przed atakami DDoS oraz wymiany doświadczeń w zakresie budowania odpornych architektur IT. Uczestnicy mieli szansę zdobyć praktyczną wiedzę i umiejętności, które pozwolą skuteczniej chronić cyberprzestrzeń przed coraz bardziej zaawansowanymi zagrożeniami.
- Warsztaty techniczne organizowane przez Trafford w dniach 19.11.2024 r. 4.12.2024 r dot. systemów CTI Recoded Future.

Współpraca w ramach programu PWCyber przynosi pozytywne rezultaty w postaci rozwoju kompetencji w zakresie cyberbezpieczeństwa oraz promowania nowych rozwiązań w sektorze publicznym.

W 2025 r. w ramach kontynuacji i dalszej ewaluacji Programu zaplanowano wprowadzenie regulaminu Programu, zwiększenie aktywności obecnych partnerów oraz powołanie kolejnych grup roboczych.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber

9.4.2 UPOWSZECHNIANIE USŁUG CHMUROWYCH W ADMINISTRACJI RZĄDOWEJ

Miniony rok był czasem dążenia do upowszechnienia usług przetwarzania w chmurze obliczeniowej w administracji rządowej. Dążąc do realizacji Cloud First Policy przygotowany został projekt nowelizacji uchwały Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (WIIP)

oraz rozpoczęły się prace nad aktualizacją dokumentu Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO).

Znowelizowana uchwała WIIP weszła w życie w dniu 29 października 2024 r. i dokonała szeregu zmian w zakresie załącznika nr 2. Zmiany te koncentrują się na znacznym poszerzeniu możliwości korzystania przez podmioty administracji rządowej z usług przetwarzania w Publicznej Chmurze Obliczeniowej (PChO) w jurysdykcji krajowej lub pozostałych państw EOG jeśli stosują prawo Unii Europejskiej.

Powyższa zmiana stanowi odpowiedź na oczekiwania i potrzeby podmiotów administracji, które zgłaszały problem zbyt wąskiego podejścia w korzystaniu z usług przetwarzania w chmurze obliczeniowej. Fakt ten ma szczególne znaczenie w aspekcie bieżących uwarunkowań geopolitycznych, które mają bezpośredni wpływ na bezpieczeństwo państwa.

W ramach nowelizacji umożliwiono również przetwarzanie w PChO informacji niejawnych o klauzuli „zastrzeżone" lub równoważnej klauzuli międzynarodowej, w przypadku podmiotów, o których mowa w art. 10 ust. 2 pkt 1 i 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych [35], w odniesieniu do których zadania w zakresie nadzoru nad funkcjonowaniem systemu ochrony informacji niejawnych realizuje Służba Kontrwywiadu Wojskowego.

Zmiany w uchwale WIIP oznaczają szerszą dostępność różnego rodzaju oprogramowania dla administracji rządowej, które nie jest już dostępne w „tradycyjnym" modelu on-premise bądź nie jest właściwym rozwiązaniem pod kątem kosztowym i bezpieczeństwa.

Jednocześnie należy zaznaczyć, że uchwała nie zakłada obligatoryjnego korzystania z usług przetwarzania w chmurze, w tym w szczególności z PChO. W dalszym ciągu to gestor systemu decyduje czy skorzystać z rozwiązań przewidzianych w uchwale. Jeżeli zdecyduje się na takie działanie to przed skorzystaniem z usług w PChO obowiązany jest do wykonania szeregu czynności, które mają na celu wykluczyć lub zminimalizować ryzyko związane ze skorzystania z tych usług.

Wejście w życie przedmiotowej uchwały dla podmiotów komercyjnych oznacza szersze możliwości świadczenia usług dla administracji rządowej, co de facto powinno przełożyć się na liczniejsze przystępowanie do umów ramowych i umieszczanie swoich ofert dotyczących usług w katalogu w systemie ZUCH[36] co pozytywnie wpłynie na konkurencyjność i różnorodność usług.

W związku z nowelizacją uchwały WIIP rozpoczęto prace nad aktualizacją SCCO. Dokument ten jest kluczowy w zakresie warunkowania dostępu określonych kategorii systemów do właściwej chmury obliczeniowej.

Szczególne znaczenie SCCO w aspekcie uchwały WIIP wynika z tego, iż decyzja o skorzystaniu z usług chmurowych dostawcy komercyjnego musi zostać podjęta na podstawie wyników analizy załącznika nr 2 do uchwały, a następnie zostać potwierdzona przez analizę dokonaną na podstawie SCCO. Dokument ten określa poziomy bezpieczeństwa determinujące stosowanie poszczególnych modeli chmur obliczeniowych. Kategoryzacja bezpieczeństwa systemu teleinformatycznego dokonana na podstawie załącznika nr 2 do Inicjatywy WIIP ma bezpośredni wpływ na określenie poziomu wymagań bezpieczeństwa determinującego wybór modelu chmur obliczeniowych. W praktyce oznacza to, że gestor systemu w pierwszej kolejności analizuje sytuację swojego podmiotu na podstawie załącznika nr 2 do Inicjatywy WIIP, a następnie na podstawie SCCO.

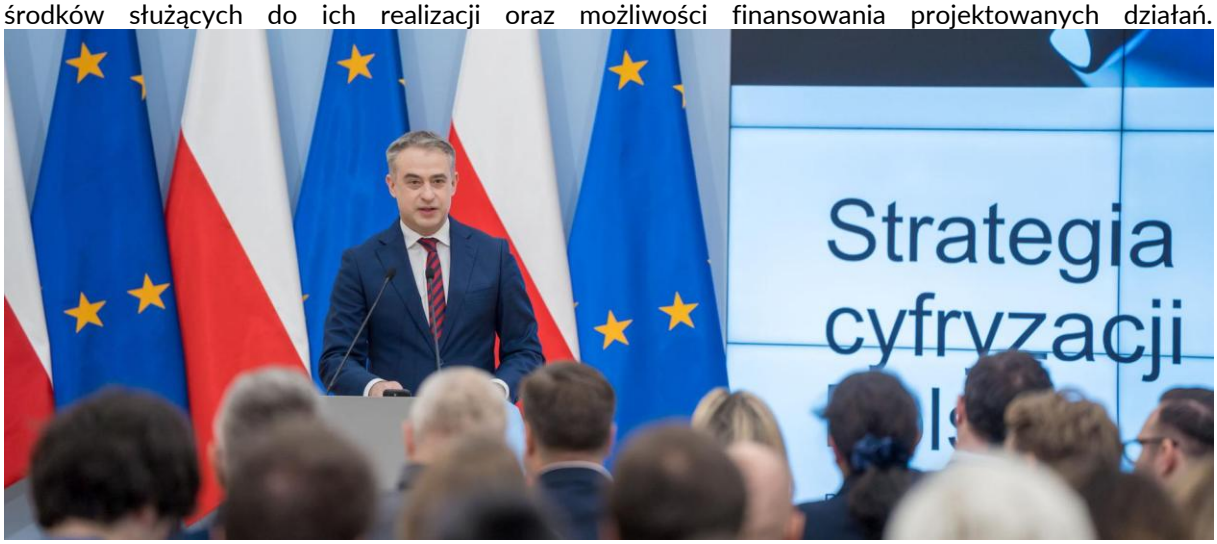
Z tego powodu konieczna jest aktualizacja m.in. katalogu zabezpieczeń właściwego rodzaju chmury obliczeniowej i kryteriów bezpieczeństwa w poziomach SCCO.

[35] Dz. U. z 2024 r. poz. 632 i 1222.
[36] System Zapewniania Usług Chmurowch.

9.4.3 PRACE NAD DOKUMENTEM STRATEGICZNYM W DZIEDZINIE INFORMATYZACJI PAŃSTWA

Ministerstwo Cyfryzacji prowadzi prace nad dokumentem o charakterze strategicznym w dziedzinie informatyzacji państwa, zwanym dalej „Strategią Cyfryzacji", określającym kierunki procesu transformacji cyfrowej państwa w perspektywie do 2035 r. Podstawę prawną dla dokumentu będzie stanowić art. 12aa-12ad ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Przepisy stanowiące podstawę prawną dla Strategii Cyfryzacji zostały zamieszczone w projekcie ustawy (UC44). Wejście w życie przepisów ustawy planuje się na I połowę 2025 r.

W Strategii zostały wyznaczone cele w najważniejszych obszarach cyfryzacji wraz ze wskazaniem środków służących do ich realizacji oraz możliwości finansowania projektowanych działań.



Rysunek 18. Konferencja prasowa dot. publikacji Strategii Cyfryzacji Polski

Nadrzędnym celem, który realizować ma Strategia Cyfryzacji jest poprawa jakości życia obywateli przy pomocy technologii cyfrowych. W pracy nad dokumentem zidentyfikowano kluczowe (horyzontalne) obszary, stanowiące czynniki o fundamentalnym wpływie na realizację celu głównego tj. zapewnienie cyberbezpieczeństwa, zapewnienie dostępu do szybkich, wydajnych i bezpiecznych usług telekomunikacyjnych, a także wzmocnienie kompetencji przyszłości oraz poprawa koordynacji cyfrowej transformacji kraju. Horyzontalne obszary mają również kluczowe znaczenie dla powodzenia realizacji pozostałych szczegółowych celów Strategii Cyfryzacji, które zostały zgrupowane w trzech kategoriach: Państwo (obszary związane z funkcjonowaniem administracji publicznej), Ludzie (obszary koncentrujące się na obywatelach) oraz Biznes i nowe technologie (obszary odnoszące się do cyfrowej transformacji gospodarki).

Szczególną rolę w procesie wdrażania i realizacji Strategii odegrają pełnomocnicy ds. informatyzacji, powoływani w urzędach obsługujących ministrów kierujących działami administracji rządowej oraz w Kancelarii Prezesa Rady Ministrów, których głównymi zadaniami będzie koordynacja realizacji strategii, nadzorowanie jej wdrażania oraz diagnozowanie obszaru koniecznych zmian w zakresie działu."

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku

9.4.4 FORUM OCHRONY INFRASTRUKTURY KRYTYCZNEJ MINISTRA CYFRYZACJI

W dniu 5 grudnia 2024 roku, Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji, zorganizował w formule on-line „Forum Ochrony Infrastruktury Krytycznej dla systemów: łączności, sieci teleinformatycznych i zapewniającego ciągłość działania administracji publicznej" zrealizowane na podstawie (art. 6 ust 1. pkt 5 w związku z art. 5b ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122, z 2024 r. poz. 834, 1222, 1473, 1572, 1907). Celem wydarzenia było wzmocnienie świadomości oraz wymiana doświadczeń w zakresie m.in. „Nowych i przełomowych technologii" w zakresie zagrożeń stwarzanym przez wykorzystanie nowych technologii oraz zagadnieniom związanym z bezpieczeństwem obiektów Infrastruktury Krytycznej.

W wydarzeniu uczestniczyło około **100** osób. W 2025 roku planowane jest kolejne takie przedsięwzięcie.

Więcej informacji pod adresem: *https://www.gov.pl/web/rcb/xi-krajowe-forum-ochrony-infrastruktury-krytycznej*

9.4.5 KRAJOWY PLANU DZIAŁANIA DO PROGRAMU POLITYKI „DROGA KU CYFROWEJ DEKADZIE" DO 2030 R.

Ministerstwo Cyfryzacji, we współpracy z właściwymi interesariuszami na poziomie krajowym, opracowało Krajowy plan działań do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r., który został przyjęty uchwałą nr 125 Rady Ministrów z dnia 22 października 2024 r. i został opublikowany w Monitorze Polskim poz. 989. Przyjęcie planu jest odpowiedzią na zobowiązania wynikające z Decyzji Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r. Celem programu „Droga ku cyfrowej dekadzie" jest osiągnięcie wspólnych dla całej Unii Europejskiej celów cyfrowych do 2030 roku.

Projekt Krajowego planu wskazuje m.in. na wdrożone i planowane polityki, interwencje i działania, które Polska zobowiązuje się podjąć w celu przyśpieszenia transformacji cyfrowej, zmierzając do osiągnięcia celów ogólnych i celów cyfrowych programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. Jednym z celów ogólnych ww. programu polityki jest poprawa odporności na cyberataki, przyczynianie się do zwiększenia świadomości ryzyka oraz szerzenia wiedzy na temat procedur cyberbezpieczeństwa, przy intensyfikacji wysiłków organizacji publicznych i prywatnych na rzecz osiągnięcia co najmniej podstawowego poziomu cyberbezpieczeństwa.

Aktualnie trwa rewizja Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. Polska, tak jak wszystkie państwa członkowskie, zobowiązana jest przedłożyć Komisji korektę dokumentu, zgodnie z rekomendacjami zawartymi w sprawozdaniu krajowym[37] w ramach raportu na temat stanu cyfrowej dekady.

Więcej informacji pod adresem: *https://www.gov.pl/web/cyfryzacja/program-polityki-droga-ku-cyfrowej-dekadzie-do-2030-r2*

9.4.6 POZYSKANIE PLATFRMY CYBER THREAT INTELLIGENCE, CTI

W 2024 r. Ministerstwo Cyfryzacji wdrożyło platformę Cyber Threat Intelligence (CTI) do rozpoznawania zagrożeń w cyberprzestrzeni na poziomie operacyjnym. Wprowadzona została na potrzeby Ministerstwa oraz siedmiu instytucji zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym.

Platforma wykorzystywana jest do pozyskiwania oraz przetwarzanie informacji dotyczących aktywności grup APT oraz innych potencjalnych zagrożeń dla bezpieczeństwa państwa. Narzędzie te, jest niezbędne do zapobiegania występowaniu incydentów bezpieczeństwa oraz minimalizowania ich potencjalnych negatywnych skutków ich wystąpienia. Platforma CTI poziomu operacyjnego wykorzystana jest m.in.

[37] https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports

przez zespoły reagowania na incydenty komputerowe (CSIRT) wchodzące w skład krajowego systemu cyberbezpieczeństwa. Jest to narzędzie umożliwiające znaczące podniesienie bezpieczeństwa polskiej cyberprzestrzeni poprzez między innymi:

- wykrycie prowadzonych ataków hakerskich;
- wykrycie wystąpienia incydentu komputerowego;
- śledzenie skutków wystąpienia incydentu oraz identyfikację ofiar danej kampanii;
- badanie głębokich zasobów internetu (dark-web, deep-web) poprzez dostęp do zamkniętych forów zrzeszających cyberprzestępców;
- badanie mediów społecznościowych celem zbierania informacji o zagrożeniach w cyberprzestrzeni;
- wykrycie wycieku danych uwierzytelniających użytkowników oraz przeciwdziałanie ich nielegalnej sprzedaży;
- monitorowanie rejestracji domen wykorzystywanych w atakach phishingowych;
- pozyskiwanie informacji o taktykach, technikach oraz procedurach stosowanych przez adwersarzy;
- pozyskiwanie informacji o podatnościach na rozwiązania stosowane w systemach teleinformatycznych.

Pozyskanie platformy zostało zrealizowane na rzecz podmiotów wchodzących w skład KSC, co w sposób znaczący przyczyniło się do podniesienia bezpieczeństwa państwa oraz w konsekwencji sektora publicznego i prywatnego.

Rosnąca liczba cyberataków w Polsce i na świecie wskazuje na eskalację zagrożeń w sferze cyberprzestrzeni. Ataki te mogą powodować znaczne szkody finansowe, utratę danych, naruszenie prywatności. Wykorzystanie platformy CTI poziomu operacyjnego umożliwi skuteczną i szybką reakcję na te zagrożenia i minimalizację potencjalnych strat. Pozyskanie rozwiązania to strategiczny krok, który pomoże utrzymać stabilność systemów teleinformatycznych w Polsce oraz w czasie rzeczywistym ochronić kluczowe zasoby przed atakami – również w zakresie funkcjonowania infrastruktury krytycznej państwa. Dodatkowo w kontekście wojny w Ukrainie i napiętej sytuacji geopolitycznej, istnieje zwiększone ryzyko cyberataków skierowanych przeciwko infrastrukturze naszego kraju. Zaopatrzenie kluczowych dla cyberbezpieczeństwa państwa podmiotów w rozwiązanie z zakresu CTI wzmocni zdolności do skutecznego śledzenia oraz przeciwdziałania zagrożeniom w cyberprzestrzeni.

9.5 BUDOWANIE ŚWIADOMOŚCI I KOMPETENCJI SPOŁECZNYCH W ZAKRESIE CYBERBEZPIECZEŃSTWA

9.5.1 PORTAL „BEZPIECZENEDANE.GOV.PL"

W 2024 r. powierzono utrzymanie i rozwój portalu bezpiecznedane.gov.pl NASK-PIB. Portal był aktualizowany o nowe wycieki umożliwiając użytkownikom sprawdzenie, czy ich dane trafiły w ręce cyberprzestępców. Dzięki działaniu portalu BezpieczneDane.gov.pl możliwe jest wyeliminowanie bądź ograniczenie negatywnych skutków wycieku danych polskich użytkowników internetu, które mogą mieć poważne skutki o charakterze zarówno materialnym jak i niematerialnym. Portal ma także wartość edukacyjną przejawiającą się w informowaniu jego użytkowników o tym jakie działania powinien podjąć, aby zapobiegać wyciekom danych bądź skutkom tych wycieków.

Więcej informacji pod adresem: https://bezpiecznedane.gov.pl/

Rysunek 19. Bezpiecznedane.gov.pl

9.5.2 USTAWA O OCHRONIE MAŁOLETNICH PRZED DOSTĘPEM DO TREŚCI NIEODPOWIEDNICH W INTERNECIE

W 2024 r. kontynuowano prace nad projektem ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie, mającej zapewnić bezpieczeństwo małoletnim w internecie i ograniczenie negatywnego dla ich rozwoju wpływu treści szkodliwych, jak np. powszechny i niemal nieograniczony dostęp przez dzieci i młodzieży do treści pornograficznych. 13 grudnia 2024 r. odbył się Kongres Ogólnopolskiej Sieci Edukacyjnej, organizowany przez Ministerstwo Cyfryzacji, Naukową i Akademicką Sieć Komputerową (NASK) oraz Uniwersytet Jagielloński, na którym zaprezentowano m.in. założenia projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych, a także omówiono najważniejsze zagadnienia z prac powołanej przez Ministerstwo Cyfryzacji grupy roboczej ds. ochrony małoletnich przed treściami szkodliwymi w internecie, zrzeszającej przedstawicieli środowiska naukowego, prawniczego, przedstawicieli organizacji pozarządowych oraz przedsiębiorców telekomunikacyjnych.

W grudniu 2024 r. Ministerstwo Cyfryzacji złożyło wniosek o wpis projektowanej ustawy do wykazu prac legislacyjnych i programowych Rady Ministrów.

9.5.3 USTAWA O ZWALCZANIU NADUŻYĆ W KOMUNIKACJI ELEKTRONICZNEJ

W minionym roku zostały wdrożone ostatnie rozwiązania techniczne służące stosowaniu ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej, mającej na celu zwiększenie ochrony użytkowników przed szkodliwymi działaniami dokonywanymi za pośrednictwem technologii komunikacyjnych. W szczególności uruchomiony został system umożliwiający automatyczne blokowanie wiadomości, które są zgodne z wzorcem wiadomości smishingowej. W wyniku zastosowania tego systemu do grudnia 2024 r. udało się zablokować 1 064 907 szkodliwych wiadomości sms.

Na podstawie ww. ustawy funkcjonuje również Lista Ostrzeżeń przed niebezpiecznymi stronami, na którą wpisywane są domeny, które wprowadzają użytkowników w błąd i wyłudzają od nich dane. W 2024 r. na listę wpisano 84 179 domen. Na podstawie wpisów na liście zostało zablokowanych 75 864 441 prób połączenia z niebezpiecznymi domenami[38].

[38] Dane z listopada 2024 r.

9.5.4 PROGRAM „HIGIENA CYFROWA”

W 2024 r. Ministerstwo Cyfryzacji udzieliło NASK-PIB dotacji celowej w wysokości 249 728,17 zł na realizację zadania publicznego pn. „Higiena cyfrowa”. Zadanie było realizowane od 1 września do 31 grudnia 2024 r. Zadanie składało się z 3 głównych działań:

- przygotowanie koncepcji zadania publicznego, w tym przygotowanie księgi znaku (Key-visual) materiałów edukacyjnych i programu szkoleń dla nauczycieli.
- rekrutacja nauczycieli oraz organizacja szkoleń - webinarów dla nauczycieli.
- przeprowadzenie zajęć dla uczniów.

W ramach zadania publicznego prowadzono zajęcia z higieny cyfrowej obejmujące w szczególności zajęcia z bezpieczeństwa w sieci dla uczniów szkół podstawowych. Zajęcia z bezpieczeństwa w sieci przeprowadzili nauczyciele z poszczególnych szkół uprzednio przeszkoleni przez specjalistów z NASK - PIB.

Więcej informacji pod adresem: https://www.gov.pl/web/cppc/cyfrowa-higiena--czyli-gdzie-zaczyna-sie-dobrostan-kompetencjecyfrowedlakazdego

9.5.5 MONITORING TREŚCI O POTENCJALE DEZINFORMACYJNYM W MEDIACH SPOŁECZNOŚCIOWYCH

Centrum Rozwoju Kompetencji Cyfrowych MC (CRKC) we współpracy z NASK zrealizowało w 2024 roku działania w zakresie przeciwdziałania dezinformacji w ramach zadania „Monitoring treści o potencjale dezinformacyjnym w mediach społecznościowych oraz prace rozwojowe nad usprawnieniem narzędzi wspierających budowanie odporności administracji publicznej oraz społeczeństwa wobec zjawiska dezinformacji poprzez działania naukowe i edukacyjne” (umowa nr 364/C/CRKC/2023 z dnia 17.11.2023):

- ciągły monitoring sfery informacyjnej,
- analizy narracji o charakterze dezinformacyjnym, w tym opracowanie ilościowe i jakościowe narracji pojawiających się w polskiej infosferze,
- edukacja interesariuszy z administracji publicznej oraz różnych grup społecznych w zakresie przeciwdziałania dezinformacji

W ramach zadania realizowany był monitoring polskiej infosfery, wykrywano grupy botów realizujące działania dezinformacyjne, edukowano społeczeństwo poprzez m.in.:

- kampanie społeczne, udział w konferencjach, stworzono i rozwijano portal dzięki któremu istnieje możliwość zgłaszania treści o charakterze dezinformacyjnym.
- ponadto na stronie *www: kompetencjecyfrowe.gov.pl* znajdują się kursy oraz poradniki dotyczące tematyki cyberbezpieczeństwa skierowane do różnych grup, w tym przedsiębiorców, nauczycieli, rodziców czy też seniorów. W IV kwartale 2024 r.
- Centrum rozpoczęło realizację kampanii internetowej promującej rozwój kompetencji cyfrowych, podczas której nie zabrakło działań edukacyjno-informacyjnych obejmujących temat bezpieczeństwa w sieci, edukacji w zakresie dezinformacji i misinformacji oraz higieny cyfrowej. Ponadto, w ramach działań komunikacyjnych, w tym samym okresie, na antenach 17 rozgłośni regionalnych Polskiego Radia realizowana była emisja kampanii radiowej pod nazwą „W cyfrowym świecie”, a podczas łącznie 119 audycji słuchaczy zachęcano do stałego podnoszenia kompetencji cyfrowych oraz wzmacniania świadomości o zagrożeniach występujących w świecie cyfrowym, a także zbudowania przekonania o konieczności przemyślanego i bezpiecznego korzystania z otaczającej nas technologii.

9.5.6 PROJEKT „SZKOŁA MIĘDZYPOKOLENIOWA”

Wśród wielu inicjatyw realizowanych przez Centrum Rozwoju Kompetencji Cyfrowych należy wyróżnić także rozpoczęty w połowie grudnia 2024 r. projekt „Szkoła międzypokoleniowa”, w ramach którego uczniowie klas VII-VIII szkół podstawowych i ponadpodstawowych pod przewodnictwem swoich nauczycieli będą przeprowadzać warsztaty dla seniorów poświęcone kompetencjom cyfrowym oraz cyberbezpieczeństwu. Poza podstawami bezpieczeństwa w internecie, wśród zaproponowanych do

przeprowadzenia podczas warsztatów zagadnień pojawia się temat oszustw w sieci, w tym phishingu i metody „na wnuczka”.

Rysunek 20. Podpisanie projektu

9.5.7 USŁUGA „BAZA WIEDZY”

W dniu 10.09.2024 r. do usługi aplikacji mObywatel została dodana „Baza wiedzy – przestrzeń”, w której użytkownicy mają możliwość zapoznania się z artykułami na temat zasad bezpiecznego poruszania się po Internecie oraz szerokorozumianej higieny cyfrowej.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/

9.5.8 CERTYFIKACJA W CYBERBEZPIECZEŃSTWIE

W 2024 r. MC zleciło realizację zadania pn. **„Realizowanie zadań uczestnika oraz akredytowanej Jednostki Certyfikującej spełniającej wymagania**”.

NASK-PIB, w ramach udzielonej dotacji, realizował zadania na poziomie operacyjnym polegające na wykonywaniu w imieniu Rządu RP zadań Uczestnika w ramach Umowy o wzajemnym uznawaniu certyfikatów oceny bezpieczeństwa teleinformatycznego oraz w ramach Porozumienia w sprawie uznawania Certyfikatów Common Criteria w dziedzinie bezpieczeństwa teleinformatycznego, a także wykonywaniu zadań Jednostki Certyfikującej Spełniającej Wymagania (*ang. Compliant Certification Body*), odpowiedzialnej za zarządzanie Programem Oceny i Certyfikacji Bezpieczeństwa IT oraz za autoryzację laboratoriów badawczych. Pozwala to jednostce certyfikacyjnej zlokalizowanej w NASK-PIB na wydawanie certyfikatów Common Criteria uznawanych w państwach tego Porozumienia jak np. USA, Kanada, Niemcy czy Japonia.

Ponadto, zlecono realizację zadania pn. „**Realizacja zadań w obszarze przygotowań Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych w IŁ-PIB do przejścia z powodzeniem procesu autoryzacji dla celów EUCC**”. Celem działań IŁ-PIB w ramach zadania było zapewnienie dla Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych w IŁ-PIB poziomu uzasadnienia zaufania „wysoki”, czyli wyższego poziomu z CSA.

Wskazaniem IŁ-PIB do realizacji zadania było zwiększanie przedmiotowe poziomu wysokiego uzasadnienia zaufania w dokumentach na poziomie europejskim w najbliższych latach – nowe obowiązki nakłada Akt o cyberodporności (CRA), Dyrektywa NIS 2 i Rozporządzenie UE o Sztucznej Inteligencji (AI Act). Aby zapewnić realną możliwość przeprowadzania certyfikacji oraz rozwijać rynek certyfikacji w Polsce, konieczny jest rozwój jednostek certyfikacyjnych oraz laboratoriów.

Ponadto 2024 r. przygotowany został projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42), który ma na celu dostosowanie polskiego porządku prawnego do europejskich regulacji w tym obszarze, a także pozwoli wprowadzić krajowe schematy certyfikacyjne.

Dzięki temu możliwe będzie wydawanie w Polsce certyfikatów opartych na europejskich programach certyfikacji cyberbezpieczeństwa, które są automatycznie uznawane we wszystkich państwach członkowskich Unii Europejskiej. Projekt określa również zasady nadzoru nad wydanymi certyfikatami oraz wprowadza możliwość wydawania krajowych certyfikatów cyberbezpieczeństwa. Dzięki temu możliwa będzie promocja cyberbezpiecznych rozwiązań w nowych obszarach nieobjętych europejskimi programami cyberbezpieczeństwa. Ustawa przewiduje też wprowadzenie certyfikacji osób z zakresu cyberbezpieczeństwa co umożliwi specjalistom uzyskać dodatkowe potwierdzenie swoich kompetencji, a także będzie stanowić cenne wsparcie w ocenie kompetencji.

Projekt ustawy 20 maja 2025 r. został przekazany do uzgodnień, opiniowania oraz konsultacji publicznych. Na podstawie zgromadzonych uwag zaktualizowano projekt ustawy, który został skierowany na Komitet do spraw Europejskich. 30 grudnia 2024 r. komitet zaakceptował przedstawiony projekt.

Jednostka Certyfikacyjna NASK-PIB oraz współpracujące z nią laboratoria podjęły już działania w celu dostosowania się do wymogów wynikających z europejskich programów certyfikacji cyberbezpieczeństwa.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/akt-o-cyberbezpieczenstwie

9.5.9 PROGRAM „CYBERSECIDENT”

W 2024 r. kontynuowano realizację projektów w ramach programu CYBERSECIDENT „Cyberbezpieczeństwo i eTożsamość”. Celem tego programu jest wytwarzanie rozwiązań nakierowanych na podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP. W wyniku zakończonych projektów wypracowanych w ramach programu, Minister Cyfryzacji nabył autorskie prawa majątkowe do tych rozwiązań, a następnie udzielił wykonawcy projektu licencji na ww. rozwiązania.

Więcej informacji pod adresem:
https://www.gov.pl/web/ncbr/cybersecidenthttps://www.gov.pl/web/ncbr/cybersecident

9.5.10 ZWALCZANIE NIEGODZIWEGO TRAKTOWANIA DZIECI W CELACH SEKSUALNYCH W INTERNECIE

W 2024 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1307, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1232 w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w celu zwalczania niegodziwego traktowania dzieci w celach seksualnych w Internecie. Nowelizacja wydłużyła okres obowiązywania rozporządzenia 2021/1232 o dwa lata, tj. do 3 sierpnia 2026 r. oraz, w celu usprawnienia procesu sprawozdawczego, znormalizowane szablony dla dostawców usług łączności interpersonalnej niewykorzystujących numerów. W pozostałym zakresie nie zmieniła przepisów tego aktu. Przedłużenie obowiązywania tymczasowych regulacji umożliwi dalsze stosowanie przepisów dotyczących wykrywania i usuwania pornografii dziecięcej, wykrywania praktyk nagabywania dzieci w Internecie w celach pedofilskich do czasu uchwalenia docelowych, długookresowych przepisów unijnych dotyczących ochrony dzieci przed niegodziwym traktowaniem w celach seksualnych w Internecie. Obecnie w instytucjach unijnych trwają prace nad takimi docelowymi przepisami. Ze względu jednak na złożoność tej tematyki nie ma pewności, czy zakończą się w terminie gwarantującym wejście w życie rozporządzenia długoterminowego przed wygaśnięciem rozporządzenia przejściowego.

W 2024 r. przygotowano ponadto dla Komisji Europejskiej, na podstawie art. 8 rozporządzenia 2021/1232, sprawozdanie w sprawie wykrytych przypadków niegodziwego traktowania dzieci w celach seksualnych w internecie. W 2025 r. planowane jest przekazanie kolejnej informacji dla Komisji.

9.5.11 PROJEKT „SECUREV” - SZKOLENIA Z CYBERBEZPIECZEŃSTWA DLA NAJWAŻNIEJSZYCH OSÓB W PAŃSTWIE

W 2024 r. Ministerstwo Cyfryzacji kontynuowało prowadzone od 2021 r. działania prewencyjno-edukacyjne dla najważniejszych osób w państwie (projekty SecureV). W ramach działania prowadzone są specjalistyczne szkolenia z zakresu cyberbezpieczeństwa adresowane do najważniejszych osób

w państwie. Terminy i zakres merytoryczny szkoleń dostosowywane są do konkretnych potrzeb szkolonej osoby. Dodatkowo, każda indywidualnie przeszkolona osoba zostaje wyposażona w uniwersalne narzędzia służące do silnego uwierzytelnienia wraz z instruktażem stosowania narzędzia. Z uwagi na dynamiczną sytuację w cyberprzestrzeni kraju oraz duże zainteresowanie szkoleniami, kolejne edycje projektu uwzględniają coraz większą grupę odbiorców. Początkowo projekt SecureV obejmował wyłącznie parlamentarzystów i kadrę kierowniczą administracji centralnej.

Od 2023 r. zasięg działań prewencyjno-edukacyjnych objął już terytorium całego kraju, a projektem szkoleniowym objęci są parlamentarzyści, kadra kierownicza administracji centralnej i samorządowej, przedstawiciele Krajowego Biura Wyborczego oraz pracownicy Podstawowej Opieki Zdrowotnej.

W edycji SecureV 2024 udział w szkoleniach wzięło prawie 5 000 osób, a od 2021 r., w ramach działań SecureV przeszkolono niemal 12 000 osób.

Dzięki zdobytemu doświadczeniu z poprzednich lat oraz zbudowaniu zespołu trenerskiego, ww. szkolenia będą realizowane również w kolejnych latach 2025-2026 r.

Tabela 36. Szkolenia w ramach programu SecureV

Rok	2021	2022	2023	2024	Łącznie
l. szkoleń	442	1 006	2 959	3 731`	8 138
l. przeszkolonych osób	442	1 048	5 288	4 981	11 759

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-w-sprawie-oszustw-w-komunikacji-z-osobami-publicznymi

9.5.12 SZKOLENIA ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

W roku 2024 Ministerstwo Cyfryzacji kontynuowało prowadzone od 2020 r. szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa. Szkolenia prowadzone są przez ekspertów i praktyków na co dzień zajmujących się kwestiami cyberbezpieczeństwa – ekspertów NASK-PIB, partnerów technologicznych PWCyber. Szkolenia realizowane są na różnym poziomie zaawansowania wiedzy z zakresu cyberbezpieczeństwa, dostosowane do bieżącej sytuacji i zgłaszanych potrzeb (od 2024 r. część szkoleń realizowana jest z udziałem tłumaczy na Polski Język Migowy (PJM)).

W ramach szkoleń online w 2024 r. zorganizowano:

- 8 szkoleń z zakresu higieny cyfrowej (4 cykle) we współpracy z NASK-PIB. Cykl składa się z dwóch szkoleń: Cyberzagrożenia - bądź na bieżąco! oraz Podstawowe zasady cyberhigieny w pracy i w życiu prywatnym. Z uwagi na ogromne zainteresowanie szkoleniami z podstaw cyberbezpieczeństwa, od 2023 roku cykl jest powtarzany regularnie raz na kwartał. W 2024 r. w szkoleniach z podstaw higieny cyfrowe udział wzięło 12 492 osób.
- 7 szkoleń w ramach cyklu szkoleń dla podmiotów publicznych wykonujących działalność leczniczą (kontynuacja cyklu specjalistycznych szkoleń skierowany do kadry kierowniczej, personelu IT i osób zarządzających cyberbezpieczeństwem w podmiotach świadczących usługi z zakresu ochrony zdrowia). 3 022 Cały cykl objął 10 szkoleń online i był realizowany we współpracy z ekspertami partnerów technologicznych Programu PWCyber
- 27 szkoleń online zrealizowanych we współpracy z partnerami PWCyber, w których udział wzięło 18 125 osób.

Celem szkoleń jest nie tylko zwiększenie świadomości kadr KSC na temat cyberzagrożeń, ale również podniesienie umiejętności praktycznych związanych z wykorzystywaniem narzędzi informatycznych oraz radzenia sobie w sytuacjach kryzysowych.

Łącznie, w 2024 r. zrealizowano **42 szkolenia online**, w których uczestniczyło prawie **34 tys. osób**.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen

9.5.13 PROJEKTY WSPIERAJĄCE EDUKACJE O CYBERBEZPIECZEŃSTWIE – „CYBERLEKCJE”

Minister Cyfryzacji realizuje różnego rodzaju inicjatywy wspierające edukacje o bezpieczeństwie online wśród najmłodszych użytkowników sieci. Projekt Cyber lekcje realizowany jest od 2021 roku wspólnie z Państwowym Instytutem Badawczym NASK. Adresowany jest do nauczycieli i pedagogów, chcących podczas swoich zajęć przekazywać dzieciom i młodzieży zasady i wskazówki dotyczące bezpiecznego poruszania się w Internecie. W ramach projektu Cyberlekcje powstało 18 gotowych scenariuszy zajęć lekcyjnych o cyberbezpieczeństwie, które obejmują różne tematy, takie jak bezpieczeństwo online, prywatność, relacje w sieci, zagrożenia online, zarządzanie danymi, nadużywanie nowych technologii i dobrostan psychiczny

Rysunek 21. Cyberlekcje

W 2024 r. zrealizowano pilotażowo kolejną odsłonę projektu, której celem było m.in. upowszechnienie przygotowanych materiałów w latach poprzednich, poprzez bezpośredni kontakt z pedagogami. Celem pilotażu była również organizacja szkoleń, które wyposażą nauczycieli w wiedzę z obszaru cyberhigieny i socjotechnik wykorzystywanych przez oszustów w cyberprzestrzeni.

W ramach pilotażu zrealizowano:

- 7 całodniowych szkoleń dla nauczycieli z zakresu cyberbezpieczeństwa w miastach województwa mazowieckiego w których uczestniczyło 263 nauczycieli.
- 18 dwugodzinnych szkoleń dla nauczycieli, w których udział wzięło 571 nauczycieli.
- 48 lekcji dla uczniów szkół podstawowych i ponadpodstawowych, w których wzięło udział 1876 uczniów
- 14 lekcji online w których uczestniczyło 2 181 klas i 55 617 uczniów, co oznacza, że średnio w 1 lekcji online uczestniczyło 156 klas.
- W ramach tegorocznego projektu powstały także 4 nowe scenariusze zajęć lekcyjnych.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/jak-rozmawiac-o-cyberbezpieczenstwie-w-szkole-przedstawiamy-cyberlekcje

9.5.14 „BAZA WIEDZY” O CYBERBEZPIECZEŃSTWIE NA PORTALU GOV.PL

W trybie ciągłym rozwijana jest baza wiedzy o cyberbezpieczeństwie na portalu gov.pl. W 2024 r. w bazie wiedzy opublikowano ponad 99 nowych publikacji (artykuły, rekomendacje dotyczące problematyki bezpieczeństwa w cyberprzestrzeni a także komunikaty o bieżących ostrzeżeniach CSIRT NASK).

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

9.5.15 ĆWICZENIA CYBERBEZPIECZEŃSTWA UE

W dniach 19-20 czerwca 2024 r. przeprowadzono ćwiczenia Cyber Europe 2024 (CE 2024). Ćwiczenia CE 2024 organizowane są cyklicznie przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Celem ćwiczeń było testowanie procedur reagowania na incydenty cyberbezpieczeństwa oraz procedur zarządzania kryzysowego w obliczu międzynarodowego kryzysu bezpieczeństwa w cyberprzestrzeni. W ćwiczeniach udział wzięły zespoły CSIRT poziomu krajowego (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego), agencje zarządzania kryzysowego, podmioty infrastruktury krytycznej oraz podmioty mające kluczowe znaczenie dla funkcjonowania społeczno-gospodarczego krajów UE. Każda edycja dotyczy innego sektora gospodarki, w tym roku obejmowała podmioty sektora energii w Europie.

Ćwiczenie ogólnoeuropejskie zgromadziło 30 narodowych zespołów reagowania na incydenty cyberbezpieczeństwa, liczne agencje i instytucje UE oraz ponad 1000 ekspertów zajmujących się różnymi obszarami, od reagowania na incydenty po podejmowanie decyzji.

Ze strony Ministerstwa Cyfryzacji (MC) w ćwiczeniu uczestniczyli przedstawiciele Departamentu Cyberbezpieczeństwa, zarówno w roli ćwiczących jako: Pojedynczy Punkt Kontaktowy, Zespół Reagowania Kryzysowego, Oficer CyCLONe oraz osoby odgrywające rolę kierownictwa MC, Pełnomocnika Rządu ds. Cyberbezpieczeństwa, jak również w roli obserwatora-planisty. Ponadto w ćwiczeniu udział wziął przedstawiciel Biura Komunikacji MC w roli zespołu prasowego.

Przedmiotem tegorocznej siódmej edycji ćwiczeń były cyberataki wymierzone w infrastrukturę energetyczną UE, o kluczowym znaczeniu dla funkcjonowania państw członkowskich Unii. Ćwiczenia przebiegły zgodnie z wcześniej opracowanym i uzgodnionym przez ekspertów fikcyjnym scenariuszem, który obejmował pięć głównych wydarzeń:

- Problemy z dostawą gazu;
- Problemy z dostawą energii elektrycznej;
- Utrata reputacji podmiotów sektora energii spowodowanej wyciekiem danych poufnych;
- Niedziałające serwisy internetowe spowodowane atakiem DDOS połączone z atakami ransomware;
- Atak typu "WaterHole" - zainfekowanie serwisów internetowych podmiotów sektora energii.

Ćwiczenia te stanowią okazję do przeanalizowania złożonych cyberincydentów i zareagowania na sytuacje zakłócające ciągłość działania i wymagające zarządzania kryzysowego. Ponadto, na szczeblu krajowym ćwiczenia dają możliwość przetestowania wewnętrznych procedur niezbędnych do zarządzania incydentami, wzmacniania współpracy w ramach krajowego systemu cyberbezpieczeństwa oraz weryfikacji planów ciągłości działania.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/udzial-ministerstwa-cyfryzacji-w-cwiczeniach-cyber-europe-2024

9.5.16 ĆWICZENIA KSC – „KSC-EXE 2024"

W dniu 29 lis. 2024 r. odbyły się ćwiczenia krajowego systemu cyberbezpieczeństwa KSC-EXE 2024.

W ćwiczeniach udział wzięło prawie 60 przedstawicieli podmiotów krajowego systemu cyberbezpieczeństwa, w tym:

- organy właściwe: Ministerstwo Klimatu i Środowiska, Ministerstwo Infrastruktury, Ministerstwo Zdrowia, Komisja Nadzoru Finansowego, Ministerstwo Cyfryzacji,
- zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego, czyli: CSIRT GOV, CSIRT MON, CSIRT NASK.
- przedstawiciele: Ministerstwa Spraw Zagranicznych, Prokuratury Krajowej, Rządowego Centrum Bezpieczeństwa, Urzędu Komunikacji Elektronicznej, Centralnego Biura Zwalczania Cyberprzestępczości.

Rysunek 22. Ćwiczenia KSC-EXE 2024

Ćwiczenia KSC-EXE 2024 pozwoliły na szczegółową weryfikację procedur reagowania na incydenty oraz współpracy między podmiotami odpowiedzialnymi za cyberbezpieczeństwo.

Ćwiczenia były szczególnie ważne z uwagi na nadchodzącą nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, która w 2025 roku wdroży unijne wymogi dyrektywy NIS 2[39]. Ćwiczenia stanowią istotny element w przygotowaniach do zmian w przepisach prawnych, które wprowadzą wyższe standardy bezpieczeństwa w obszarze cyberprzestrzeni.
Planujemy, aby takie ćwiczenia z udziałem ekspertów i praktyków z różnych dziedzin, odbywały się przynajmniej raz w roku.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/ksc-exe-2024-cwiczenia-krajowego-systemu-cyberbezpieczenstwa

[39] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

9.6 BUDOWANIE SILNEJ POZYCJI MIĘDZYNARODOWEJ RZECZYPOSPOLITEJ POLSKIEJ W OBSZARZE CYBERBEZPIECZEŃSTWA

9.6.1 WSPÓŁPRACA W RAMACH UNII EUROPEJSKIEJ

W ramach współpracy unijnej Ministerstwo Cyfryzacji realizowało zadania związane z koordynacją współpracy między organami właściwymi ds. cyberbezpieczeństwa RP z odpowiednimi organami w innych państwa członkowskich UE. Dotyczy to udziału w grupie współpracy NIS oraz w pracach następujących zespołów: WS5 - dostawcy usług cyfrowych, WS3 - raportowanie incydentów, WS7 – WS2 – środki bezpieczeństwa, WS5 - dostawcy usług cyfrowych, WS8 - sektor energii, WS10 - infrastruktura cyfrowa, WS12 - sektor zdrowia, WS on 5G and Telecom Security, WS on Supply Chain Security, 5G Toolbox, Sub-group standaryzacja i certyfikacja, europejska sieć zarządzania kryzysami cyfrowymi CyCLONE, Europejska Sieć Bezpieczeństwa Wyborów (ECNE), Horyzontalna Grupa Robocza ds.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/nasi-eksperci-aktywnie-wspieraja-grupe-wspolpracy-nis

9.6.1.1 ZESPÓŁ „CYBERPRZESTRZENI”

Cyberprzestrzeni (Cyber) (HWPCI), Grupa Robocza ds. Egzekwowania Prawa (LEWP) w zakresie CSAM. Przy czym warto podkreślić, że Polska przewodniczyła pracom zespołu WS10 - infrastruktura cyfrowa.

9.6.1.2 POJEDYNCZY PUNKT KONTAKTOWY

Ministerstwo Cyfryzacji realizowało również zadania Pojedynczego Punktu Kontaktowego, o którym mowa w Dyrektywie NIS, oraz koordynowało współpracę z podmiotami odpowiedzialnymi za cyberbezpieczeństwo, jak również prowadziło konsultacje z przedstawicielami resortów kluczowych w ramach współpracy w ramach cyberbezpieczeństwa.

MSZ realizowało działania na rzecz operacjonalizacji i wzmocnienia narzędzi cyberdyplomacji, szczególnie poprzez zgłoszenie non-paper ws. rozszerzenia narzędzi restrykcyjnych Cyber Diplomacy Toolbox o sankcje sektorowe. Resort ten brał też udział w pracach Horyzontalnej Grupy Roboczej ds. Cyberbezpieczeństwa (HWPCI), przede wszystkim w zakresie tematyki cyberdyplomacji. Bierze również aktywny udział w pracach unijnej sieci ambasadorów/krajowych koordynatorów ds. cyberbezpieczeństwa (cyber ambassador’s network) oraz wsparcie udziału Polski w sieci dyplomacji cyfrowej (digital diplomacy).

Więcej informacji pod adresem: https://www.gov.pl/web/ia/pojedynczy-punkt-kontaktowy

9.6.1.3 PRACE LEGISLACYJNE W RAMACH UE

Ministerstwo Cyfryzacji brało ponadto udział w pracach legislacyjnych na poziomie europejskim nad:

- Rozporządzeniem Parlamentu Europejskiego i Rady ustanawiającym środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty 2023/0109 (Cyber Solidarity Act),
- Rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020 (Cyber Resilience Act), Rozporządzeniem UE ustanawiającym przepisy mające na celu zapobieganie i zwalczanie seksualnego wykorzystywania dzieci (CSAM).
- Ministerstwo Cyfryzacji brało także udział w pracach Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa oraz Europejskiego Komitetu Certyfikacji Cyberbezpieczeństwa. W ramach tych prac prezentowane było stanowisko Polski dotyczące europejskich programów certyfikacji cyberbezpieczeństwa. W szczególności Ministerstwo brało udział w przyjęciu

pierwszego aktu implementującego europejski program certyfikacji cyberbezpieczeństwa – European Union Common Criteria.

Od stycznia 2025 r. Polska przejmuje przewodnictwo w Radzie UE. Cyberbezpieczeństwo jest jednym z głównych priorytetów polskiej prezydencji. W ramach prac Rady będą między innymi omawiane następujące tematy:

- Przełamanie silosów i wzmocnienie współpracy między różnymi społecznościami. Poprawa koordynacji i współpracy między organami ds. cyberbezpieczeństwa w UE, aby sprostać wyzwaniom związanym z cyberbezpieczeństwem w bardziej ujednolicony i skuteczny sposób oraz aby uczyć się na podstawie najlepszych praktyk w każdym państwie członkowskim, zwłaszcza poprzez współpracę w ramach Grupę Współpracy NIS.
- Prace nad przyjęciem zmienionego planu cyberbezpieczeństwa i zapewnienie silnego nacisku na jego wdrożenie. Skoncentrowanie się na wzmocnieniu koordynacji i wymiany informacji między państwami członkowskimi i odpowiednimi zainteresowanymi stronami na szczeblu unijnym i krajowym.
- Usprawnienie obowiązków sprawozdawczych na podstawie Dyrektywy NIS2, Zaproponowane modelu „Single Entry Point for incydent notification", platformy, która pozwalałby na zgłaszanie incydentów na podstawie innych regulacji: DORA, RODO, PSD2. Dyskusja nad zbadaniem możliwości ujednolicenia szablonów dla podmiotów w ramach NIS2 i promowanie pojedynczych punktów wprowadzania powiadomień o incydentach zgodnie z NIS2.
- Dalszy rozwój, dostosowanie i wzmocnienie współpracy cywilno-wojskowej.
- Finansowanie w cyberbezpieczeństwie, dyskusja nad systemowym rozwiązaniem finansowania cyberbezpieczeństwa na poziomie unijnym. Dyskusja w ramach nieformalnej Rady ds. Transportu, Telekomunikacji i Energii, ma na celu wskazanie kierunków jakie powinna podjąć UE by zapewnić spójne i całościowe finansowanie sektora cyberbezpieczeństwa.

9.6.2 WSPÓŁPRACA W RAMACH ENISA

W 2024 r. Ministerstwo Cyfryzacji kontynuowało prace w ramach ENISA Support Action Fund – krótkoterminowych projektów wsparcia zapewnianych przez Komisję Europejską za pośrednictwem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) państwom członkowskim w świetle podwyższonego zagrożenia złośliwymi działaniami w cyberprzestrzeni w związku z trwającymi konfliktami. Wsparcie ma na celu uzupełnienie już realizowanych działań przez państwa członkowskie na rzecz zwiększenia poziomu bezpieczeństwa i odporności na cyberzagrożenia.

To wsparcie odbywa się poprzez realizowanie przez ENISA usług ex-ante i ex-post. ENISA wspiera państwa członkowskie w ich działaniach na rzecz zapobiegania, wykrywania, analizowania oraz wzmacniania zdolności w zakresie reagowania na zagrożenia i cyberincydenty. Ministerstwo Cyfryzacji jako punkt kontaktowy, przekazuje do ENISA listę beneficjentów wraz z określonym priorytetem, współpracując z podmiotami KSC, mogącymi ubiegać się o środki.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/konsultacje-spoleczne-w-sprawie-oceny-agencji-unii-europejskiej-ds.-bezpieczenstwa-sieci-i-informacji-enisa

9.6.3 WSPÓŁPRACA BILATERALNA I MULTILATERALNA

W październiku 2024 r. zawarto Memorandum Of Understanding pomiędzy Ministerstwem Cyfryzacji a Departamentem Bezpieczeństwa Krajowego Stanów Zjednoczonych w zakresie cyberbezpieczeństwa. Głównymi obszarami współpracy jest wymiana informacji dotyczących zagrożeń w cyberprzestrzeni, cyberbezpieczeństwo nowych technologii, rozwiązania legislacyjne w cyberbezpieczeństwie. Jednocześnie Ministerstwo Cyfryzacji prowadzi uzgodnienia z Indiami, Filipinami, Słowenią oraz Wietnamem w celu podpisania porozumień o wzajemnej współpracy w ramach cyberbezpieczeństwa.

3-5 września, w ramach XXXIII Forum Ekonomicznego w Karpaczu, odbyło się 6. Forum Cyberbezpieczeństwa organizowane przez Ministerstwo Cyfryzacji. Goście Forum Cyberbezpieczeństwa mieli okazję wysłuchać dyskusji krajowych i międzynarodowych ekspertów z obszaru cyberbezpieczeństwa podczas 3-dniowej sesji paneli tematycznych. Forum to znakomita okazja do

wymiany doświadczeń i poglądów w środowisku międzynarodowym, a część dyskusji dotyczyła zbliżającej się Prezydencji Polski w Radzie UE.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/polsko--amerykanska-wspolpraca-w-zakresie-cyberbezpieczenstwa

9.6.4 COUNTER RANSOMWARE INITIATIVES

Ministerstwo Cyfryzacji uczestniczyło w międzynarodowej inicjatywie koordynowanej przez USA pn. „Counter Ransomware Initiatives", która ma na celu połączenie wysiłku działań zaangażowanych państw w zwalczanie zagrożeń typu ransomware. Inicjatywa została zapoczątkowana w październiku 2021 r. przez U.S. National Security Council przy Białym Domu i aktualnie liczy prawie 70 członków. Ministerstwo Cyfryzacji aktywnie uczestniczy w pracach grup roboczych CRI. W szczególności w ramach filaru ICRTF (The International Counter Ransomware Task Force), wspólnie z NASK-PIB, amerykańskim Departamentem Bezpieczeństwa Krajowego (DHS) oraz instytutem SANS Ministerstwo Cyfryzacji w pierwszym kwartale 2024 zakończyło projekt RACER (Ransomware Attack Collective Effective Resilience). Obecnie Ministerstwo Cyfryzacji rozpoczęło prace nad analizą działalności grup Advanced Persistent Threat Groups działających w polskiej cyberprzestrzeni. Zakończenie prac przewidziane jest na 2 kwartał 2025 r.

9.6.5 WSPARCIE DLA UKRAINY I WSPÓŁPRACA Z UKRAINĄ

W 2024 r. Polska była największym dostawcą terminali Starlink zapewniających dostęp do internetu, co ma kluczowe znaczenie dla zapewnienia ciągłości funkcjonowania państwa ukraińskiego, udzielania pomocy humanitarnej oraz zagwarantowania bezpiecznej łączności, także dla realizowania zadań wojskowych.

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/polska-najwiekszym-dostawca-terminali-starlink-dla-ukrainy--realne-wsparcie-dla-obywateli

9.6.6 MECHANIZM TALLIŃSKI

Polska bierze aktywny udział w inicjatywach wspierających Ukrainę zaatakowaną przez Federację Rosyjską. Jedną z nich jest Mechanizm Talliński. Jest to grupa państw sojuszniczych w ramach NATO, która ma na celu koordynację i wzajemne wspieranie działań poprawiających cyberbezpieczeństwo Ukrainy oraz budowanie jej odporności na cyberzagrożenia. W ramach tej inicjatywy Polska pełni rolę tzw. Back Office zbierającego zapotrzebowanie strony ukraińskiej w zakresie cyberbezpieczeństwa z jednej strony, a z drugiej oferty konkretnej pomocy i wsparcia od członków grupy. Od momentu powołania do życia inicjatywy do końca 2024 r. kraje Mechanizmu Tallińskiego dostarczyły Ukrainie usług oraz sprzętu software/hardware w obszarze cyberbezpieczeństwa na kwotę prawie 200 mln USD.

Rysunek 23. Mechanizm Talliński

Więcej informacji pod adresem: https://www.gov.pl/web/cyfryzacja/uruchomienie-mechanizmu-tallinskiego--polska-wspiera-cyberbezpieczenstwo-ukrainy

9.6.7 INNE ORGANIZACJE MIĘDZYNARODOWE

Ministerstwo Cyfryzacji było zaangażowane w działania w zakresie cyberbezpieczeństwa w ramach Organizacji Narodów Zjednoczonych (ONZ), Organizacji Współpracy Gospodarczej i Rozwoju (OECD),

Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), Międzynarodowego Związku Telekomunikacyjny (ITU).

Polska od października 2022 r. jest członkiem Regionalnego Centrum Cyberobrony (RCDC). W ramach tej inicjatywy Ministerstwo Cyfryzacji współpracuje z pozostałymi krajami Litwy, Stanów Zjednoczonych Ameryki, Ukrainy i Gruzji. Regionalne Centrum Cyberbezpieczeństwa zostało otwarte w lipcu 2021 r. i służy jako główna platforma praktycznej współpracy z USA w zakresie cyberobrony, a pozostałymi członkami są Ukraina i Gruzja. RCDC przeprowadza regionalne analizy zagrożeń cybernetycznych i wymienia odpowiednie dane z partnerami, organizuje ćwiczenia i szkolenia, a także badania analityczne w dziedzinie cyberbezpieczeństwa.

9.6.8 ROZPOCZĘCIE REALIZACJI PROJEKTU „NATIONAL COORDINATION CENTRE – POLAND", WSPÓŁFINANSOWANEGO Z PROGRAMU CYFROWA EUROPA

Od stycznia 2024 r. rozpoczęła się realizacja projektu „National Coordination Centre – Poland, NCC-PL", na który przyznane zostało dofinansowanie ze środków Programu Cyfrowa Europa. Celem projektu jest rozwój działalności Krajowego Centrum Kompetencji Cyberbezpieczeństwa (NCC-PL) zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887. Projekt obejmuje szereg działań nakierowanych na rozwijanie krajowych zdolności w zakresie cyberbezpieczeństwa, w tym:

NCC-PL
Krajowe Centrum Kompetencji Cyberbezpieczeństwa

Rysunek 24. NCC-PL

- budowanie silnej społeczności cyberbezpieczeństwa w Polsce,
- wzmacnianie współpracy krajowej i transgranicznej oraz wymiany informacji,
- działania zmierzające do zwiększenia konkurencyjności polskich podmiotów na europejskim i globalnym rynku.

Więcej informacji pod adresem: https://www.gov.pl/web/cyber-nccpl/projekt-national-coordination-centre--poland-ncc-pl

9.6.9 ROZPOCZĘCIE NABORU DO SPOŁECZNOŚCI KOMPETENTNEJ W ZAKRESIE CYBERBEZPIECZEŃSTWA

Od kwietnia 2024 r. polskie podmioty działające w obszarze cyberbezpieczeństwa i posiadające wiedzę fachową w tej dziedzinie mogą dołączyć do Społeczności kompetentnej w zakresie Cyberbezpieczeństwa.

Celem utworzenia tej Społeczności jest wzmacnianie zdolności Unii Europejskiej i jej krajów członkowskich w zakresie cyberbezpieczeństwa oraz wspólna odpowiedź na wyzwania cyfrowego świata, poprzez budowanie współpracy ponad granicami i sektorami. Podmioty posiadające wiedzę specjalistyczną mogą zgłosić do Społeczności poprzez formularz dostępny na stronie NCC-PL.

9.6.10 REALIZACJA INICJATYW PROMUJĄCYCH POLSKIE INNOWACJE W CYBERBEZPIECZEŃSTWIE

W 2024 r. MC zrealizowało dwie inicjatywy wspierające polskich przedsiębiorców działających w branży cyberbezpieczeństwa. Celem tych inicjatyw było zwiększenie rozpoznawalności rozwiązań oferowanych przez te podmioty oraz stworzenie przestrzeni do nawiązania kontaktów biznesowych pomiędzy przedsiębiorcami a ich potencjalnymi klientami i inwestorami. Te inicjatywy to:

- **CyberMarket** w ramach Europejskiego Kongresu Gospodarczego - to wydarzenie matchmakingowe stworzyło przestrzeń dla przedsiębiorców oferujących rozwiązania w obszarze cyberbezpieczeństwa, by zaprezentować swoje produkty i usługi przed potencjalnymi klientami oraz inwestorami; wydarzenie przyjęło formułę konkursu na najlepsze rozwiązanie w obszarze cyberbezpieczeństwa;

- **Let's Be More Cyber!** w ramach VI Forum Cyberbezpieczeństwa - konkurs miał na celu popularyzowanie ofert szkoleniowych zwiększających świadomość zagrożeń w sieci oraz metod ochrony przed nimi. Finaliści konkursu zaprezentowali swoje rozwiązania przed Jury oraz publicznością.

Więcej informacji pod adresem: https://www.gov.pl/web/cyber-nccpl/final-konkursu-cybermarket-2024

9.6.11 STWORZENIE NOWYCH MOŻLIWOŚCI UDZIELANIA WSPARCIA W RAMACH POMOCY DE MINIMIS DLA POLSKICH PRZEDSIĘBIORCÓW W OBSZARZE CYBERBEZPIECZEŃSTWA.

W 2024 r. utworzono podstawę prawną do udzielenia przez Ministra Cyfryzacji pomocy publicznej, w tym pomocy de minimis – umożliwia to ustawa z dnia 15 maja 2024 r. o zmianie niektórych ustaw związanych z funkcjonowaniem administracji rządowej. Z kolei 18 grudnia 2024 r. zostało podpisane rozporządzenie, które umożliwi Ministrowi Cyfryzacji udzielenie grantów polskim małym i średnim przedsiębiorcom z branży cyberbezpieczeństwa. Wsparcie to pomoże przedsiębiorcom zrealizować nowe projekty i wprowadzić je na rynek, co wesprze ich konkurencyjność na europejskim rynku technologii.

9.6.12 WSPARCIE DLA BUDOWANIA MIĘDZYSEKTOROWYCH I TRANSGRANICZNYCH PARTNERSTW POMIĘDZY PODMIOTAMI DZIAŁAJĄCYMI W OBSZARZE CYBERBEZPIECZEŃSTWA.

Podczas VI Forum Cyberbezpieczeństwa (3-5 września 2024 r. w Karpaczu) NCC-PL zrealizowało inicjatywy, które przyczyniły się do zacieśnienia współpracy międzysektorowej i transgranicznej w obszarze cyberbezpieczeństwa. Były to w szczególności:

- sesja pitchingowa z udziałem podmiotów krajowych i zagranicznych, której celem było budowanie partnerstw projektowych i wspólne aplikowanie o środki z programów Cyfrowa Europa i Horyzont Europa; wydarzenie spotkało się z ogromnym zainteresowaniem uczestników;
- panele dyskusyjne, podczas których eksperci z różnych sektorów dzielili się doświadczeniami i omawiali kluczowe tematy, takie jak:
  - europejskie innowacje w cyberbezpieczeństwie,
  - współpraca nauki, biznesu i administracji,
  - wzmacnianie pozycji polskich MŚP na rynku europejskim,
  - wzmocnienie udziału kobiet w branży cyberbezpieczeństwa.

Więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/vi-forum-cyberbezpieczenstwa

9.6.13 ZACHĘCANIE MŁODYCH TALENTÓW DO PODJĘCIA KARIERY W CYBERBEZPIECZEŃSTWIE

Na przełomie lipca i sierpnia 2024 r. grupa polskich uczennic wzięła udział w międzynarodowym obozie letnim CyberWizards w Estonii, zorganizowanym przez estoński Krajowy Ośrodek Koordynacji (NCC-EE). Podczas obozu uczestniczki:

- poznawały tajniki cyberbezpieczeństwa,
- uczestniczyły w praktycznych zajęciach i warsztatach,
- zyskały inspirację do rozwijania kariery w jednej z najbardziej przyszłościowych branż technologicznych.

Inicjatywa miała na celu zachęcenie młodych kobiet do odkrywania swoich talentów w cyberbezpieczeństwie i pokazanie, że ta ścieżka zawodowa jest dla nich pełna możliwości.

Więcej informacji pod adresem: https://www.gov.pl/web/cyber-nccpl/estonski-cyberwizards-camp-za-nami

10 WNIOSKI I REKOMENDACJE

10.1.1 POZIOM REALIZACJI WNIOSKÓW ZE SPRAWOZDANIA Z ROKU 2023

Rozdział 3 Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2023 zawiera wykaz wniosków i rekomendacji płynących z podsumowania ww. Sprawozdania. Tabela poniżej mieści wymienione wnioski wraz z określeniem poziomu ich realizacji i komentarzem.

Należy pamiętać, iż proces zarządzania KSC jest zrazem dynamiczny i długotrwały. Specyfika implementacji zmian w KSC następuję w średnio terminowym okresie i wynika z charakteru systemu prawnego i legislacyjnego obowiązującego w Polsce.

Wnioski podsumowujące zostały zaadaptowane w procedowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa i ich pełna realizacja będzie możliwa w czasie następującym po implementacji niezbędnych przepisów prawa.

Tabela 37. Poziom realizacji wniosków z ze Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2023

Nr z 2023	Wniosek ze Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa za rok 2023	Poziom realizacji	Komentarz
1.	Powołanie instytucji koordynującej KSC, o odpowiedniej pozycji ustrojowej i kompetencyjnej.	Prace koncepcyjne	Zawarto w projekcie nowelizacji UKSC zwiększenie kompetencji i poszerzenie zakresu zadań MC i Pełnomocnika oraz sformalizowanie działania PCOC, co jest pierwszym krokiem w realizacji.
2.	Zwiększenie zdolności operacyjnych podmiotów KSC.	W realizacji	Rozwijanie potencjału podmiotów KSC poprzez rozwój narzędzi technicznych i podnoszenie kompetencji specjalistów oraz poszerzenie kompetencji podmiotów KSC ujęte zostało w nowelizacji UKSC.
3.	Uregulowanie kwestii działań ofensywnych w cyberprzestrzeni, aktywnej obrony oraz rozwoju zdolności do tego rodzaju działań, w tym uszczegółowienie zadań służb specjalnych.	Prace koncepcyjne	
4.	Opracowanie krajowego planu przejścia na kryptografię postkwantową.	Prace koncepcyjne	
5.	Budowanie świadomość zagrożeń i znaczenia odpowiedniej strategii bezpieczeństwa.	W stałej realizacji	Proces stale realizowany
6.	Nacisk na stosowanie najnowszych technologii i aktualizację oprogramowania.	W realizacji	Poszerzenie kompetencji Pełnomocnika w zakresie mechanizmu rekomendacji zawarto w projekcie nowelizacji UKSC, Pełnomocnik na bieżąco wydaje komunikaty z zaleceniami.
7.	Zapewnienie odpowiednich zasobów kadrowych, w aspekcie ilościowym i jakościowym w podmiotach kluczowych.	W stałej realizacji	Świadczenie Teleinformatyczne wyraźnie wpływa na utrzymanie i jakościowych kadr związanych cyberbezpieczeństwem.
8.	Fundusz Cyberbezpieczeństwa.	W stałej realizacji	Fundusz Cyberbezpieczeństwa posiada zagwarantowane środki budżetowe niezbędne do dalszego funkcjonowania. Środki w 2024 zostały znacząco podniesione.
9.	Szerokie zastosowanie audytów bezpieczeństwa	Procedowanie zmian legislacyjnych	Kompetencje ww. zakresie zawarto w projekcie nowelizacji UKSC
10.	Wprowadzenie wiążącego charakteru przekazywanych zaleceń w zakresie cyberbezpieczeństwa (np. związanych z koniecznością aktualizacji systemów czy niekorzystania/wyłączenia systemów i oprogramowania w podatnych wersjach)	Procedowanie zmian legislacyjnych	Kompetencje ww. zakresie zawarto w projekcie nowelizacji UKSC

	wydawanych przez Pełnomocnika czy CSIRT-y poziomu krajowego.		
11.	Usprawnienie i zautomatyzowanie procesu wymiany informacji pomiędzy podmiotami KSC oraz rozważenie utworzenia platformy do wymiany informacji.	W stałej realizacji	Rozbudowano i zintensyfikowano działalność PCOC. Ponadto zwiększone kompetencje ww. zakresie zawarto w projekcie nowelizacji UKSC (np. wzmocnienie roli systemu S46 i rozwój tego systemu).
12.	W związku z nabywaniem pilnych usług i produktów związanych z cyberbezpieczeństwem zasadne jest wprowadzenie rozwiązań umożliwiających wyłączenie stosowania Prawa Zamówień Publicznych (PZP).	Planowane zmiany legislacyjne	
13.	Dostosowanie systemu wymiany informacji o incydentów oraz nadużyć w komunikacji elektronicznej. Powołanie CSIRT w podsektorze komunikacji elektronicznej.	W realizacji	Kompetencje ww. zakresie zawarto w projekcie nowelizacji UKSC. Ponadto w MC rozpoczęto pracę nad powołaniem CSIRT sektorowego dla organu właściwego ds. cyberbezpieczeństwa ministra ds. informatyzacji oraz rozwijany jest zakres funkcjonalności systemu S-46.
14.	Organizacja kolejnej edycji ćwiczeń KSC EXE.	Zrealizowano	Zrealizowano ww. ćwiczenia w 2024. Planowana organizacja o charakterze cyklicznym.
15.	Wprowadzenie rozwiązań teleinformatycznych oraz przepisów prawnych, które spowodują wykorzystanie rządowych sieci odseparowanych od internetu jako głównych mediów służących do wymiany danych pomiędzy instytucjami rządowymi.	W przygotowaniu	W ramach tworzenia Systemu Bezpiecznej Łączności Rządowej przez MSWiA, rozwijany jest też system SKR-Z, planowane jest wdrożenie EZD-N.
16.	Standardy Cyberbezpieczeństwa.	W stałej realizacji	MC stale publikuje i aktualizuje standardy. Trwają prace nad modyfikacją formatu standardów.
17.	Implementacja tzw. Toolbox'a 5G,	Procedowanie zmian legislacyjnych	Implementacja ww. rozwiania zostało zawarte w projekcie nowelizacji UKSC
18.	Pogłębienie współpracy w obszarze pozyskiwania i wymiany informacji na temat zagrożeń i podatności – rozbudowa struktury Kolegium ds. Cyberbezpieczeństwa.	Procedowanie zmian legislacyjnych	Zmiana znacznie i zakresu kompetencji Kolegium została zawarta w projekcie nowelizacji UKSC

11 WNIOSKI I REKOMENDACJE ZA ROK 2024

1. **Platforma wymiany informacji i harmonizacji KSC – CYBER.GOV.PL**
   Zwiększenie efektywności wymiany informacji oraz samego funkcjonowania KSC, wymaga konsolidacji aktualnie funkcjonujących rozwiązań technicznych działających na rzecz podmiotów KSC. Aktualnie istnieje wiele wysokiej klasy rozwiązań, z których mogą korzystać zainteresowane podmioty. Usługi te jednak są rozproszone. Należy opracować portal który będzie „jednym okienkiem obsługi" dla wszystkich chcących skorzystać z pomocy państwa w ramach KSC. Portal powinien umożliwiać nawigację po wszystkich aktualnie oferowanych rozwiązaniach, które są aktualnie nieuporządkowane i dostęp do nich nie jest dostatecznie eksponowany. Projekty takie jak s46, moje.cert.pl, snitch, bezpiecznedane.gov.pl, bezpiecznapoczta.cert.pl, szkolenia dla podmiotów KSC, baza wiedzy o cyberbezpieczeństwie i inne powinny być udostępnione z wykorzystaniem istniejącej domeny CYBER.GOV.PL, która będzie centralnym miejscem dla wszystkich, którzy chcą zgłosić incydent, zwiększyć świadomości na temat zagrożeń, zbadać poziom zabezpieczenia swoich rozwiązań, uzyskać pomoc w realizacji wymagań nakładanych przez UKSC, czy zapoznać się z aktualnymi dobrymi praktykami, komunikatami i rekomendacjami wydawanymi przez Pełnomocnika. W ramach podsystemów objętych projektem powinna istnieć możliwość zautomatyzowanej wymiany informacji o cyberzegrożeniach oraz roboczej komunikacji pomiędzy przedstawicielami CSIRTów, organów ścigania, służb, organów właściwych do spraw cyberbezpieczeństwa oraz podmiotami objętymi KSC. Agregacja danych w jednym systemie pozwoli na uzyskanie pełnego i aktualnego obrazu KSC. Na postawie takich informacji Pełnomocnik będzie mógł podejmować świadome inicjatywy na poziomie krajowym celem podniesienia cyberbezpieczeństwa Rzeczpospolitej Polskiej.

2. **Wzrost liczby zagrożeń cyberbezpieczeństwa**
   Na podstawie agregowanych przez MC danych dot. skali, charakteru i liczby incydentów cyberbezpieczeństwa występujących w polskiej cyberprzestrzeni (23% rdr) należy wskazać trend wzrostowy w zakresie występowania zagrożeń. Postępująca cyfryzacja procesów życia publicznego, społecznego i gospodarczego sprawiać będzie umacnianie się i tak już newralgicznego znacznie sfery cyfrowej dla ogólnego i wielopoziomowego bezpieczeństwa RP, wpływającego na zrównoważony i stabilny rozwój Polski. Napięta sytuacja w sferze geografii politycznej i stosunków międzynarodowych sprawia, iż trend wzrostowy występowania zagrożeń zostanie utrzymany. Obserwowany również będzie wzrost skali incydentów związanych z wykorzystaniem nowych trendów technologicznych, jak m.in. AI, która stosowana będzie do automatyzacji elementów ataków różnego typu, co związane jest rozwojem międzynarodowych usług przestępczych na zlecenie (as a service), do których zaliczyć należy m.in. ataki typu *ransomware*, *phishing*, *speraphishing*, *spam*, *scam*.

3. **Rewolucja AI - konieczne wsparcie podmiotów odpowiedzialnych i rozwój krajowych kompetencji prywatnych i publicznych w tym zakresie**
   W obliczu dynamicznego rozwoju technologii sztucznej inteligencji oraz jej rosnącego znaczenia w obszarze cyberbezpieczeństwa, konieczne jest podjęcie skoordynowanych działań mających na celu wsparcie podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni oraz rozwój krajowych kompetencji zarówno w sektorze prywatnym, jak i publicznym. Do kluczowy obszarów ww. wsparcia należy zaliczyć:
   - zwiększenie finansowania implementacji i rozwoju technologii oraz zwiększenie zasobów ludzkich i technologicznych w podmiotach kluczowych dla rozwoju ww. obszaru.
   - szkolenie i edukacja pracowników administracji publicznej w bezpiecznym wykorzystaniu AI oraz budowaniu świadomości zagrożeń związanych z technologią w społeczeństwie.

4. **Rewolucja kwantowa (kryptografia post kwantowa), głównie w systemach szyfrowania i transmisji danych/łączności**
   Nadchodząca era komputerów kwantowych, które mogą zagrozić obecnym systemom kryptograficznym, konieczne jest wdrożenie kryptografii post-kwantowej (PQC) w systemach szyfrowania i transmisji danych oraz rozwój kryptografii i łączności kwantowej. Proces ten należy

rozpatrywać okresie średnioterminowym. W ramach dostosowania systemów bezpieczeństwa stosowanych przez podmioty KSC należy podjąć działania w celu wdrożenia standaryzacji i certyfikacji na poziomie krajowym w zakresie rozwiązań szyfrowania post-kwantowego również dla systemów komunikacyjnych (przesyłu danych). Zagadnienia te powinny zostać objęte krajowym planem migracji do kryptografii post kwantowej.

5. **Wzrost napięć geopolitycznych, w tym związanych z ograniczaniem dostępności technologicznej (modele AI, półprzewodniki)**
   Wzrost napięć geopolitycznych, szczególnie w kontekście ograniczania dostępności technologicznej, stanowi poważne wyzwanie dla bezpieczeństwa narodowego. Zagrożenia wynikające z ograniczeń dystrybucji nowych technologii oraz narzędzi i wiedzy niezbędnych do ich tworzenia powoduje konieczność podjęcia działań celem minimalizacji potencjalnych efektów ww. procesów.
   Do kluczowych przedsięwzięć, które należy podjąć w celu zabezpieczenia krajowej infrastruktury technologicznej zaliczyć trzeba:
   - Dywersyfikacja Dostawców - zmniejszenie zależności od pojedynczych źródeł dostaw półprzewodników i technologii AI poprzez nawiązanie współpracy z różnymi dostawcami z niezależnych regionów geograficznych.
   - Wsparcie dla Krajowych Producentów - inwestowanie w rozwój krajowego przemysłu półprzewodników i technologii AI, aby zwiększyć samowystarczalność produktowo-technologiczną i zmniejszyć ryzyko związane z globalnymi zakłóceniami.
   - Współpraca Międzynarodowa - poprzez aktywne uczestnictwo w międzynarodowych inicjatywach i sojuszach technologicznych, aby zapewnić stabilność dostaw i wymianę wiedzy wrażliwej.
   - Monitorowanie i analiza ryzyka - stała obserwacja sytuacji geopolitycznej oraz analiza potencjalnych zagrożeń dla łańcuchów dostaw technologii, aby móc szybko reagować na zmieniające się warunki i być możliwie wcześnie przygotowanym na zmiany uwarunkowań.
   - Rozwój Kompetencji Krajowych - poprzez wspieranie edukacji i szkoleń w zakresie zaawansowanych technologii, tak by krajowe zasoby ludzkie były przygotowane do pracy z najnowszymi technologiami oraz z użyciem najaktualniejszych zdobyczy naukowych.

6. **Nowelizacja UKSC – zmiana strukturalna KSC**
   Konieczność dostosowania KSC do wymogów przepisów europejskich (w tym m.in. dyrektywy NIS 2) oraz dynamicznie zmieniającą się sytuacją w cyberprzestrzeni, powoduje niezbędne wprowadzenie zmian strukturalnych w KSC, w UKSC zawarto szereg rozwiązań gwarantujących dostawanie systemu do aktualnego środowiska cyberbezpieczeństwa w Polsce. Powyższe umożliwi zarazem zwiększenie kompetencji pełnomocnika w zakresie:
   - reagowania na zagrożenia (Procedura dostawcy wysokiego ryzyka – HRV),
   - wzmocni nadzór i zapewni środki egzekwowania przepisów przez organy właściwe ds. cyberbezpieczeństwa,
   - zmieni zakres obowiązków Pełnomocnika ds. cyberbezpieczeństwa i Kolegium ds. cyberbezpieczeństwa, zwiększając sprawczość zarządzania KSC w zakresie reagowania na zagrożenia.

7. **Uregulowanie działań ofensywnych w cyberprzestrzeni**
   W obliczu rosnących zagrożeń w cyberprzestrzeni, konieczne jest uregulowanie działań ofensywnych, aby zapewnić skuteczną ochronę interesów narodowych oraz zgodność z międzynarodowymi normami prawnymi. Do kluczowych działań zaliczyć należy:
   - **Opracowanie ram prawnych**. Stworzenie kompleksowych ram prawnych regulujących działania ofensywne w cyberprzestrzeni, które będą zgodne z międzynarodowymi standardami i konwencjami.
   - **Zasady użycia siły.** Określenie jasnych zasad i procedur dotyczących użycia siły w cyberprzestrzeni, w tym warunków, w których działania ofensywne mogą być podejmowane zarówno w warunkach pokoju, kryzysu i wojny oraz jakie instytucje mogą takie działania prowadzić w jakich warunkach.

- **Współpraca międzynarodowa** - wzmocnienie współpracy z sojusznikami i partnerami międzynarodowymi w zakresie wymiany informacji i koordynacji działań ofensywnych.

Podjęcie tych działań pozwoli na skuteczne i zgodne z prawem prowadzenie działań ofensywnych w cyberprzestrzeni, co przyczyni się do wzmocnienia bezpieczeństwa narodowego.

8. **Kształtowanie i edukacja świadomości zagrożeń związanych z cyberbezpieczeństwem - w zakresie społeczeństwa i administracji publicznej**
   Edukacja na temat higieny cyfrowej i budowanie świadomości zagrożeń jest prawdopodobnie jedynym i najlepszym narzędziem pozwalającym zniwelować ryzyka wynikające z najsłabszego elementu systemów IT – człowieka. Powyższe należy realizować za pośrednictwem kampanii informacyjnych, dystrybucji materiałów edukacyjnych, dedykowanych programów edukacyjnych i szkoleń oraz współpracy z sektorem pozarządowym.

9. **Zapewnienie zasobów kadrowych podmiotów KSC**
   Skuteczne realizowanie zadań związanych z cyberbezpieczeństwem wymagają zapewnienia odpowiednich zasobów kadrowych dla podmiotów wchodzących w skład KSC. Ww. zagadnienie powinno być realizowane poprzez utrzymanie tzw. Świadczenia Teleinformatycznego wyrównującego zarobki specjalistów od cyberbezpieczeństwa w administracji publicznej z wynagrodzeniami w sektorze pytywanym. Należy zwiększać wydatki w tym zakresie ze względu na ciągły wzrost istotności bezpieczeństwa systemów teleinformatycznych w wielu dziedzinach życia oraz poszerzenie podmiotów objętych KSC po nowelizacji UKSC.

10. **Utworzenie podmiotu koordynującego KSC, w związku z planowanym powstaniem CSIRTów sektorowych**
    Skuteczne zarządzanie KSC i planowanym powstaniem sektorowych CSIRT-ów, wymaga utworzenie centralnego podmiotu koordynującego, który będzie dysponował zasobami umożliwiającymi sprawne koordynowanie potencjałem podmiotów krajowych i sektorowych, zapewniając właściwy **nadzór i monitorowanie**: umożlwiający skoordynowaną współpracę międzyinstytucjonalną oraz optymalne wykorzystanie ich kompetencji technicznych oraz rozwiązywanie sporów kompetencyjnych.

11. **Publikacja dobrych praktyk przez Pełnomocnika Rządu**
    W celu podniesienia standardów cyberbezpieczeństwa oraz promowania najlepszych praktyk, Pełnomocnik Rządu ds. Cyberbezpieczeństwa powinien regularnie publikować zbiory dobrych praktyk. Powyższe obejmować powinno:
    - **Opracowanie zbioru dobrych praktyk** - stworzenie i aktualizacja zbioru dobrych praktyk w zakresie cyberbezpieczeństwa, które będą dostępne dla wszystkich podmiotów KSC.
    - **Dystrybucja i promocja** - tych praktyk wśród instytucji publicznych i prywatnych, aby zapewnić ich szerokie zastosowanie.
    - **Współpraca z ekspertami** branżowymi- z krajowymi i międzynarodowymi ekspertami w celu opracowania i aktualizacji ich zbioru.

    Podjęcie tych działań pozwoli na podniesienie standardów cyberbezpieczeństwa oraz promowanie najlepszych praktyk wśród podmiotów KSC, powyższe jest możliwe do realizacji i przy wykorzystaniu nowatorskiego programu partnerska publiczno-prywatnego PWCyber realizowanego przez Ministerstwo Cyfryzacji.

12. **Ćwiczenia KSC na poziomie krajowym**
    Organizacja kolejnej edycji ćwiczeń KSC EXE – do tej pory tego typu ćwiczenia odbyły się dwukrotnie. W związku ze zmieniająca się sytuacją geopolityczną i krajobrazem zagrożeń, powinno się dokonywać regularnych ćwiczeń o zmiennych scenariuszach z zakresu cyberbezpieczeństwa. Organizacja ww. działa integracyjnie na środowisko KSC oraz umożliwia weryfikację procedur i wymianę doświadczeń, między kluczowymi podmiotami - niezastąpionych w przypadku wystąpienia prawdziwego zagrożenia.

13. Wsparcie podmiotów lokalnych w zwiększaniu poziomu cyberbezpieczeństwa

Obserwowane są ataki na łańcuchy dostaw, w tym na podmioty o wyraźnym znaczeniu dla stabilnego funkcjonowania sfery publiczno-społecznej, które jednak nie są częścią administracji centralnej, infrastruktury krytycznej ani operatorami usług kluczowych – czyli podmiotów otrzymujących szczególne wsparcie CSIRTów poziomu krajowego. Do tej grupy atakowanych podmiotów można zaliczyć instytucje o znaczeniu lokalnym, takie jak administracja samorządowa oraz lokalni dostawcy usług niezbędnych dla dobrostanu miejscowych społeczności.

Instytucje te, ze względu na ograniczone budżety przeznaczone na cyberbezpieczeństwo oraz stosunkowo małą dostępność specjalistów IT na rynku lokalnym, nie są w stanie samodzielnie zapewnić sobie akceptowalnego poziomu cyberbezpieczeństwa.

Aby zwiększyć odporność cyfrową na poziomie lokalnym, należy dążyć do migracji lokalnych usług publicznych do rozwiązań chmurowych, takich jak projekty: Rządowa Chmura Obliczeniowa (RChO) i Krajowe Centrum Przetwarzania Danych (KCPD). Udostępnienie publicznego środowiska chmurowego, dzięki centralizacji zarządzania bezpieczeństwem systemów oraz unifikacji rozwiązań, umożliwi skokowo zwiększyć efektywność kosztową bezpieczeństwa IT oraz jakość świadczonych usług, w tym lokalnych, zwiększając jednocześnie ich dostępność cyfrową.

Jednakże, ze względu na średnioterminową perspektywę czasową osiągnięcia pełnego stopnia działania ww. rozwiązań centralnych, należy rozważyć zwiększenie wsparcia dla samorządów przy tworzeniu nie tylko CSIRTów, ale również SOCów na poziomie lokalnym oraz sektorowym.

12 PLANOWANE DZIAŁANIA W 2025 R.

W 2025 r. przewidziano wprowadzenie szeregu daleko idących zmian, które znacząco przeformatują obecną strukturę Krajowego Systemu Cyberbezpieczeństwa.

12.1.1 NOWELIZACJA USTAWY O KSC

Na 2025 r. przewidziano wprowadzenie daleko idących zmian w ramach Krajowego Systemu Cyberbezpieczeństwa. W związku z planowanym wejściem w życie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa znacząco rozszerzony zostanie zakres podmiotowy tego systemu. W miejsce dotychczasowych operatorów usług kluczowych oraz dostawców usług cyfrowych wprowadzone zostaną pojęcia podmiotów kluczowych i ważnych. Równocześnie doprowadzi to do kilkukrotnego poszerzenia zakresu podmiotów objętych tymi przepisami. Wprowadzony zostanie również nowy podział na sektory, co będzie wiązało się z pojawieniem się nowych organów właściwych w sprawach cyberbezpieczeństwa. Wprowadzone zostaną także CSIRT sektorowe, które będą wspierać podmioty funkcjonujące w danych sektorach z uwzględnieniem konkretnej specyfiki ich działalności. Ponadto rozwinięty zostanie system S46, który ma stać się głównym kanałem komunikacji między podmiotami krajowego systemu cyberbezpieczeństwa.

12.1.2 PRZYJĘCIE STRATEGII CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2025-2029.

W br. planowane jest przyjęcie nowej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, która będzie obowiązywać w latach 2025-2029 i zastąpi obecnie obowiązujący dokument.

12.1.3 USTAWA O KRAJOWYM SYSTEMIE CERTYFIKACJI CYBERBEZPIECZEŃSTWA (UC42)

Na 2025 r. przewidywane jest również uchwalenie ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42), która ma na celu dostosowanie polskiego porządku prawnego do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) oraz stworzenie ram prawnych dla funkcjonowania krajowych schematów cyberbezpieczeństwa. Rozwiązania te dadzą impuls do rozwoju rynku certyfikacji cyberbezpieczeństwa oraz przyczynią się do większego wykorzystania certyfikatów cyberbezpieczeństwa w kluczowych sektorach gospodarki.

Również na 2025 r. przewidziano wdrożenie do polskiego porządku prawnego dyrektywy CER.

12.1.4 DALSZA REALIZACJA PROJEKTU „NATIONAL COORDINATION CENTRE – POLAND”

Planowane są dalsze działania nakierowane na wspieranie polskiego ekosystemu cyberbezpieczeństwa, w tym promowanie polskich innowacji w cyberbezpieczeństwie, łączenie partnerów, wspieranie współpracy i synergii między działaniami podmiotów w branży cyberbezpieczeństwa.

12.1.5 REALIZACJA BADANIA POLSKICH MAŁYCH I ŚREDNICH PRZEDSIĘBIORCÓW DZIAŁAJĄCYCH W OBSZARZE CYBERBEZPIECZEŃSTWA

Celem badania jest identyfikacja barier hamujących rozwój polskich małych i średnich przedsiębiorców na rynku, stojących przed nimi wyzwań, a także form wsparcia, którego potrzebują i oczekują ze strony instytucji publicznych. Wyniki tego badania posłużą do planowania przyszłych działań wspierających małych i średnich cyber przedsiębiorców.

12.1.6 PRZEPROWADZENIE KONKURSU GRANTOWEGO DLA PRZEDSIĘBIORCÓW DZIAŁAJĄCYCH W BRANŻY CYBERBEZPIECZEŃSTWA

Celem konkursu jest wzmocnienie konkurencyjności polskich cyber MŚP i start-upów na rynku lokalnym i międzynarodowym poprzez udzielenie im wsparcia finansowego na wybrane obszary działalności. Planowane jest udzielanie dofinansowania w obszarach: rozwoju istniejącego produktu lub usługi, stworzenia nowego rozwiązania, zwiększenia rozpoznawalności na rynku oraz certyfikacji produktu. Całkowita wartość planowanego dofinansowania to 1 800 000 EUR.

12.1.7 DALSZE BUDOWANIE SPOŁECZNOŚCI KOMPETENTNEJ W OBSZARZE CYBERBEZPIECZEŃSTWA

Planowane są działania w zakresie rozpowszechniania informacji o Społeczności kompetentnej i jej celach wśród podmiotów działających w obszarze cyberbezpieczeństwa, a także zachęcania ww. podmiotów do zaangażowania się w działania tej Społeczności oraz we współpracę z Europejskim Centrum Kompetencji i siecią krajowych ośrodków koordynacji.

13 OZNACZENIA TLP

Traffic Light Protocol (TLP) jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Tabela 38. Oznaczenia TLP

Oznaczenie	Odbiorca wiadomości	Autor wiadomości
TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie TLP:AMBER+STRICT, które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP:GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP:CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: *cert.pl*