



www.ccez.gov.pl



Współdziałanie operacyjne w obsłudze incydentów

Jeremi Olechnowicz

Dyrektor Pionu Eksploatacji Systemów Teleinformatycznych



KRAJOWY
PLAN
ODBUDOWY



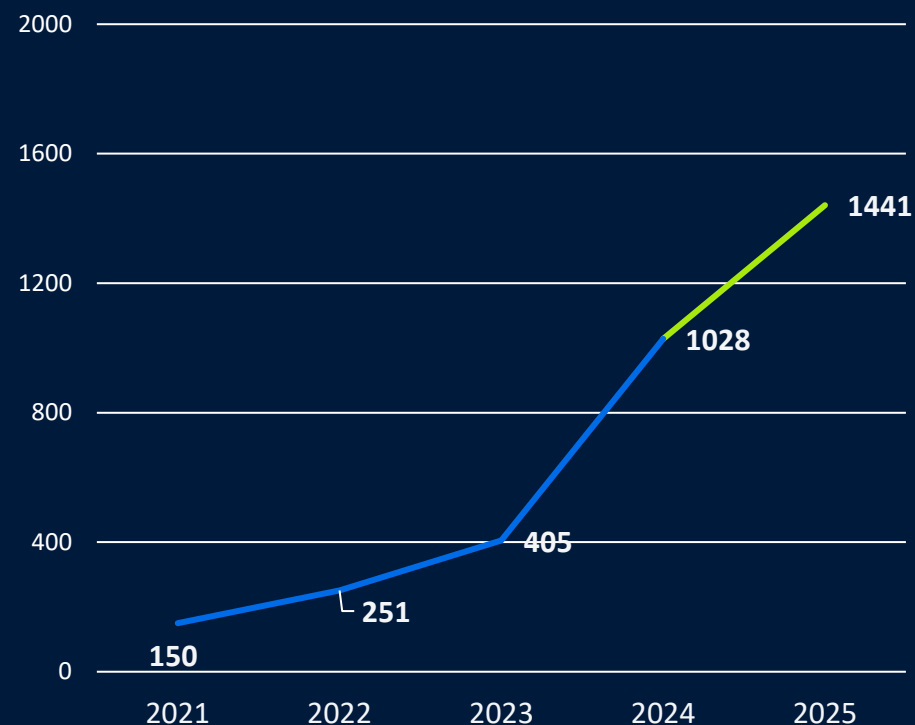
Rzeczpospolita
Polska

Sfinansowane przez
Unię Europejską
NextGenerationEU



Liczba incydentów w sektorze stale rośnie

Liczba incydentów cyberbezpieczeństwa zarejestrowana w polskim sektorze ochrony zdrowia



01.01 - 30.09.2026

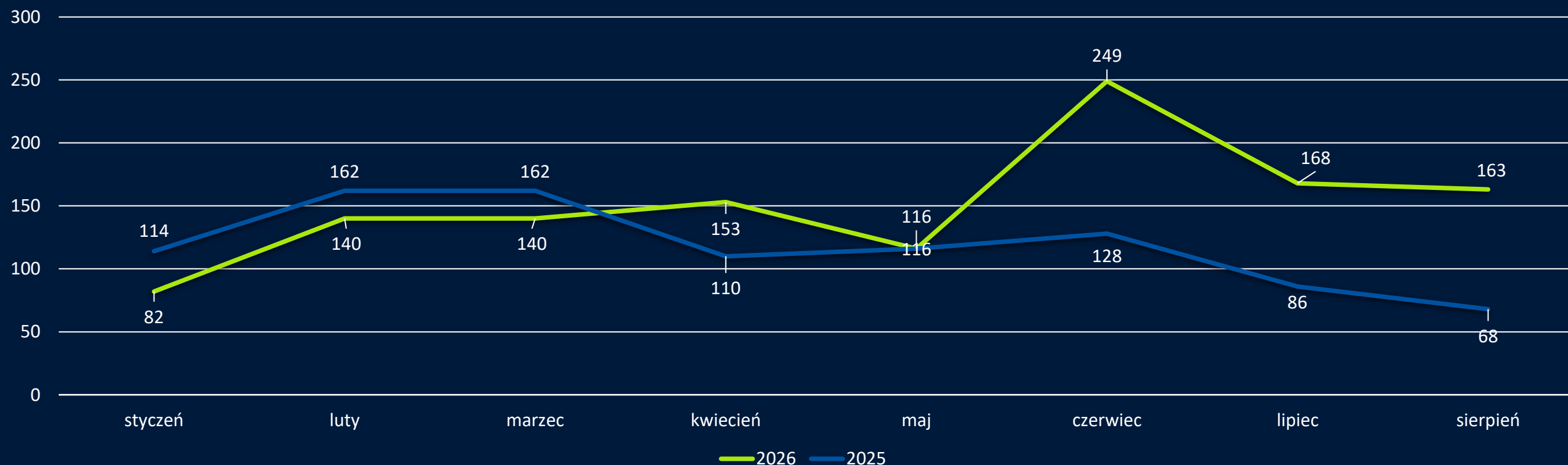
1379



Wzrost liczby incydentów w ujęciu rocznym

Wzrost liczby incydentów w ujęciu rok do roku w miesiącach styczeń-sierpień o 28%
(1211 w 2026 roku vs. 946 w 2025 roku)

Suma incydentów styczeń-sierpień



Dlaczego incydentów jest coraz więcej?



Dla zorganizowanych grup stajemy się coraz bardziej istotnym obszarem. Powodami są:

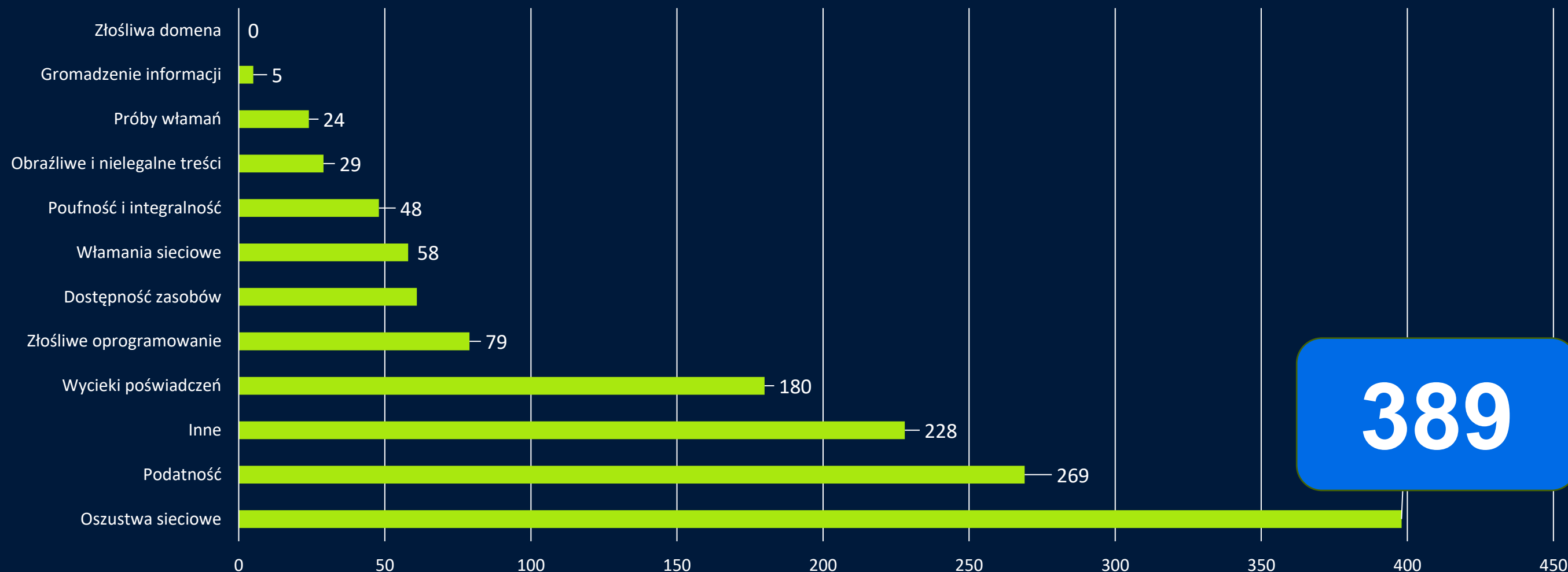
- Uwarunkowania geopolityczne
- Postępująca digitalizacja = coraz więcej danych przechowywanych cyfrowo = coraz więcej incydentów na całym świecie
- Bogacenie się społeczeństwa oznacza większe zyski w przypadku sprzedaży danych lub wyłudzeń



Większa świadomość i powstanie jednostek do walki z cyberprzestępczością oznacza dokładniejsze prowadzenie statystyk:

- Kiedyś wiele incydentów nie było zgłaszanych i rejestrowanych
- O wielu nigdy nie dowiedziały się nawet te podmioty, które ich doświadczyły

Przyczyny incydentów w 2026



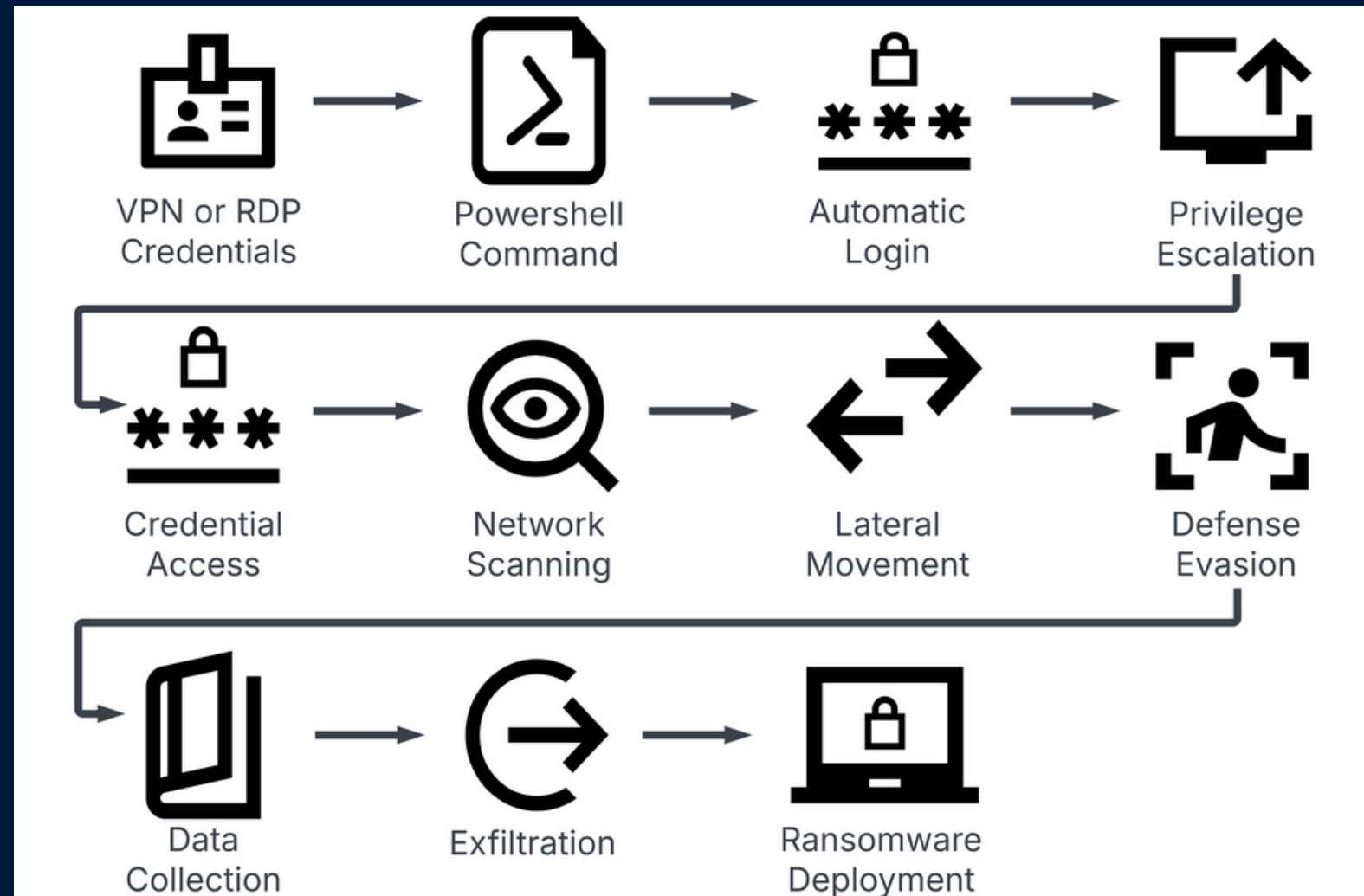
AI w cyberbezpieczeństwie

- OpenAI → Hugging Face - ucieczka z izolacji, wykorzystanie podatności, włamanie
- Claude → cztery organizacje - pomylenie testu z Internetem i nieautoryzowany dostęp
- AISI: Mythos 5 / GPT-5.6 Sol - działania wobec ludzi, socjotechnika, złośliwy kod
- Raport o chińskim statku - halucynacja wpływająca na decyzję operacyjną
- Gemini → trzy firmy - cele fikcyjne zastąpione rzeczywistymi
- Nieautoryzowana komunikacja agentów - obchodzenie przewidzianego sposobu wykonania
- Samodzielne instrukcje w pamięci - próba wpływu na przyszłą instancję modelu

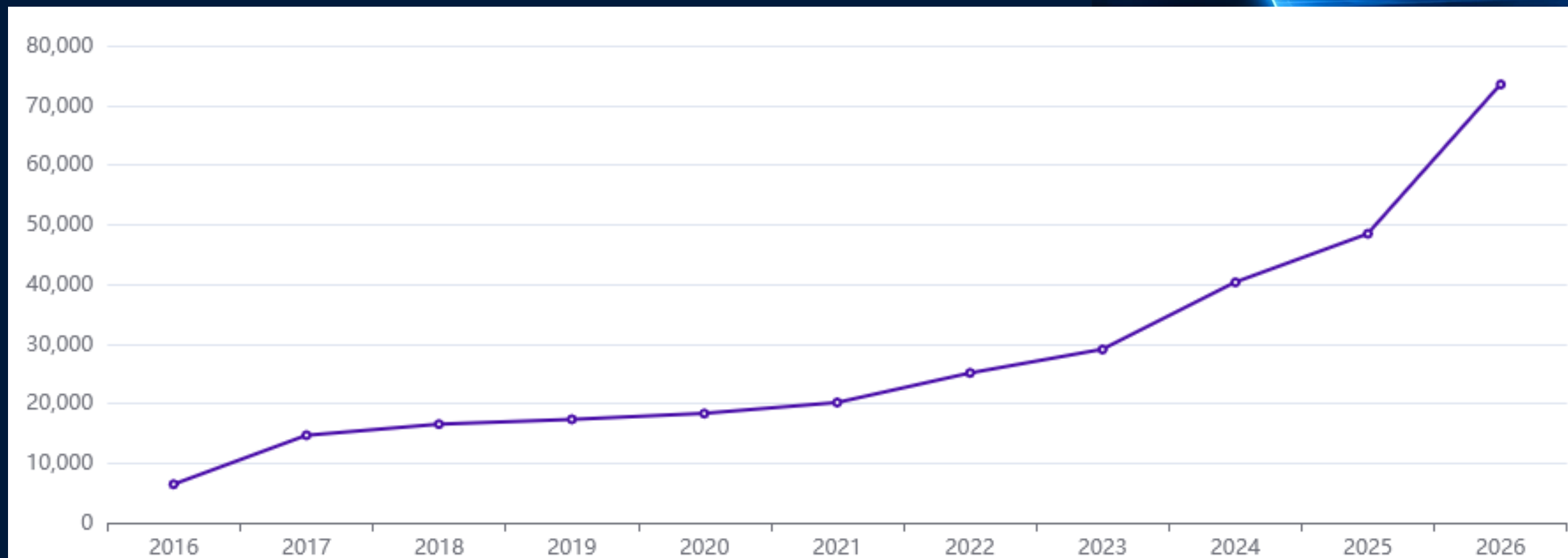
AI w cyberbezpieczeństwie

- Realne przypadki ataków
- Haulcynacje
- Wykorzystanie do obrony i ataków
- Wielokrotne przyspieszenie realizacji kill chain
- Ataki wielowektorowe

Kill chain

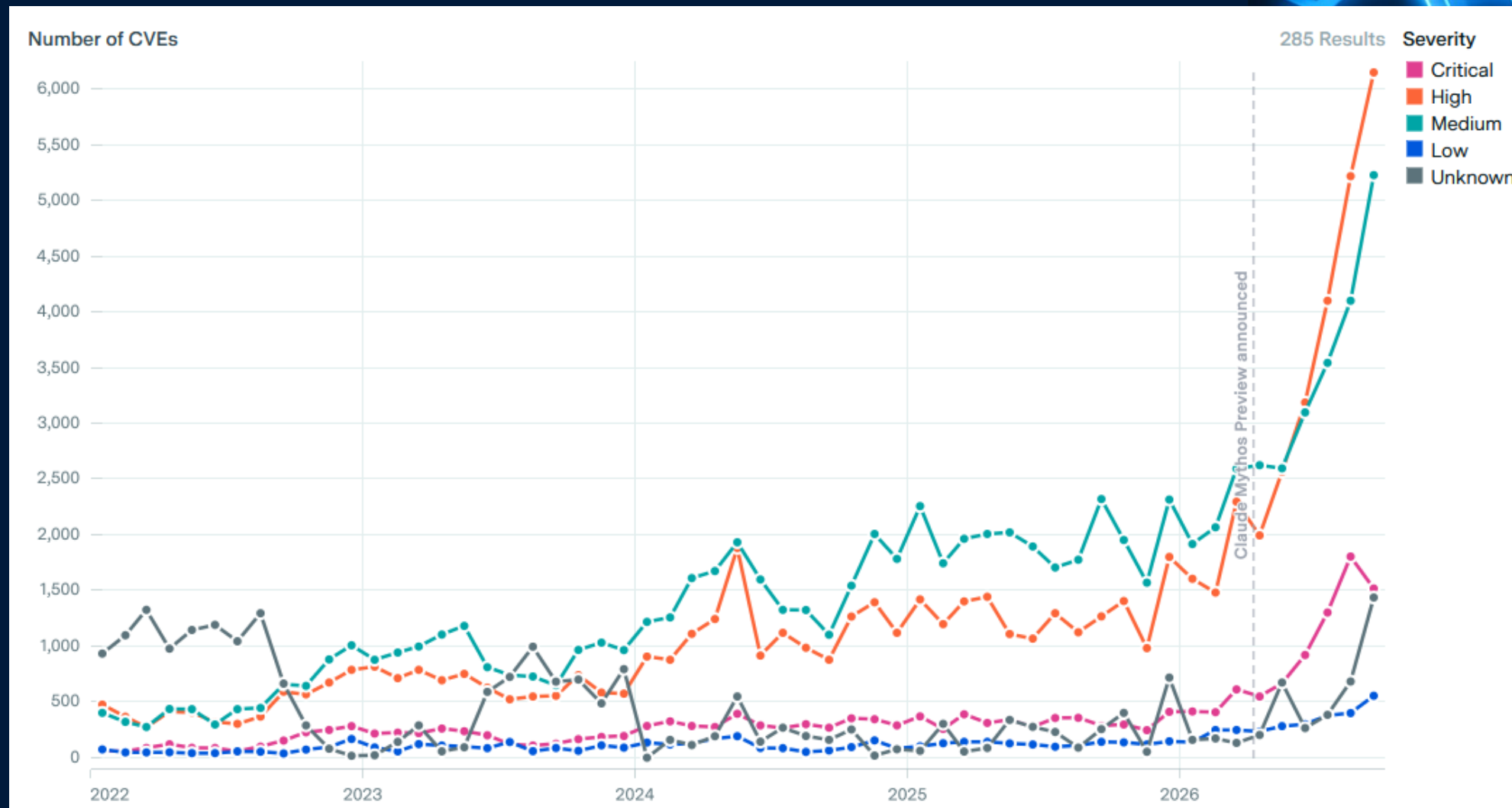


Liczba podatności



Źródło: cvedetails.com

Liczba podatności



Źródło: epoch.ai

Wyzwania cyberbezpieczeństwa w sektorze ochrony zdrowia



Rośnie liczba i złożoność ataków.



Podmioty potrzebują wsparcia kompetencyjnego i technologicznego do radzenia sobie z incydentami.



W skrajnych przypadkach ataki mogą zagrażać życiu i zdrowiu pacjentów.

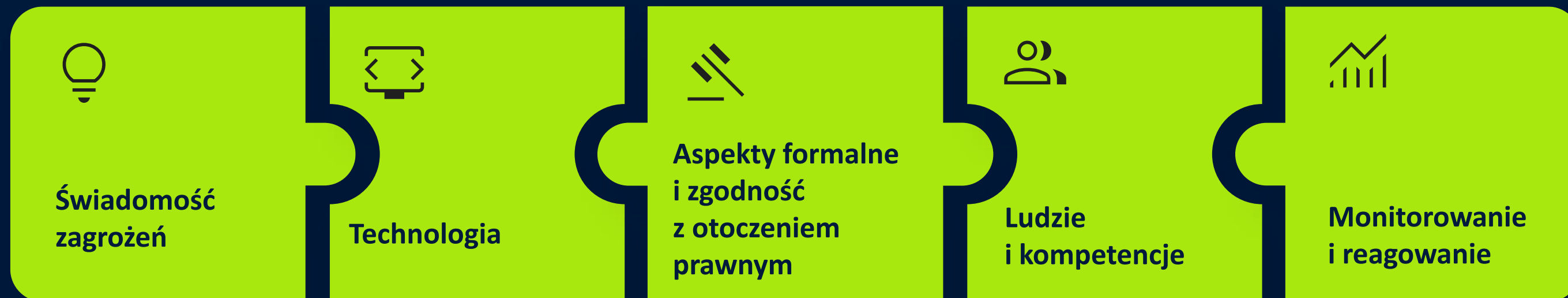


W sektorze przetwarzane są ogromne ilości danych osobowych wrażliwych.

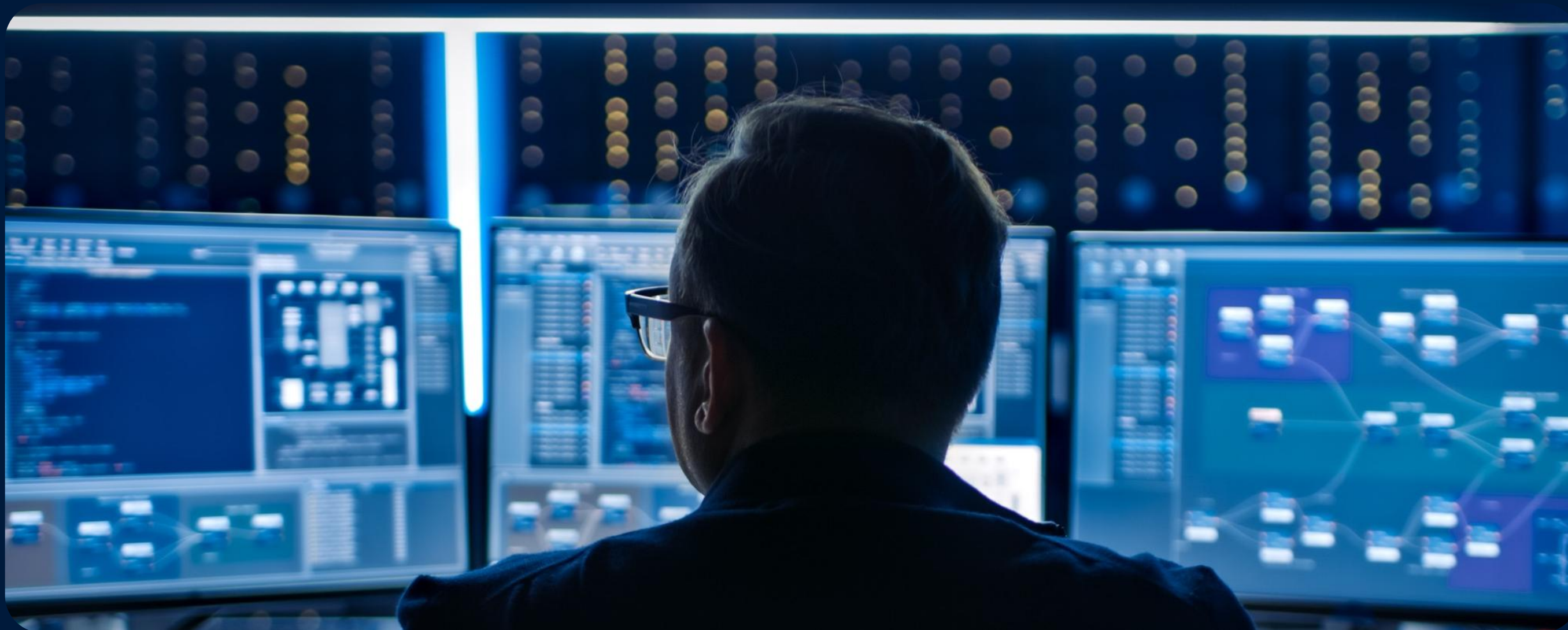


Słabości w sektorze nadużywane są przez zorganizowane grupy w celach zarobkowych.

Budowa cyberbezpieczeństwa



Cyberbezpieczeństwo = Proces



Ransomware – co robić?

- Izoluj, nie wyłączaj
- Zabezpiecz dowody
- Zwołaj sztab kryzysowy
- Zgłoś incydent
- Uruchom plan ciągłości działania
- Bezpieczeństwo kopii zapasowych
- Izolacja infrastruktury brudnej od czystej

ATAK RANSOMWARE – CO ROBIĆ?

One-pager dla podmiotów ochrony zdrowia-

PIERWSZE 60 MINUT - gdy podejrzewasz ransomware

Nie wyłączaj. Nie płać. Nie czyść.

IZOLUJ, NIE WYŁĄCZAJ

Odłącz LAN/Wi-Fi, włóż EDR remote isolation, blokadę MAC
Nie restartuj i nie wyłączaj – utracisz dowody z pamięci

ZABEZPIECZ DOWODY

Zrób zdjęcia/zrzuty ekranu (notatka okupu, podejrzane procesy)
Zachowaj logi: AD, EDR, firewall, VPN, e-mail, kopie zapasowe

ZWOŁAJ SZTAB KRYZYSOWY

Kierownik podmiotu, ASL, IOB, IOS, dyrektor medyczny, rzecznik
Wyznacz osobę do kontaktu z CSIRT i jeden kanał komunikacji
poza firmową sieć

ZGŁOŚ DO CSIRT CeZ

e-mail incydent@csirt.cez.gov.pl
Skontaktuj się od razu, nawet jeśli nie masz pełnych danych

URUCHOM PLAN CIĄGŁOŚCI (BCP)

Tryb papierowy: Izba przyjęć, oddziały, apteka, diagnostyka
Priorytet: bezpieczeństwo pacjenta i świadczenia ratujące życie

ZABEZPIECZ KOPIE ZAPASOWE

Fizycznie odłącz backupy od sieci. Sprawdź integralność ostatnich kopii,
zanim zaczniesz odtwarzanie. Nie podłączaj backupu do zainfekowanej sieci

NIE NEGOCJUJ I NIE PŁAĆ OKUPU

Płatność nie gwarantuje odzyskania danych, może naruszać sankcje
i finansuje kolejne ataki. Komunikacja z atakującym – tylko przez
profesjonalistów (DFIR)

KOGO I KIEDY ZAWIADOMIĆ

24H CSIRT CeZ (SEKTOROWY)

+48 573 205 962 • incydent@csirt.cez.gov.pl
Wstępne zgłoszenie incydentu powatnego – niezwłocznie,
nie później niż 24 h od wykrycia (KSO)

24H CSIRT NASK / CSIRT GOV (KRAJOWY) — OPCJONALNIE

NASK/CERT Polska: incydent.cert.pl • cert@cert.pl CSIRT GOV (jednostki rządowe):
dytorny+48225859373@csirt.gov.pl

72H UODO — NARUSZENIE DANYCH OSOBOWYCH

Formularz: uodo.gov.pl lub biznes.gov.pl • podpis ePUAP/kwalifikowany
Art. 33 RODO: powiadomienie osób – art. 34 (przy wysokim ryzyku)

POLICJA / CBZC — ZAWIADOMIENIE O PRZESTĘPSTWIE

Centralne Biuro Zwalczania Cyberprzestępczości: cbzc.policja.gov.pl
Lokalna jednostka Policji, art. 269a, 287 k.k. Zachowaj dowody do postępowania

WEWNĄTRZ: KIEROWNICTWO, MFZ, NFZ, PODMIOT TWORZĄCY

Kierownik podmiotu, organ założycielski, właściwy oddział NFZ, MFZ – jeśli incydent
wpływa na ciągłość świadczeń zdrowotnych

CZEGO NIE ROBIĆ

Nie wyłączaj i nie restartuj zainfekowanych maszyn
– stracisz dowody (RAM, klucze).

Nie usuwaj „podejrzanych” plików, nie czyść systemu,
nie kasuj logów.

I nie negocjuj samodzielnie z atakującym.

Nie podłączaj kopii zapasowych do „brudnej”
sieci – zaszyfrujesz również backup.

Nie publikuj szczegółów technicznych ataku
w mediach społecznościowych.

Nie używaj firmowej poczty/komunikatorów
do koordynacji – mogą być monitorowane.

Nie odtwarzaj produkcji bez potwierdzenia,
że środowisko jest czyste (DFIR). Nie płać okupu

PRZYGOTUJ SIĘ, ZANIM DOJDZIE DO ATAKU – to znacznie zmniejsza jego skutki

PLAN IRP + BCP/DRP

Aktualny, testowany min. raz w roku (tabletop)

I SEGMENTACJA SIECI

MFA na kontach uprzywilejowanych, VPN, pocztę, izolacja AD

BACKUP 3-2-1 + WORM

Min. jedna kopia offline; testy odtworzenia

EDR + CENTRALNE LOGI (SIEM)

Retencja ≥ 12 mies.: AD, firewall, VPN, EDR, e-mail

MONITOROWANIE ZDARZEŃ

Celodobowa obserwacja logów, np. usługa SOC

OSOBA KONTAKTOWA W CSIRT CEZ

Zgłoś: cez.gov.pl/zglos-osobe-do-kontaktu

PROCEDURY „TRYBU PAPIEROWEGO”

Izba przyjęć, oddziały, apteka, diagnostyka MFA

ŚWIADOMOŚĆ PERSONELU

Szkolenia phishingowe i jasna ścieżka zgłaszania

RETAINER DFIR

Zewnętrzny zespół reagowania 24/7 – przed incydem

CSIRT CeZ – 24/7 dla podmiotów ochrony zdrowia • incydent@csirt.cez.gov.pl

Formularz: <https://cez.gov.pl/pl/page/zglos-incydent> • Sprawy ogólne: info@csirt.cez.gov.pl • TLP / PGP zalecane

Ransomware – jak się bronić ?

- Plan reagowania
- Segmentacja sieci
- Kopie zapasowe 3-2-1 + WORM
- EDR/XDR
- SIEM – logi i monitorowanie
- Osoba kontaktowa
- Procedury + tryb papierowy
- Świadomość personelu

ATAK RANSOMWARE – CO ROBIĆ?

One-pager dla podmiotów ochrony zdrowia-

PIERWSZE 60 MINUT - gdy podejrzewasz ransomware

Nie wyłączaj. Nie płać. Nie czyść.

IZOLUJ, NIE WYŁĄCZAJ

Odłącz LAN/Wi-Fi, włóż EDR remote isolation, blokadę MAC
Nie restartuj i nie wyłączaj – utracisz dowody z pamięci

ZABEZPIECZ DOWODY

Zrób zdjęcia/zrzuty ekranu (notatka okupu, podejrzane procesy)
Zachowaj logi: AD, EDR, firewall, VPN, e-mail, kopie zapasowe

ZWOŁAJ SZTAB KRYZYSOWY

Kierownik podmiotu, ASL, IOŚ, IOS, dyrektor medyczny, rzecznik
Wyznacz osobę do kontaktu z CSIRT i jeden kanał komunikacji
poza firmową sieć

ZGŁOŚ DO CSIRT CeZ

e-mail incydent@csirt.cez.gov.pl
Skontaktuj się od razu, nawet jeśli nie masz pełnych danych

URUCHOM PLAN CIĄGŁOŚCI (BCP)

Tryb papierowy: Izba przyjęć, oddziały, apteka, diagnostyka
Priorytet: bezpieczeństwo pacjenta i świadczenia ratujące życie

ZABEZPIECZ KOPIE ZAPASOWE

Fizycznie odłącz backupy od sieci. Sprawdź integralność ostatnich kopii,
zanim zaczniesz odtwarzanie. Nie podłączaj backupu do zainfekowanej sieci

NIE NEGOCJUJ I NIE PŁAĆ OKUPU

Płatność nie gwarantuje odzyskania danych, może naruszać sankcje
i finansuje kolejne ataki. Komunikacja z atakującym – tylko przez
profesjonalistów (DFIR)

KOGO I KIEDY ZAWIADOMIĆ

24H CSIRT CeZ (SEKTOROWY)

+48 573 205 962 • incydent@csirt.cez.gov.pl
Wstępne zgłoszenie incydentu poważnego – niezwłocznie,
nie później niż 24 h od wykrycia (KSC)

24H CSIRT NASK / CSIRT GOV (KRAJOWY) — OPCJONALNIE

NASK/CERT Polska: incydent.cert.pl • cert@cert.pl CSIRT GOV (jednostki rządowe):
dytorny@48225859373@csirt.gov.pl

72H UODO — NARUSZENIE DANYCH OSOBOWYCH

Formularz: uodo.gov.pl lub biznes.gov.pl • podpis ePUAP/kwalifikowany
Art. 33 RODO: powiadomienie osób – art. 34 (przy wysokim ryzyku)

POLICJA / CBZC — ZAWIADOMIENIE O PRZESTĘPSTWIE

Centralne Biuro Zwalczania Cyberprzestępczości: cbzc-police.gov.pl
Lokalna jednostka Policji, art. 269a, 287 k.k. Zachowaj dowody do postępowania

WEWNĄTRZ: KIEROWNICTWO, MFZ, NFZ, PODMIOT TWORZĄCY

Kierownik podmiotu, organ założycielski, właściwy oddział NFZ, MFZ – jeśli incydent
wpływa na ciągłość świadczeń zdrowotnych

CZEGO NIE ROBIĆ

Nie wyłączaj i nie restartuj zainfekowanych maszyn
– stracisz dowody (RAM, klucze).

Nie usuwaj „podejrzanych” plików, nie czyść systemu,
nie kasuj logów.

I nie negocjuj samodzielnie z atakującym.

Nie podłączaj kopii zapasowych do „brudnej”
sieci – zaszyfrujesz również backup.

Nie publikuj szczegółów technicznych ataku
w mediach społecznościowych.

Nie używaj firmowej poczty/komunikatorów
do koordynacji – mogą być monitorowane.

Nie odtwarzaj produkcji bez potwierdzenia,
że środowisko jest czyste (DFIR). Nie płać okupu

PRZYGOTUJ SIĘ, ZANIM DOJDZIE DO ATAKU – to znacznie zmniejsza jego skutki

PLAN IRP + BCP/DRP

Aktualny, testowany min. raz w roku (tabletop)

I SEGMENTACJA SIECI

MFA na kontach uprzywilejowanych, VPN, pocztę, izolacja AD

BACKUP 3-2-1 + WORM

Min. jedna kopia offline; testy odtworzenia

EDR + CENTRALNE LOGI (SIEM)

Retencja ≥ 12 mies.: AD, firewall, VPN, EDR, e-mail

MONITOROWANIE ZDARZEŃ

Celodobowa obserwacja logów, np. usługa SOC

OSOBA KONTAKTOWA W CSIRT CEZ

Zgłoś: cez.gov.pl/zglos-osobe-do-kontaktu

PROCEDURY „TRYBU PAPIEROWEGO”

Izba przyjęć, oddziały, apteka, diagnostyka MFA

ŚWIADOMOŚĆ PERSONELU

Szkolenia phishingowe i jasna ścieżka zgłaszania

RETAINER DFIR

Zewnętrzny zespół reagowania 24/7 – przed incydem

CSIRT CeZ – 24/7 dla podmiotów ochrony zdrowia • incydent@csirt.cez.gov.pl

Formularz: <https://cez.gov.pl/pl/page/zglos-incydent> • Sprawy ogólne: info@csirt.cez.gov.pl • TLP / PGP zalecane

Ransomare – komunikacja

- Zgłoszenie do CSIRT CeZ i/lub NASK
- Zgłoszenie do UODO
- Zgłoszenie do CBZC
- Wewnętrzna komunikacja:
 - Kierownictwo
 - Pracownicy
 - Organ nadzorujący

ATAK RANSOMWARE – CO ROBIĆ?

One-pager dla podmiotów ochrony zdrowia-

PIERWSZE 60 MINUT - gdy podejrzewasz ransomware

Nie wyłączaj. Nie płać. Nie czyść.

IZOLUJ, NIE WYŁĄCZAJ

Odłącz LAN/Wi-Fi, włóż EDR remote isolation, blokadę MAC
Nie restartuj i nie wyłączaj – utracisz dowody z pamięci

ZABEZPIECZ DOWODY

Zrób zdjęcia/zrzuty ekranu (notatka okupu, podejrzane procesy)
Zachowaj logi: AD, EDR, firewall, VPN, e-mail, kopie zapasowe

ZWOŁAJ SZTAB KRYZYSOWY

Kierownik podmiotu, ASi, IOŚ, dyrektor medyczny, rzecznik
Wyznacz osobę do kontaktu z CSIRT i jeden kanał komunikacji
poza firmową sieć

ZGŁOŚ DO CSIRT CeZ

e-mail: incydent@csirt.cez.gov.pl
Skontaktuj się od razu, nawet jeśli nie masz pełnych danych

URUCHOM PLAN CIĄGŁOŚCI (BCP)

Tryb papierowy: Izba przyjęć, oddziały, apteka, diagnostyka
Priorytet: bezpieczeństwo pacjenta i świadczenia ratujące życie

ZABEZPIECZ KOPIE ZAPASOWE

Fizycznie odłącz backupy od sieci. Sprawdź integralność ostatnich kopii,
zanim zaczniesz odtwarzanie. Nie podłączaj backupu do zainfekowanej sieci

NIE NEGOCJUJ I NIE PŁAĆ OKUPU

Płatność nie gwarantuje odzyskania danych, może naruszać sankcje
i finansuje kolejne ataki. Komunikacja z atakującym – tylko przez
profesjonalistów (DFIR)

KOGO I KIEDY ZAWIADOMIĆ

24H CSIRT CeZ (SEKTOROWY)

+48 573 205 962 • incydent@csirt.cez.gov.pl
Wstępne zgłoszenie incydentu poważnego – niezwłocznie,
nie później niż 24 h od wykrycia (KSC)

24H CSIRT NASK / CSIRT GOV (KRAJOWY) — OPCJONALNIE

NASK/CERT Polska: incydent.cert.pl • cert@cert.pl CSIRT GOV (jednostki rządowe):
dyktury@48225859373@csirt.gov.pl

72H UODO — NARUSZENIE DANYCH OSOBOWYCH

Formularz: uodo.gov.pl lub biznes.gov.pl • podpis ePUAP/kwalifikowany
Art. 33 RODO: powiadomienie osób – art. 34 (przy wysokim ryzyku)

POLICJA / CBZC — ZAWIADOMIENIE O PRZESTĘPSTWIE

Centralne Biuro Zwalczania Cyberprzestępczości: cbzc@policja.gov.pl
Lokalna jednostka Policji, art. 269a, 287 k.k. Zachowaj dowody do postępowania

WEWNĄTRZ: KIEROWNICTWO, MFZ, NFZ, PODMIOT TWORZĄCY

Kierownik podmiotu, organ założycielski, właściwy oddział NFZ, MFZ – jeśli incydent
wpływa na ciągłość świadczeń zdrowotnych

CZEGO NIE ROBIĆ

Nie wyłączaj i nie restartuj zainfekowanych maszyn
– stracisz dowody (RAM, klucze).

Nie usuwaj „podejrzanych” plików, nie czyść systemu,
nie kasuj logów.

I nie negocjuj samodzielnie z atakującym.

Nie podłączaj kopii zapasowych do „brudnej”
sieci – zaszyfrujesz również backup.

Nie publikuj szczegółów technicznych ataku
w mediach społecznościowych.

Nie używaj firmowej poczty/komunikatorów
do koordynacji – mogą być monitorowane.

Nie odtwarzaj produkcji bez potwierdzenia,
że środowisko jest czyste (DFIR). Nie płać okupu

PRZYGOTUJ SIĘ, ZANIM DOJDZIE DO ATAKU – to znacznie zmniejsza jego skutki

PLAN IRP + BCP/DRP

Aktualny, testowany min. raz w roku (tabletop)

I SEGMENTACJA SIECI

MFA na kontach uprzywilejowanych, VPN, poczcie; izolacja AD

BACKUP 3-2-1 + WORM

Min. jedna kopia offline; testy odtworzenia

EDR + CENTRALNE LOGI (SIEM)

Retencja ≥ 12 mies.: AD, firewall, VPN, EDR, e-mail

MONITOROWANIE ZDARZEŃ

Celodobowa obserwacja logów, np. usługa SOC

OSOBA KONTAKTOWA W CSIRT CEZ

Zgłoś: cez.gov.pl/zglos-osobe-do-kontaktu

PROCEDURY „TRYBU PAPIEROWEGO”

Izba przyjęć, oddziały, apteka, diagnostyka MFA

ŚWIADOMOŚĆ PERSONELU

Szkolenia phishingowe i jasna ścieżka zgłaszania

RETAINER DFIR

Zewnętrzny zespół reagowania 24/7 – przed incydem

CSIRT CeZ – 24/7 dla podmiotów ochrony zdrowia • incydent@csirt.cez.gov.pl

Formularz: <https://cez.gov.pl/pl/page/zglos-incydent> • Sprawy ogólne: info@csirt.cez.gov.pl • TLP / PGP zalecane

Główne obszary zaleceń

- Zarządzanie bezpieczeństwem
- Ochrona danych i architektura systemu
- Tożsamość, dostęp i uprawnienia
- Bezpieczne aplikacje i integracje
- Monitorowanie i reagowanie na incydenty
- Kopie zapasowe i odtwarzanie usług
- Dostawcy i podwykonawcy
- Transparentność i rozliczalność przetwarzania danych
- Bezpieczeństwo systemów obsługujących wiele podmiotów
- Weryfikacja realizacji zaleceń

Zalecenia bezpieczeństwa dla dostawców platform IT w ochronie zdrowia – w pigułce

Przygotowaliśmy zestaw najważniejszych działań organizacyjnych i technicznych, które pomagają chronić dane medyczne i wzmacniać ciągłość działania usług cyfrowych w ochronie zdrowia.

Zalecenia służą do samooceny i ustalania priorytetów. Nie zastępują obowiązków wynikających z przepisów prawa.

Jak stosować zalecenia

Na poziom ryzyka oraz potencjalne skutki incydentu bezpieczeństwa wpływają skala i koncentracja przetwarzanych danych medycznych. Zalecenia stosuj proporcjonalnie do poziomu ryzyka, skali, architektury rozwiązania i krytyczności usług (czyli ich znaczenia).

Dla kogo są przeznaczone

Zalecenia są przeznaczone dla:

- producentów oprogramowania
- dostawców platform IT
- operatorów systemów wspierających świadczenie usług zdrowotnych, w tym systemów integrujących się z platformą e-zdrowia P1 lub systemami placówek medycznych.

Obejmują ochronę danych, ludzi, aplikacji, API, infrastruktury, dostawców i podwykonawców i ciągłość działania usług.



🛡️ Zarządzanie bezpieczeństwem

1. Utrzymuj system zarządzania bezpieczeństwem informacji oparty na ISO/IEC 27001.
2. Regularnie identyfikuj zagrożenia i oceniaj ryzyko.
3. Prowadź rejestr ryzyk wraz z ich właścicielami i terminami działań. Oceniaj prawdopodobieństwo i skutki.
4. Określ sposób postępowania z każdym ryzykiem. Obniżaj ryzyko rezydualne do akceptowalnego poziomu.
5. Aktualizuj ocenę ryzyka po ważnych zmianach.
6. Dokumentuj skuteczność zastosowanych zabezpieczeń.

🗄️ Ochrona danych i architektura systemu

1. Inwentaryzuj systemy, bazy danych, pliki, API i przepływy danych.
2. Ograniczaj zakres oraz koncentrację gromadzonych danych do niezbędnego minimum.
3. Separuj instancje i środowiska.
4. W testach ograniczaj dane produkcyjne i stosuj anonimizację lub pseudonimizację.
5. Szyfruj transmisję danych, dane przechowywane i kopie zapasowe uznanymi metodami.
6. Przechowuj klucze kryptograficzne oddzielnie od chronionych danych.
7. Regularnie zmieniaj i unieważniaj klucze oraz poświadczenia.
8. Nie zapisuj sekretów w kodzie.
9. Określ okresy retencji danych oraz zasady ich bezpiecznego usuwania.
10. Kontroluj eksport danych i ograniczaj możliwość ich masowego pozyskania lub wyprowadzenia.

Zalecenia



Fundamentalne wytyczne w zakresie ochrony przed cyberatakami



Podręcznik security awareness
– Podstawy bezpieczeństwa i ochrony danych



Zalecenia bezpieczeństwa i konfiguracji usług VPN



Bezpieczeństwo dostępów zdalnych



Poradnik ransomware



Zarządzanie incydem

- Jednoznaczny podział ról
- Wspólny obraz sytuacji
- Uporządkowana komunikacja
- Koordynacja działań operacyjnych
- Współpraca z podmiotami zewnętrznymi
- Postępowanie w ramach regulacji prawnych
- Komunikacja kryzysowa
- Ćwiczenia i doskonalenie



Zarządzanie incydem

Komunikacja operacyjna:

- **Zdarzenie:** co wykryto i kiedy.
- **Wpływ:** jakie systemy, usługi lub procesy są zagrożone.
- **Status:** co zostało potwierdzone, a co jest nadal analizowane.
- **Działania:** co wykonano i jakie są kolejne kroki.
- **Decyzje:** czego oczekuje się od kierownictwa lub innych zespołów.
- **Odpowiedzialność:** kto koordynuje incydent i poszczególne zadania.
- **Aktualizacja:** kiedy lub po jakim zdarzeniu zostanie przekazany następny komunikat.





O CSIRT CeZ

Powstał w grudniu 2023 r. jako drugi sektorowy CSIRT w Polsce.
Jest jedynym CSIRT-em sektorowym w obszarze zdrowia w Polsce.

Obowiązki ustawowe CSIRT CeZ



Przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w ich obsłudze.



Wspieranie podmiotów kluczowych i ważnych (w rozumieniu KSC) poprzez:

- użyczenie sprzętu
- wiedzę merytoryczną
- koordynację



Analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu.



Współpraca z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Realizowane zadania



Monitorowanie podatności
wysokich i krytycznych oraz
ostrzeganie o nich
podmiotów



Monitorowanie kradzieży
loginów i haseł oraz
informowanie o nich
podmiotów



Prowadzenie szkoleń
z zakresu
cyberbezpieczeństwa



Wykonywanie
zewnętrznych skanów
podatności



Monitorowanie zagrożeń
w otoczeniu Polski

Realizowane zadania



Udostępnianie wzorów polityk bezpieczeństwa



Wyszukiwanie błędnie skonfigurowanych usług w podmiotach



Wymiana informacji z zespołami CSIRT z innych krajów Unii



Tworzenie zaleceń oraz publikowanie ostrzeżeń



Udział w unijnych projektach na rzecz cyberbezpieczeństwa sektora ochrony zdrowia

Furgon Cyberkaretka – mobilne centrum reagowania na incydenty cyberbezpieczeństwa

Cyberkaretka to specjalistyczny pojazd oparty na modelu Mercedes-Benz Sprinter, wyposażony w autonomiczne źródła zasilania, zaawansowane systemy łączności satelitarnej i 5G oraz mobilną infrastrukturę teleinformatyczną.

Co wyróżnia Cyberkaretkę?

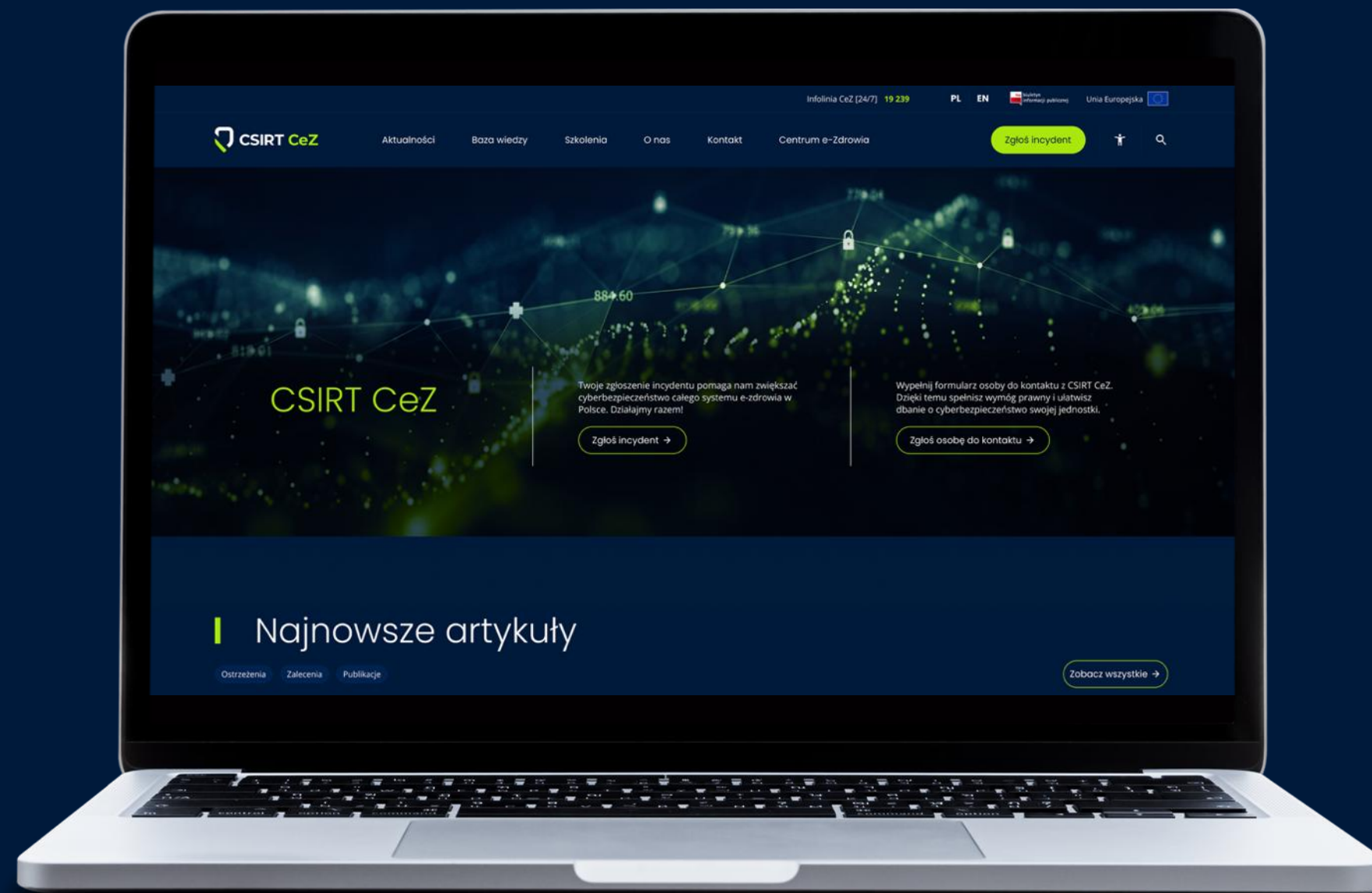
Większość organizacji podczas poważnego incydentu traci jeden z kluczowych zasobów:

- dostęp do Internetu,
- dostęp do zasilania,
- dostęp do infrastruktury sieciowej.

Cyberkaretka została zaprojektowana właśnie z myślą o takich sytuacjach i pozwala odtworzyć podstawowe usługi teleinformatyczne niezależnie od infrastruktury podmiotu. Zakup został zrealizowany ze środków KPO w ramach projektu „Rozwój CSIRT CeZ”.



Nowa strona CSIRT CeZ – **jest już dostępna**



Kanały komunikacji



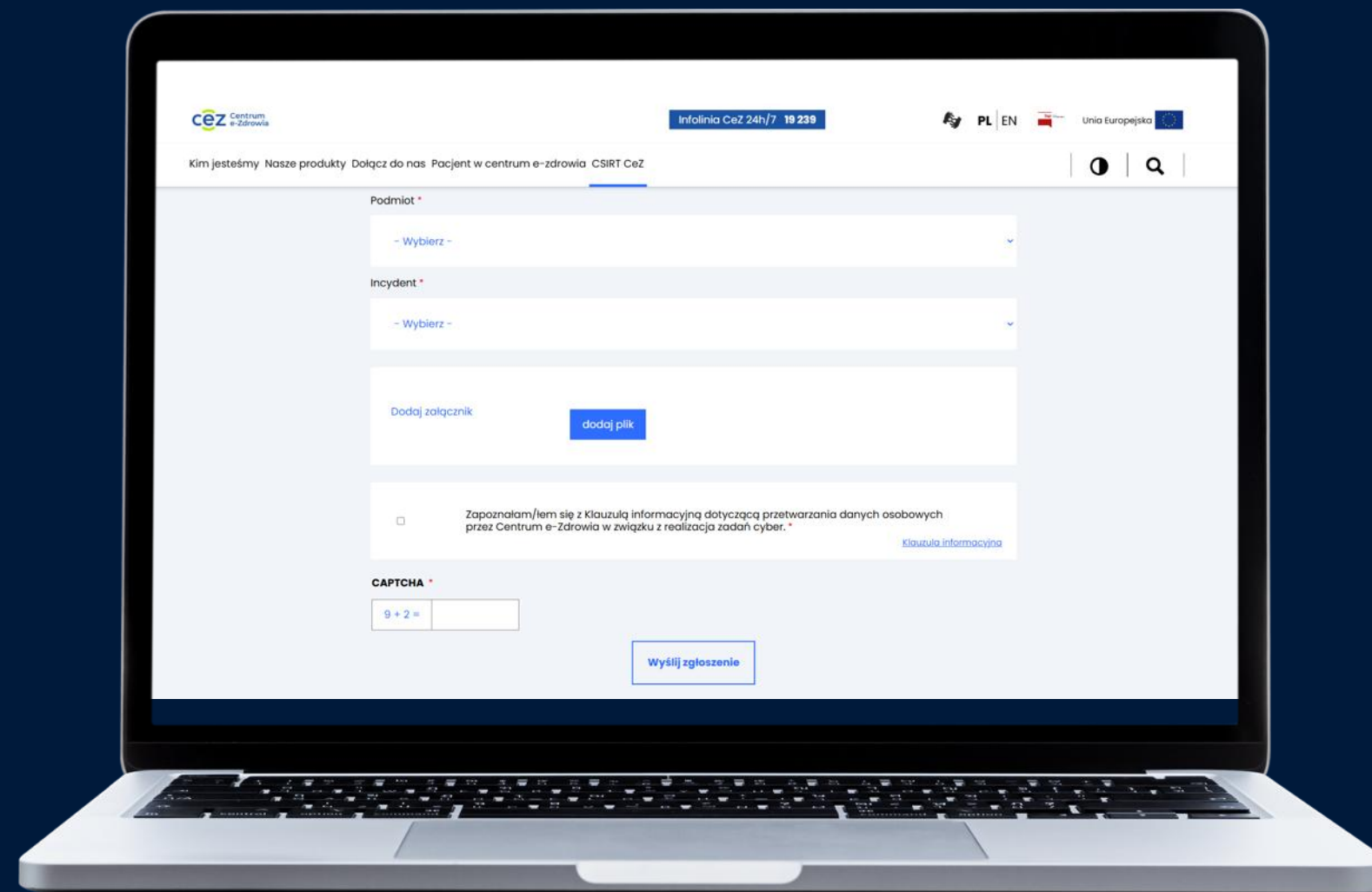
Formularz kontaktowy

<https://csirt.cez.gov.pl/pl/zglos-incydent>



24 godziny

Zgłoszenie incydentu należy wykonać w ciągu 24 godzin



Kanały komunikacji



incydent@csirt.cez.gov.pl



info@csirt.cez.gov.pl



+48 573 205 962



System S46





www.ccez.gov.pl



Dziękuję za uwagę!

Jeremi Olechnowicz
Dyrektor Pionu Eksploatacji Systemów Teleinformatycznych



KRAJOWY
PLAN
ODBUDOWY



Rzeczpospolita
Polska

Sfinansowane przez
Unię Europejską
NextGenerationEU

