małopolskie parki zdrowia Sp. z o.o.

Raport o zagrożeniach cybernetycznych w sektorze zdrowia

Analiza IV kwartału i podsumowanie 2025 roku

Kraków, 27.01.2026 r.

Spis treści

Źródła: Raporty CSIRT CeZ, CERT Polska i UODO; ENISA Threat Landscape 2025; Dane Centrum e-Zdrowia za 2025; HIPAA Journal & HHS OCR (USA, statystyki incydentów); Raporty IBM Security (Cost of a Data Breach 2025); Verizon DBIR 2025; Materiały Komisji Europejskiej dot. planu cyberbezpieczeństwa sektora zdrowia; Artykuły branżowe (CyberDefence24, Rynek Zdrowia, etc.) za IV kw. 2025.

Globalny i europejski krajobraz zagrożeń – IV kw. 2025

W czwartym kwartale 2025 roku sektor ochrony zdrowia pozostał jednym z głównych celów cyberataków na świecie. **Atakujący nadal intensywnie wykorzystywali oprogramowanie ransomware oraz kradzież danych (tzw. *data theft extortion*) jako dominujące formy działań**.

W skali globalnej nie odnotowano wyraźnego spadku liczby poważnych incydentów – miesięcznie rejestrowano średnio kilkadziesiąt istotnych naruszeń, choć w końcowych miesiącach roku pojawiła się lekka tendencja spadkowa w niektórych regionach (np. zmniejszenie liczby dużych wycieków danych w USA).

Sektor zdrowia pozostał najbardziej narażoną gałęzią gospodarki cyfrowej pod względem kosztów incydentów – średni koszt naruszenia danych medycznych w 2025 r. szacowano na ok. 7,4 mln USD, najwyżej spośród wszystkich branż. Równocześnie **zmieniła się taktyka cyberprzestępców**: zamiast rzadkich, bardzo dużych ataków z wysokimi żądaniami okupu, coraz częściej stosowali oni podejście masowe – liczne ataki na mniejsze podmioty, z niższymi żądaniami finansowymi (średnio ok. 300 tys. USD, a zapłacone ok. 150 tys. USD) w celu maksymalizacji zasięgu przy mniejszym ryzyku wykrycia.

W Europie sytuacja odzwierciedlała globalne trendy. **Służba zdrowia pozostawała najczęściej atakowanym sektorem spośród wszystkich gałęzi infrastruktury krytycznej w Unii Europejskiej**.

Według analiz Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) ponad połowa incydentów w europejskich placówkach medycznych w 2025 r. była związana z ransomware, a znaczącą część pozostałych stanowiły włamania skutkujące wyciekiem danych (ok. 28%) oraz kampanie phishingowe. Europejskie szpitale i przychodnie były celem zarówno zorganizowanych grup cyberprzestępczych działających dla zysku, jak i sponsorowanych przez państwa grup APT, prowadzących cyberoperacje szpiegowskie i sabotażowe.

Najsilniejszą presję odnotowano w krajach na wschodniej flance UE (m.in. w Polsce i państwach bałtyckich), co wiązano bezpośrednio z trwającym konfliktem za wschodnią granicą i wrogimi kampaniami w ramach wojny hybrydowej.

Jednocześnie instytucje UE podejmowały działania zaradcze – wdrażano program **Action Plan on Hospital Cybersecurity** finansujący poprawę zabezpieczeń w służbie zdrowia, a sektor ochrony zdrowia objęto nowymi regulacjami (dyrektywa NIS2, akty prawne dot. odporności cyfrowej i wyrobów medycznych).

Pod koniec roku **Europa odnotowała wzrost poziomu świadomości zagrożeń oraz skuteczne operacje organów ścigania** wymierzone w cyberprzestępców (m.in. koordynowane przez Europol akcje przeciwko infrastrukturze *cybercrime-as-a-service* i aresztowania członków grup ransomware).

Pomimo tych postępów utrzymywały się istotne wyzwania, takie jak **niedobór specjalistów ds. cyberbezpieczeństwa w ochronie zdrowia oraz podatność tysięcy urządzeń medycznych IoT na ataki**.

Sytuacja w Polsce – IV kwartał 2025

Polski sektor ochrony zdrowia w IV kwartale 2025 r. doświadczył dalszej eskalacji zagrożeń, stając się jednym z głównych frontów cyberwojny hybrydowej. Według szacunków Ministerstwa Cyfryzacji i Agencji Bezpieczeństwa Wewnętrznego, infrastruktura krytyczna kraju – w tym system opieki zdrowotnej – była codziennie narażona na **20–50 prób cyberataków pochodzących od grup powiązanych z Federacją Rosyjską**.

Punktem kulminacyjnym wrogich działań był **10 września 2025 r.**, kiedy równolegle z incydentem fizycznym (wykryciem dronów rozpoznawczych nad terytorium RP) odparto największą od 2022 roku falę skoordynowanych cyberataków na polskie sieci. Kampania ta dotknęła wiele sektorów, w tym liczne jednostki ochrony zdrowia. Dzięki współdziałaniu zespołów reagujących (CERT Polska, CSIRT MON, CSIRT CeZ i innych służb) udało się zapobiec trwałym szkodom. **Ataki przyjmowały różnorodne formy** – od masowych kampanii phishingowych wymierzonych w personel medyczny, po próby uzyskania nieautoryzowanego dostępu do systemów szpitalnych (skanowanie portów, ataki słownikowe na hasła, wykorzystanie znanych podatności).

Źródła rządowe potwierdziły, że w 2025 r. **rosyjski wywiad potroił zasoby dedykowane cyberoperacjom przeciwko Polsce**, uznając sektor zdrowia za „punkt wrażliwy" o wysokim potencjale destabilizacji.

Na tle tych zagrożeń liczba incydentów odnotowanych w polskiej służbie zdrowia rosła bardzo dynamicznie. Do końca sierpnia 2025 r. **zgłoszono 946 incydentów cyberbezpieczeństwa w podmiotach medycznych**, niemal tyle co w całym poprzednim roku (w 2024 r. – 1028). **Prognozowano, że cały 2025 rok mógł zamknąć się liczbą ponad 1300 zgłoszeń**, co oznacza prawie **trzykrotny wzrost w ciągu zaledwie dwóch lat** (dla porównania: w 2023 r. – 405 incydentów, w 2022 r. – 251, w 2021 r. – 150).

Incydenty rejestrowane w IV kwartale 2025 r. obejmowały liczne przypadki naruszeń bezpieczeństwa o różnej skali. Nie doszło wprawdzie do zdarzenia tak poważnego jak w marcu 2025 r. (atak ransomware na Szpital MSWiA w Krakowie, który czasowo sparaliżował pracę placówki), jednak **regularnie raportowano pomniejsze incydenty**.

W październiku CSIRT CeZ ostrzegł przed nasileniem **kampanii phishingowych wymierzonych w użytkowników systemu e-zdrowia (Internetowe Konto Pacjenta)** – atakujący rozsyłali fałszywe e-maile o rzekomych zaległościach finansowych, próbując wyłudzić dane logowania.

W listopadzie odnotowano kilka prób **infekcji ransomware** w mniejszych placówkach (m.in. w jednym z powiatowych ZOZ-ów na Mazowszu); dzięki sprawnym zabezpieczeniom i kopiom zapasowym udało się jednak uniknąć zaszyfrowania danych i przerw w działalności.

Zwracały uwagę incydenty naruszenia ochrony danych osobowych – przykładowo w grudniu Urząd Ochrony Danych Osobowych (UODO) poinformował o wycieku danych pacjentek warszawskiej poradni leczenia niepłodności, w wyniku którego dane wrażliwe dostały się w niepowołane ręce. UODO nałożył na placówkę karę **40 tys. zł** za uchybienia w zabezpieczeniach. W analizowanym okresie ogłoszono również decyzje o sankcjach za wcześniejsze incydenty: **Uniwersytecki Szpital Dziecięcy w Białymstoku ukarano kwotą 66 500 zł** za niewystarczające zabezpieczenia techniczne, które umożliwiły zaszyfrowanie danych ok. 2000 pracowników, zaś **Szpital we Wrześni – 29 648 zł** za niezgłoszenie do UODO incydentu błędnego wydania dokumentacji medycznej. Te przypadki stanowią ważny sygnał dla całego sektora – **nawet jednostkowe naruszenia mogą skutkować dotkliwymi sankcjami**, jeśli procedury ochrony danych nie są prawidłowo wdrożone.

Ocena stanu zabezpieczeń polskich placówek medycznych w IV kwartale 2025 r. wykazała utrzymujące się braki i luki w odporności systemów. Audyty prowadzone przez CSIRT CeZ potwierdziły, że ok. **60% placówek nie prowadzi regularnego monitoringu podatności**, a **40% nie testuje posiadanych kopii zapasowych ani procedur ich odtwarzania**. Nadal około **10% jednostek nie wdrożyło podstawowych mechanizmów ochronnych**, takich jak zapory sieciowe (firewalle), oprogramowanie antywirusowe czy systemy wykrywania i reagowania na ataki (EDR/XDR). Stosowanie **wieloskładnikowego uwierzytelniania (MFA)** pozostaje ograniczone głównie do poczty elektronicznej, co zwiększa ryzyko powodzenia phishingu i przejęcia kont użytkowników. **Audyty przeprowadzone w IV kwartale 2025 r. ujawniły m.in. przypadki korzystania z przestarzałych systemów (np. obecność Windows 7/XP), stosowanie domyślnych haseł administracyjnych oraz brak segmentacji sieci (brak oddzielenia sieci medycznej od biurowej)**. Zespoły audytowe wydały rekomendacje naprawcze – w tym pilne wdrożenie procesów zarządzania aktualizacjami (łatkami bezpieczeństwa), segmentację sieci oraz szkolenia personelu z rozpoznawania ataków socjotechnicznych.

Pozytywnym sygnałem w Polsce była rosnąca aktywność zespołu CSIRT CeZ na polu prewencji i budowania świadomości. **W 2025 roku przeszkolono ponad 1700 pracowników ochrony zdrowia** w zakresie cyberbezpieczeństwa, uruchomiono też pilotażową platformę e-learningową dla personelu medycznego. Kontynuowano coroczną **ankietę samooceny cyberbezpieczeństwa szpitali**, pozwalającą placówkom porównać swój poziom zabezpieczeń z innymi. W ramach działań proaktywnych CSIRT CeZ zidentyfikował również ponad **120 podatności** w systemach szpitalnych, zanim zostały one wykorzystane przez cyberprzestępców – co pozwoliło na ich załatanie i zapobiegło potencjalnym incydentom.

Władze publiczne w IV kwartale 2025 r. podejmowały intensywne działania na rzecz wzmocnienia cyberbezpieczeństwa sektora zdrowia. 22 października Rada Ministrów przyjęła projekt nowelizacji ustawy o

krajowym systemie cyberbezpieczeństwa dostosowującej polskie przepisy do dyrektywy NIS2. Nowe regulacje **rozszerzają obowiązki systemu cyberbezpieczeństwa na sektor ochrony zdrowia** – szpitale zostaną formalnie uznane za operatorów usług kluczowych i będą musiały spełniać zaostrzone wymogi (posiadanie polityk bezpieczeństwa, procedur zgłaszania incydentów, systemów monitorowania itd.). Nowelizacja przewiduje także możliwość tworzenia sektorowych zespołów CSIRT (w tym dla zdrowia) oraz przyznaje Ministrowi Cyfryzacji i organom nadzorczym nowe uprawnienia kontrolne (np. prawo wydawania wiążących zaleceń i poleceń zabezpieczenia).

W budżecie państwa na 2026 r. zagwarantowano dodatkowe fundusze na dofinansowanie projektów poprawy cyberbezpieczeństwa w szpitalach powiatowych – m.in. modernizację systemów kopii zapasowych i zabezpieczenie infrastruktury energetycznej na potrzeby podtrzymania działania systemów IT. Kontynuowano również ścisłą **współpracę międzyresortową przy reagowaniu na poważne incydenty** – każdy przypadek o dużej skali (jak wspomniany atak na Szpital MSWiA) skutkował powołaniem zespołu interdyscyplinarnego z udziałem ekspertów CSIRT CeZ, policji oraz przedstawicieli Ministerstw Zdrowia i Cyfryzacji. W sferze edukacyjnej władze prowadziły kampanie informacyjne skierowane do pacjentów, promując **bezpieczne korzystanie z e-usług zdrowotnych** (m.in. ochronę konta IKP i danych e-recept).

Podsumowując, Polska zakończyła rok 2025 z rekordową liczbą incydentów i wciąż niepełną implementacją nowych regulacji, lecz jednocześnie z rosnącą świadomością zagrożeń oraz lepszą koordynacją działań obronnych. Sektor ochrony zdrowia wykazał zauważalną poprawę w zakresie procedur awaryjnych i wymiany informacji o zagrożeniach – współpraca między podmiotami krajowymi (w tym CSIRT-ami) stanowi solidny fundament do dalszego wzmacniania odporności cyfrowej w nadchodzącym okresie.

Profil zagrożeń – Polska vs Świat[1]

Obszar porównania	Profil światowy / UE (kontekst)	Profil krajowy (Polska)
Poziom aktywności incydentów	W 2025 r. utrzymuje się wysoka liczba naruszeń danych medycznych; w USA (probierz trendów globalnych) do **20.09.2025 zgłoszono 508** poważnych naruszeń wobec **739** w całym 2024 r., co odpowiada ok. **63 incydentom miesięcznie**. Końcówka roku przyniosła sygnały niewielkiej poprawy (m.in. niższa liczba zgłoszeń w wybranych miesiącach).	Skokowy wzrost skali zgłoszeń: do końca sierpnia 2025 r. zgłoszono **946 incydentów** w podmiotach medycznych (prawie tyle, co w całym 2024 r. – **1028**). Raport wskazuje, że 2025 r. mógł zamknąć się poziomem >1300–1500 zgłoszeń (szacunki).
Skala skutków dla pacjentów / rekordów danych	Łączna liczba pacjentów dotkniętych wyciekami od początku 2025 r. do 30.09 przekroczyła **43 mln** (USA jako probierz).	Oprócz „twardych" incydentów bezpieczeństwa raport podkreśla wagę **naruszeń ochrony danych** oraz ryzyk procesowych (błędy w przetwarzaniu dokumentacji). W 2025 r. UODO nakładał kary m.in. **40 tys. zł**, **66 500 zł**, **29 648 zł** (przykłady opisane w raporcie).

[1] Profil zagrożeń należy czytać jako **opis środowiska operacyjnego** (kto atakuje, dlaczego, jakimi metodami i jak często), a nie jako ocenę ryzyka konkretnej organizacji. Zestawienie światowe/UE pełni rolę **tła porównawczego** – pozwala zrozumieć, które zjawiska są trendem globalnym (np. ewolucja ransomware w kierunku wymuszeń opartych o kradzież danych, wzrost jakości phishingu wspomaganego AI), a które są **wzmocnione lokalnie** przez uwarunkowania krajowe. Część krajowa profilu jest kluczowa, ponieważ wskazuje **dominujące wektory w Polsce** (np. phishing/socjotechnika, wykorzystanie podatności, malware) oraz czynniki zwiększające presję (np. kontekst wojny hybrydowej).

Z analizy profilu zagrożeń można wyciągnąć wniosek, że priorytetem dla ochrony zdrowia jest **ograniczanie skuteczności najczęstszych i najtańszych dla napastnika metod wejścia** (socjotechnika + podatności), zanim dojdzie do eskalacji do ransomware lub kradzieży danych. W praktyce profil zagrożeń powinien prowadzić do sformułowania krótkiej listy „Top zagrożeń" oraz **wskaźników ostrzegawczych**, które organizacja monitoruje (np. wzrost kampanii phishingowych, wzrost aktywności skanowania usług, incydenty w łańcuchu dostaw).

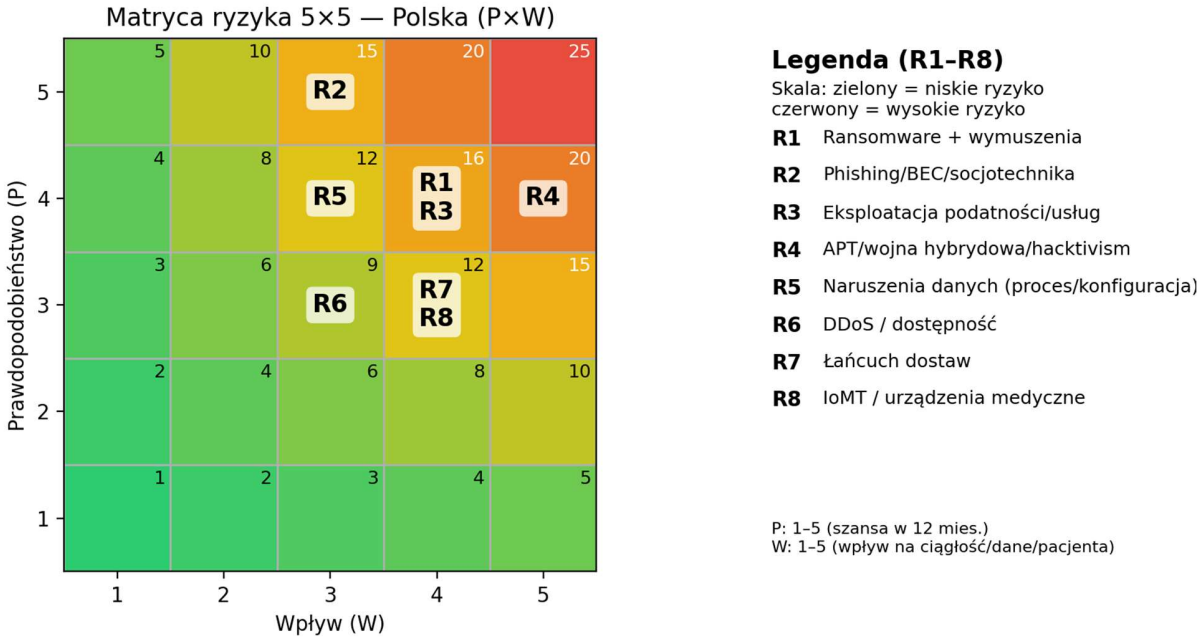
Dominujące typy ataków	Ransomware pozostaje głównym zagrożeniem; w Europie ok. **54%** ataków na sektor zdrowia stanowi ransomware, a w pozostałych przypadkach znaczący udział mają włamania skutkujące wyciekiem danych (ok. **28%**) oraz phishing/malware.	Polska doświadcza podobnego zestawu zagrożeń, przy silnym „dociążeniu" geopolitycznym (wojna hybrydowa). W IV kwartale 2025 r. nie odnotowano incydentu o skali porównywalnej z atakiem ransomware na Szpital MSWiA (marzec 2025), ale występowały liczne mniejsze zdarzenia (phishing, próby infekcji ransomware).
Ewolucja taktyk ransomware	Wyraźny trend ku „data theft extortion": w ochronie zdrowia tylko ok. **34%** przypadków ransomware skutkuje szyfrowaniem, natomiast ok. **96%** obejmuje kradzież danych (presja szantażem publikacyjnym).	Krajowo obserwowane są zarówno próby infekcji ransomware, jak i kampanie phishingowe nakierowane na przejęcia kont oraz dostęp do systemów e-zdrowia. CSIRT CeZ wskazywał m.in. na kampanie podszywające się pod komunikację dotyczącą P1/IKP.
Najczęstsze wektory wejścia	W skali globalnej istotny udział mają: (1) **podatności oprogramowania** (ok. **33%** incydentów) oraz (2) **phishing i socjotechnika** (ok. **42%** zdarzeń).	W Polsce (do sierpnia 2025): **phishing/socjotechnika – 311 przypadków**, **luki/podatne usługi – 238**, **malware (w tym ransomware) – 90**.
AI jako katalizator zagrożeń	Raport wskazuje, że w 2025 r. „co szósty" incydent naruszenia danych wiązał się z użyciem AI przez napastników; jednocześnie ok. **82% phishingu** ma zawartość częściowo generowaną przez AI (industrializacja socjotechniki).	W Polsce AI jest istotna przede wszystkim jako „wzmacniacz" phishingu i podszyć (większa wiarygodność i skala kampanii). Priorytetem operacyjnym pozostaje redukcja skuteczności socjotechniki (MFA, szkolenia, symulacje). Raport wskazuje m.in., że czynnik ludzki to istotny komponent incydentów (ok. 1/3 zdarzeń – błędy użytkowników i socjotechnika).
Koszty i czas obsługi incydentu	Średni globalny koszt naruszenia w ochronie zdrowia w 2025 r.: **7,42 mln USD**; średni czas identyfikacji i powstrzymania: **241 dni** (spadek o 17 dni r/r).	W Polsce koszty nie są w raporcie zestandaryzowane jedną miarą, ale rośnie „koszt ryzyka" poprzez skalę incydentów, presję geopolityczną oraz konsekwencje regulacyjne (UODO).
Czynniki geopolityczne / presja ataków	Najintensywniejsze ataki w UE obserwowano m.in. na wschodniej flance (w tym w Polsce i krajach bałtyckich), co raport wiąże z kontekstem wojny hybrydowej.	Według szacunków MC i ABW infrastruktura krytyczna (w tym zdrowie) była codziennie narażona na **20–50 prób cyberataków** od grup powiązanych z FR. Raport wskazuje również na istotną falę skoordynowanych ataków 10.09.2025 r. obejmującą sektor zdrowia.
Dojrzałość zabezpieczeń / słabości	W ujęciu UE podkreślana jest potrzeba systemowego wsparcia, szkolenia i koordynacji; raport wskazuje na działania ENISA (m.in. ćwiczenia Cyber Europe 2025 i intensyfikacja szkoleń).	Audyty CSIRT CeZ: **60%** placówek bez regularnego monitoringu podatności, **40%** bez testów odtwarzania backupów; ok. **10%** bez podstawowych narzędzi ochrony (firewall/AV/EDR/XDR), MFA wdrażane wybiórczo. W Q4 wskazano też m.in. obecność Windows 7/XP, hasła domyślne i brak segmentacji sieci.
Odpowiedź instytucjonalna / regulacje	UE: działania systemowe (Action Plan on Hospital Cybersecurity) oraz regulacje i instrumenty (NIS2, CRA, EHDS) oraz wsparcie ćwiczeń i koordynacji.	Polska: w 2025 r. wzmożono działania CeZ/CSIRT CeZ (m.in. szkolenia, e-learning, ankieta samooceny; identyfikacja >120 podatności) oraz przyjęto 22.10 projekt nowelizacji KSC pod NIS2 (z obowiązkami dla sektora zdrowia).

Profil ryzyka – Polska vs Świat[2]

Kategoria ryzyka	Świat			Polska			Uzasadnienie (odniesienie do raportu)
	P	W	R	P	W	R	
Ransomware + wymuszenia	5	4	20	4	4	16	Ransomware dominuje w atakach (UE ~54%); trend „data theft extortion" (34% szyfrowanie vs 96% kradzież danych).
Phishing/BEC/socjotechnika	5	3	15	5	3	15	Phishing stanowi istotną część incydentów; AI zwiększa skuteczność (82% phishingu z treściami AI). W PL: 311 przypadków do VIII 2025; kampanie na P1/IKP w Q4.
Eksploatacja podatności / ekspozycja usług	4	4	16	4	4	16	Globalnie podatności stanowią znaczący wektor (ok. 33% incydentów). W PL: 238 przypadków; dodatkowo audyty wskazują braki (patching, segmentacja, systemy legacy).
APT / wojna hybrydowa / hacktivism	3	5	15	4	5	20	W UE nasilone ataki na wschodniej flance; w PL stała presja (20–50 prób dziennie) i incydenty skoordynowane (10.09.2025).
Błędy procesowe/konfiguracji i naruszenia RODO	4	3	12	4	3	12	W PL widoczne konsekwencje regulacyjne (kary UODO) oraz znaczenie błędów użytkowników/socjotechniki jako źródła incydentów.
DDoS / ataki na dostępność	3	3	9	3	3	9	Raport wskazuje na występowanie ataków DDoS m.in. w kontekście europejskim (systemy rejestracji, platformy).
Łańcuch dostaw	3	4	12	3	4	12	W raporcie podkreślono długotrwałe skutki ataków na dostawców (przykłady i wnioski operacyjne).
IoMT / urządzenia medyczne i sieci kliniczne	2	4	8	3	4	12	W PL audyty: systemy legacy (Windows 7/XP), brak segmentacji, domyślne hasła – zwiększa to ryzyko incydentów w środowiskach klinicznych. W UE wskazywana potrzeba wzmocnienia ochrony tysięcy urządzeń IoT/IoMT.

[2] Profil ryzyka (matryca P×W) należy czytać jako **narzędzie priorytetyzacji**: łączy on prawdopodobieństwo wystąpienia danego zdarzenia (P) z jego wpływem na ciągłość działania, bezpieczeństwo pacjentów i dane (W). Położenie kategorii w macierzy pokazuje, które ryzyka wymagają **działań natychmiastowych** (wysokie P i wysokie W – strefa najwyższego priorytetu), a które mogą być zarządzane planowo, w cyklu doskonalenia.

Wnioskiem z profilu ryzyka jest to, że zasoby (czas, budżet, kompetencje) należy kierować w pierwszej kolejności na obszary „wysokie–krytyczne", czyli tam, gdzie **częstotliwość i skutki nakładają się na siebie** (typowo: ransomware/wymuszenia, phishing/BEC, eksploatacja podatności, presja APT/geopolityczna). Ryzyka „średnie" (np. naruszenia procesowe/RODO, łańcuch dostaw, IoMT) również wymagają działań, ale zwykle w formie **kontroli systemowych** (procedury, standardy, audyty dostawców, segmentacja, polityki dostępu), a nie doraźnej reakcji. Matryca ryzyka powinna być traktowana jako element zarządczy: uzasadnia „dlaczego" dana inwestycja jest priorytetem, oraz stanowi punkt odniesienia do **mierzenia postępu** (np. po wdrożeniu MFA i programu testów backupów dążymy do obniżenia P dla określonych ryzyk w kolejnych kwartałach).



Podsumowanie roku 2025 – kluczowe trendy i wnioski

Liczba zgłoszonych incydentów cyberbezpieczeństwa w polskim sektorze zdrowia od 2021 r. narasta lawinowo, osiągając szacunkowo ponad 1300 przypadków w 2025 roku. **Rok 2025 potwierdził utrzymanie się i eskalację negatywnych trendów z lat poprzednich w obszarze cyberzagrożeń dla ochrony zdrowia.** Globalnie, liczba naruszeń danych medycznych i ataków na systemy opieki zdrowotnej pozostawała na bardzo wysokim poziomie. W samym tylko 2024 roku wycieki danych osobowych dotknęły ponad 1,7 mld osób na

świecie, a w 2025 odnotowano dalszy wzrost tego wskaźnika. Cyberprzestępcy coraz skuteczniej wykorzystywali nowe techniki – **według branżowych analiz aż 82% obecnie krążących wiadomości phishingowych zawiera treści wygenerowane przy użyciu sztucznej inteligencji**, co czyni je bardziej przekonującymi i spersonalizowanymi. Pojawiły się również pierwsze przykłady wykorzystania AI do tworzenia złośliwego oprogramowania (np. prototyp ransomware *PromptLock* współtworzony przez algorytmy AI).

Średni globalny koszt naruszenia danych w sektorze zdrowia pozostał najwyższy spośród wszystkich branż, choć po raz pierwszy od pięciu lat nieco spadł (z 9,8 mln USD w 2024 do 7,42 mln USD w 2025). **Zmienił się natomiast charakter ataków** – zamiast szyfrowania danych coraz częściej celem cyberprzestępców jest ich kradzież i późniejsze szantażowanie ujawnieniem (w 96% incydentów ransomware w ochronie zdrowia w 2025 r. sprawcy wykradli dane, podczas gdy tylko w 34% przypadków doszło do faktycznego zaszyfrowania plików).

Europa potwierdziła swoją podatność na cyberzagrożenia w sektorze zdrowia – już w 2023 r. **ochrona zdrowia była najczęściej atakowanym sektorem spośród infrastruktury krytycznej w UE (309 poważnych incydentów)**, a w 2024–2025 trend ten utrzymał się.

W 2025 r. **ponad połowa incydentów w europejskich placówkach medycznych wiązała się z ransomware**, a znaczną część reszty stanowiły poważne wycieki danych i ataki phishingowe. **Najbardziej narażone były kraje graniczne UE, w tym Polska**, co wynikało z kontekstu geopolitycznego (wojna w Ukrainie i związane z nią działania grup APT).

Unia Europejska zareagowała uruchomieniem programów wsparcia i zaostrzeniem ram prawnych (NIS2, plan cyberbezpieczeństwa szpitali), co ma w perspektywie lat podnieść odporność systemową sektora.

W Polsce rok 2025 okazał się okresem przełomowym pod względem skali i charakteru incydentów. Łączna liczba zgłoszonych przypadków cyberataków osiągnęła rekordowy poziom, wyższy niż suma incydentów z kilku poprzednich lat razem wziętych.

Napędzany czynnikami geopolitycznymi i przestępczymi **wzrost liczby incydentów przyspieszał z kwartału na kwartał**: w I kw. 2025 odnotowano ok. 130 zdarzeń (w tym ~60 infekcji złośliwym oprogramowaniem), w II kw. blisko 200, w III kw. ponad 300, a IV kwartał przekroczył pułap 400 incydentów. Oznacza to nieprzerwany wzrost intensywności zagrożeń, podczas gdy w niektórych innych regionach świata (np. w Ameryce Północnej) pod koniec roku obserwowano względną stabilizację lub nawet spadek liczby ataków.

Pod względem jakościowym w drugiej połowie 2025 r. ataki stały się bardziej **ukierunkowane, zaawansowane i agresywne**. O ile na początku roku dominowały kampanie masowe typu *spray-and-pray* (np. automatyczne skanowanie losowych podatności), o tyle pod koniec roku coraz częściej notowano **działania celowane, poprzedzone rekonesansem infrastruktury ofiary**. W rezultacie ofiarami padły głównie większe sieci klinik oraz szpitale o rozbudowanej infrastrukturze IT, które przyciągnęły uwagę zorganizowanych grup.

Techniki socjotechniczne uległy wyrafinowaniu – phishing w IV kw. 2025 często zawierał precyzyjnie spersonalizowane komunikaty odwołujące się do bieżących tematów (np. kampanii szczepień czy spraw kadrowych), nierzadko wykorzystujące dane wykradzione we wcześniejszych wyciekach. Odnotowano nawet próby **oszustw z użyciem technologii *deepfake*** – podszywania się pod głosy kadry kierowniczej w celu wyłudzenia transferu pieniędzy (BEC).

W drugiej połowie roku uwidoczniła się również **większa aktywność grup motywowanych politycznie**. O ile w I półroczu przeważały ataki finansowe (ransomware dla okupu), o tyle w III i IV kwartale coraz częściej dochodziło do **incydentów o charakterze propagandowym i sabotażowym**: próby podmiany treści na stronach internetowych szpitali (defacement) czy ataki DDoS w symboliczne dni (np. święta narodowe) przeprowadzane przez ugrupowania haktywistyczne.

Zgodnie z raportem Verizon DBIR 2025 incydenty szpiegowskie w sektorze zdrowia stanowiły już 16% wszystkich zdarzeń na świecie, podczas gdy rok wcześniej było to tylko kilka procent – co wskazuje na rosnące zainteresowanie służb wywiadowczych danymi medycznymi (np. dotyczącymi nowych technologii czy badań farmaceutycznych).

Wpływ incydentów na funkcjonowanie placówek medycznych pozostawał znaczący, choć w IV kwartale udało się uniknąć tak poważnych zakłóceń świadczenia usług jak w poprzednich okresach. W III kwartale 2025 poważne ataki za granicą (np. paraliż laboratoriów Synnovis w Wielkiej Brytanii czy atak na regionalne agencje zdrowia we Francji) pokazały, jak dotkliwe skutki mogą mieć cyberataki – proces odbudowy infrastruktury Synnovis trwał ponad rok i objął miliony rekordów danych.

W Polsce jednak, dzięki doświadczeniom z marcowego incydentu w Krakowie, **usprawniono procedury awaryjne w szpitalach**, co pozwoliło w IV kwartale w razie potrzeby sprawnie przejść na tryb pracy manualnej i ograniczyć zakłócenia dla pacjentów. Ewentualne utrudnienia miały charakter krótkotrwały i administracyjny – kluczowe procesy kliniczne pozostały zabezpieczone i nieprzerwane nawet podczas incydentów.

Pod kątem ochrony danych pacjentów sytuacja w 2025 r. nadal budziła duże obawy. W każdym z pierwszych trzech kwartałów w samych tylko Stanach Zjednoczonych liczba rekordów objętych ujawnieniami przekraczała 10 milionów. Choć w końcówce roku nie doszło do pojedynczego wycieku na skalę kilkunastu milionów osób (jak incydent PharMerica na początku 2025), to łączna liczba poszkodowanych nadal rosła. Co istotne, **spadał przeciętny rozmiar pojedynczego incydentu** – mediana liczby osób dotkniętych jednym wyciekiem pod koniec 2025 r. wynosiła już tylko kilka tysięcy, wobec kilkuset tysięcy na początku roku. Sugeruje to, że **atakujący częściej wybierali mniejsze, słabiej chronione podmioty**, podczas gdy duże organizacje – wzmocnione inwestycjami w bezpieczeństwo – stawały się trudniejszym celem.

W Polsce brak jest centralnego rejestru naruszeń, ale **szacuje się, że w ostatnich latach nawet 60% szpitali doświadczyło jakiejś formy wycieku danych osobowych**. Skutki ekonomiczne incydentów są równie niepokojące: koszt przywracania systemów i usuwania skutków jednego poważnego ataku ransomware w szpitalu może sięgnąć **kilku milionów złotych**, nie licząc strat spowodowanych przestojem czy ewentualnych kar administracyjnych za uchybienia (np. kary UODO za opóźnione zgłoszenie naruszenia lub braki w analizie ryzyka).

Reasumując, rok 2025 w sektorze ochrony zdrowia ujawnił zarówno **gwałtownie rosnącą skalę zagrożeń**, jak i pilną potrzebę systemowych zmian w podejściu do cyberbezpieczeństwa. **Strukturalne braki w zabezpieczeniach, niedobory kadrowe i ograniczone możliwości monitorowania** w wielu placówkach sprawiły, że służba zdrowia stała się łatwym celem, szczególnie w obliczu zorganizowanych kampanii.

Z drugiej strony podjęto **istotne kroki naprawcze**: zaangażowanie organów państwa (regulacje, finansowanie), wzmożona współpraca zespołów reagujących i pierwsze oznaki zmiany podejścia zarządów placówek do kwestii bezpieczeństwa informacji. Te doświadczenia stanowią cenną lekcję i punkt wyjścia do poprawy odporności cyfrowej sektora w kolejnym roku.

Prognozy na 2026 rok (I połowa roku)

Analiza zidentyfikowanych trendów oraz uwarunkowań geopolitycznych wskazuje, że pierwsze półrocze 2026 r. będzie okresem utrzymującej się wysokiej aktywności cyberzagrożeń wobec sektora zdrowia, ale zarazem czasem wdrażania nowych regulacji i wzmocnienia obrony.

Największe wyzwanie nadal stanowić będzie **ransomware**, jednak spodziewana jest dalsza **ewolucja taktyk** grup przestępczych. Coraz powszechniejsze mogą stać się kampanie typu *data theft extortion* – polegające wyłącznie na kradzieży danych i groźbie ich upublicznienia, **bez szyfrowania systemów**. Ten model wymuszania okupu zyska na znaczeniu w miarę, jak szpitale usprawnią procedury backupu i odzyskiwania danych, ograniczając skuteczność tradycyjnego ransomware.

Możliwe jest także zwiększenie kwot żądań finansowych – średnia wysokość okupu wobec organizacji medycznych w 2025 r. wynosiła ok. 7 mln USD, lecz odnotowano przypadki sięgające 100 mln USD. W 2026 r. grupy mogą testować granice możliwości finansowych dużych sieci placówek.

Nie można wykluczyć incydentów skutkujących realnym zagrożeniem zdrowia lub życia pacjentów, zwłaszcza jeśli celem ataku będą systemy monitorowania parametrów życiowych czy urządzenia podtrzymujące funkcje życiowe – zapobieżenie takim scenariuszom będzie priorytetem dla administracji i służb.

Utrzymujące się napięcia międzynarodowe sprawiają, że należy oczekiwać nasilenia cyberataków o podłożu geopolitycznym oraz ideologicznym. Sektor ochrony zdrowia w krajach NATO i UE pozostaje potencjalnym celem **sponsorowanych przez państwa grup APT**.

W przypadku Polski prawdopodobna jest kontynuacja **zorganizowanych działań ze strony grup rosyjskich** w ramach cyberwojny hybrydowej. Ataki te mogą przybierać także formę **uderzeń w łańcuch dostaw** kluczowych usług dla służby zdrowia – np. systemów logistycznych, energetycznych czy zaopatrzeniowych szpitali – w celu wywołania pośrednich zakłóceń.

Spodziewany jest również wzrost aktywności **grup powiązanych z Chińską Republiką Ludową**, ukierunkowanych na cyberszpiegostwo gospodarcze wobec firm farmaceutycznych i ośrodków badawczych w Europie (co pośrednio zwiększa ryzyko dla polskich jednostek współpracujących z tymi podmiotami).

Narastać może także zagrożenie ze strony tzw. haktywistów – luźno zorganizowanych grup motywowanych ideologicznie lub politycznie. Niewykluczone incydenty o charakterze „cyberprotestów", takie jak ataki DDoS na strony internetowe czy systemy szpitali w ramach symbolicznych akcji, co będzie wymagało od instytucji przygotowania scenariuszy reagowania na niestandardowe zdarzenia.

W 2026 roku pojawią się również nowe wektory ataków związane z rozwojem technologii medycznych i informatycznych. Coraz powszechniejsze staje się zjawisko **Internetu Rzeczy Medycznych (IoMT)** – rosnąca liczba urządzeń medycznych podłączonych do sieci (pompy infuzyjne, monitory życia, implanty telemetryczne) tworzy nową powierzchnię ataku. Wiele z tych urządzeń **nie spełnia współczesnych standardów bezpieczeństwa**, co rodzi ryzyko przejęcia nad nimi kontroli lub zakłócenia ich działania przez osoby niepowołane. Placówki medyczne wraz z producentami sprzętu będą musiały wdrożyć wzmocnione mechanizmy zabezpieczające – od solidnego uwierzytelniania po segmentację sieci i stały monitoring stanu urządzeń.

Drugim obszarem ryzyka stanie się rosnąca skala wykorzystania **usług chmurowych** przez podmioty medyczne (np. systemy e-rejestracji pacjentów, elektronicznej dokumentacji medycznej w modelu SaaS). Incydenty w chmurze mogą mieć charakter **łańcuchowy** – awaria lub atak na dostawcę usługi może jednocześnie uderzyć w dziesiątki szpitali korzystających z tego samego rozwiązania.

Dodatkowym czynnikiem będzie pojawienie się **złośliwego oprogramowania wykorzystującego AI** – malware zdolnego do autonomicznej modyfikacji swojego kodu (polimorficzne wirusy) czy samodzielnego wyszukiwania niezaktualizowanych systemów w sieci ofiary. Ta ewolucja zagrożeń wymusi **skrócenie czasu reakcji zespołów bezpieczeństwa oraz większą automatyzację analiz** (np. szersze wdrożenie rozwiązań SIEM z mechanizmami AI do detekcji anomalii).

W kontekście regulacyjnym kluczowym wydarzeniem początku 2026 r. będzie wdrożenie dyrektywy NIS2. Polska i pozostałe państwa członkowskie UE wejdą w fazę pełnej implementacji nowych przepisów – jednostki ochrony zdrowia zostaną formalnie uznane za operatorów usług kluczowych i będą **zobligowane do wdrożenia kompleksowych polityk bezpieczeństwa**, prowadzenia analiz ryzyka, utrzymywania systemów detekcji i reagowania oraz zgłaszania incydentów w określonych terminach (wstępne zgłoszenie w ciągu 24h, pełny raport w 72h). W efekcie **można spodziewać się wzrostu liczby raportowanych incydentów**, wynikającego głównie z lepszej wykrywalności i obowiązków notyfikacji, a niekoniecznie z faktycznego nasilenia ataków.

Krótko po wejściu w życie NIS2 wiele podmiotów może odczuć **dodatkowe obciążenia administracyjne i finansowe**, jednak w dłuższej perspektywie regulacja ta przyczyni się do zwiększenia odporności sektora. Utworzenie dedykowanych **zespołów CSIRT sektorowych (w tym dla sektora zdrowia)** usprawni wymianę informacji o zagrożeniach i skróci czas reakcji na incydenty.

Przewiduje się również dalszy wzrost zaangażowania kadry zarządczej placówek medycznych w kwestie cyberbezpieczeństwa. Wydarzenia z 2025 r. oraz nowe obowiązki prawne wzmacniają strategiczne znaczenie bezpieczeństwa informacji w służbie zdrowia.

Już w budżetach na 2026 r. wiele szpitali planuje **inwestycje w systemy monitorowania (SIEM)**, usługi całodobowego nadzoru (SOC-as-a-Service) oraz **ubezpieczenia od skutków incydentów cybernetycznych**. Coraz częściej tworzone będą stanowiska dedykowane (Inspektor Bezpieczeństwa Teleinformatycznego lub CISO) w miejsce dotychczasowych rozwiązań doraźnych.

Rozwinie się rynek zewnętrznych usług doradczych i audytowych – testów penetracyjnych, oceny zgodności z regulacjami, szkoleń specjalistycznych. Ogólnie **cyberbezpieczeństwo stanie się trwałym elementem**

strategii zarządzania placówkami medycznymi, raportowanym na poziomie organów nadzorczych i gremiów branżowych.

Podsumowując prognozy: pierwsze półrocze 2026 nie przyniesie spadku ryzyka cyberataków na sektor zdrowia – dynamika zagrożeń pozostanie wysoka, napędzana zarówno przez grupy przestępcze, jak i czynniki geopolityczne. Jednocześnie jednak wzrośnie **dojrzałość obrony**: dzięki wdrożeniu NIS2, intensyfikacji współpracy międzynarodowej oraz zwiększonym inwestycjom w ochronę cyfrową, sektor zdrowia wejdzie w 2026 rok bardziej świadomy i lepiej przygotowany. Kluczowym testem będą pierwsze miesiące roku, które zweryfikują stopień przełożenia doświadczeń z 2025 r. na praktykę operacyjną placówek.

Rekomendacje dla placówek ochrony zdrowia

Na podstawie wniosków z roku 2025 oraz obserwowanych trendów globalnych i krajowych sformułowano **siedem kluczowych rekomendacji** mających na celu wzmocnienie cyberbezpieczeństwa w sektorze zdrowia.

Ich konsekwentna realizacja pozwoli ograniczyć ryzyko ataków oraz zapewnić zgodność z nowymi wymogami prawnymi (m.in. dyrektywą NIS2, zaleceniami ENISA, CSIRT CeZ, UODO i innych instytucji nadzorczych).

Przeprowadzenie kompleksowej analizy ryzyka i dostosowanie polityki bezpieczeństwa (zgodność z NIS2)

Każda placówka powinna zidentyfikować krytyczne systemy i zasoby (np. systemy HIS/ERP, sprzęt laboratoryjny, kluczowe aplikacje) oraz ocenić wpływ ich awarii na bezpieczeństwo pacjentów. Na tej podstawie należy zaktualizować politykę bezpieczeństwa informacji, wdrażając adekwatne środki techniczne i organizacyjne.

Rekomenduje się ustanowienie formalnych procedur zgłaszania incydentów (do CSIRT CeZ, MC i UODO), wyznaczenie osoby odpowiedzialnej za bezpieczeństwo teleinformatyczne oraz prowadzenie rejestru incydentów – zgodnie z wymogami NIS2. **Każde naruszenie ochrony danych lub bezpieczeństwa systemów musi być niezwłocznie raportowane** właściwym organom, by umożliwić szybką pomoc i uniknąć sankcji administracyjnych.

Wzmocnienie ochrony przed ransomware i innym malware (obrona warstwowa)

Mając na uwadze dominację ataków ransomware, placówki powinny wdrożyć wielowarstwową strategię obrony. Kluczowe działania to: **regularne aktualizacje i łatki bezpieczeństwa** dla wszystkich systemów (a izolacja lub wycofanie systemów niewspieranych), **zasada minimalnych uprawnień** (ograniczenie kont administracyjnych), **nowoczesne systemy zabezpieczeń** – instalacja rozwiązań EDR/XDR oraz zapór sieciowych z funkcjami IPS/IDS – oraz **skuteczne kopie zapasowe** (regularnie wykonywane, testowane i przechowywane offline).

Niezbędne jest opracowanie **planu reagowania na incydent ransomware**, obejmującego procedury izolacji zainfekowanych segmentów sieci, komunikację kryzysową i współpracę z organami ścigania. Tylko przećwiczone i sprawdzone procedury backupu i odtwarzania danych zagwarantują ciągłość działania placówki w razie realnego ataku.

Podniesienie świadomości i kompetencji personelu

Czynnik ludzki pozostaje najsłabszym ogniwem – według danych CSIRT CeZ około 1/3 incydentów w sektorze zdrowia wynika z błędów użytkowników lub udanych ataków socjotechnicznych. Wszystkie grupy pracowników (medyczni, administracyjni, techniczni) powinny przechodzić **cykliczne szkolenia** z zakresu rozpoznawania zagrożeń, zasad tworzenia silnych haseł, stosowania MFA, bezpiecznego korzystania z poczty i pracy z nośnikami danych. Rekomenduje się również **testy socjotechniczne** – okresowe, kontrolowane kampanie phishingowe sprawdzające czujność personelu. Zasady *cyberhigieny* powinny być komunikowane wewnętrznie (intranet, plakaty informacyjne).

Budowanie kultury cyberbezpieczeństwa należy traktować na równi z innymi szkoleniami z zakresu bezpieczeństwa pacjentów.

Wdrożenie silnego uwierzytelniania i rygorystycznej kontroli dostępu

Należy w maksymalnym zakresie zaimplementować **uwierzytelnianie wieloskładnikowe (MFA)** – zwłaszcza dla kont uprzywilejowanych, zdalnych dostępów (VPN/RDP) oraz systemów krytycznych. Równolegle placówki muszą prowadzić **regularne audyty uprawnień** (usuwanie zbędnych kont, nadawanie dostępów zgodnie z zasadą *zero trust*). Wskazane jest wprowadzenie nowoczesnej **polityki haseł** (preferowanie długich

passphrases zamiast częstej zmiany krótkich haseł, użycie menedżerów haseł) oraz **segmentacja sieci** na wydzielone strefy (oddzielenie sieci biurowej od klinicznej i sieci urządzeń medycznych IoT).

Systemy monitorowania logowań i aktywności (SIEM/EDR) powinny być skonfigurowane tak, by wykrywać próby nieautoryzowanego dostępu (np. logowania poza godzinami pracy lub z nietypowych lokalizacji).

Zapewnienie stałego monitoringu bezpieczeństwa i współpraca z CSIRT

Mając na uwadze ograniczone wewnętrzne zasoby kadrowe IT, placówki powinny korzystać z zewnętrznego wsparcia i dostępnych programów pomocowych. Warto **subskrybować ostrzeżenia i komunikaty CSIRT CeZ oraz CERT Polska**, uczestniczyć w sektorowych telekonferencjach i grupach wymiany informacji. **Wszystkie incydenty i próby ataków należy zgłaszać** do CSIRT – pozwoli to ostrzec inne podmioty i uzyskać fachową pomoc.

Rozważyć należy również **outsourcing monitoringu** bezpieczeństwa (np. model *SOC-as-a-Service*) albo przynajmniej wdrożenie podstawowych narzędzi open-source do logowania i wykrywania anomalii (jak Wazuh czy Security Onion). Celem jest wczesne wykrycie ataku i reakcja zanim dojdzie do poważnych szkód.

Wzmocnienie ochrony danych wrażliwych i zgodności z RODO

Placówki medyczne muszą wdrożyć techniczne i organizacyjne środki ograniczające ryzyko wycieku danych osobowych oraz medycznych pacjentów. Rekomendowane działania obejmują **szyfrowanie danych w spoczynku i w tranzycie** (szyfrowanie baz danych, dysków, komunikacji protokołami TLS/VPN), **minimalizację przechowywanych danych osobowych** (przechowywanie tylko niezbędnych informacji, pseudonimizacja/anonymizacja gdzie możliwe), **wdrożenie systemów monitorowania dostępu i ochrony danych (DLP)** oraz **regularne audyty logów i operacji na bazach danych**.

Każde naruszenie bezpieczeństwa danych powinno być bez zwłoki zgłoszone do UODO oraz zakomunikowane osobom, których dane dotyczą – zgodnie z wymaganiami RODO. Warto przećwiczyć wewnętrznie procedurę notyfikacji incydentu (np. jako ćwiczenie scenariuszowe), aby uniknąć opóźnień lub błędów organizacyjnych w sytuacji realnego wycieku.

Ciągłe testowanie, audyty i doskonalenie cyberbezpieczeństwa

Cyberbezpieczeństwo to proces ciągły – **zaleca się przeprowadzanie regularnych audytów i testów penetracyjnych** (co najmniej raz w roku) najlepiej z udziałem niezależnych ekspertów. Wyniki powinny służyć jako podstawa do planu działań usprawniających. Warto organizować okresowo **ćwiczenia symulacyjne typu *table-top***, angażujące zarówno personel techniczny, jak i kierownictwo – przećwiczenie scenariusza poważnego incydentu (np. ataku na system rejestracji pacjentów) pozwoli ujawnić ewentualne luki w procedurach i poprawić współpracę różnych zespołów podczas realnego kryzysu.

Placówki powinny również na bieżąco **śledzić aktualne raporty branżowe i zalecenia** (ENISA, H-ISAC, raporty CERT/CSIRT itp.), a także aktywnie uczestniczyć w forach wymiany doświadczeń i konferencjach sektora. **Stałe podnoszenie dojrzałości cyberbezpieczeństwa** – poprzez naukę z incydentów i adaptację do nowych zagrożeń – jest niezbędne, by sprostać rosnącym wyzwaniom.

Wdrożenie powyższych rekomendacji umożliwi polskim podmiotom ochrony zdrowia **osiągnięcie zgodności z nadchodzącymi przepisami oraz znaczące obniżenie ryzyka poważnych incydentów**.

Doświadczenia innych sektorów pokazują, że inwestycje w prewencję i przygotowanie są wielokrotnie mniej kosztowne niż reagowanie na skutki udanego ataku. **Cyberbezpieczeństwo musi być traktowane jako integralna część misji systemu ochrony zdrowia – gwarantująca nie tylko ciągłość działania systemów, ale przede wszystkim bezpieczeństwo pacjentów.**

małopolskie parki zdrowia Sp. z o.o.

Partner małopolskich szpitali w budowie operacyjnej odporności cyfrowej