Cyberodporny Szpital 360° 365/7/24

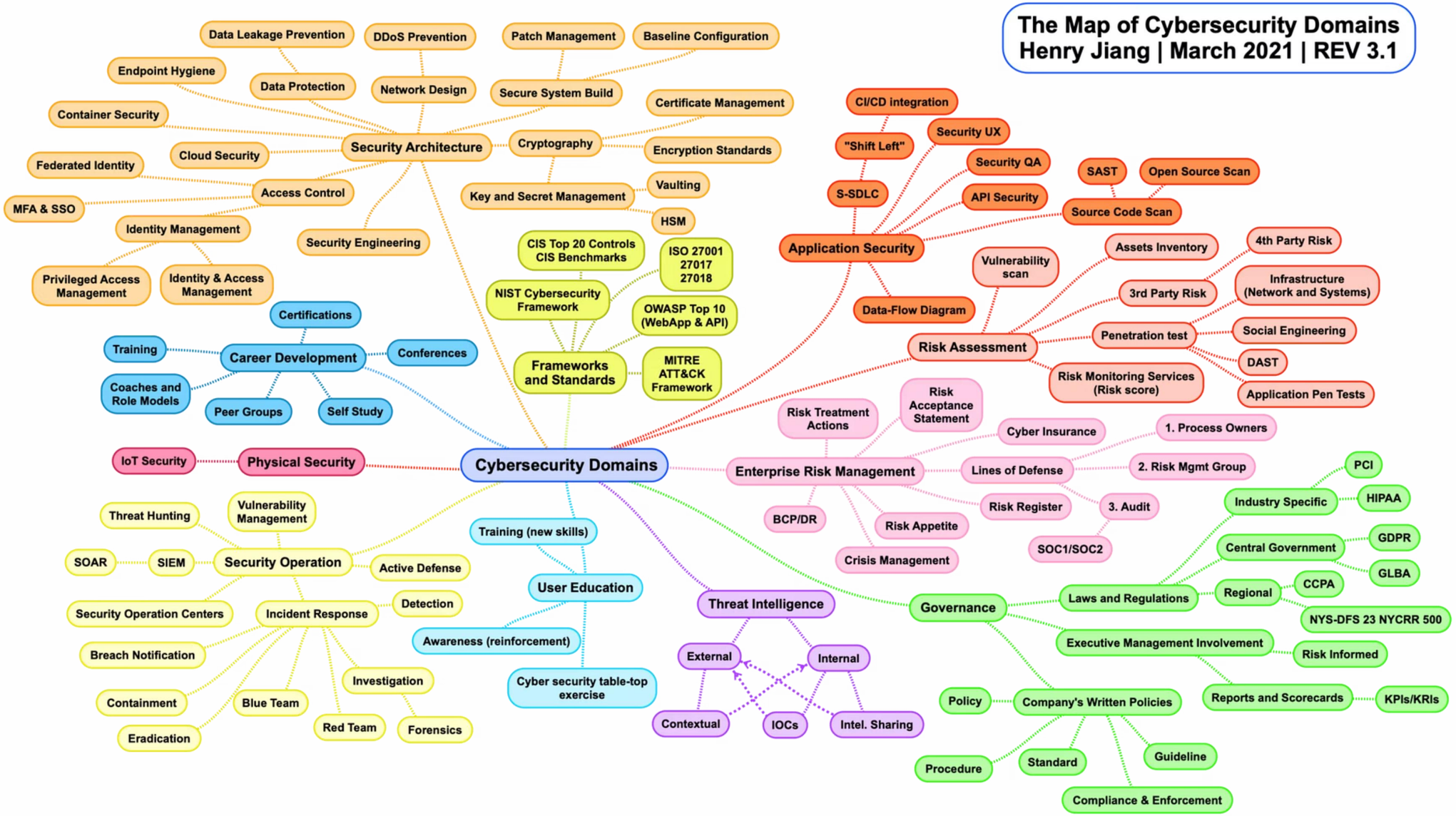
Odkryj skuteczne metody budowania odporności cyfrowej dla bezpieczeństwa pacjentów i danych!

Michał Gembal
ISSA POLSKA, IT AUDIT, ARCUS SA

Hospital 360. Scientific & Practical Conference

Olsztyn, 25.09.2025

Domeny cyberbezpieczeństwa i cyberodporności wg Henry'ego Jianga



Cyberodporność w szpitalach. Dlaczego? Po co?

Cyfryzacja ochrony zdrowia ver. wyzwania

Niewydolność systemu i kolejki do specjalistów

Brak sprawnej koordynacji pomiędzy placówkami, utrudniony dostęp do dokumentacji, powtarzalne badania diagnostyczne.

Ograniczona prewencja i brak narzędzi do zarządzania zdrowiem populacyjnym

System skupia się głównie na leczeniu, a mniej na zapobieganiu chorobom.

Fragmentacja danych pacjentów

Brak jednolitego systemu: pacjent jest „niewidoczny" w różnych placówkach, a informacje są rozproszone.

Niedobór personelu medycznego i przeciążenie lekarzy

Lekarze i pielęgniarki poświęcają zbyt wiele czasu na biurokrację i ręczną obsługę dokumentacji.

Zintegrowane systemy

Cyfrowe zarządzanie placówką medyczną.

Elektroniczna dokumentacja

Dane wrażliwe pacjentów w systemach EDM.

Sprzęt medyczny

Urządzenia podłączone do sieci wewnętrznej.

Usługi w chmurze

Zdalne przechowywanie i przetwarzanie danych medycznych.

Bariery systemowe

Braki strukturalne

Niedostateczna obsada działu IT. Brak wydzielonego zespołu bezpieczeństwa.

Niska świadomość

Niewystarczające zrozumienie zagrożeń wśród kierownictwa i personelu.

Ograniczenia budżetowe

Niedostateczne finansowanie obszaru cyberbezpieczeństwa.

Przestarzała infrastruktura

Systemy bez aktualizacji. Brak segmentacji sieci.

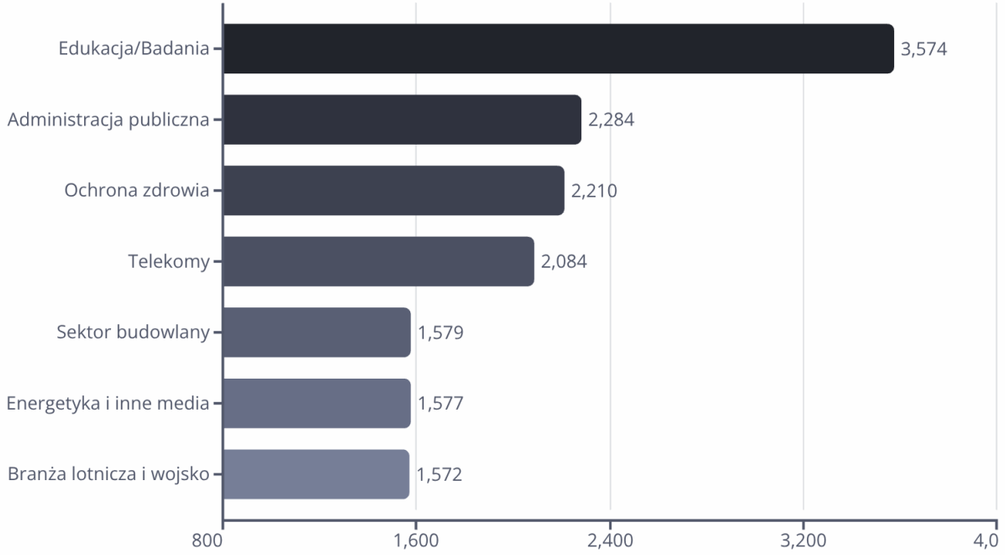
Ochrona zdrowia na tle innych atakowanych branż

NEWS

Healthcare ranks as third-most targeted ransomware victim

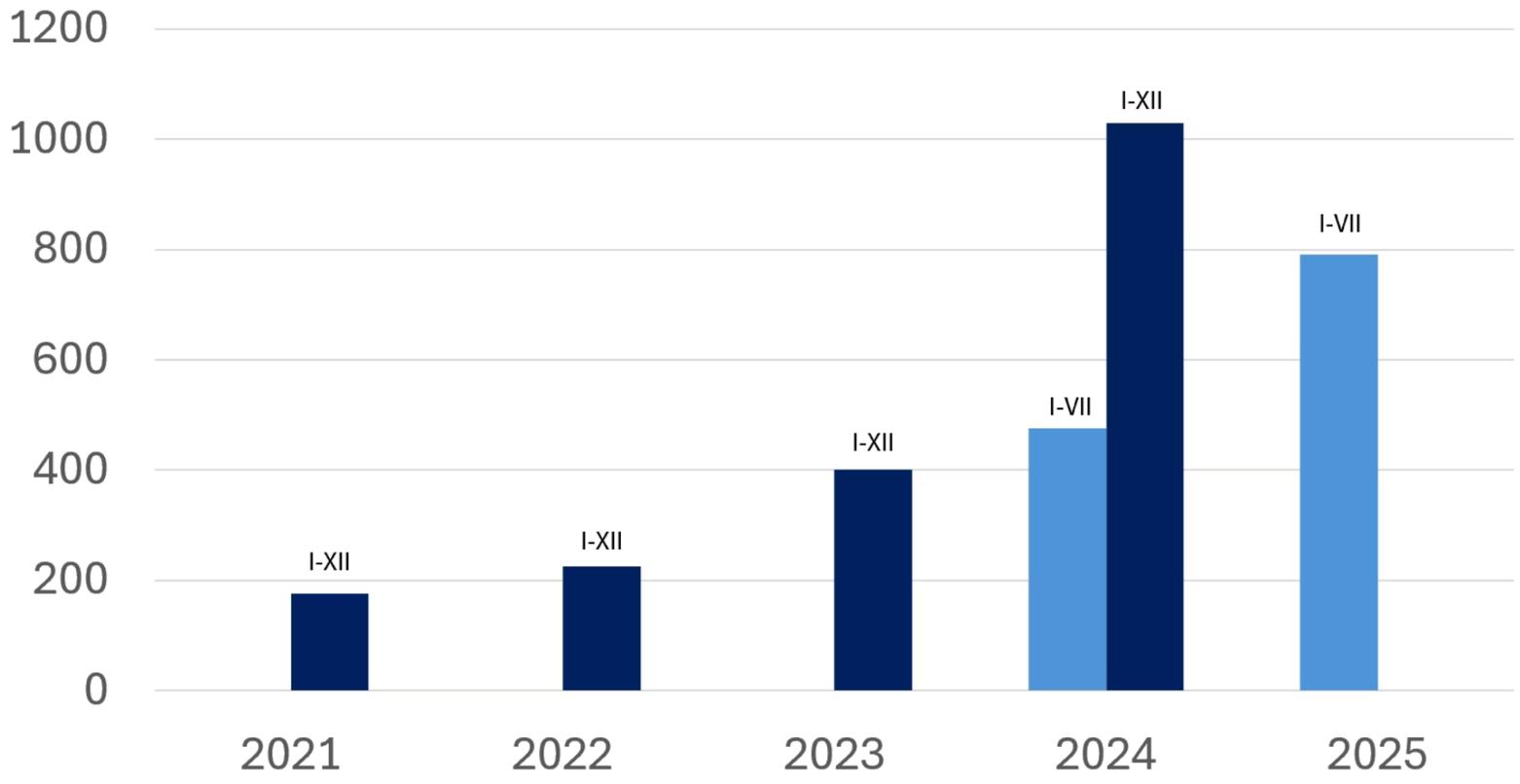
Research shows that healthcare is now the third-most targeted ransomware victim, and attacks against physician practices as well as hospitals are on the rise.

średnia tygodniowa liczba ataków na świecie



Źródło: CHECK POINT 2025

Wzrost liczby incydentów w latach 2021-2025 (do VII 2025)



Coraz więcej incydentów cyberbezpieczeństwa w ochronie zdrowia

Redaktor: Jacek Janik | Data: 04.02.2025 Źródło: Centrum e-Zdrowia Udostępnij:

Działy: Aktualności w Menedżer Zdrowia | Aktualności

Tagi: cyberbezpieczeństwo, CSIRT CeZ, zagrożenie, atak hakerski, Tomasz Jeruzalski

Zwiększa się liczba incydentów dotyczących cyberbezpieczeństwa w sektorze ochrony zdrowia. Dane medyczne są szczególnie wrażliwe, a zatem cenne. Dlatego tak ważne jest wdrażanie skutecznych mechanizmów zabezpieczeń.

Z opublikowanych przez Centrum e-Zdrowia danych wynika, że liczba ataków typu ransomware na placówki ochrony zdrowia na świecie wzrosła drastycznie – z 69 incydentów w 2020 r. do 506 w 2024 r. To ponad siedmiokrotny wzrost na przestrzeni zaledwie pięciu lat. Ta dynamika jest alarmująca, a same liczby pokazują, że cyberprzestępcy coraz częściej celują w systemy medyczne, wykorzystując ich wrażliwość i znaczenie dla społeczeństwa.

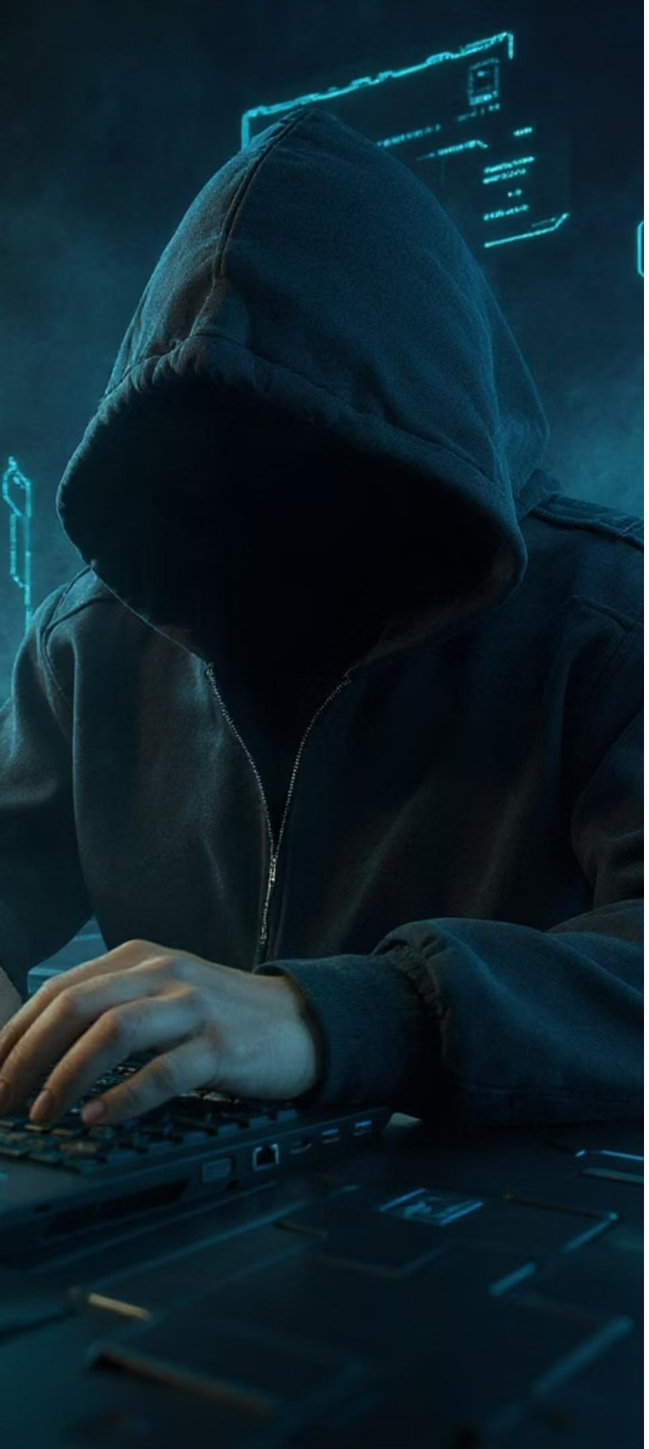
Serwisy Zdrowie

/ Zdrowie / OCHRONA ZDROWIA

Rośnie liczba incydentów cyberbezpieczeństwa w sektorze ochrony zdrowia

W 2024 roku odnotowano 1028 incydentów w ochronie zdrowia wobec 405 incydentów w 2023 roku – wynika z danych CSIRT CeZ.

Czas na poznanie adwersarza….
i sposób jego działania



Kto za tym stoi?

Grupy Ransomware

Motywacja: Finansowa

Przykłady: Conti, LockBit, BlackCat

Szyfrują dane szpitali, żądając okupu za ich odblokowanie. Często publikują skradzione dane pacjentów w przypadku odmowy zapłaty.

Hakerzy Oportunistyczni

Motywacja: Różna

Charakterystyka: Ataki przypadkowe

Wykorzystują słabe zabezpieczenia szpitali. Choć mniej zaawansowani, stanowią realne zagrożenie dla nieprzygotowanych placówek.

Grupy APT Państwowe

Motywacja: Polityczna i wywiadowcza

Przykłady: APT28 (Fancy Bear, RU), APT29 (Cozy Bear, RU), APT38 Lazarus (KPN), APT35 Charming Kitten, APT44, Sandworm (GRU, RU), IRAN, FIN11/UNC1878 (RU, BLR, UHS Universal Health Services, 2020)

zbierają dane medyczne na potrzeby wywiadu, destabilizują infrastrukturę krytyczną (APT44, sabotaż łańcuchów dostaw - UKR) lub testują możliwości cyberataków. Ransomware (UHS).

Zagrożenia cyberbezpieczeństwa w szpitalach

Ransomware

Blokowanie systemów i wymuszanie okupu. Paraliż działalności medycznej.

Phishing

Wyłudzanie danych uwierzytelniających od personelu medycznego.

Wycieki danych

Kradzież i ujawnienie wrażliwych informacji o pacjentach.

Ataki na urządzenia

Ingerencja w sprzęt medyczny podłączony do sieci.

WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE CULTURE REVIEWS NEWSLETTERS

WILLIAM RALSTON SECURITY NOV 11, 2020 7:30 AM

The untold story of a cyberattack, a hospital and a dying woman

German prosecutors tried to prove that a ransomware attack on a hospital was to blame for someone losing their life. Their story is a warning

All products featured on WIRED are independently selected by our editors. However, we may receive compensation from retailers and/or from purchases of products through these links. Learn more.

University Hospital Düsseldorf (UHD), 10.09.2020

Case Study: Kraków 2025
8.03.2025

W marcu 2025 roku Szpital MSWiA w Krakowie został dotknięty zmasowanym atakiem ransomware. Cyberprzestępcy zaszyfrowali kluczowe systemy informatyczne, odpowiedzialne za diagnostykę i zarządzanie danymi pacjentów (EDM).

- **Paraliż diagnostyki:** Brak dostępu do wyników badań, historii chorób i systemów laboratoryjnych.
- **Odwołane wizyty i operacje:** Wielu pacjentów musiało mieć przełożone terminy zabiegów i konsultacji, generując chaos i frustrację.
- **Zagrożenie dla pacjentów:** Opóźnienia w diagnozowaniu i leczeniu, potencjalnie wpływające na stan zdrowia i życie chorych.
- **Straty finansowe:** Wysokie koszty związane z odbudową systemów, utraconymi przychodami i potencjalnymi odszkodowaniami.

Obrona i odporność

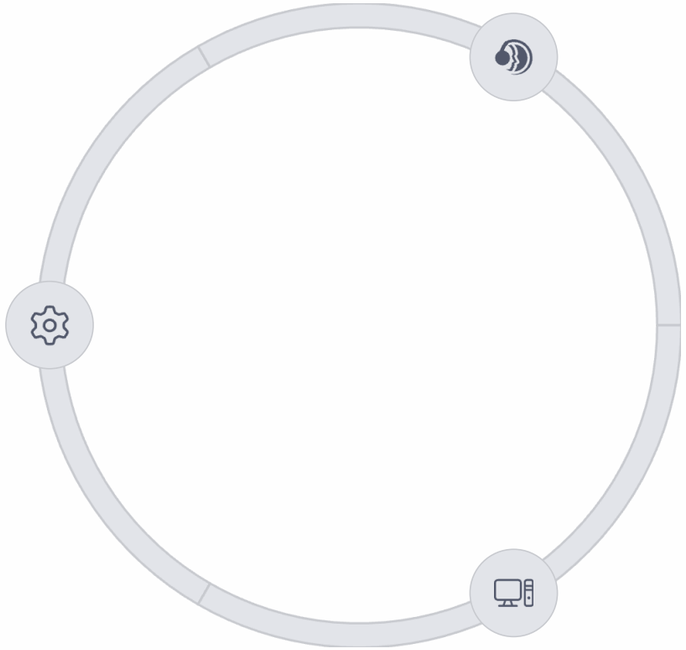
Kluczowe filary cyberodporności szpitala

Człowiek

Budowanie świadomości cyberbezpieczeństwa wśród personelu, regularne szkolenia, jasne przypisanie ról i odpowiedzialności oraz wspieranie proaktywnej kultury bezpieczeństwa w całej organizacji.

Procesy i Procedury

Ustanowienie i konsekwentne przestrzeganie jasnych zasad bezpieczeństwa, zarządzania ryzykiem, polityk dostępu oraz planów reagowania na incydenty. Zapewnienie ciągłości działania.



Technologia

Wdrożenie i utrzymanie zaawansowanych rozwiązań technologicznych, takich jak systemy detekcji zagrożeń, szyfrowanie danych, bezpieczne sieci i regularne aktualizacje oprogramowania.

Wyzwania Regulacyjne

Sektor ochrony zdrowia musi spełniać coraz więcej wymagań regulacyjnych w zakresie cyberbezpieczeństwa. **Dyrektywa NIS2** wymaga od szpitali wdrożenia odpowiednich środków bezpieczeństwa, a **ustawa o Krajowym Systemie Cyberbezpieczeństwa** nakłada obowiązki raportowania incydentów.

RODO

Ochrona danych osobowych pacjentów, kary do 20 mln euro

Dyrektywa NIS2

Wymogi cyberbezpieczeństwa dla podmiotów świadczących usługi medyczne

ISO 27001/27799

Standardy zarządzania bezpieczeństwem informacji w ochronie zdrowia

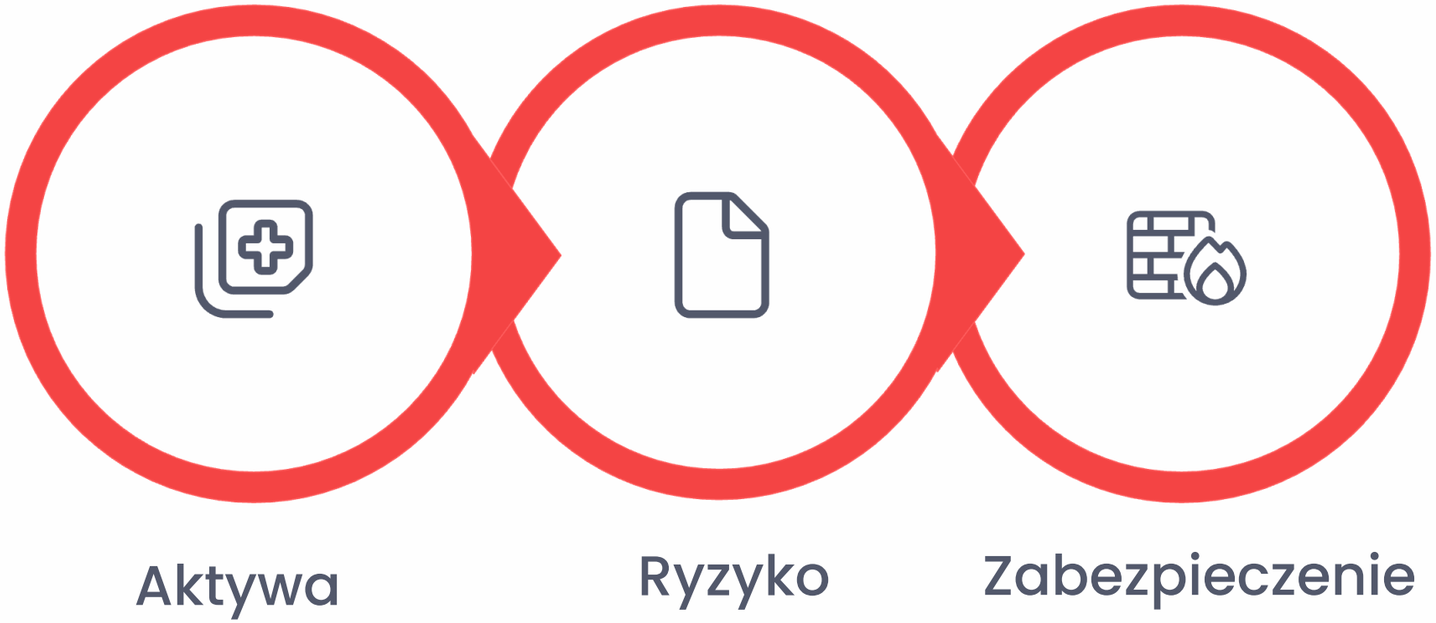
ISO 22301

Zarządzanie ciągłością działania w sytuacjach kryzysowych

Luka regulacyjna: Przepisy określają wymagania, ale nie gwarantują rzeczywistej gotowości kryzysowej szpitali.

Aktywo → Ryzyko → Zabezpieczenie

Aby skutecznie zarządzać cyberbezpieczeństwem w sektorze ochrony zdrowia, kluczowe jest zrozumienie związku między aktywami, ryzykiem i środkami ochronnymi.



Ten trzystopniowy model pomaga identyfikować, oceniać i wdrażać odpowiednie strategie obrony przed zagrożeniami, chroniąc najcenniejsze zasoby placówek medycznych.

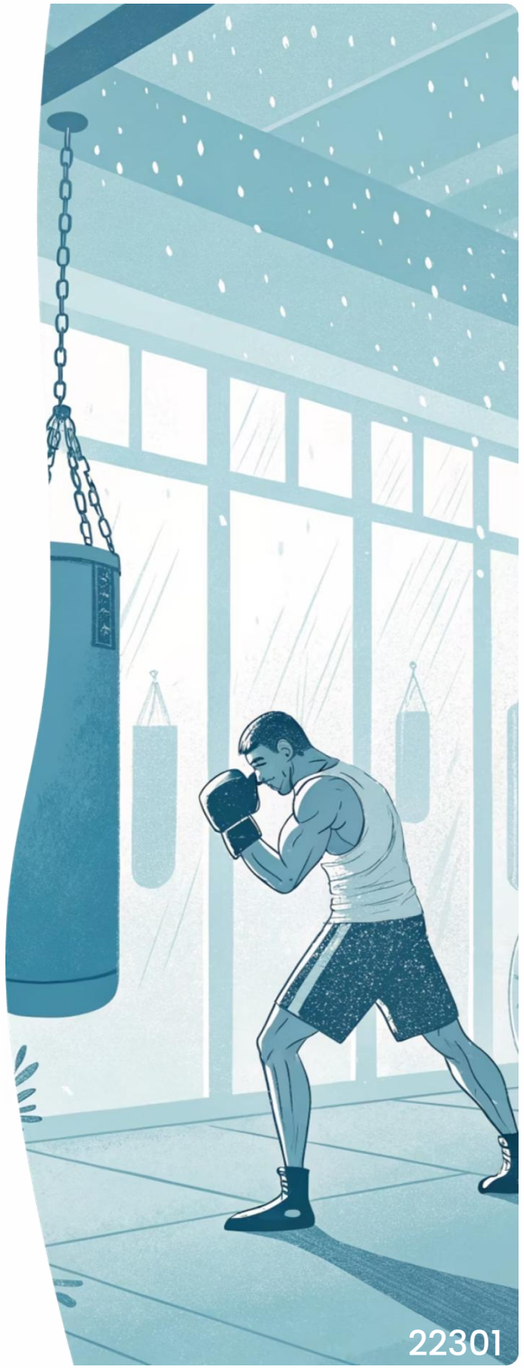
Cyberodporność ≠ Cyberbezpieczeństwo

Cyberbezpieczeństwo

- Ochrona przed atakiem
- Zapobieganie incydentom
- Blokowanie zagrożeń
- Koncentracja na prewencji

Cyberodporność

- Zdolność do przetrwania
- Szybka odbudowa po ataku
- Ciągłość świadczenia usług
- Adaptacja do nowych zagrożeń



Cyberbezpieczeństwo to **szczepionka** – chroni przed chorobą.
Cyberodporność to **odporność organizmu** – pozwala przetrwać atak i szybko powrócić do zdrowia.

Zasada 1.
Prewencja (Profilaktyka)

Podobnie jak w medycynie, **zapobieganie jest lepsze niż leczenie**. Filar prewencji koncentruje się na eliminowaniu podatności zanim staną się bramą dla cyberprzestępców.

Audyty Bezpieczeństwa

Regularne przeglądy infrastruktury IT i OT, identyfikacja słabych punktów w zabezpieczeniach systemów medycznych

Monitoring 24/7

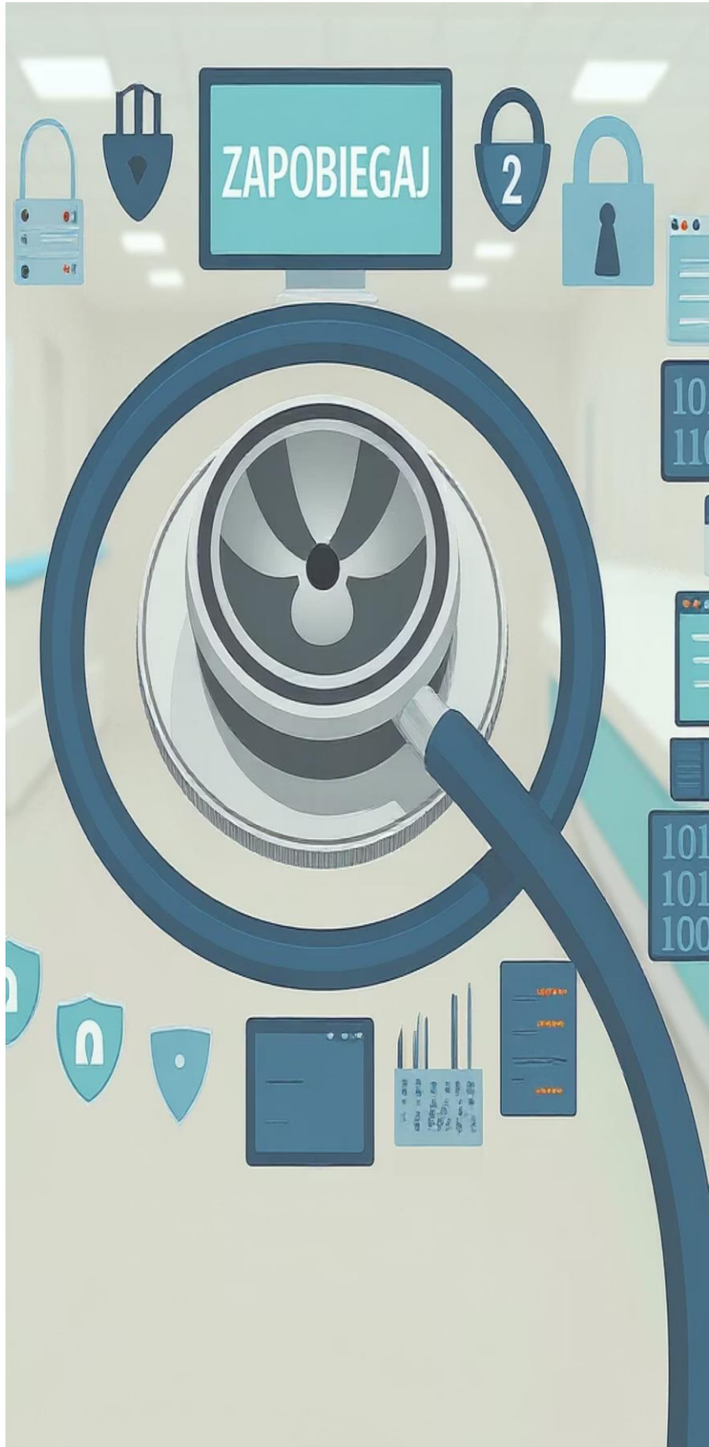
Ciągłe monitorowanie ruchu sieciowego, wykrywanie anomalii i podejrzanych aktywności w czasie rzeczywistym

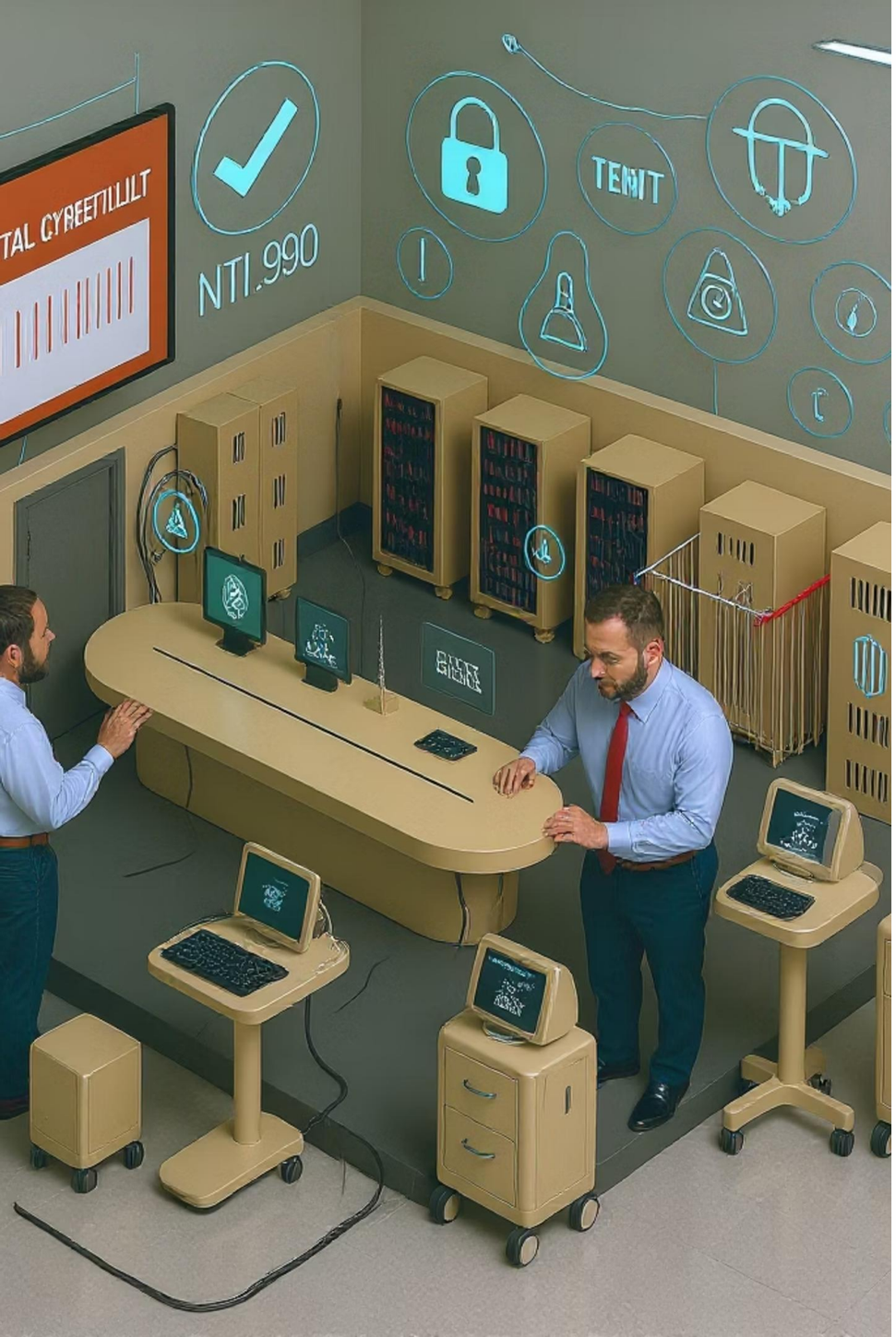
Zarządzanie Podatnościami

Systematyczne wyszukiwanie i łatanie luk bezpieczeństwa w systemach i oprogramowaniu medycznym

Segmentacja Sieci

Izolacja krytycznych systemów medycznych od sieci ogólnej, ograniczenie rozprzestrzeniania się ataków





Rekomendacje dla Praktyków

1 Audyt i Test Systemów Backup

Przeprowadzaj kwartalną weryfikację kopii zapasowych i testuj procedury odtwarzania danych. Upewnij się, że backup'y są odizolowane od sieci produkcyjnej i chronione przed ransomware.

2 Szkolenia Personelu

Organizuj regularne szkolenia z cyberbezpieczeństwa dla personelu medycznego i administracyjnego. Koncentruj się na rozpoznawaniu phishingu i bezpiecznym korzystaniu z systemów medycznych.

3 Cyber w Strategii Ryzyka Klinicznego

Włącz cyberbezpieczeństwo do systemu zarządzania ryzykiem klinicznym. Cyberincydenty to nie tylko problem IT – to bezpośrednie zagrożenie dla bezpieczeństwa pacjentów.

Pamiętaj: Każda złotówka wydana na prewencję to oszczędność dziesiątek tysięcy w przypadku ataku.

Zasada 2.
Reakcja (SOR Cybernetyczny)

Gdy atak już się wydarzy, liczy się każda minuta – podobnie jak w szpitalnym SOR. **Szybka i skoordynowana reakcja** może zadecydować o tym, czy incydent będzie niewielkim zakłóceniem, czy katastrofą dla pacjentów.

Plan Reagowania na Incydenty

- Procedury eskalacji i powiadamiania
- Role i odpowiedzialności zespołu kryzysowego
- Protokoły izolacji zainfekowanych systemów
- Procedury przełączania na systemy zapasowe

Komunikacja Kryzysowa

- Informowanie personelu medycznego
- Komunikacja z pacjentami i ich rodzinami
- Współpraca z organami ścigania
- Kontakt z mediami i opinią publiczną

Kluczowe: Zespół kryzysowy musi być dostępny 24/7 i regularnie ćwiczyć procedury reagowania.

Zasada 3.
Odbudowa (Rehabilitacja Cyfrowa)

Po przejściu przez kryzys następuje faza odbudowy – **cyfrowa rehabilitacja szpitala**.
To nie tylko przywrócenie systemów, ale także wzmocnienie odporności na przyszłe ataki.

Backupy i Odtwarzanie

Regularne kopie zapasowe krytycznych danych
oraz testowanie procedur odtwarzania systemów

Business Continuity Plan

Plan ciągłości działania zapewniający kontynuację krytycznych procesów medycznych

Lessons Learned

Analiza incydentu, identyfikacja obszarów do poprawy i aktualizacja procedur bezpieczeństwa

Efektywna rehabilitacja oznacza nie tylko powrót do normalności, ale wzmocnienie całego systemu bezpieczeństwa szpitala.

Przywództwo

„Ludźmi nie należy zarządzać.
Zadaniem jest przewodzenie ludziom.
A celem jest czerpanie wydajności z wiedzy i silnych stron każdego pracownika.”

Peter F. Drucker

Rola CISO/lidera cyberbezpieczeństwa

Przed incydentem
- Budowanie strategii ochrony
- Tworzenie procedur
- Szkolenia personelu

W trakcie **incydentu**
- Koordynacja zespołu
- Komunikacja kryzysowa
- Podejmowanie decyzji

Po **incydencie**
- Analiza zagrożenia
- Raportowanie
- Wdrażanie usprawnień

Przywództwo pod presją

Wyzwania decyzyjne

- Ograniczone dane
- Wysoki poziom stresu
- Presja czasu
- Chaos organizacyjny

Przejawy skutecznego przywództwa

- Opanowanie i stanowczość
- Jasna komunikacja
- Elastyczne reagowanie
- Zdolność priorytetyzacji

Studium wykazało, że odporność psychiczna lidera bezpośrednio wpływa na morale zespołu.
Umiejętność podejmowania decyzji mimo niepełnych informacji okazała się kluczowa.

> "...ucisk wyrabia wytrwałość, a wytrwałość – wypróbowaną cnotę, wypróbowana zaś cnota – nadzieję..."
> (Rz 5, 1-5)

Rekomendacje dla Regulatora i praktyki

Formalizacja roli CISO

Umocowanie funkcji w strukturze organizacyjnej z jasnymi uprawnieniami decyzyjnymi.

Regularne ćwiczenia

Symulacje incydentów dla zespołów technicznych i kierownictwa.

Budżet dedykowany

Zapewnienie stabilnego finansowania działań z zakresu cyberbezpieczeństwa.

Edukacja zarządu

Uświadamianie najwyższego kierownictwa w zakresie zagrożeń cybernetycznych.

Propozycja modeli zespołu cyberbezpieczeństwa

Model hybrydowy dla małych placówek

- Wyznaczony koordynator bezpieczeństwa
- Outsourcing monitoringu
- Zewnętrzny zespół reagowania

Model podstawowy dla średnich placówek

- Dedykowany CISO
- 2-3 specjalistów wewnętrznych
- Wsparcie zewnętrzne w sytuacjach kryzysowych

Model rozbudowany dla dużych placówek

- CISO raportujący bezpośrednio do zarządu
- Zespół SOC (5+ osób)
- Wewnętrzny zespół reagowania

arcus

Podsumowanie

Cyberodporność = Bezpieczeństwo Pacjentów

W dzisiejszym świecie **cyberodporność szpitala to nie opcja, lecz konieczność**.
Każdy dzień zwłoki w budowaniu odporności cyfrowej to zwiększone ryzyko dla życia i zdrowia pacjentów.

Trzy filary cyberodporności:

Prewencja – jak profilaktyka w medycynie

Reakcja – jak SOR w sytuacji kryzysowej

Odbudowa – jak rehabilitacja po chorobie

Budowanie cyberodpornego szpitala to inwestycja w bezpieczeństwo pacjentów, ciągłość opieki medycznej i przyszłość ochrony zdrowia w erze cyfrowej.

arcus

"Nie pytaj, czy zostaniesz zaatakowany.
Zapytaj, jak szybko wrócisz do pracy."

Hospital 360. Scientific & Practical Conference

KONKURS
#belegit
with IT AUDIT & ARCUS