CYBERODPORNOŚĆ

Sektorowy Zespół Cyberbezpieczeństwa – CSIRT CeZ

dr Małgorzata Olszewska
Dyrektor Centrum e-Zdrowia

XVI Konferencja Bezpieczeństwo w Internecie - Cyberodporność

Warszawa 5 grudnia 2024 r.

Organizatorzy: UKSW, Ministerstwo Cyfryzacji, Naukowe Centrum Prawno-Informatyczne

Partner wspierający: NASK

Partner merytoryczny: SAMSUNG

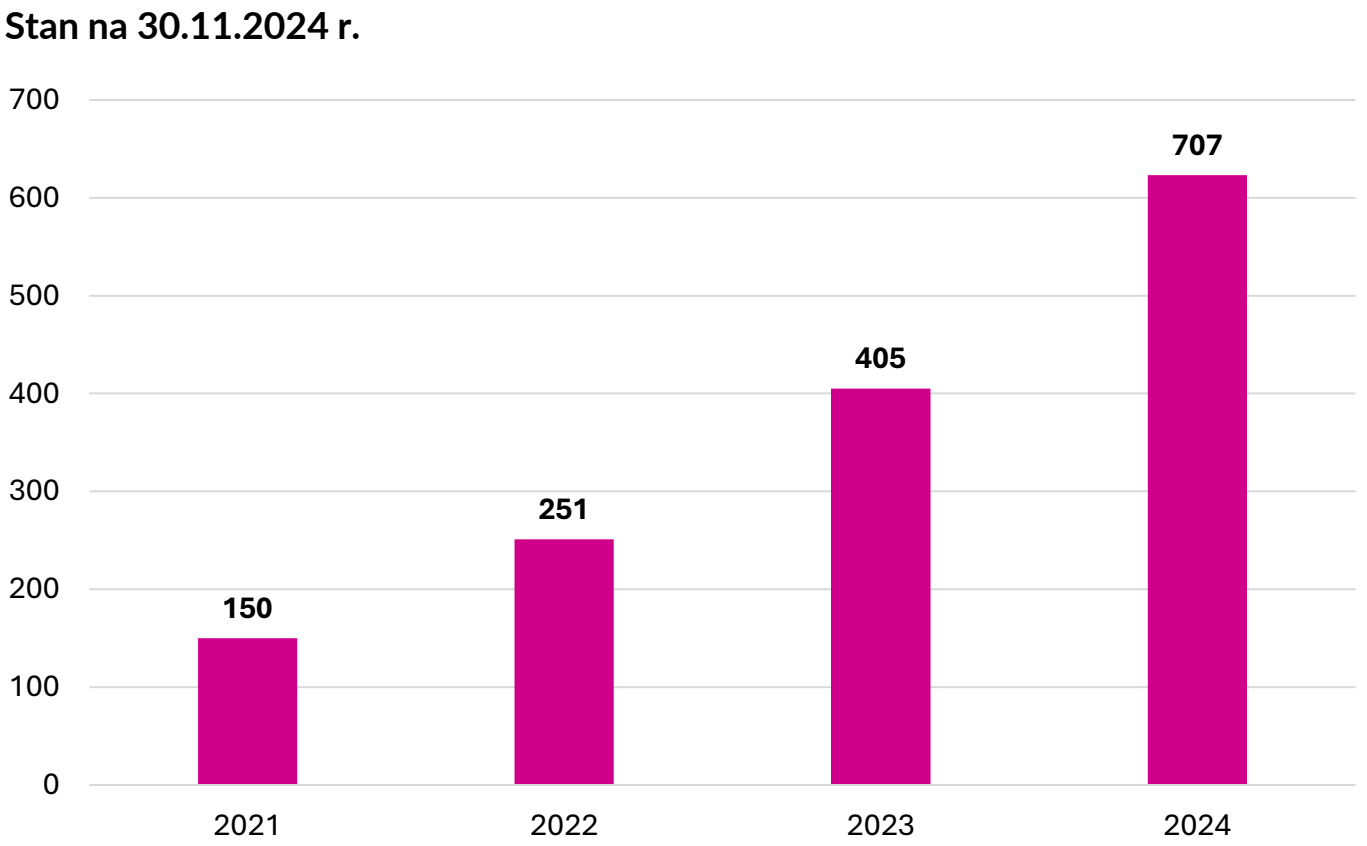
Agenda

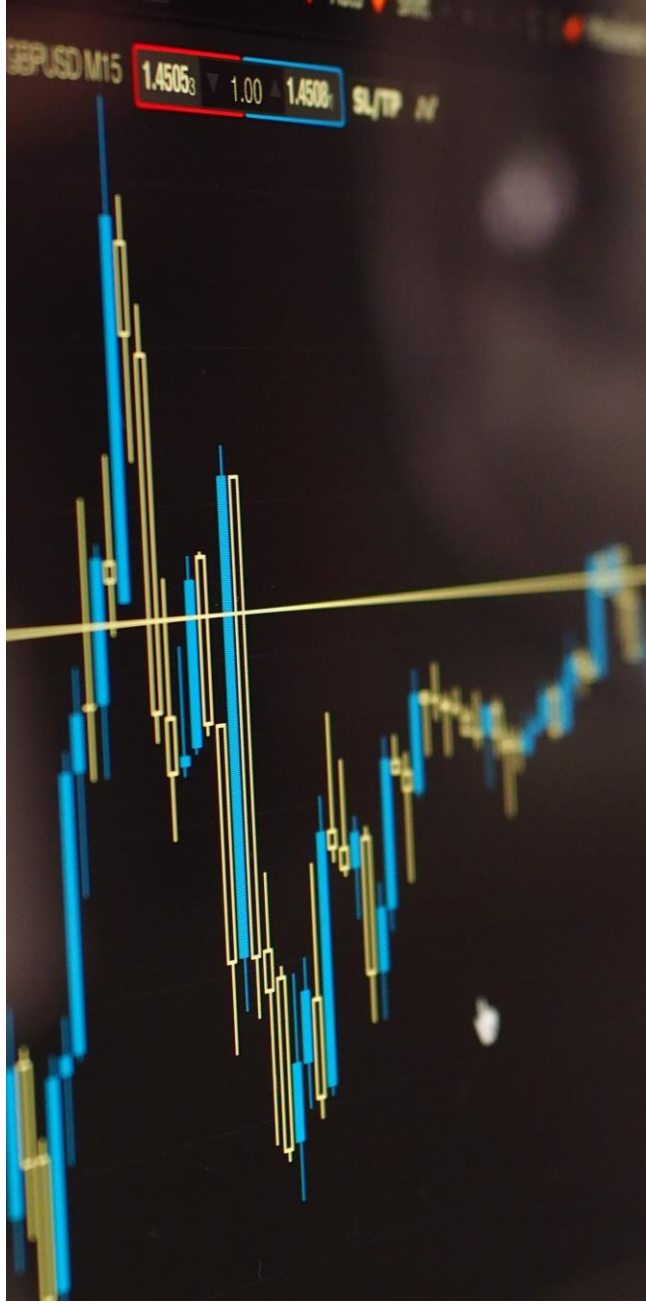
- Czym jest CSIRT CeZ
- Potrzeba utworzenia CSIRT CeZ
- Zadania CSIRT CeZ
- Podstawa prawna
- CSIRT sektora ochrony zdrowia w UE
- Rozwój i perspektywy CSIRT CeZ

Czym jest CSIRT CeZ

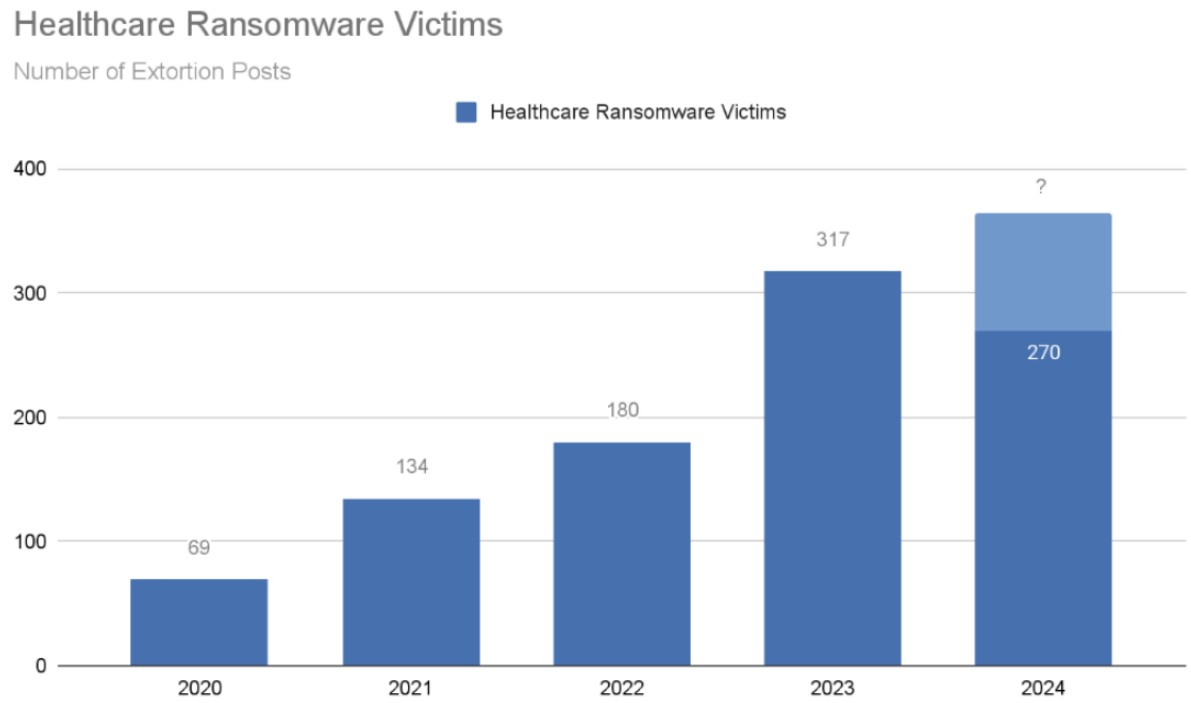
Sektorowy zespół reagowania na incydenty bezpieczeństwa komputerowego, czyli CSIRT CeZ to grupa specjalistów IT świadcząca dla sektora ochrony zdrowia usługi i wsparcie w zakresie oceny, zarządzania i zapobiegania sytuacjom kryzysowym związanym z cyberbezpieczeństwem, a także koordynacji działań w zakresie reagowania na incydenty.

Liczba incydentów w sektorze ochrony zdrowia w Polsce

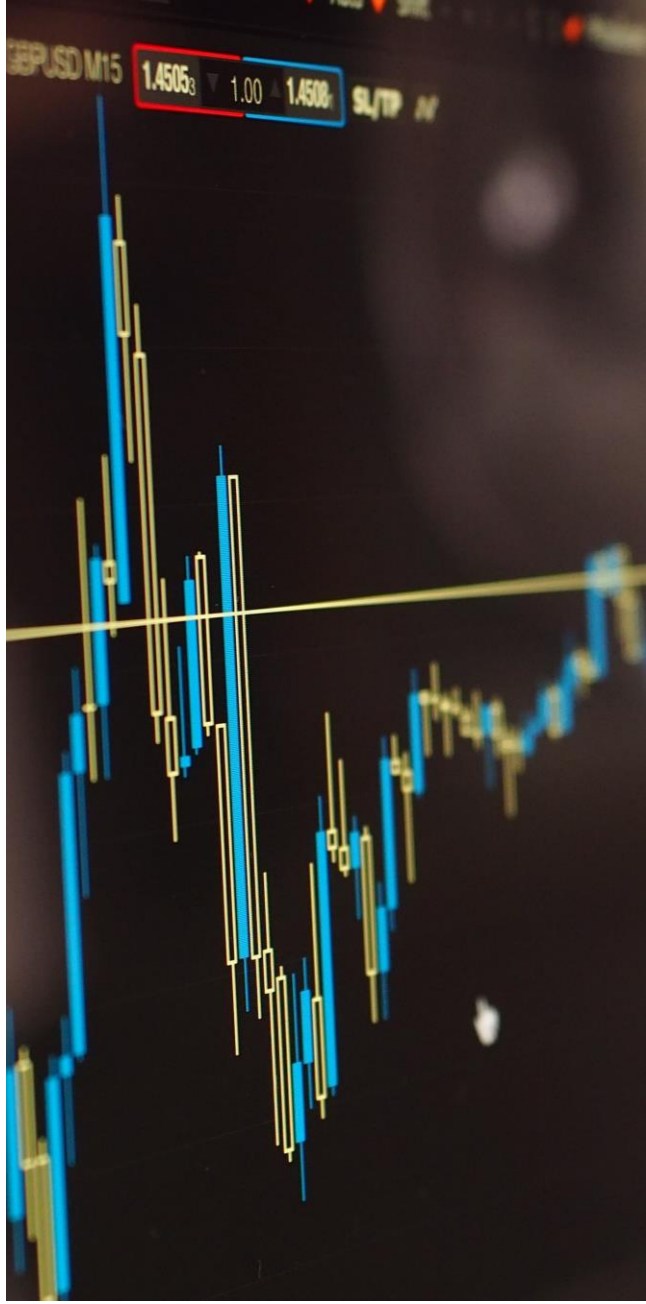




Ataki ransomware na świecie – sektor ochrony zdrowia



Źródło: Raport firmy Recorded Future z dnia 22.10.2024



Wyzwania cyberbezpieczeństwa w sektorze ochrony zdrowia

Rośnie ilość i złożoność ataków.

Podmioty są często słabo przygotowane do radzenia sobie z incydentami.

Skuteczne ataki wpływają na świadczenie usług ochrony zdrowia i życia.

W sektorze przetwarzane są ogromne ilości danych osobowych wrażliwych.

Słabości w sektorze nadużywane są przez zorganizowane grupy w celach zarobkowych.

Zadania CSIRT CeZ

Celem Sektorowego Zespołu Cyberbezpieczeństwa jest:

- Działanie na rzecz podmiotów w sektorze ochrony zdrowia,
- Podnoszenie odporności całego sektora na cyberzagrożenia,
- Ograniczenie strat poprzez wsparcie podmiotów w sektorze w obsłudze incydentów,
- Działania z zakresu prewencji oraz profilaktyki w zakresie cyberprzestrzeni na rzecz sektora,
- Wsparcie w zwalczaniu nadużyć.

Podstawa prawna powołania CSIRT-u

Według Ustawy o Krajowym Systemie Cyberbezpieczeństwa
(Ustawa KSC z 05.07.2018r. – Dz. U. 2018 poz. 1560 ze zm.)

Art. 44. 1. Organ właściwy do spraw cyberbezpieczeństwa może ustanowić, zgodnie z odrębnymi przepisami, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, odpowiedzialny w szczególności za…

Organ właściwy dla sektora to Ministerstwo Zdrowia

Stanowi część składową **Krajowego Systemu Cyberbezpieczeństwa** – art. 4 pkt 6

Aktualnie realizowane zadania na rzecz sektora

- Monitorowanie podatności wysokich i krytycznych oraz ostrzeganie o nich podmiotów.
- Monitorowanie kradzieży loginów i haseł oraz informowanie o nich podmiotów.
- Wyszukiwanie błędnie skonfigurowanych usług w podmiotach.
- Prowadzenie szkoleń z zakresu cyberbezpieczeństwa.
- Promowanie dobrych praktyk.
- Przyjmowanie, rejestrowanie i ewidencjonowanie incydentów w sektorze 7 dni w tygodniu przez cały rok.
- Wsparcie podmiotów w obsłudze incydentów.
- Monitorowanie zagrożeń w otoczeniu Polski.
- Korelowanie zdarzeń.
- Wymiana informacji z zespołami CSIRT poziomu krajowego.
- Wykonywanie skanów podatności w podmiotach.

CSIRT sektora ochrony zdrowia w UE

Na 27 państw członkowskich UE jest 6 sektorowych zespołów cyberbezpieczeństwa

+1 w Wielkiej Brytanii

Lista:

- Holandia
- Wielka Brytania
- Francja
- Luksemburg
- Norwegia
- Słowacja
- Austria

CSIRT sektora ochrony zdrowia w UE

Charakterystyka

- Bardzo zróżnicowany zakres działalności
- Niektóre są prawie niewidoczne w sferze publicznej
- Nie wszystkie funkcjonują jako zarejestrowany CSIRT

Rozwój i perspektywy CSIRT CeZ

CSIRT CeZ dąży do proaktywnego przeciwdziałania zagrożeniom i wspierania sektora ochrony zdrowia, planując następujące przedsięwzięcia:

- Udoskonalenie narzędzi do monitorowania incydentów i analizy zagrożeń.
- Rozwój systemów wymiany informacji o incydentach i zagrożeniach w obrębie sektora ochrony zdrowia oraz innymi CSIRT-ami.
- Opracowanie i wdrożenie standardowych procedur reagowania na incydenty, dostosowanych do specyfiki sektora ochrony zdrowia.
- Stworzenie pełnej, aktualnej listy podmiotów wchodzących w skład sektora ochrony zdrowia, z uwzględnieniem ich roli i znaczenia.
- Wzmocnienie współpracy między CSIRT CeZ a podmiotami sektora zdrowia w zakresie wymiany wiedzy i doświadczeń – dotychczasowa responsywność podmiotów oscyluje w granicach 10%.

Podsumowanie

Działalność CSIRT CeZ (Computer Security Incident Response Team Centrum e-Zdrowia) jest kluczowa i niezwykle istotna, ponieważ sektor ochrony zdrowia jest szczególnie narażony na cyberataki, takie jak ransomware czy próby wyłudzenia danych, które mogą bezpośrednio zagrażać bezpieczeństwu pacjentów, ich rodzin oraz podmiotów wchodzących w skład sektora.

CYBERODPORNOŚĆ

Dziękuję za uwagę

dr Małgorzata Olszewska
Dyrektor Centrum e-Zdrowia

UKSW

Ministerstwo Cyfryzacji

Naukowe Centrum Prawno-informatyczne

SAMSUNG

NASK