KPRM | KANCELARIA PREZESA RADY MINISTRÓW

Jakie zmiany niesie nowelizacja ustawy o KSC dla podmiotów publicznych

Marcin Domagała
Główny Specjalista
Wydział Krajowego Systemu Cyberbezpieczeństwa
Departament Cyberbezpieczeństwa

O czym jest prezentacja?

- Incydenty cyberbezpieczeństwa – garść statystyk
- Podmiot publiczny w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa.
- Zadania i obowiązki podmiotów publicznych
- Najważniejsze zmiany w nadchodzącej nowelizacji ustawy o ksc
- Działania DC KPRM w zakresie podnoszenia wiedzy
- Co ciekawego w Krajowym Planie Odbudowy w zakresie cyberbezpieczeństwa?

KPRM | KANCELARIA PREZESA RADY MINISTRÓW

Incydenty cyberbezpieczeństwa – garść statystyk

Prawie 3 lata doświadczeń z ksc

- 170 operatorów usług kluczowych:

Sektor	Zdrowia	Transportu	Energii	Bankowości i infrastruktury finansowej	Zaopatrzenia w wodę	Infrastruktury cyfrowej	Suma
Liczba OUK	**40**	**25**	**70**	**20**	**6**	**9**	**170**

- Powstanie jednego sektorowego CSIRT – CSIRT KNF
- Utworzenie pierwszego ISAC – ISAC Kolej
- Międzysektorowe ćwiczenia KSC-EXE 2020

Incydenty cyberbezpieczeństwa 2019-2021

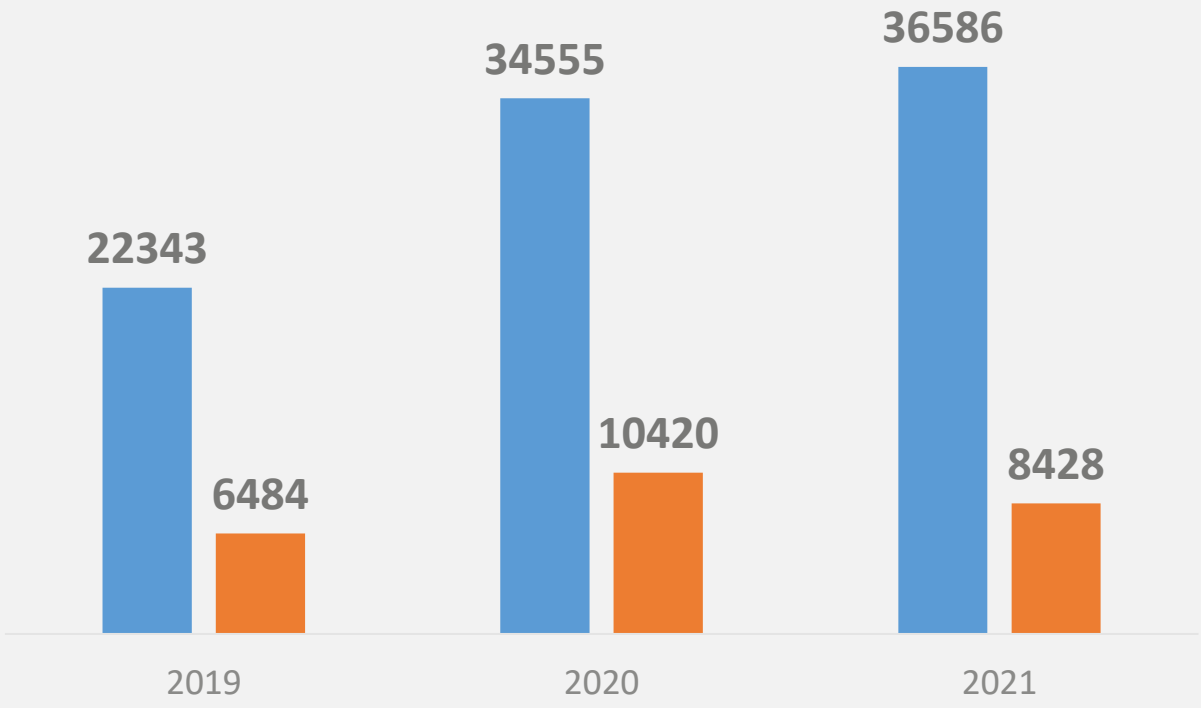
CSIRT NASK

Podmioty publiczne (w tym JST), podmioty prywatne, operatorzy usług kluczowych

Oszustwa komputerowe, w tym phishing, są najczęstszą przyczyną zgłoszenia incydentu cyberbezpieczeństwa – z udziałem na poziomie 81% we wszystkich rodzajach cyberataków w pierwszych **5 miesiącach 2021 r.** Na drugim miejscu znajduje się złośliwe oprogramowanie z 7% udziałem.

Jednocześnie w 2020 r. 380 incydentów dotyczyło podmiotów publicznych (3,7%). **W 2021 r. w ciągu 5 pierwszych miesięcy** liczba incydentów w podmiotach publicznych osiągnęła **200 (2,3%)**.

Liczba zgłoszonych i zarejestrowanych incydentów cyberbezpieczeństwa w latach 2019-2021



KPRM | KANCELARIA PREZESA RADY MINISTRÓW

Podmiot publiczny w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa

Zadania i obowiązki podmiotów publicznych

Podmioty Publiczne wg ustawy o KSC

Podmiotem publicznym w rozumieniu ustawy o krajowym systemie bezpieczeństwa są:

- **Organy władzy publicznej w tym organy administracji samorządowej**, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,
- Jednostki budżetowe, **samorządowe zakłady budżetowe**, agencje wykonawcze, **instytucje gospodarki budżetowej**,
- Uczelnie publiczne i Polska Akademia Nauk,
- Zakład Ubezpieczeń Społecznych, Kasa Rolniczych Ubezpieczeń Społecznych, Narodowy Fundusz Zdrowia, Narodowy Bank Polski, Bank Gospodarstwa Krajowego,
- Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej.

Obowiązki podmiotów publicznych

- **wyznaczanie osoby odpowiedzialnej za utrzymywanie kontaktów** z podmiotami krajowego systemu cyberbezpieczeństwa – przede wszystkim z zespołem CSIRT,
- zapewnia zarządzanie incydentem w podmiocie publicznym,
- **zgłasza incydent** w podmiocie publicznym niezwłocznie, nie później niż w **ciągu 24 godzin** od momentu wykrycia do CSIRT,
- **zapewnia obsługę incydentu** w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT,

Współpraca z CSIRT NASK oraz zgłaszanie osoby do kontaktu

W jaki sposób wyznaczyć osobę do kontaktu do właściwego CSIRT?

Pełnomocnik rządu ds. cyberbezpieczeństwa rekomenduje, aby osoby wyznaczone do kontaktu z zespołami CSIRT, były:

- Dyspozycyjne,
- Decyzyjne,
- Posiadały podstawowe informacje o systemach informacyjnych/usługach cyfrowych w danej organizacji,
- Miały silnie rozwiniętą sieć kontaktów wewnętrznych w organizacji.

Jak zgłosić osoby do kontaktu?

To bardzo proste. Wystarczy wejść na stronę CSIRT NASK, wybrać kategorię *podmiot publiczny* i wypełnić formularz.

Po wypełnieniu formularza należy zapisać go w pliku .pdf, podpisać elektronicznie i także elektronicznie przekazać do CSIRT NASK. Wygenerowany dokument można też wydrukować i po podpisaniu podpisem odręcznym, wysłać pocztą na adres korespondencyjny CSIRT NASK, ul. Kolska 12, 01-045 Warszawa.

WAŻNE!
W przypadku większych jednostek samorządu terytorialnego - rekomendujemy, aby były to co najmniej dwie osoby zapewniające niezakłóconą komunikację w sytuacjach kryzysowych.

Co podmiot publiczny powinien zgłaszać?

- **incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny
  - **Zadanie publiczne** – brak definicji, w skrócie: zadanie realizowane na podstawie ustawy i dla dobra ogólnego
  - **Obowiązek ustawowy zgłoszenia incydentu w podmiocie publicznym!**
- **incydent** – każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo (Nie trzeba zgłaszać, ale można – zachęcamy do tego)

Obowiązki JST względem ustawy o ksc – zgłaszanie incydentów

Obowiązki podmiotów publicznych w zakresie obsługi incydentów:

- Zgłoszenie incydentu nie później niż **24 godziny po jego wykryciu** do CSIRT NASK
- Współpraca z CSIRT NASK, **przekazując niezbędne dane**, w tym osobowe
- Zgłoszenie przekazywane jest w **postaci elektronicznej**, jeśli to niemożliwe to przy użyciu innych środków komunikacji

Ważne!
Właściwym zespołem CSIRT dla **jednostek samorządu terytorialnego jest zespół CSIRT NASK**, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, instytucję podległą Kancelarii Prezesa Rady Ministrów.

KPRM | KANCELARIA PREZESA RADY MINISTRÓW

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa

Podmioty publiczne – nowe obowiązki

- Podmioty publiczne będą musiały zgłaszać 2 osoby odpowiedzialne do kontaktów w ramach ksc. Administracyjna kara pieniężna za nie zgłoszenie tych osób wynosi do 10 000 zł – karę nakłada minister do spraw informatyzacji.
- Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych.
- Do podmiotów publicznych w rozumieniu ustawy KSC zostaną dołączone kolejne instytucje.

Wojewodowie – koordynacja cyberbezpieczeństwa

- Wojewoda zapewnia współpracę pomiędzy administracją rządową a administracją samorządową w województwie. W szczególności:
  - wymienia informacje o incydentach, cyberzagrożeniach i podatnościach
  - zapewnia jednostkom samorządu terytorialnego dostęp do rekomendacji, zaleceń oraz zestawów poradników i dobrych praktyk, wydawanych przez zespoły CSIRT poziomu krajowego oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa
  - prowadzi listę danych kontaktowych osób wskazanych przez właściwego wójta, burmistrza, prezydenta miasta, starostę albo marszałka województwa, do współpracy z właściwymi CSIRT GOV, CSIRT MON lub CSIRT NASK
- Do realizacji tych zadań wojewoda będzie korzystał z systemu S46

CSIRTy – nowe obowiązki

- Nowe zadania CSIRT poziomu krajowego m.in.:
  - wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi i właściwymi podmiotami,
  - gromadzenie informacji dotyczących cyberzagrożeń podatności i incydentów
  - przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa
- CSIRT sektorowy – obowiązkowe (18 miesięcy od wejścia w życie ustawy) oraz nowe obowiązki:
  - koordynować, w ramach sektora lub podsektora, w uzgodnieniu z operatorami usług kluczowych obsługę incydentów;
  - Finansowanie powstania CSIRT sektorowych -> rezerwa celowa budżetu państwa
  - Wyznaczony przez OW – podmioty nadzorowane przez dane OW

ISAC – centra wymiany informacji i analiz

Wprowadzenie do KSC ISAC (Information Sharing and Analysis Center)

- ISAC – **wspiera wymianę i analizę informacji, dobrych praktyk i doświadczeń** dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów dla podmiotów krajowego systemu
- Centra ISAC **współpracują z CSIRT MON, CSIRT NASK lub CSIRT GOV**

Operacyjne centra bezpieczeństwa SOC

Wprowadzenie do KSC operacyjnych centrów bezpieczeństwa (Security Operations Center)

- SOC realizuje zadania związane z zapewnieniem cyberbezpieczeństwa usług kluczowych
  - w tym **na podstawie przeprowadzonego szacowania ryzyka**, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów
  - **Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury lub zawiera umowę dotyczącą prowadzenia SOC na jego zlecenie z innym podmiotem**
  - SOC powołany przez operatora usługi kluczowej **może realizować zadania, o których mowa w także na rzecz innych podmiotów**

Rozwój S46

- System teleinformatyczny utworzony na podstawie art. 46 ustawy KSC, prowadzony przez ministra właściwego do spraw informatyzacji
- Uruchomiony w styczniu 2021 r.
- Umożliwia wymianę informacji o incydentach, podatnościach, cyberzagrożeniach
- Nowelizacja wprowadza obowiązek korzystania z S46 przez:
  - Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa
  - Prezesa Urzędu Komunikacji Elektronicznej
  - CSIRT GOV, CSIRT MON, CSIRT NASK
  - CSIRT sektorowe
  - wojewodów

Nowe środki przeciwdziałania incydentom krytycznym

Ostrzeżenie (przed wystąpieniem incydentu)	Polecenie zabezpieczające (po wystąpieniu incydentu)
• wydawane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa w razie ryzyka wystąpienia incydentu krytycznego • nie jest decyzją administracyjną, jest miękkim środkiem • zawiera wskazanie podmiotów, których dotyczy, a także wskazanie określonego zachowania, które **ograniczy ryzyko wystąpienia incydentu**	• wydawane przez ministra właściwego do spraw informatyzacji po wystąpieniu incydentu krytycznego • jest decyzją administracyjną • zawiera wskazanie podmiotów, których dotyczy, a także wskazanie określonego zachowania, które **zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się**

Krajowy System Certyfikacji Cyberbezpieczeństwa

- Tworzy ramy dla certyfikacji cyberbezpieczeństwa produktów, usług i procesów ICT na podstawie europejskich i krajowych programów certyfikacyjnych
- Certyfikaty wydane w ramach europejskich programów certyfikacyjnych będą uznawane we wszystkich krajach UE
- W ramach systemu będą funkcjonować:
  - Krajowy Organ ds. Certyfikacji Cyberbezpieczeństwa - tę rolę będzie pełnił minister właściwy do spraw informatyzacji
  - Polskie Centrum Akredytacji (PCA)
  - Jednostki oceniające zgodność
  - Producenci i dystrybutorzy chcący certyfikować swoje produkty
- Krajowy Organ ds. Certyfikacji Cyberbezpieczeństwa będzie sprawował ogólny nadzór nad stosowaniem tych przepisów

KPRM | KANCELARIA PREZESA RADY MINISTRÓW

Działania wspierające DC KPRM dla podmiotów publiczny

Działania wspierające JST prowadzone przez Departament Cyberbezpieczeństwa KPRM (1)

Nasze plany rozwoju szkoleń

- E-learning, weryfikacja wiedzy i jej certyfikowanie,
- Rozwój szkoleń online – utworzenie ścieżek kompetencyjnych – zaświadczenia,
- Rozwój ćwiczeń cyberbezpieczeństwa,
- Rozwój bazy wiedzy https://www.gov.pl/web/baza-wiedzy/ - anonimowa ankieta z zakresu stosowania podstaw cyberhigieny + rekomendacje,
- Rekomendacje dot. realizowania polityki szkoleniowej w podmiotach publicznych (bhp),
- W ramach współpracy z wojewodami będziemy stymulować realizację polityki szkoleniowej (np. poprzez zachęcanie kierownictwa do uzyskiwania przez pracowników certyfikatów z kursu e-learningowego raz w roku).

Działania wspierające JST prowadzone przez Departament Cyberbezpieczeństwa KPRM (2)

Baza wiedzy – Cyberbezpiecznysamorząd

Materiały źródłowe:

- **Aktualności:**
  - https://www.gov.pl/web/baza-wiedzy/aktualności.
- **Szkolenia:**
  - https://www.gov.pl/web/baza-wiedzy/szkolenia.
- **Subskrypcja:**
  - https://www.gov.pl/web/baza-wiedzy/subskrypcja.

Plany Departamentu Cyberbezpieczeństwa KPRM: Krajowy Plan Odbudowy (1)

- RegioSOC - regionalne centra cyberbezpieczeństwa dla jednostek samorządu terytorialnego
- Zakłada się powstanie 7 takich centrów do IV kwartału 2025 r.
- Będą świadczyć usługi na rzecz JST według podziału NUTS 1 (makroregiony)
- Ich utworzenie zostanie sfinansowane z Krajowego Planu Odbudowy
- Ich celem będzie wsparcie jednostek samorządu terytorialnego w wykonywaniu ich ustawowych obowiązków dotyczących cyberbezpieczeństwa

Plany Departamentu Cyberbezpieczeństwa KPRM: Krajowy Plan Odbudowy (2)

Obsługa CyberIncydentu CROIOD (**Cyber-Ratownik, Obsługa Incydentu i Odtwarzanie Działania**)

Najważniejsze założenia ***I Etapu*** projektu:

- Bieżąca analiza incydentu,
- Koordynacja działań w przypadku poważnych incydentów,
- Realizacja szkoleń dla kadr zespołów odpowiadających za obsługę incydentu,

Najważniejsze założenia ***II Etapu*** projektu:

- Realizacja systematycznych szkoleń,
- Uruchomienie Portalu Wiedzy oraz ***Portalu Wiedzy*** i ***Wspomagania Obsługi Incydentu,***
- Uruchomienie analiza wykonalności projektu **chumowego.**

KPRM | KANCELARIA PREZESA RADY MINISTRÓW

Dziękuję za uwagę

Marcin Domagała
Departament Cyberbezpieczeństwa
e-mail: marcin.domagala@mc.gov.pl