CSIRT CeZ

cez.gov.pl

Raport 2025

Krajobraz cyberbezpieczeństwa w sektorze ochrony zdrowia

Spis treści

Słowo wstępne

Rok 2025 był dla CSIRT CeZ okresem intensyfikacji działań operacyjnych i koordynacyjnych. Odnotowaliśmy wyraźny wzrost zagrożeń w sektorze ochrony zdrowia. CSIRT CeZ obsłużył 1441 incydentów cyberbezpieczeństwa, czyli o ponad 60% więcej niż rok wcześniej. Potwierdza to, że ochrona systemów przetwarzających dane medyczne staje się kluczowa dla bezpieczeństwa państwa i ciągłości świadczeń zdrowotnych.

CSIRT CeZ realizował zadania obejmujące m.in. analizę incydentów, wymianę informacji o zagrożeniach, przygotowywanie rekomendacji oraz współpracę z innymi zespołami i instytucjami. Istotnym elementem było wsparcie podmiotów leczniczych w wypełnianiu obowiązków wynikających z regulacji krajowych i unijnych, w tym przygotowań do zmian w ustawie o KSC oraz wdrażania dyrektywy NIS2.

Rosnąca skala i złożoność incydentów pokazują, że cyberbezpieczeństwo w ochronie zdrowia wykracza poza kwestie techniczne. Zakłócenia działania systemów lub naruszenia danych mogą bezpośrednio wpływać na bezpieczeństwo pacjentów i procesy kliniczne. Dlatego działania CSIRT CeZ koncentrują się także na prewencji i budowaniu odporności organizacyjnej.

Raport podsumowuje działania zespołu w ubiegłym roku, prezentuje najważniejsze trendy i wskazuje obszary wymagające dalszego wzmocnienia. Mam nadzieję, że będzie on praktycznym wsparciem dla wszystkich podmiotów sektora ochrony zdrowia.

dr Tomasz Jeruzalski

Dyrektor Pionu Eksploatacji Systemów Teleinformatycznych

Pełnomocnik ds. CSIRT CeZ

Słowo wstępne

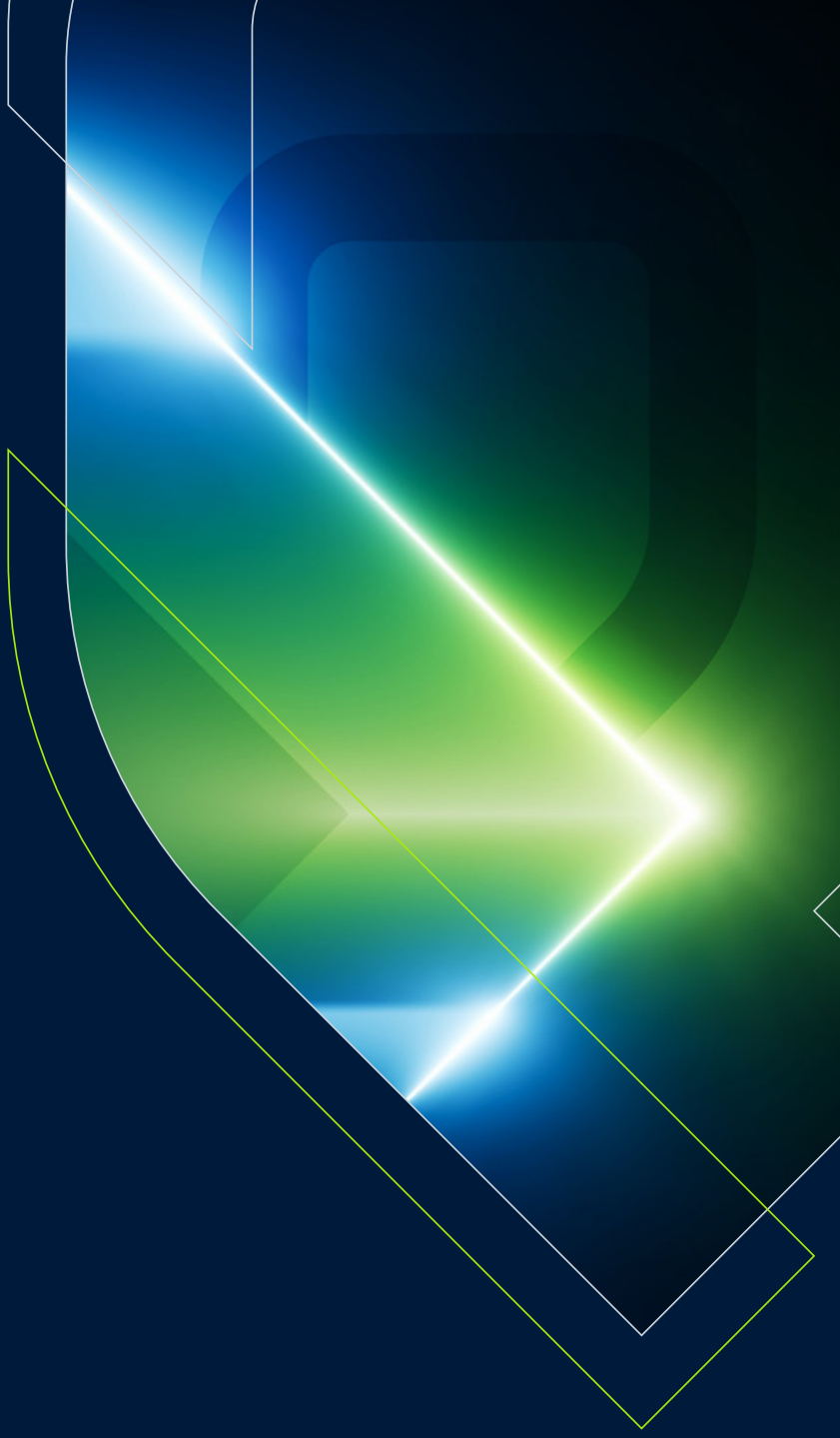
Skala cyberzagrożeń stale rośnie. Cyberprzestępcy wciąż stosują podobne mechanizmy ataków, ale są one coraz bardziej dopracowane. Potwierdzają to również dane, które zebraliśmy w ostatnim roku. Jednocześnie wdrożona dyrektywa NIS2 oraz nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa istotnie zmieniły otoczenie regulacyjne, rozszerzając obowiązki w zakresie cyberbezpieczeństwa na szerszą grupę podmiotów, w tym wiele organizacji medycznych.

W obliczu tych zmian rola CSIRT CeZ ulega wzmocnieniu. Zespół przygotowuje się do obsługi większej liczby zgłoszeń, rozwija działania wspierające dostosowanie sektora do nowych wymagań oraz intensyfikuje inicjatywy edukacyjne i prewencyjne. Kluczowe pozostaje także wzmacnianie współpracy z innymi zespołami CSIRT i instytucjami odpowiedzialnymi za nadzór i bezpieczeństwo.

CSIRT CeZ pełni istotną funkcję pomostu między regulacjami a praktyką operacyjną, wspierając podmioty ochrony zdrowia nie tylko w reagowaniu na incydenty, ale również w budowaniu trwałej odporności cyberbezpieczeństwa.

Jeremi Olechnowicz

Kierownik CSIRT CeZ



Poznaj CSIRT CeZ

CSIRT
Centrum e-Zdrowia

CSIRT CeZ jest jednym z pierwszych dwóch zespołów sektorowych CSIRT w Polsce, które pełnią rolę centralnego punktu wsparcia dla podmiotów swojego sektora w zakresie cyberbezpieczeństwa i jedynym, który pełni taką rolę w sektorze ochrony zdrowia. Utworzenie zespołu stanowiło element wdrażania założeń dyrektywy NIS oraz budowy krajowego systemu cyberbezpieczeństwa w sektorach o kluczowym znaczeniu dla funkcjonowania państwa.

CSIRT CeZ pełni rolę centralnego punktu wsparcia dla podmiotów w zakresie cyberbezpieczeństwa w sektorze ochrony zdrowia. Zespół działa w strukturach Centrum e-Zdrowia i odpowiada na specyficzne potrzeby sektora, w którym bezpieczeństwo systemów teleinformatycznych bezpośrednio przekłada się na ciągłość leczenia oraz bezpieczeństwo pacjentów.

Zakres działalności CSIRT CeZ

CSIRT CeZ wspiera podmioty ochrony zdrowia na każdym etapie zarządzania incydentami cyberbezpieczeństwa.

Działalność CSIRT CeZ koncentruje się na praktycznym wsparciu podmiotów sektora ochrony zdrowia w reagowaniu na zagrożenia cyfrowe. Oprócz bieżącej obsługi incydentów zespół prowadzi systematyczne analizy zdarzeń oraz ocenia zmieniający się krajobraz zagrożeń, identyfikując obszary wymagające szczególnej uwagi.

Szczególny nacisk kładziemy na ochronę danych medycznych oraz zapewnienie ciągłości usług e zdrowia. Mamy świadomość ich kluczowego znaczenia dla bezpieczeństwa pacjentów i funkcjonowania systemu ochrony zdrowia. Każde zgłoszenie traktowane jest jako odrębny przypadek, analizowany zarówno pod kątem technicznym, jak i organizacyjnym, a przekazywane rekomendacje ukierunkowane są na ograniczanie skutków incydentów oraz wzmacnianie odporności sektora. Realizujemy również działania informacyjne i ostrzegawcze, wspierając podmioty w reagowaniu na aktualne zagrożenia. Wyniki tych działań, wraz z obserwowanymi trendami i statystykami, zostały przedstawione w dalszej części raportu.

Podstawa prawna i zadania ustawowe

CSIRT CeZ został powołany na bazie ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC). Zespół realizuje zadania sektorowego zespołu cyberbezpieczeństwa, o których mowa w art. 44 ustawy o KSC, wspierając podmioty sektora zdrowia, w tym Operatorów Usług Kluczowych (obecnie: podmiotów kluczowych i ważnych).

Do kluczowych zadań CSIRT CeZ należą:

- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w ich obsłudze
- wspieranie podmiotów kluczowych i ważnych w wykonywaniu obowiązków wynikających z ustawy o KSC
- analizowanie incydentów oraz identyfikowanie powiązań i trendów zagrożeń
- współpraca z CSIRT-ami poziomu krajowego w zakresie koordynacji reagowania na incydenty.

CSIRT CeZ w kontekście NIS2 i przyszłych obowiązków podmiotów medycznych

Przepisy wdrażające dyrektywę NIS2 znacząco rozszerzają katalog podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa, w tym w sektorze ochrony zdrowia. Oprócz podmiotów kluczowych i ważnych coraz większa liczba organizacji kwalifikowana będzie jako podmioty kluczowe lub podmioty ważne, zobowiązane do wdrażania odpowiednich środków organizacyjnych i technicznych oraz raportowania incydentów.

W tym kontekście rola CSIRT CeZ będzie systematycznie rosła. Zespół regularnie wzmacnia swoje kompetencje w zakresie:

- obsługi większej liczby zgłoszeń incydentów
- wsparcia podmiotów sektora zdrowia w dostosowaniu się do nowych wymagań regulacyjnych
- rozwijania działań prewencyjnych i edukacyjnych
- usprawniania współpracy z innymi zespołami CSIRT oraz instytucjami nadzorczymi.

CSIRT CeZ pełni i będzie pełnił istotną funkcję łącznika pomiędzy regulacjami prawnymi a praktycznymi działaniami operacyjnymi, wspierając sektor ochrony zdrowia w budowaniu cyberbezpieczeństwa.

Współpraca w obszarze cyberbezpieczeństwa

CSIRT
Centrum e-Zdrowia

Współpraca krajowa

CSIRT CeZ realizuje swoje zadania w ścisłej współpracy z podmiotami krajowego systemu cyberbezpieczeństwa, w szczególności z zespołami CSIRT poziomu krajowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON.

Współpraca ta obejmuje przede wszystkim wymianę informacji o zagrożeniach, koordynację obsługi poważnych incydentów oraz budowanie wspólnej świadomości sytuacyjnej w cyberprzestrzeni. Dzięki temu możliwe jest skoordynowane reagowanie na zagrożenia o charakterze systemowym oraz zapewnienie spójności działań na poziomie sektorowym i krajowym.

W ramach codziennej działalności CSIRT CeZ ściśle współpracuje nie tylko z krajowymi zespołami CSIRT, ale również z innymi instytucjami zajmującymi się zwalczaniem cyberprzestępczości. Efektywna wymiana informacji o incydentach i zagrożeniach pozwala na szybką reakcję oraz ograniczanie występowania nowych zdarzeń. Wspólne działania obejmują także dzielenie się wiedzą o nowych technikach ataków, podatnościach i najlepszych praktykach, co przekłada się na rozwój metod obrony i skuteczniejsze wsparcie podmiotów w przywracaniu ciągłości działania usług.

W 2025 roku CSIRT CeZ podpisał porozumienia operacyjne z CERT Polska (NASK), CSIRT GOV (ABW) oraz Dowództwem Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC). Dodatkowo zostało uzgodnione porozumienie z Zakładem Ubezpieczeń Społecznych, którego celem jest wzmocnienie bezpieczeństwa usług elektronicznych świadczonych obywatelom oraz zapewnienie bezpiecznej wymiany informacji między CeZ a ZUS.

Współpraca międzynarodowa

Współpraca międzynarodowa stanowi jeden z kluczowych filarów skutecznego reagowania na zagrożenia w cyberprzestrzeni. Cyberbezpieczeństwo nie zna granic, a charakter współczesnych zagrożeń wymaga stałej wymiany wiedzy, doświadczeń oraz wypracowywania wspólnych standardów działania na poziomie europejskim i międzynarodowym. Aktywne uczestnictwo ekspertów CSIRT CeZ w inicjatywach międzynarodowych pozwala nie tylko na podnoszenie własnych kompetencji, lecz także na realny wkład w kształtowanie rozwiązań wzmacniających bezpieczeństwo cyfrowe, w szczególności w sektorze ochrony zdrowia.

Warsztaty Digital Security Authority of Cyprus i European Security and Defence College

W lutym 2025 r. specjaliści z CSIRT CeZ wzięli udział w międzynarodowych warsztatach dla operatorów zespołów reagowania na incydenty w Nikozji na Cyprze. Organizatorem wydarzenia była Cypryjska Agencja ds. Bezpieczeństwa Cyfrowego (Digital Security Authority of Cyprus – DSA) oraz Europejskie Kolegium Bezpieczeństwa i Obrony (European Security and Defence College – ESDC). Warsztaty obejmowały szereg zagadnień związanych z podstawami funkcjonowania zespołów CSIRT, w tym zarządzanie incydentami, analizę zagrożeń oraz podstawy analizy śledczej. Program wydarzenia koncentrował się na przekazaniu wiedzy teoretycznej, a także na praktycznych aspektach pracy zespołów. Udział specjalistów CSIRT CeZ umożliwił poszerzenie wiedzy oraz wymianę doświadczeń w obszarze funkcjonowania zespołów CSIRT na poziomie międzynarodowym.

Współpraca z Portugalią

W sierpniu odbyło się spotkanie z przedstawicielem Servicos Partilhados do Ministerio de Saude (SPMS), Dep. ds. cyberbezpieczeństwa sektora ochrony zdrowia w Portugalii, podczas którego podzieliliśmy się doświadczeniami oraz podjęliśmy decyzję o umówieniu kolejnych spotkań aby wymienić się wiedzą i doświadczeniem.

Medical Devices Cybersecurity Task Force

Przedstawiciele CSIRT CeZ uczestniczyli w pracach Medical Devices Cybersecurity Task Force. Celem działania było sformułowanie wniosków dotyczących zmian regulacyjnych dotyczących cyberbezpieczeństwa urządzeń medycznych. Zespół rozważał potrzebę aktualizacji załączników I i II do MDR (Medical Device Regulation – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 dotyczące wyrobów medycznych i IVDR (In Vitro Diagnostic Medical Device Regulation – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 dotyczące wyrobów medycznych do diagnostyki in vitro) lub konieczności utworzenia wspólnej specyfikacji (CS) cyberbezpieczeństwa. Uczestnicy warszatatów wzięli pod uwage także potrzebę aktualizacji wytycznych MDCG dotyczących cyberbezpieczeństwa urządzeń medycznych. Wynikiem prac zespołu jest raport Task Force Report on Cybersecurity of connected medical devices – where we are and what's next. Jego zakres objął kwestie związane z zarządzaniem ryzykiem cyberbezpieczeństwa urządzeń medycznych, które zostały zidentyfikowane w wyniku ankiety przeprowadzonej w ramach polskiej prezydencji, w tym:

- rozbieżności wymagań pomiędzy CRA (Cyber Resilience Act) a MDR/IVDR
- brak wymogów dotyczących zgłaszania oraz zarządzania (łatania) podatności
- bardzo wysoki poziom wymagań w MDR/IVDR oraz brak norm zharmonizowanych lub wspólnych specyfikacji dotyczących cyberbezpieczeństwa wyrobów medycznych

- brak harmonizacji wymagań pomiędzy jednostkami notyfikowanymi (różne podejścia różnych JB) oraz pomiędzy państwami członkowskimi (różne dodatkowe wymagania), co skutkuje trudnościami w funkcjonowaniu wspólnego rynku.

Raport został przedstawiony MDCG.

Work Stream on Health

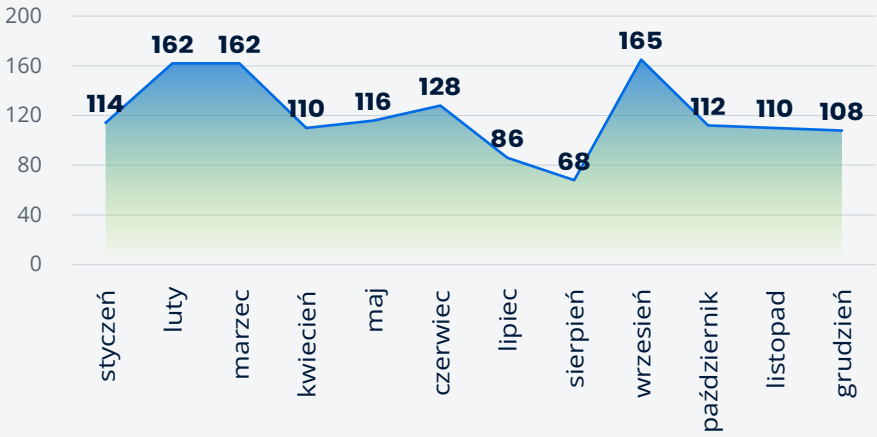
CSIRT CeZ uczestniczył także w wymianie doświadczeń i informacji w ramach Work Stream on Health, który wchodzi w skład Grupy współpracy NIS. Informacje dotyczyły w szczególności incydentów w placówkach sektora, postępów we wdrażaniu dyrektywy NIS2 w sektorze zdrowia i bieżących prac w poszczególnych państwach członkowskich, w tym wsparcia podmiotów w realizacji obowiązków wynikających z implementacji dyrektywy. Omawiano informacje Komisji Europejskiej dotyczące w szczególności europejskiego planu cyberbezpieczeństwa szpitali oraz prac dotyczących planowanych zmian regulacyjnych (Cybersecurity Act, MDR/IVDR, EHDS).

Statystyki incydentów

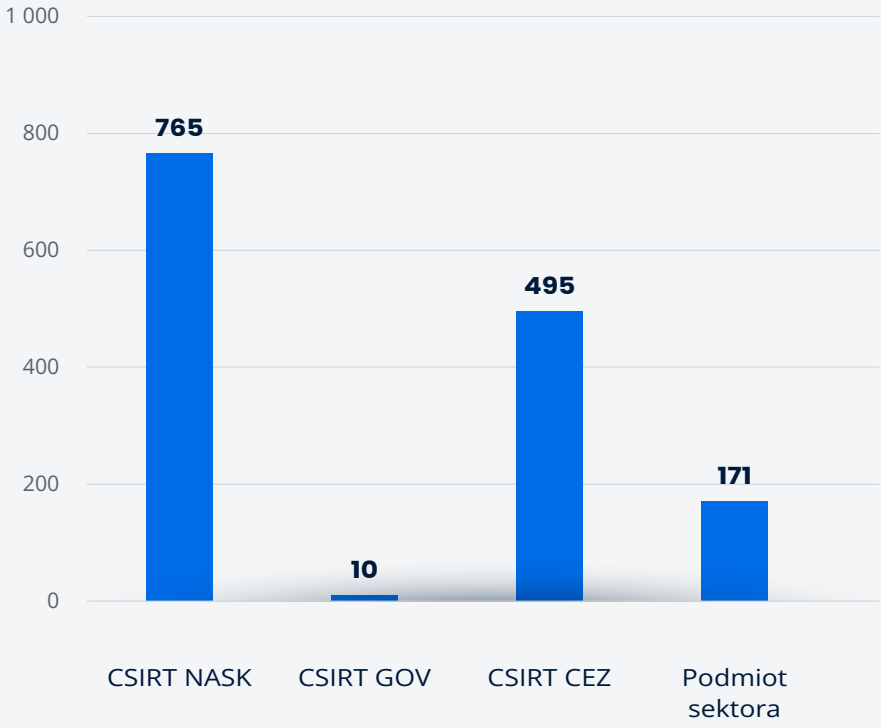
CSIRT
Centrum e-Zdrowia

Z danych CSIRT CeZ wynika, że w 2025 roku w sektorze zdrowia odnotowano 1441 incydentów bezpieczeństwa, w tym 5 incydentów poważnych oraz 8 ataków z wykorzystaniem ransomware. Jest to duży wzrost (ponad 60%) w stosunku do roku 2024. Analizując ostatnie lata widzimy, że tendencja wzrostowa się utrzymuje.

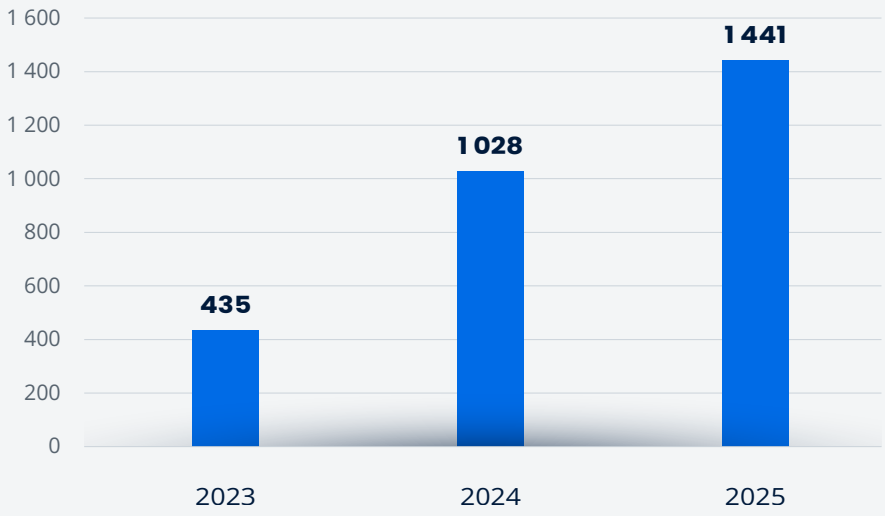
WYKRES 1. Liczba incydentów w poszczególnych miesiącach 2025 roku



WYKRES 2. Liczba incydentów z podziałem na źródło zgłoszenia



WYKRES 3. Liczba incydentów w sektorze ochrony zdrowia w latach 2023-2025



Klasyfikacja incydentów

Poniższy wykres przedstawia incydenty zarejestrowane w roku 2025 zgodnie z przyjętą klasyfikacją.

WYKRES 4. Incydenty sklasyfikowane według kategorii

Analizując dane CSIRT CeZ można zauważyć wyraźne zróżnicowanie liczby zdarzeń w zależności od typu incydentu. Zdecydowanie dominują oszustwa komputerowe (580 przypadków) oraz podatne usługi (344), które razem stanowią największą część wszystkich odnotowanych zdarzeń (64%). W dalszej kolejności pojawiają się kategorie o średniej liczbie zgłoszeń, takie jak wycieki poświadczeń (148), szkodliwe oprogramowanie (146) oraz obraźliwe i nielegalne treści (74). Pozostałe kategorie, w tym m.in. naruszenia dostępności zasobów, ataki na bezpieczeństwo informacji czy próby włamań, występują znacznie rzadziej – zazwyczaj poniżej 40 przypadków każda. Zestawienie pokazuje, że największym wyzwaniem dla sektora pozostają incydenty związane z działaniami przestępczymi w cyberprzestrzeni oraz podatnościami technicznymi, natomiast klasyczne ataki infrastrukturalne mają relatywnie mniejszy udział.

Należy jednak podkreślić, że sama liczba incydentów nie zawsze odzwierciedla ich rzeczywisty wpływ na funkcjonowanie organizacji. Pojedyncze, skuteczne ataki o wysokiej szkodliwości, takie jak ransomware, mogą powodować znacznie poważniejsze konsekwencje operacyjne, finansowe i wizerunkowe niż liczne, lecz mniej dotkliwe zdarzenia innych kategorii. Oznacza to, że ocena poziomu zagrożeń powinna uwzględniać nie tylko skalę zjawiska, ale również jego wagę i potencjalne skutki dla ciągłości działania sektora ochrony zdrowia.

Phishing - najczęstsza przyczyna incydentów

W CSIRT CeZ identyfikowaliśmy i komunikowaliśmy najważniejsze kampanie, które były coraz bardziej zaawansowane i precyzyjnie ukierunkowane na personel medyczny oraz placówki.

Ostrzegaliśmy m.in. przed atakami, które polegały na podszywaniu się pod Medfile i Narodowy Fundusz Zdrowia, w których rozsyłano fałszywe SMS-y i e maile z linkami do aplikacji imitujących systemy Elektronicznej Dokumentacji Medycznej. W innych kampaniach cyberprzestępcy wykorzystywali wizerunek gabinet.gov.pl i eZUS, kierując przekaz szczególnie do lekarzy, a wiadomości sugerowały np. utratę możliwości wystawiania e recept i prowadziły do fałszywych stron logowania.

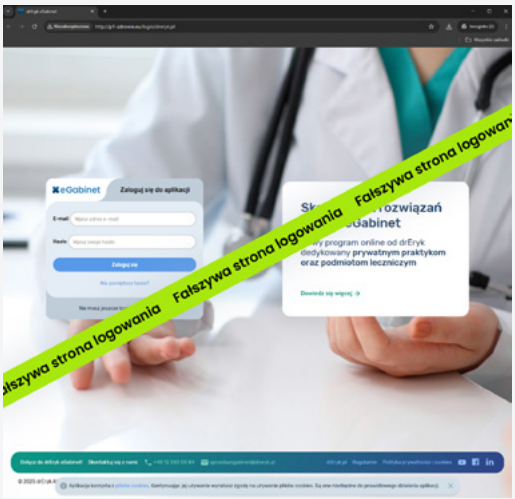
RYSUNEK 1. Przykładowa wiadomość e-mail wysyłana w ramach kampanii phishingowej, w której cyberoszuści podszywali się pod RPWDL

Szczególnie niebezpieczne były kampanie wykorzystujące autorytet instytucji publicznych. Przestępcy podszywali się pod NFZ, oferując rzekomo „darmową apteczkę" za symboliczną opłatą. Wiadomości kierowały do spreparowanych stron płatności, które do złudzenia przypominały oficjalne serwisy i służyły do wyłudzania danych kart płatniczych. Tego typu ataki łączyły element socjotechniki z próbą bezpośredniego osiągnięcia korzyści finansowych.

RYSUNEK 2. Przykładowy sms wysyłany w ramach kampanii phishingowej, w której cyberprzestępcy podszywali się pod NFZ

Równolegle obserwowaliśmy kampanie wymierzone bezpośrednio w system ochrony zdrowia, m.in. podszywanie się pod RPWDL czy usługi Centrum e Zdrowia. Fałszywe wiadomości nakłaniały do aktualizacji certyfikatów lub logowania do rzekomych systemów, prowadząc do przejęcia danych dostępowych. W wielu przypadkach wykorzystywano SMS-y i e maile kierujące do aplikacji wyglądających jak systemy EDM, co zwiększało wiarygodność ataków i ich skuteczność.

RYSUNEK 3. Przykładowy fałszywy panel logowania wykorzystywany przez cyberprzestępców



Dzięki szybkim ostrzeżeniom CSIRT CeZ możliwe było ograniczanie skutków tych działań i budowanie świadomości zagrożeń w środowisku medycznym.

Incydenty poważne

W 2025 roku CSIRT CeZ obsłużył 5 incydentów poważnych w rozumieniu ustawy o KSC.

Jednym z tych incydentów był cyberatak na SPZOZ MSWiA w Krakowie, do którego doszło 8 marca 2025 roku. Placówka natychmiast otrzymała wsparcie Centralnego Biura Zwalczania Cyberprzestępczości, CSIRT NASK oraz CSIRT CeZ, a działania operacyjne zostały szybko skoordynowane. Zespół CSIRT CeZ zapewnił szpitalowi niezbędny sprzęt do odbudowy

infrastruktury oraz wsparcie ekspertów w przywracaniu systemów i ich zabezpieczeniu. Dzięki szybkiemu zgłoszeniu incydentu i współpracy wszystkich zaangażowanych podmiotów możliwe było sprawne rozpoczęcie odbudowy. Atak ten pokazał, jak istotna jest profilaktyka, w tym regularne aktualizacje systemów, silne hasła, segmentacja sieci oraz wykonywanie i testowanie kopii zapasowych, które znacząco zwiększają odporność placówek na zagrożenia typu ransomware.

Przeskanowane podmioty i wykryte podatności

CSIRT
Centrum e-Zdrowia

W obliczu rosnącej liczby incydentów cyberbezpieczeństwa, w tym zdarzeń wynikających bezpośrednio z wykorzystania znanych podatności, regularna weryfikacja poziomu zabezpieczeń infrastruktury teleinformatycznej staje się kluczowym elementem zarządzania ryzykiem w sektorze zdrowia. Skany bezpieczeństwa umożliwiają wczesne wykrycie luk i błędów konfiguracyjnych, które, jeśli pozostaną niezaadresowane, mogą zostać wykorzystane przez atakujących. Tym samym działania te pozwalają nie tylko ograniczyć liczbę potencjalnych incydentów, ale przede wszystkim zmniejszyć ich skalę i skutki dla funkcjonowania organizacji.

W 2025 roku Sektorowy Zespół Cyberbezpieczeństwa CSIRT CeZ przeprowadził skany bezpieczeństwa infrastruktury teleinformatycznej w ośmiu podmiotach. Działania te obejmowały identyfikację potencjalnych podatności oraz nieprawidłowości konfiguracyjnych, które mogły wpływać na poziom bezpieczeństwa wykorzystywanych systemów i usług. Prace zostały zrealizowane w oparciu o wcześniej uzgodniony zakres oraz na podstawie zgód udzielonych przez właściwe placówki medyczne.

Najczęściej identyfikowane podatności i błędy konfiguracyjne:

- brak aktualizacji oprogramowania
- wygasłe certyfikaty SSL/TLS
- komunikacja przy użyciu przestarzałych protokołów TLSv1.0 i/lub TLSv1.1
- brak stosowania nagłówków typu Security-Headers
- brak stosowania w usługach pocztowych nagłówków SPF, DKIM, DMARC
- brak wsparcia producentów systemów operacyjnych po okresie podstawowym
- podatne niewspierane dłużej systemy EOL

Wnioski

Najczęściej identyfikowane podatności wynikają przede wszystkim z zaniedbań w utrzymaniu i konfiguracji systemów. Brak regularnych aktualizacji, nieaktualne certyfikaty oraz wykorzystywanie przestarzałych protokołów i systemów wycofanych ze wsparcia (End Of Life - EOL) istotnie zwiększają ryzyko skutecznych ataków. Dodatkowo pomijanie mechanizmów ochronnych, takich jak nagłówki bezpieczeństwa czy konfiguracje SPF/DKIM/DMARC, osłabia poziom zabezpieczenia usług. Wszystkie te czynniki wskazują na potrzebę systematycznego i kompleksowego zarządzania bezpieczeństwem oraz aktualizacjami infrastruktury IT.

Statystyki błędów konfiguracyjnych i podatności

CSIRT
Centrum e-Zdrowia

W 2025 roku zespół CSIRT CeZ wykrył znaczną ilość błędów konfiguracyjnych i podatności, które były wynikiem analiz pasywnych, raportów generowanych przez specjalistyczne systemy wykrywania oraz zgłoszeń od osób prywatnych.

Zakres wykorzystanych danych obejmował kilka uzupełniających się źródeł informacji dotyczących bezpieczeństwa infrastruktury teleinformatycznej. Przeprowadzano pasywną analizę zasobów publicznych, w tym identyfikację subdomen oraz badanie ogólnodostępnych elementów infrastruktury, takich jak konfiguracje sieciowe, otwarte usługi i porty oraz dostępne panele logowania. Podczas wykrywania nowych nieprawidłowości w systemach istotne okazywały się dane pochodzące z systemu n6, który dostarczał informacji o wykrytych podatnościach i błędach konfiguracji w obrębie krytycznych usług i zasobów IT, mogących stanowić potencjalne wektory ataku. Uzupełnieniem były wyniki skanów realizowanych w ramach rozwiązania Artemis oraz zgłoszenia zewnętrzne, w tym od osób prywatnych.

Najczęściej występujące błędy konfiguracyjne

01. Publicznie dostępne panele logowania

W analizowanym okresie CSIRT CeZ wykrył publicznie dostępne panele administracyjne, w szczególności usług pocztowych oraz wymiany plików. Ich dostępność z poziomu internetu znacząco zwiększa ryzyko nieautoryzowanego dostępu, zwłaszcza w przypadku stosowania słabych haseł lub braku mechanizmów dodatkowego uwierzytelniania. W konsekwencji mogą one zostać wykorzystane przez atakujących do przejęcia kontroli nad usługami, kradzieży danych lub prowadzenia dalszych działań w infrastrukturze organizacji.

02. Publicznie dostępne, otwarte porty

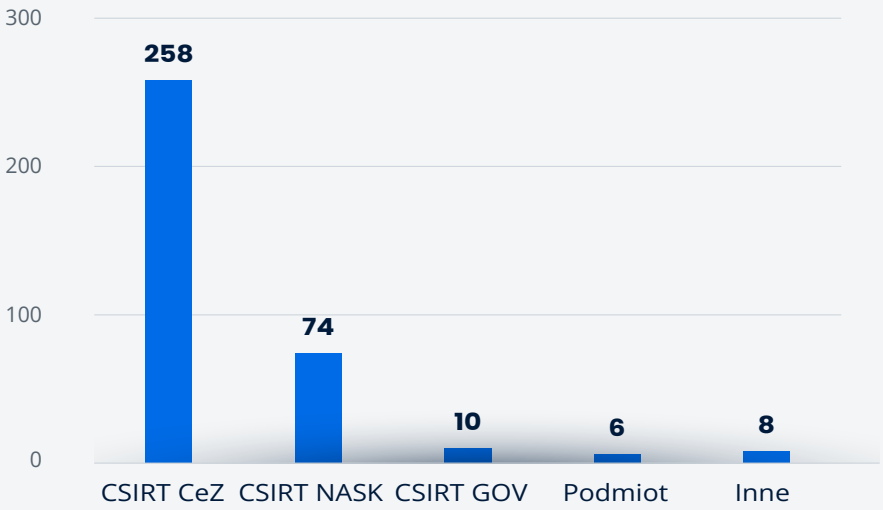
W trakcie analizy wykryto obecność otwartych portów, takich jak SSH, RDP, SMB, VNC, Telnet. Ich dostępność z poziomu internetu może stanowić bezpośredni wektor ataku i umożliwić próby nieautoryzowanego logowania lub wykorzystania znanych podatności w usługach sieciowych. W przypadku niewłaściwej konfiguracji lub braku odpowiednich zabezpieczeń, takich jak ograniczenia dostępu czy uwierzytelnianie wieloskładnikowe, mogą one prowadzić do przejęcia kontroli nad systemami oraz dalszej kompromitacji infrastruktury.

Dzięki regularnym kontrolom oraz szybkiemu wykryciu błędów konfiguracyjnych, można usuwać podatności zanim zostaną nadużyte przez potencjalnych atakujących.

Wyniki i statystyki

W 2025 roku CSIRT CeZ zapewnił obsługę łącznie 356 zgłoszeń dotyczących podatności i błędów konfiguracyjnych.

WYKRES 5. Źródło wykrycia błędów konfiguracyjnych i podatności



Zalecenia przeciwdziałania wobec zidentyfikowanych zagrożeń technicznych i systemowych

CSIRT
Centrum e-Zdrowia

Analiza statystyczna incydentów bezpieczeństwa wskazuje, że najczęściej wykorzystywane przez atakujących wektory obejmują: oszustwa komputerowe, podatne usługi oraz wycieki poświadczeń. Ich występowanie ma istotny wpływ na poziom ryzyka w organizacjach, dlatego konieczne jest wdrażanie skoordynowanych działań technicznych i organizacyjnych.

Prawidłowo zaprojektowane i konsekwentnie wdrażane mechanizmy ochronne, w połączeniu z działaniami edukacyjnymi, przekładają się na ograniczenie skuteczności ataków oraz wzrost cyberodporności w sektorze zdrowia.

Oszustwa komputerowe

Oszustwa komputerowe obejmują przede wszystkim kampanie phishingowe, spoofing oraz inne formy socjotechniki, których celem jest nakłonienie użytkownika do ujawnienia danych lub wykonania niepożądanych działań.

Rekomendowane działania:

- systematyczne podnoszenie świadomości użytkowników w zakresie rozpoznawania prób phishingu i manipulacji
- wdrożenie oraz utrzymanie prawidłowej konfiguracji systemów poczty elektronicznej (SPF, DKIM, DMARC) w celu ograniczenia fałszywych wiadomości
- zastosowanie rozwiązań antyspamowych oraz mechanizmów analizy załączników i linków
- regularne testy phishingowe wśród pracowników w celu weryfikacji poziomu odporności organizacji

Podatne usługi

Podatne usługi stanowią istotny wektor ataku, szczególnie jeżeli podmiot nie aktualizuje oprogramowania lub ma nieprawidłowo skonfigurowane systemy. Wykorzystanie znanych luk bezpieczeństwa może prowadzić do kompromitacji systemów i eskalacji uprawnień.

Rekomendowane działania:

- zapewnienie szybkiego wdrażania aktualizacji oraz korzystanie wyłącznie ze stabilnych, wspieranych wersji oprogramowania
- wdrożenie cyklicznego procesu zarządzania podatnościami oraz regularne skanowanie infrastruktury
- monitorowanie komunikatów producentów oraz baz podatności CVE w celu szybkiej reakcji na nowe zagrożenia
- określenie procedur dotyczących maksymalnego czasu wdrażania poprawek bezpieczeństwa

Wycieki poświadczeń

Wycieki poświadczeń stanowią jedno z najpoważniejszych zagrożeń, ponieważ umożliwiają nieautoryzowany dostęp do systemów bez konieczności bezpośredniego włamania.

Rekomendowane działania:

- wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), obejmującego polityki haseł oraz kontrolę dostępu
- egzekwowanie stosowania silnych, unikalnych haseł oraz wdrożenie uwierzytelniania wieloskładnikowego (MFA)

- monitorowanie logowań oraz wykrywanie anomalii z wykorzystaniem narzędzi klasy SIEM
- edukacja użytkowników w zakresie bezpiecznego przechowywania i używania poświadczeń

Wnioski

Zidentyfikowane wektory ataków wskazują, że główne ryzyka wynikają zarówno z czynników technicznych, jak i systemowych. W związku z tym skuteczna poprawa poziomu cyberbezpieczeństwa wymaga równoległego wdrażania rozwiązań technologicznych, procedur organizacyjnych oraz działań edukacyjnych. Kompleksowe podejście do zarządzania ryzykiem pozwoli na istotne ograniczenie liczby incydentów, a także ich skutków.

Analiza sektora

CSIRT
Centrum e-Zdrowia

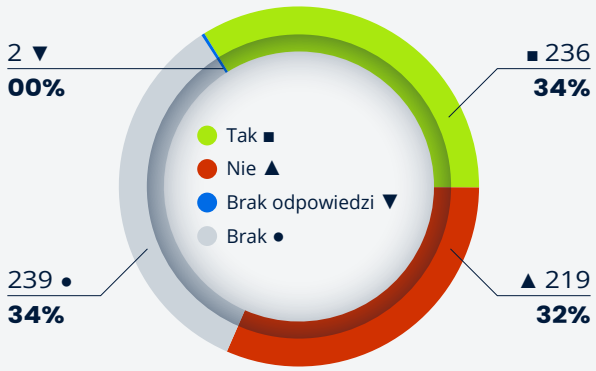
W 2025 roku w badaniu poziomu cyberbezpieczeństwa uczestniczyło 696 podmiotów. Ankieta skierowana była do szpitali podlegających bezpośrednio Ministerstwu Zdrowia oraz Ministrowi Zdrowia, czyli około 1600 podmiotów. W badaniu wzięło więc udział 43% potencjalnych respondentów. Obraz całego sektora nie jest pełny, ale pozwala już wyciągnąć wiele trafnych wniosków.

Z zebranych danych wynika, że ponad 60% ankietowanych placówek posiada dedykowane stanowisko i wyznaczoną osobę odpowiedzialną za cyberbezpieczeństwo. Zadeklarowano uczestnictwo 42% dyrektorów placówek w szkoleniu z zakresu cyberbezpieczeństwa. Zgodnie z wynikiem badania 70% dyrektorów cyklicznie zapoznaje się z przeglądem ryzyka w jednostce, zawierającym dane z obszaru cyberbezpieczeństwa.

76% podmiotów deklaruje wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), a niemal 62% - prowadzenie okresowych szkoleń z cyberhigieny dla wszystkich pracowników.

Odpowiedzi na wybrane pytania ankiety

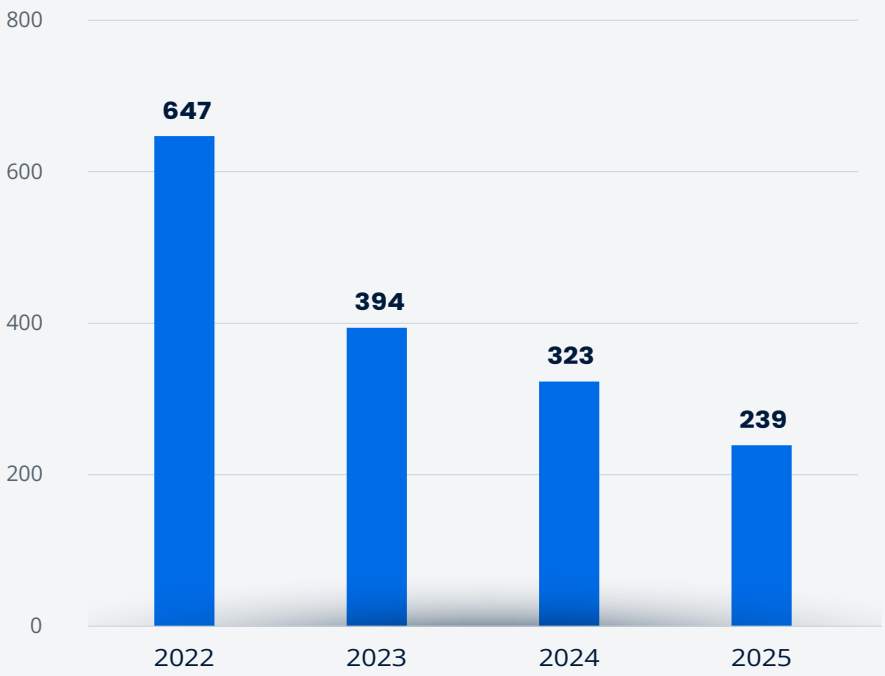
WYKRES 6. Odpowiedzi na pytanie: Czy w jednostce jest dedykowana osoba odpowiedzialna za cyberbezpieczeństwo



Wykres prezentuje rozkład odpowiedzi dotyczących organizacyjnego przypisania odpowiedzialności za cyberbezpieczeństwo. Około jedna trzecia jednostek posiada dedykowaną osobę ds. cyberbezpieczeństwa zatrudnioną w pełnym wymiarze czasu pracy. Nieco mniejsza grupa jednostek realizuje zadania z zakresu cyberbezpieczeństwa w formule niepełnego etatu, Ponad 34% jednostek nie wyznaczyło osoby odpowiedzialnej za cyberbezpieczeństwo.

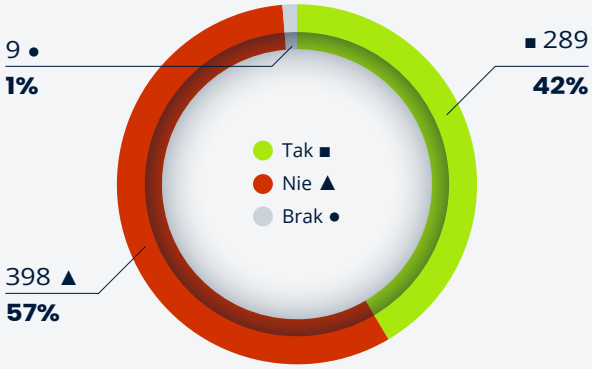
Kolejny wykres obrazuje liczbę jednostek, w których nie wskazano osoby odpowiedzialnej za cyberbezpieczeństwo, w ujęciu rocznym.

WYKRES 7. Liczba podmiotów, w których nie wskazano osoby odpowiedzialnej za cybernezpieczeństwo



W badaniach widoczny jest także spadek udziału w badanej próbie jednostek bez wyznaczonej odpowiedzialności za cyberbezpieczeństwo.

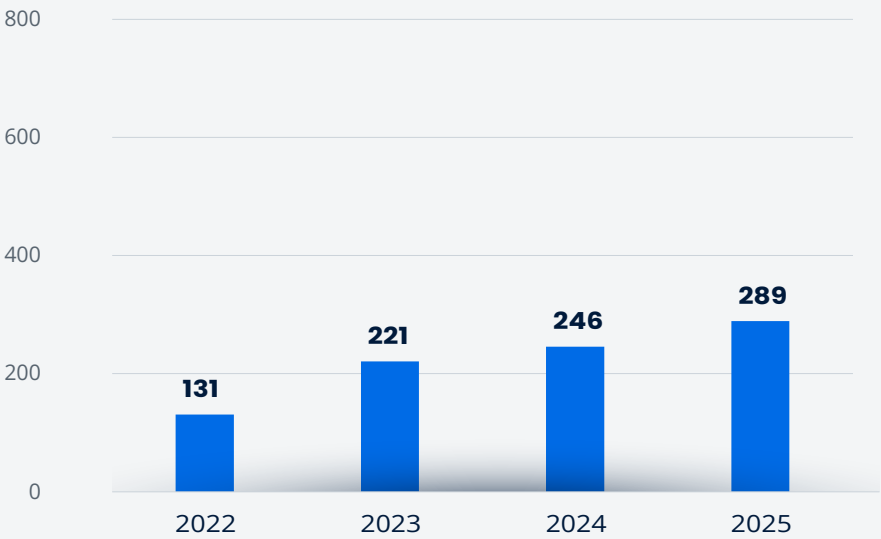
WYKRES 8. Odpowiedzi na pytanie: Czy dyrektor jednostki odbył szkolenie w zakresie cyberbezpieczeństwa w ciągu ostatniego roku?



Wykres 8. przedstawia rozkład odpowiedzi dotyczących udziału dyrektorów jednostek w szkoleniach z zakresu cyberbezpieczeństwa w ciągu ostatnich 12 miesięcy. Mniej niż połowa z ankietowanych dyrektorów uczestniczyła w takim szkoleniu w analizowanym okresie, natomiast zdecydowana większość nie brała udziału w żadnej formie doskonalenia w tym zakresie w ciągu ostatniego roku.

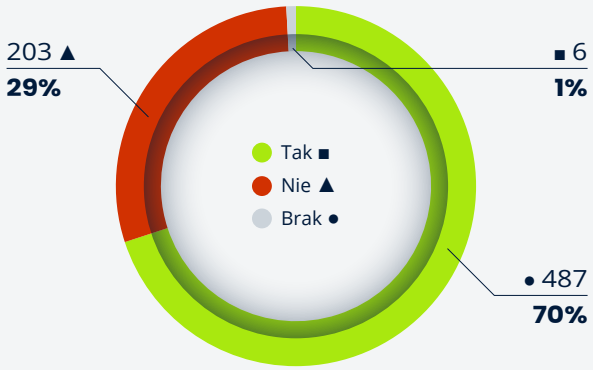
Kolejny wykres prezentuje, jak odpowiedzi na to pytanie kształtowały się w poszczególnych latach.

WYKRES 9. Liczba podmiotów deklarujących szkolenie kadry zarządzającej



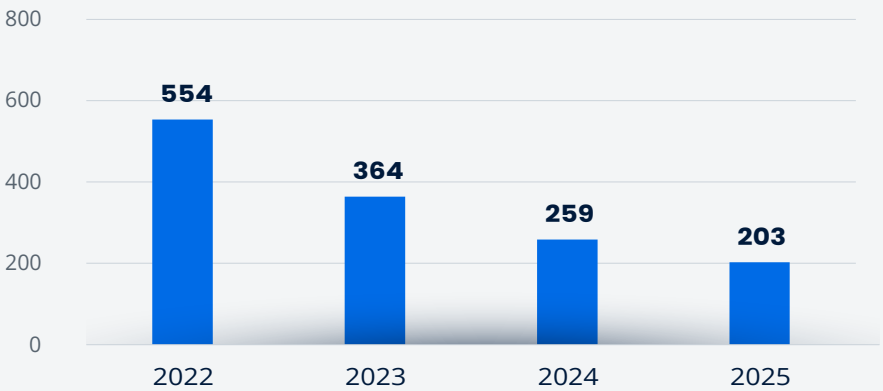
W latach 2022–2025 widoczny jest systematyczny wzrost udziału dyrektorów w szkoleniach z zakresu cyberbezpieczeństwa – z 131 osób w 2022 roku do 289 w 2025 roku. Mimo wyraźnego trendu wzrostowego, poziom uczestnictwa kadry kierowniczej nadal pozostaje relatywnie niski w odniesieniu do ogólnej liczby jednostek. Niedostateczne zaangażowanie dyrektorów w rozwijanie kompetencji w tym obszarze może ograniczać skuteczność podejmowanych decyzji zarządczych, a tym samym wpływać na poziom bezpieczeństwa informacji w organizacjach

WYKRES 10. Odpowiedzi na pytanie: Czy dyrektor jednostki cyklicznie przegląda raport oceny ryzyka w jednostce?



Zdecydowana większość dyrektorów deklaruje regularne zapoznawanie się z raportami oceny ryzyka. Niemal co trzeci nie robi tego jednak w sposób systematyczny, co może wskazywać na lukę w procesach zarządczych.

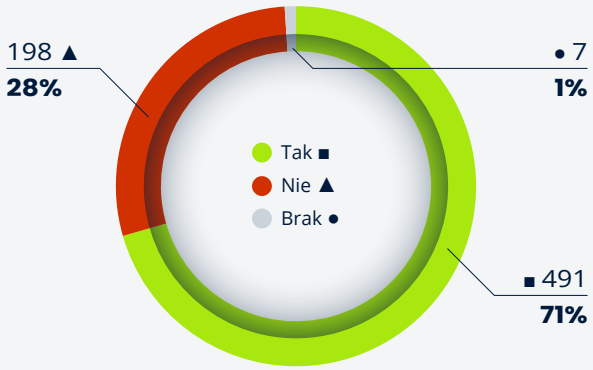
WYKRES 11. Liczba jednostek bez cyklicznego przeglądu raportów ryzyka



Wykres 11. przedstawia liczbę jednostek, w których dyrektor nie dokonuje cyklicznego przeglądu raportów oceny ryzyka w kolejnych latach.

W 2022 roku takich jednostek było 554, natomiast w kolejnych latach liczba ta systematycznie maleje (364 w 2023, 259 w 2024 i 203 w 2025), co może wskazywać na stopniowy wzrost dojrzałości w zakresie zarządzania cyberbezpieczeństwem.

WYKRES 12. Odpowiedzi na pytanie: Czy dyrektor jednostki opublikował politykę bezpieczeństwa jednostki z uwzględnieniem cyberbezpieczeństwa?

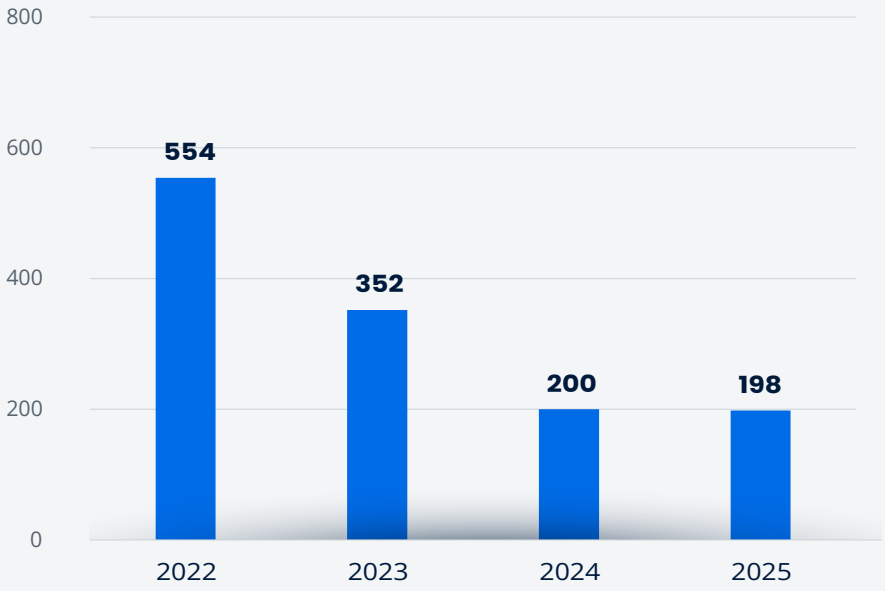


Na pytanie zawarte w ankiecie: „Czy dyrektor jednostki opublikował politykę bezpieczeństwa jednostki z uwzględnieniem cyberbezpieczeństwa?", większość respondentów udzieliła odpowiedzi twierdzącej – 491 jednostek (70,55%).

Jednocześnie 198 jednostek (28,45%) zaznaczyło brak publikacji takiej polityki, a 7 odpowiedzi (1,01%) oznaczono jako brak danych. Oznacza to, że choć polityka bezpieczeństwa uwzględniająca cyberbezpieczeństwo jest wdrożona w większości jednostek, to ponad jedna czwarta organizacji nadal nie posiada formalnie opublikowanego dokumentu w tym zakresie, co może ograniczać spójność i skuteczność działań związanych z ochroną informacji.

Polityka bezpieczeństwa stanowi podstawowy dokument określający zasady ochrony informacji oraz odpowiedzialności w organizacji. Jej brak może prowadzić do niespójnych działań oraz zwiększonego ryzyka wystąpienia incydentów związanych z cyberbezpieczeństwem.

WYKRES 13. Liczba podmiotów, które nie opublikowały polityki bezpieczeństwa



Wyniki ankiety wskazują na systematyczny spadek liczby jednostek, w których dyrektor nie opublikował polityki bezpieczeństwa – z 554 w 2022 roku, przez 352 w 2023 roku, do 200 w 2024 i 198 w 2025 roku.

Propozycje działań na rzecz cyberbezpieczeństwa sektora

CSIRT
Centrum e-Zdrowia

Analiza wyników ankiety z 2025 roku wskazuje na istotne zróżnicowanie poziomu dojrzałości w obszarze cyberbezpieczeństwa w badanych jednostkach. Mimo widocznego postępu w wielu obszarach, nadal identyfikujemy istotne luki zarówno w zakresie rozwiązań technicznych, jak i procesów organizacyjnych.

W odpowiedzi na zdiagnozowane wyzwania stworzyliśmy zestaw kluczowych rekomendacji, których wdrożenie pozwoli zwiększyć odporność jednostek na zagrożenia cybernetyczne oraz poprawić skuteczność zarządzania bezpieczeństwem informacji. Na podstawie zebranych i przeanalizowanych danych wskazujemy najważniejsze działania dla podmiotów sektora.

Wdrożenie pełnego procesu zarządzania kopiami zapasowymi

Prawidłowo wdrożone kopie odmiejscowione są jedną z kluczowych metod odzyskania ciągłości działania po udanym ataku oraz wdrożenie niezbędnych procedur oraz zaplecza technicznego w celu cyklicznego testowania odzyskiwania kopii zapasowych. Tylko wykonując testy można mieć pewność, że kopia jest prawidłowa i będzie użyteczna, jeżeli nastąpi konieczność przywrócenia działania systemu.

Monitorowanie nieautoryzowanego dostępu i potencjalnych zdarzeń cyberbezpieczeństwa

Wykrywanie nieuprawnionej aktywności w systemach pozwala na szybkie identyfikowanie prób włamań i umożliwia reagowanie, zanim dojdzie do poważnych szkód.

01. Segmentacja sieci

Część podmiotów nie stosuje lub nie wie, czy odpowiednia segmentacja sieci jest stosowana. Jest to istotne, ponieważ stosując odpowiednią segmentację sieci wewnętrznej można znacznie ograniczyć skuteczność ataków z użyciem ransomware.

02. Wdrożenie systemów klasy Firewall (FW), antywirus lub jego zaawansowane wersje (AV lub EDR/XDR) oraz dedykowane systemy kopii zapasowych

Nie da się zapewnić bezpieczeństwa bez tych elementarnych rozwiązań. Systemy klady EDR (Endpoint Detection and Response) oraz IPS (Intrusion Prevention System) lub IDS (Intrusion Detection System) są kluczowe dla cyberbezpieczeństwa. Z ankiety CSIRT CeZ wynika, że sytuacja uległa znacznej poprawie i są to coraz bardziej popularne rozwiązania w sektorze.

03. Wdrożenia MFA we wszystkich systemach, które przetwarzają wrażliwe dane

Część podmiotów nie wdrożyło takich rozwiązań lub jest na etapie wdrażania, a jest to jedna z podstawowych metod ochrony dostępu do danych.

04. Cykliczne monitorowanie podatności zarządzaną infrastrukturą

Ponad 43% podmiotów nie wdrożyło procesu zarządzania podatnościami. Każda nieusunięta lub niezabezpieczona w inny sposób podatność to potencjalna furtka dla atakującego.

05. Wdrożenie niezbędnych procesów zarządzania cyberbezpieczeństwem

Ponad 28% podmiotów nie publikuje polityk bezpieczeństwa. Ponad 16% nie zgłasza incydentów. Zapewnienie udokumentowanych procesów zarządzania cyberbezpieczeństwem jest kluczowe dla spójnego i skutecznego reagowania na zagrożenia, ponieważ ich brak utrudnia identyfikację incydentów oraz właściwe przypisanie odpowiedzialności i procedur działania.

Plany rozwoju CSIRT CeZ

CSIRT
Centrum e-Zdrowia

W 2026 roku planujemy konsekwentnie wzmacniać zdolności operacyjne CSIRT CeZ, rozwijać kompetencje zespołu oraz zwiększać zakres wsparcia dla podmiotów sektora ochrony zdrowia. Nasze działania koncentrują się zarówno na rozwoju narzędzi i infrastruktury, jak i na budowie nowoczesnego, skalowalnego modelu funkcjonowania, który odpowie na rosnące wymagania regulacyjne oraz dynamiczny wzrost liczby podmiotów objętych systemem cyberbezpieczeństwa.

Równolegle stawiamy na intensyfikację współpracy krajowej i międzynarodowej, rozwój działań edukacyjnych oraz dalsze podnoszenie poziomu dojrzałości organizacyjnej CSIRT CeZ, tak aby skuteczniej identyfikować zagrożenia i wspierać sektor w reagowaniu na incydenty cyberbezpieczeństwa.

Działania planowane do realizacji w 2026 r. obejmują:

- uruchomienie platformy e-learningowej, która umożliwi szeroki dostęp do szkoleń z cyberbezpeczeństwa w sektorze
- nowa strona CSIRT CeZ – prace są na zaawansowanym poziomie
- systematyczny rozwój działań w obszarze komunikacji, w tym dalsze zwiększenie liczby publikacji oraz intensyfikacja kontaktów z podmiotami sektora
- rozwój kadry CSIRT CeZ w związku z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa oraz radykalnym zwiększeniem liczby podmiotów sektora objętych zakresem ustawy - ze wstępnych szacunków wynika, że liczba podmiotów zwiększy się co najmniej z 238 operatorów usług kluczowych do ponad 2800 podmiotów kluczowych i ważnych
- wdrożenie działania w trybie całodobowym (24/7/365)
- dalszy rozwój współpracy krajowej oraz międzynarodowej, w tym bezpośrednich kontaktów z zespołami CSIRT z innych krajów - planujemy podpisanie porozumienia z zespołem Cyber WOT i Orange
- nowe projekty rozwojowe CSIRT CeZ, przeprowadzenie audytu dojrzałości oraz aktualizacja i opracowanie nowych procedur

- regularne wzmacnianie kompetencji zespołu CSIRT CeZ poprzez wyspecjalizowane szkolenia
- pozyskanie zasobów sprzętowych oraz programowych na potrzeby reagowania kryzysowego, czyli projekt Cyberkaretka, który obejmuje zakup 2 pojazdów oraz sprzętu. W wyposażeniu znadzie się podstawowy zestaw serwerów, urządzeń sieciowych oraz komputerów wraz z akcesoriami i oprogramowaniem, które są niezbędne do wsparcia podmiotów będących ofiarami incydentów
- utworzenie laboratorium na potrzeby zespołu CSIRT CeZ
- modernizacja stanowisk pracy zespołu CSIRT CeZ oraz stanowiska analizy śledczej (DFIR)
- wzmacnianie rozpoznawalności zespołu CSIRT CeZ oraz prowadzenie działań edukacyjnych
- zakup platformy szkoleniowej typu Cyber Range na potrzeby podnoszenia kompetencji zespołu CSIRT CeZ oraz ćwiczeń z podmiotami sektora
- pozyskanie narzędzi do wykonywania zautomatyzowanych testów oraz oceny podatności w podmiotach sektora ochrony zdrowia.

Spis wykresów

Spis rysunków

Centrum e-Zdrowia

Centrum e-Zdrowia

ul. Stanisława Dubois 5A,
00-184 Warszawa

+48 22 597 09 27

skrytka ePUAP:
/csiozgovpl/SkrytkaESP

biuro@cez.gov.pl

adres e-Doręczeń:
AE:PL-81405-68798-CIRHA-30

cez.gov.pl