

CZASOPISMO O CYFRYZACJI OCHRONY ZDROWIA

BLOG.OSOZ.PL

OSOZ

ISSN 1897-5828

RAPORT SPECJALNY

TWIERDZA DANYCH

Jak bronić się przed hakerami?
Poradnik dla placówek
ochrony zdrowia.

Rekomendacje CSIRT CeZ

Strategie ochrony danych

Rozmowy z ekspertami

Przykłady cyberataków

NIS2 krok po kroku

Cyberpsychologia

PODNIĘĆ POZIOM
OCHRONY DANYCH
MEDYCZNYCH

**163 STRONY
Z AKTUALNYMI
WYTYCZNYMI**



Bezpieczne dane

Poradnik dla placówek zdrowia



CYBERBEZPIECZEŃSTWO

Statystyki

- 4 Szokujące cyberataki i niepokojące statystyki. Ale dane medyczne można skutecznie chronić
- 7 Raport CSIRT CeZ: 60% więcej incydentów cyberbezpieczeństwa
- 13 Rekordowa liczba cyberataków w 2026 roku
- 17 Stan cyberbezpieczeństwa 2026. Alarmujące dane o potrzebach placówek zdrowia
- 21 Nie tylko MyDr. Największe cyberataki 2026 roku



NOWE METODY HAKERÓW

Porady ekspertów

- 27 Jeremi Olechnowicz: „Nie karzemy, nie wręczamy mandatów. Naszym zadaniem jest pomoc placówce zdrowia w obsłudze incydentu.”
- 35 Adam Haertle: Przy tych zabezpieczeniach to cud, że jest tak mało cyberataków
- 48 Norbert Przemyk, GCM: Szpital kontra hakerzy. Jak GCM chroni dane pacjentów?
- 57 Grzegorz Mródź: Cyberbezpieczeństwo danych. Jaka jest rola placówki zdrowia, a co zapewnia KAMSOF T?
- 63 W tym szpitalu cyberatak zabił pacjenta. Lekcje z kryzysu



PODSTAWY OCHRONY DANYCH

Zabezpiecz się przed atakami

- 69 Ochrona danych w modelu sera szwajcarskiego
- 73 Za 80% poziomem bezpieczeństwa odpowiada 20% bazowych zabezpieczeń
- 78 Jaki program antywirusowy? I czy Windows wystarczy, aby dobrze chronić dane?



- 83 Ochrona danych w indywidualnej praktyce lekarskiej. „Już za ok. 1400 zł rocznie można uchronić się przed 90 proc. ataków”
- 89 6 zasad ochrony przed ransomware i reguła 3-2-1

FIREWALL Z LUDZI

Jak wzmocnić umiejętności cyfrowe?

- 94 Podstępny phishing. Jak go rozpoznać i nie dać żadnej szansy hakerom?
- 98 Hakerzy nie mają skrupułów, ale może ich zatrzymać „firewall z ludzi”
- 104 Ochrona danych polega na budowaniu procedur bezpieczeństwa wokół pracownika
- 111 Mikro-wycieki danych to plaga. „Wystarczy poczekać kilka minut przy drukarce”
- 115 Cyberpsychologia. Nowe narzędzie do walki z hakerami

SZTUCZNA INTELIGENCJA

Nowe zagrożenia i metody ochrony

- 122 Co dzieje się z danymi, które lekarz wpisuje do chatbotów jak ChatGPT?
- 128 Co to jest i jak wdrożyć strategię „zerowego zaufania”?
- 133 Tak ChatGPT pomoże wzmocnić poziom cyberbezpieczeństwa

TRENDY CYBERBEZPIECZEŃSTWA

Strategie liderów

- 139 Crash testy bezpieczeństwa danych w szpitalach. Jak się je przeprowadza?
- 143 Placówka medyczna padła ofiarą hakerów. Co robić?
- 147 5 sposobów, jak uniknąć kary Urzędu Ochrony Danych Osobowych
- 153 NIS2 w placówce zdrowia. Od czego zacząć?



Szokujące cyberataki i niepokojące statystyki. Ale dane medyczne można skutecznie chronić

Po największym w historii Polski cyberataku przeprowadzonym na MyDr i czarnej serii innych incydentów, wszyscy zadają sobie pytanie: Co zrobić, aby dane pacjentów były bezpieczne?

» Każda placówka musi szczerze zadbać o bezpieczeństwo danych. Tej odpowiedzialności nie da się zrzucić na dostawcę IT. «

Żaden inny atak hakerów – a tych było kilka w ostatnich miesiącach – nie wywołał takiej burzy jak wyciek danych ok. 19 mln osób w wyniku ataku na dostawcę oprogramowania gabinetowego MyDr. To jeden z największych cyberataków w historii Polski. Niezależnie od wyników śledztwa w tej sprawie, od dawna wiemy, że ochrona danych medycznych w placówkach zdrowia jest niewystarczająca. Cyberatak zbiegł się w czasie z corocznym raportem Centrum e-Zdrowia na temat poziomu cyfryzacji i cyberbezpieczeństwa w placówkach zdrowia. Wynika z niego jasno: placówkom zdrowia brakuje kompetencji w zakresie cyberbezpieczeństwa.

Problem jest stary jak cyfryzacja ochrony zdrowia. I niestety – jak podkreślają eksperci – nie rozwiążą go żadne nowe inicjatywy legislacyjne. Nawet „Cyber Piątka”, choć zawiera kilka pomysłów idących w dobrym kierunku, nie sprawi cudów.

Z cyberatakami mierzy się cały świat. Hakerzy kradną dane i paraliżują działanie placówek zdrowia, co w kilku przypadkach doprowadziło do śmierci pacjentów. Ale nie oznacza to, że placówki medyczne są zupełnie bezbronne w walce z hakerami. Dane są kradzione przez hakerów-amatorów, którzy wykorzystują znane od dawna luki. Przykładowo, za zdecydowaną większość udanych cyberataków odpowiada phishing – gdy pracownik kliknie w zainfekowany załącznik albo link. Najlepszą ochroną przed nimi jest wiedza o metodach socjotechniki, po które sięgają hakerzy. Z kolei włamanie do systemów komputerowych, wymagające celowego i skoordynowanego ataku doświadczonej grupy hakerów albo działania osoby z wewnątrz organizacji (tzw. insidera), są rzadkością.

Często powtarza się, że człowiek jest najsłabszym ogniwem w bezpieczeństwie danych. W naszym raporcie pokazujemy, że **pracownik jest najmocniejszym ogniwem w ochronie danych**. Tłumaczymy, jak chronić dane niskim kosztem, przypominamy podstawowe zalecenia ekspertów oraz prezentujemy nowe metody działania hakerów i sposoby walki z nimi.

Cyberbezpieczeństwo nie jest sztuką wyższą, czymś zarezerwowanym dla wybranych placówek zatrudniających ekspertów

»Cyberataki nie mogą być argumentem przeciwko inwestycjom w cyfryzację i AI. Oznaczałoby to rezygnację z ogromnych korzyści, jakie technologie te mogą przynieść pacjentom. «

ds. ochrony danych i posiadających duże budżety na ten cel. To nie jest jakieś jedno wybrane działanie, oprogramowanie albo szkolenie, które zapewni 100-proc. ochronę i spokój. Cyberochrona to procedury, które są przestrzegane w praktyce, systemy IT projektowane w filozofii „ochrony na etapie projektowania”, wyszkoleni ludzie i filozofia pracy z myślą o ochronie danych – cały system zabezpieczeń organizacyjnych i technologicznych wkomponowany w codzienną działalność placówki zdrowia.

Adam Haertle, ekspert ds. cyberbezpieczeństwa, porównuje cyberbezpieczeństwo do zamku z tysiącem okien. Hackerowi wystarczy tylko jedno źle strzeżone wejście, aby dostać się do środka. Ale nawet jeśli mu się to uda, złodziej musi jeszcze przejść przez korytarze, kolejne drzwi, posterunki straży, aby w końcu przełamać kraty dzielące go od skarbu. Dopiero jeśli wszystkie te bariery zawiodą, kradzież zakończy się sukcesem. Dlatego szczelna ochrona danych polega na stworzeniu możliwie największej liczby poziomów zabezpieczeń. Nawet jeśli haker złamie jeden z nich, polegnie na kolejnym. Im więcej tych zabezpieczeń, szansa, że cyberatak się uda, maleje proporcjonalnie. W momencie przygotowywania tego raportu dowiedzieliśmy się o kolejnych dwóch poważnych incydentach związanych z bezpieczeństwem danych. Nie zmienia to jednak faktu, że przestrzeganie podstawowych zasad bezpieczeństwa nadal zapewnia wysoki poziom ochrony danych. Dlatego każda placówka ochrony zdrowia, niezależnie od wielkości, powinna uczciwie odpowiedzieć sobie na pytanie: Czy należyście chronimy dane? A jeśli nie – dlaczego tak się dzieje i co możemy zrobić, aby to zmienić?

Nasz raport porządkuje nowe metody ochrony i radzi, jak zaktualizować strategię cyberochrony w czasach szybkiego rozwoju sztucznej inteligencji. Na bieżąco piszemy o tym na blogu OSOZ – zachęcamy do zaprenumerowania newslettera blogu OSOZ, a informacje o cyfryzacji i e-zdrowiu trafią dwa razy w miesiącu na Państwa skrzynkę mailową. ●



Więcej o e-zdrowiu?

Zapisz się do newslettera OSOZ!





Raport CSIRT CeZ: 60% więcej incydentów cyberbezpieczeństwa

W 2025 roku, kolejny rok z rzędu, rosła skala ataków hakerów na placówki ochrony zdrowia. CSIRT Centrum e-Zdrowia obsłużył 1441 incydentów cyberbezpieczeństwa, o ponad 60 proc. więcej niż rok wcześniej – wynika z raportu „Krajobraz cyberbezpieczeństwa w sektorze ochrony zdrowia”. Dobra wiadomość: coraz więcej placówek zdrowia wdraża systemy zarządzania bezpieczeństwem informacji.

Phishing największym zagrożeniem. Hakerzy atakują, gdy spada czujność

W 2023 roku odnotowano 435 incydentów bezpieczeństwa danych w sektorze zdrowia, rok później już 1028, a w 2025 roku liczba ta wzrosła do 1441.

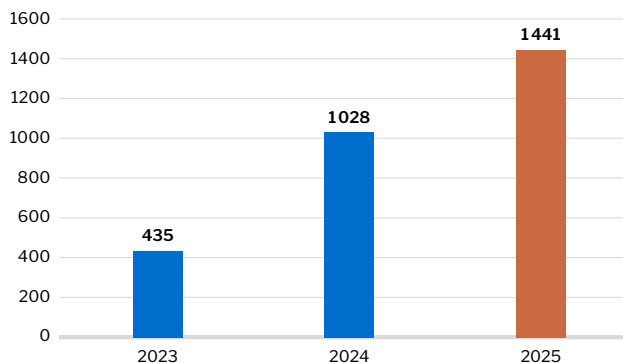
Konsekwencje ataków hakerów wykraczają daleko poza utratę danych, prowadząc do zaburzenia pracy oddziałów, utrudnionego dostępu do dokumentacji medycznej i zagrażając bezpieczeństwu pacjentów.

Największą kategorię incydentów w 2025 roku stanowiły oszustwa komputerowe (phishing). Odnotowano ich aż 580. Drugą najczęstszą grupą były podatne usługi (344). Łącznie te dwa typy zagrożeń odpowiadały za niemal dwie trzecie wszystkich incydentów zgłoszonych do CSIRT CeZ.

Cyberprzestępcy coraz rzadziej wysyłają prymitywne wiadomości z błędami językowymi. W zamian przygotowują profesjonalnie wyglądające kampanie, które wykorzystują zaufanie do znanych instytucji ochrony zdrowia.

W ubiegłym roku przestępcy podszywali się między innymi pod NFZ, RPWDL, gabinet.gov.pl, eZUS czy dostawców IT. Lekarze otrzymywali wiadomości informujące o konieczności aktualizacji certyfikatów lub groźbie utraty możliwości

Liczba incydentów w sektorze ochrony zdrowia w latach 2023–2025 (źródło: CSIRT CeZ)



Klasyfikacja częstotliwości występowania incydentów według kategorii (źródło: CSIRT CeZ)



wystawiania e-recept. Linki prowadziły do fałszywych stron logowania, których celem było przejęcie haseł dostępu. Szczególnie niebezpieczne były kampanie wykorzystujące markę NFZ. Cyberprzestępcy oferowali rzekome „darmowe apteczki” za symboliczną opłatą, kierując użytkowników na spreparowane strony płatnicze.

Na czwartym miejscu jest szkodliwe oprogramowanie, czyli ransomware.

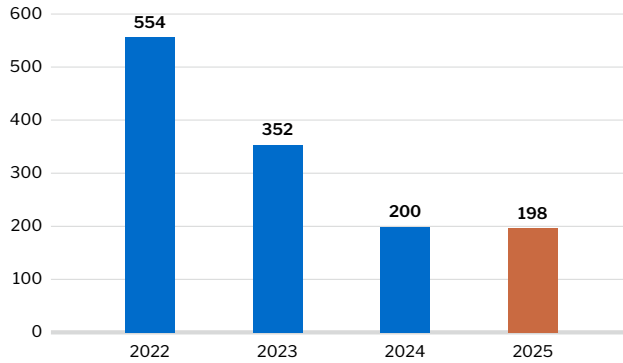
Choć najmniej incydentów w skali miesiąca występuje w lipcu i sierpniu, czujność trzeba zachować zawsze. Hakerzy wykorzystują obniżoną czujność, a do ataków często dochodzi nocą, gdy działy IT kończą pracę.

W wielu szpitalach nadal brakuje bazowych zabezpieczeń, ale sytuacja się poprawia

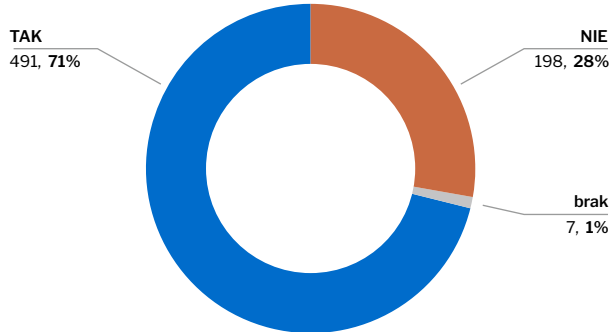
W 2025 roku CSIRT CeZ przeprowadził testy bezpieczeństwa infrastruktury w ośmiu podmiotach medycznych. Wniosek: najczęściej wykrywane problemy mają charakter organizacyjny i dotyczą podstawowego utrzymania infrastruktury IT. Na liście nieprawidłowości znalazły się brak aktualizacji oprogramowania, wygasłe certyfikaty SSL, korzystanie z przestarzałych protokołów komunikacyjnych oraz systemów operacyjnych, które od dawna nie są już wspierane przez producentów.

»Cyberprzestępcy często podszywają się pod NFZ, RPWDL, gabinet.gov.pl, eZUS czy dostawców IT, aby uśpić czujność ofiary.«

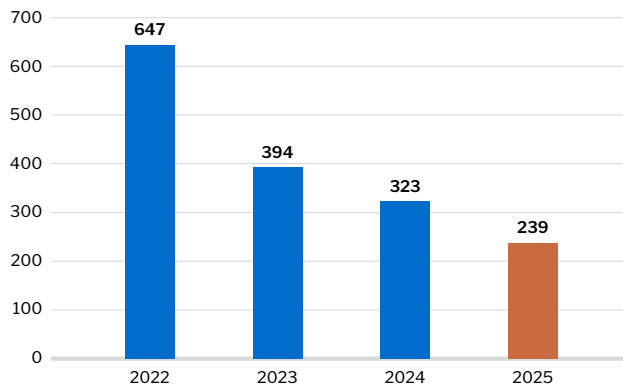
Liczba podmiotów, które nie opublikowały polityki bezpieczeństwa (źródło: CSIRT CeZ)



Czy dyrektor opublikował politykę bezpieczeństwa z uwzględnieniem cyberbezpieczeństwa? (źródło: CSIRT CeZ)



Liczba podmiotów, w których nie wskazano osoby odpowiedzialnej za cyberbezpieczeństwo (źródło: CSIRT CeZ)



»Nieaktualizowane oprogramowanie albo wygasłe certyfikaty SSL – placówki zdrowia często zaniedbują bazowe kwestie cyberbezpieczeństwa.«

Eksperti wykrywali również publicznie dostępne panele administracyjne oraz otwarte porty usług takich jak SSH (Secure Shell, usługa umożliwiająca zdalne zarządzanie serwerami i urządzeniami IT), RDP (Remote Desktop Protocol, protokół pozwalający na zdalne połączenie z komputerem i pracę tak, jakby użytkownik siedział przed nim), SMB (Server Message Block, protokół wykorzystywany do udostępniania plików, folderów i drukarek w sieci) czy Telnet (starszy protokół do zdalnego dostępu do urządzeń i systemów). Dla cyberprzestępców stanowią one potencjalną furtkę umożliwiającą uzyskanie dostępu do systemów szpitalnych.

Autorzy raportu zwracają uwagę, że cyberbezpieczeństwo musi być elementem strategii działania placówki zdrowia i tematem, którym zajmuje się także kadra zarządzająca placówkami ochrony zdrowia, a nie tylko informatycy.

Badanie CSIRT CeZ sugeruje, że świadomość zagrożeń rośnie. Już 76 proc. jednostek deklaruje wdrożenie systemu zarządzania bezpieczeństwem informacji. W 2025 roku szkolenia w tym zakresie ukończyło 42 proc. dyrektorów badanych placówek, a 70 proc. cyklicznie zapoznaje się z przeglądem ryzyka w jednostce. 60 proc. placówek posiada dedykowane stanowisko i osobę odpowiedzialną za cyberbezpieczeństwo. Z roku na rok spada liczba podmiotów, w których nie wskazała takiej osoby.

Raport pokazuje też, że wiele placówek nadal nie posiada podstawowych dokumentów i procedur. Ponad 28 proc. organizacji nie ma opublikowanej polityki bezpieczeństwa.

Jak podkreślają autorzy raportu, „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.”

CSIRT CeZ przygotowuje się na jeszcze trudniejsze lata

Flagowym projektem mającym zwiększyć poziom cyberochrony w kluczowych podmiotach zdrowia jest wdrożenie zapisów

nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC) adaptującej dyrektywę NIS2. Nowe przepisy poszerzają liczbę podmiotów zobowiązanych do wdrażania środków bezpieczeństwa, zarządzania ryzykiem oraz raportowania incydentów.

Dla organizacji będących podmiotami kluczowymi według NIS2, oznacza to konieczność stworzenia nowych procedur, przeprowadzenia analiz ryzyka, przeszkolenia pracowników, realizacji regularnych audytów oraz wdrożenia mechanizmów monitorowania zagrożeń.

CSIRT CeZ jest świadomy, że incydentów będzie nadal przybywać, a nowe metody ataków z wykorzystaniem AI zwiększą skalę zagrożeń. Dlatego planuje m.in. wdrożenie ciągłego modelu pracy 24 godziny na dobę przez siedem dni w tygodniu. Dzięki temu możliwe będzie szybsze reagowanie na incydenty oraz skuteczniejsze wsparcie placówek medycznych.

Centrum e-Zdrowia będzie nadal szkolić w zakresie cyberbezpieczeństwa. CSIRT CeZ zapowiada też „Cyberkaretkę”, której zadaniem będzie wsparcie organizacji w sytuacjach kryzysowych związanych z cyberatakami.

W badaniu poziom cyberbezpieczeństwa uczestniczyło 696 podmiotów. Ankieta była skierowana do szpitali podlegających bezpośrednio Ministerstwu Zdrowia, czyli około 1600 podmiotów. W badaniu wzięło więc udział 43% potencjalnych respondentów. ●



Kliknij tutaj, aby pobrać raport CSIRT CeZ



Wnętrze CSIRT CeZ (zdjęcie: Centrum e-Zdrowia)

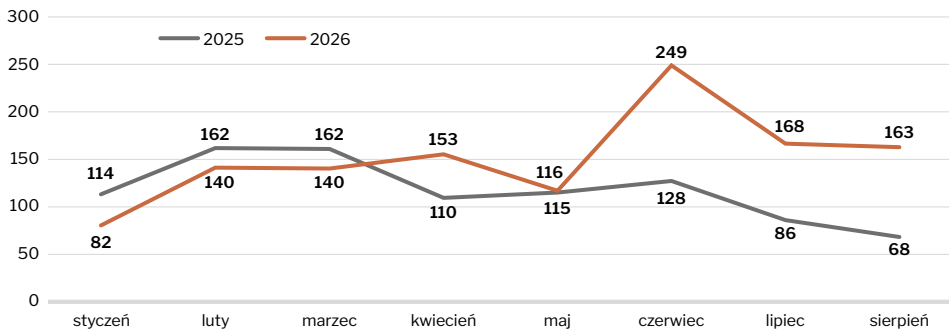
Rekordowa liczba cyberataków w 2026 roku

Tylko do końca września 2026 roku do CSIRT CeZ zgłoszono 1379 incydentów bezpieczeństwa danych. W czerwcu br. było ich 249 (o 94% więcej niż w czerwcu 2025 roku), w lipcu – 168 (+95%), a w sierpniu – 163 (+140%) – poinformowali przedstawiciele Ministerstwa Zdrowia i Centrum e-Zdrowia. To oznacza rekordowy średni wzrost o 110% w miesiącach czerwiec–sierpień.

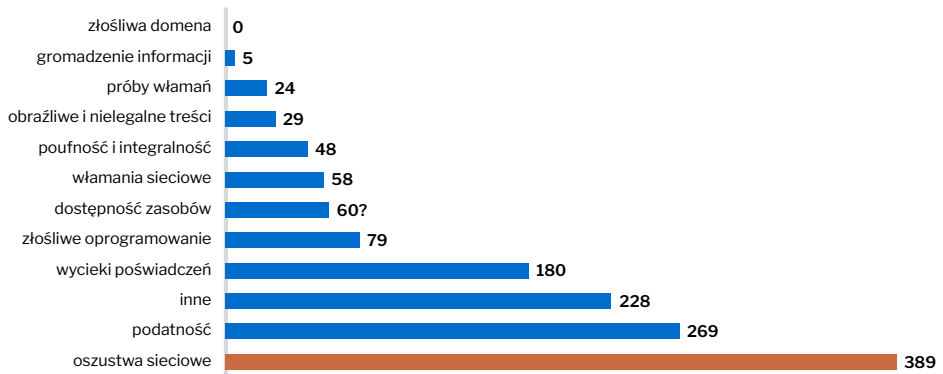
Od czerwca 2026 roku obserwujemy wyjątkową aktywność hakerów

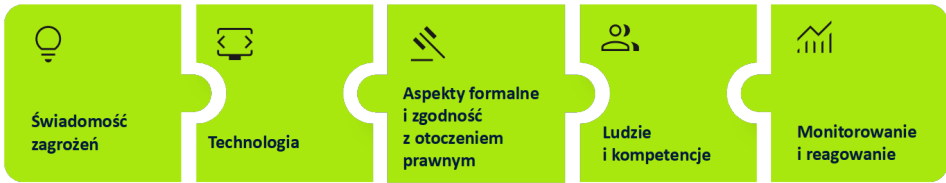
W ciągu ostatnich 3 lat liczba incydentów w ochronie zdrowia wzrosła 6-krotnie. W całym 2025 roku było ich 1441, a najczęściej rejestrowano oszustwa komputerowe, w tym phishing (580 przypadków), podatne usługi (344), wycieki poświadczeń (148), oraz szkodliwe oprogramowanie (146). Oszustwa i podatne usługi stanowiły razem około 64% zdarzeń.

Suma incydentów bezpieczeństwa danych w placówkach zdrowia w okresie styczeń-sierpień dla lat 2025 i 2026. W drugim półroczu widać wyraźny wzrost (źródło: Centrum e-Zdrowia)



Przyczyny incydentów bezpieczeństwa danych w placówkach zdrowia w 2026. Dominują oszustwa sieciowe (źródło: Centrum e-Zdrowia)





– Odpowiedzialność za bezpieczeństwo w sieci przypomina puzzle, które tworzą spójny obraz działań, zaczynając od zwiększania świadomości o zagrożeniach, przez wykorzystanie technologii i w końcu kompetencje ludzkie – mówi Jeremi Olechnowicz, dyrektor Pionu Eksploatacji Systemów Teleinformatycznych w Centrum e-Zdrowia.

Szczególnie w drugiej połowie 2026 roku mocno wzrosła liczba incydentów bezpieczeństwa danych – od czerwca do sierpnia o średnio 110%. Pod względem rodzaju zagrożeń, 2026 rok jest bardzo podobny do poprzednich lat. Dominują oszustwa komputerowe – do sierpnia br. zarejestrowano ich 389.



CSIRT CeZ dysponuje cyberkaretą. To specjalistyczny pojazd, wyposażony w autonomiczne źródła zasilania, zaawansowane systemy łączności satelitarnej i 5G oraz mobilną infrastrukturę teleinformatyczną. Jej zadaniem jest pomoc, gdy dojdzie do ataku hakerów (źródło: Centrum e-Zdrowia)

» W ostatnich tygodniach ofiarą ataków hakerów padły MyDr, Medyc, Felg Dent oraz Enel-Med. «

Z kolei badania przeprowadzone na przełomie 2025 i 2026 roku przez CSIRT CeZ wskazują, że 76% jednostek deklarowało wdrożenie systemu zarządzania bezpieczeństwem informacji, ale ponad 28% nie posiadało opublikowanej polityki bezpieczeństwa, a około 29% dyrektorów nie dokonywało regularnych przeglądów oceny ryzyka.

– Więcej usług dostępnych online to wygoda dla pacjenta, ale też wspólna odpowiedzialność instytucji państwowych, kierowników placówek i dostawców oprogramowania – mówił wiceminister zdrowia Tomasz Maciejewski prezentując nowe statystyki.

Jeremi Olechnowicz, dyrektor Pionu Eksploatacji Systemów Teleinformatycznych w Centrum e-Zdrowia, podkreślał, że odpowiedzialność za cyberbezpieczeństwo obejmuje świadomość zagrożeń, stosowanie odpowiednich technologii oraz kompetencje pracowników. To proces ciągły, dlatego organizacje muszą stale inwestować w ochronę swoich systemów i danych. Ważne jest także śledzenie wykrytych podatności i kampanii phishingowych oraz stosowanie odpowiednich procedur i dobrych praktyk. ●

Co to jest CSIRT CeZ?

CSIRT CeZ (CSIRT – skrót z angielskiego *Computer Security Incident Response Team*, po polsku *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego*) powstał w grudniu 2023 r. jako drugi sektorowy CSIRT w Polsce. Jest jedynym CSIRT-em sektorowym w obszarze zdrowia w Polsce, a do jego ustawowych zadań należą:

- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów;
- wspieranie podmiotów kluczowych i ważnych (w rozumieniu KSC) poprzez:
 - udzielenie sprzętu,
 - wiedzę merytoryczną,
 - koordynację działań, mających na celu usunięcie skutków incydentu;
- analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu;
- współpraca z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.



Stan cyberbezpieczeństwa 2026. Alarmujące dane o potrzebach placówek zdrowia

Poziom cyberbezpieczeństwa placówek zdrowia z roku na rok się poprawia, ale zaległości są nadal ogromne – wynika z raportu Centrum e-Zdrowia.

W najnowszej, 9. edycji Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą, Centrum e-Zdrowia zapytało o poziom cyberbezpieczeństwa i potrzeby z tym związane.

Potrzeby podmiotu/praktyki w zakresie cyberbezpieczeństwa (źródło: Centrum e-Zdrowia)

Potrzeby w zakresie cyberbezpieczeństwa	Szpitalne	Inne niż szpitalne	AŚZ
Zwiększenie odporności na cyberataki	87,0%	68,3%	46,0%
Zwiększenie ochrony danych osobowych	69,6%	55,8%	42,8%
Poprawa stanu wiedzy o zagrożeniach informatycznych wśród pracowników/kierownictwa jednostki	78,7%	64,0%	39,6%
Uświadomienie ryzyka związanego ze stosowaniem systemów informatycznych	70,5%	56,8%	32,0%
Poprawa ciągłości działania systemów informatycznych	72,5%	50,8%	31,2%
Zwiększenie ochrony poczty elektronicznej	60,2%	41,3%	31,1%
Zwiększenie ochrony stacji końcowych lub serwerów	64,0%	45,5%	23,3%
Poprawa bezpieczeństwa przetwarzania informacji w systemach medycznych, np. aplikacjach gabinetowych	41,6%	28,8%	22,1%
Poprawa zarządzania ryzykiem w jednostce	60,3%	42,4%	19,9%
Poprawa procesu bezpiecznego zarządzania uprawnieniami	52,0%	33,4%	14,9%
Żadne z powyższych	2,7%	8,8%	26,5%

W każdym rodzaju PWDL zaznaczono po 3 najczęściej wskazywane potrzeby w zakresie cyberbezpieczeństwa

Jakie działania podmiot/praktyka prowadzi w zakresie zapewnienia cyberbezpieczeństwa? (źródło: Centrum e-Zdrowia)

Działania prowadzone w zakresie cyberbezpieczeństwa	Szpitalne	Inne niż szpitalne	AŚZ
Monitorowanie bezpieczeństwa teleinformatycznego podmiotu	81,0%	65,9%	44,8%
Szkolenia lub inne działania edukacyjne dla pracowników dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa	63,2%	49,0%	33,4%
Opracowanie procedury zgłaszania incydentów	51,0%	35,7%	21,8%
Przeprowadzenie audytu bezpieczeństwa informacji	55,7%	36,2%	17,8%
Opracowanie i przyjęcie kompleksowej Polityki Bezpieczeństwa Informacji (BIP)	59,5%	37,8%	16,4%
Zidentyfikowanie kluczowych aktywów informacyjnych (zbiory danych/systemy/usługi) podmiotu, które należy chronić	51,2%	31,7%	16,2%
Coroczne szkolenie kierownika podmiotu/praktyki z zakresu cyberbezpieczeństwa	27,5%	17,0%	12,0%
Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) w procesach wpływających na świadczenie usług	54,2%	30,1%	11,2%

W każdym rodzaju PWDL zaznaczono po 3 najczęściej wskazywane potrzeby w zakresie cyberbezpieczeństwa

Zespół ds. cyberbezpieczeństwa posiada 40,6 proc. badanych szpitali, 31,4 proc. podmiotów innych niż szpitalne oraz 25,5 proc. AŚZ. W przypadku tych ostatnich aż 74,5 proc. respondentów wskazało, że takiego zespołu nie ma. Tam, gdzie zespoły funkcjonują, są one zazwyczaj bardzo małe – w ponad 90 proc. liczą maksymalnie 5 osób.

Własny zespół informatyczny posiada 43,4 proc. szpitali. W podmiotach innych niż szpitalne najczęściej wykorzystywana jest obsługa zewnętrzna (34,7 proc.); w AŚZ outsourcing wskazało 43,2 proc. placówek.

W porównaniu z wynikami badania z 2024 roku praktycznie nie zmienił się odsetek placówek posiadających zespoły ds. cyberbezpieczeństwa.

Półowa szpitali nie ma systemu zarządzania bezpieczeństwem informacji

Największym wyzwaniem wskazywanym przez szpitale jest zwiększenie odporności na cyberataki – potrzebę taką deklaruje 87 proc. placówek. Na kolejnych miejscach znalazły się poprawa wiedzy pracowników i kierownictwa o zagrożeniach informatycznych (78,7 proc.), poprawa ciągłości działania systemów (72,5 proc.), zwiększenie ochrony danych osobowych (69,6 proc.), ochrona stacji końcowych i serwerów (64 proc.) oraz poczty elektronicznej (60,2 proc.).

W podmiotach innych niż szpitalne, potrzeby w zakresie zwiększenia odporności na cyberataki deklaruje 68,3 proc. ankietowanych. 64 proc. dostrzega konieczność poprawy wiedzy pracowników, a 55,8 proc. – zwiększenia ochrony danych osobowych. W przypadku AŚZ, 42,8 proc. placówek wskazuje na konieczność zwiększenia ochrony danych osobowych, a 46 proc. na potrzebę zwiększenia odporności na cyberataki.

Co robią podmioty medyczne, aby chronić swoje dane?

W przypadku szpitali najczęściej wymienia się monitorowanie bezpieczeństwa teleinformatycznego (81 proc.) oraz szkolenia pracowników dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa (63,2 proc.). 59,5 proc. szpitali deklaruje

» Aż 87 proc. szpitali widzi potrzebę zwiększenia odporności na cyberataki. «

opracowanie i przyjęcie kompleksowej Polityki Bezpieczeństwa Informacji, 55,7 proc. przeprowadzenie audytu bezpieczeństwa informacji, a 51 proc. – opracowanie procedury zgłaszania incydentów. System zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług wdrożyło 54,2 proc. szpitali.

Liczba jednostek, w których dyrektor nie opublikował polityki bezpieczeństwa, spadła z 554 w 2022 r. do 352 w 2023 r., 200 w 2024 r. i 198 w 2025 r. Oznacza to spadek o 356 jednostek, czyli o 64 proc. w ciągu czterech lat.

Brak znajomości norm, niskie kompetencje pracowników

Zaskakuje też niska znajomość systemu zarządzania bezpieczeństwem informacji. Placówki nie wiedzą, jakie normy stosują w tym obszarze. Normę PN-EN ISO/IEC 27001 wskazuje 42,3 proc. szpitali, 24 proc. podmiotów innych niż szpitalne i 10,2 proc. AŚZ. Jednocześnie 28 proc. szpitali, 42,5 proc. podmiotów innych niż szpitalne i aż 65 proc. AŚZ odpowiada, że nie wie, jakie normy są uwzględniane w ich systemie zarządzania bezpieczeństwem informacji.

Bezpieczeństwo pozostaje jednym z hamulców dalszej cyfryzacji. 17,3 proc. wszystkich badanych PWDL wskazuje problemy lub obawy związane z bezpieczeństwem IT i ochroną danych. Większą barierą są jednak brak pieniędzy na inwestycje IT (63,3 proc.) i niewystarczające kompetencje cyfrowe pracowników (36,5 proc.).

Potrzebę poprawy kompetencji w zakresie bezpieczeństwa danych deklaruje 95,9 proc. pracowników szpitali, 89,2 proc. podmiotów innych niż szpitalne i 83,5 proc. AŚZ. Choć w poprzednich edycjach pytanie lekko się różniło, to w oczy rzuca się rosnący z roku na rok popyt na szkolenia z cyberbezpieczeństwa. ●

» 95,9 proc. szpitali wskazuje cyberbezpieczeństwo i ochronę danych pacjentów jako obszar, w którym pracownicy chcą się szkolić. «



Nie tylko MyDr. Największe cyberataki 2026 roku

Wyciek danych 19 mln pacjentów w efekcie cyberataku na MyDr nie jest wyjątkiem. Oto inne, duże ataki hakerów, które miały miejsce w ostatnich miesiącach.

Kasowanie danych u producenta sprzętu medycznego, paraliż wodociągów

Jednym z najgłośniejszych incydentów był atak na producenta sprzętu medycznego Stryker. 11 marca br. firma nagle utraciła dostęp do części globalnej infrastruktury Microsoftu, co zakłóciło przetwarzanie zamówień, produkcję i wysyłkę produktów.

To nie było ani ransomware, ani malware. Nie pojawiło się nawet żądanie okupu. Celem była destabilizacja działalności firmy. Z dotychczasowych ustaleń wynika, że napastnicy wykorzystali złośliwy plik do wykonywania poleceń w środowisku Microsoft Intune. W ten sposób hakerom udało się wykasować dane z komputerów w wewnętrznej sieci. Stryker został zmuszony do ręcznej obsługi części zamówień i ogromnych zmian organizacyjnych, w tym uruchomienia dodatkowych zmian, aby dostarczyć zamówiony sprzęt na czas.

W maju 2026 r. ofiarą cyberataku padła platforma edukacyjna Canvas. Grupa hakerów ukrywająca się pod pseudonimem ShinyHunters poinformowała, że uzyskała dostęp do około 3,65 TB danych i wykradła dane nawet 275 mln użytkowników. Z Canvas korzysta tysiące szkół, uczelni i instytucji edukacyjnych na całym świecie. Napastnicy zażądali okupu, grożąc publikacją skradzionych informacji.

W lutym doszło do ataku na Substack – amerykańską platformę internetową do publikowania treści dostępnych w ramach płatnego abonamentu: newsletterów, artykułów, podcastów i materiałów wideo. Cyberprzestępcy uzyskali dostęp do danych użytkowników platformy, w tym adresów e-mail i numerów telefonów. Według dostępnych ekspertyz, cyberprzestępcy wykorzystali słabość w systemach i niewystarczające mechanizmy kontroli dostępu. Ostatecznie opublikowali wykradzione dane – czyli 697 tys. rekordów – w internecie.

» Do ataków najczęściej dochodzi w nocy, gdy pracownicy działów IT śpią. «

Pod koniec lipca 2026 r. doszło do serii ataków na co najmniej 30 miejskich systemów wodociągowych w USA. Hakerzy zaatakowali podpięte do internetu sterowniki PLC firmy Rockwell Automation, czyli urządzenia sterujące fizycznymi procesami w infrastrukturze wodociągowej.

FBI poinformowało, że incydenty dotknęły przedsiębiorstwa wodociągowe w co najmniej 7 stanach. W części przypadków ataki doprowadziły do zakłócenia działania systemów uzdatniania i dystrybucji wody.

Odwołane operacje i przerwy w leczeniu na całym świecie

Aż 3 miesiące trwał atak na największy publiczny system ochrony zdrowia w Stanach Zjednoczonych, czyli NYC Health + Hospitals. Łupem padły dane co najmniej 1,8 mln osób. Po tym, jak hakerzy uzyskali dostęp do sieci wewnętrznej, krok po kroku – aby nie wykryły tego systemy cyberbezpieczeństwa – kopiowali pliki zawierające dane osobowe, dokumentację medyczną, informacje finansowe oraz dane biometryczne, w tym skany odcisków palców i dłoni.

W kwietniu, z pomocą ransomware, hakerzy zaatakowali Chip-Soft, dostawcę systemów informatycznych dla holenderskich szpitali. Co najmniej 11 szpitali musiało czasowo ograniczyć korzystanie z oprogramowania i przejść na dokumentację papierową.

Kolejny cyberatak wymierzony został w 1500 lekarzy korzystających z systemów francuskiego dostawcy oprogramowania medycznego Cegedim Santé. Wyciekły dane nawet 15 mln osób. W Australii cyberprzestępcy uzyskali dostęp do danych z co najmniej 21 klinik sieci Partnered Health. Wśród przejętych informacji znalazły się nazwiska, daty urodzenia, adresy, numery ubezpieczenia Medicare oraz dane medyczne, w tym notatki z konsultacji, skierowania i wyniki badań. Za odblokowanie systemów napastnicy zażądali okupu.

W Belgii cyberatak na szpital AZ Monica w Antwerpii doprowadził do odwołania 70 planowanych operacji i konieczności przekierowania 7 ciężko chorych pacjentów do innych placówek. Oddział ratunkowy działał w ograniczonym zakresie, a działalność zespołów ratownictwa została czasowo zawieszona. Następnego dnia szpital informował, że jest w stanie realizować zaledwie około 30 proc. planowych świadczeń.

4 duże ataki na polskie placówki w 1 miesiąc i dane 19 mln osób z systemu MyDr

W nocy z 7 na 8 marca z pomocą ransomware hakerzy zaatakowali Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie. Napastnicy zaszyfrowali część danych i zablokowali dostęp do systemów, żądając kilku milionów dolarów okupu. Szpital musiał przejść na papierowy tryb pracy, sprawą zajęła się prokuratura.

Kilka dni później podobny atak odnotowano na Bonifraterskie Centrum Medyczne. Ransomware zaszyfrował dane na serwerach placówki, cyberprzestępcy mogli również uzyskać dostęp do danych osobowych pacjentów.

26 marca 2026 r. cyberatak zarejestrowano też w Centrum Medycznym „Eskulap” w Raciborzu. Cyberprzestępcy zaszyfrowali dane, w efekcie czego placówka utraciła czasowo dostęp do m.in. dokumentacji medycznej.

Serię marcowych incydentów zamyka cyberatak z 31 marca 2026 r. na Świętokrzyskie Centrum Rehabilitacji w Czarneckiej Górze. Złośliwe oprogramowanie zaszyfrowało dane przetwarzane przez placówkę i doprowadziło do blokady działania systemów informatycznych.

28 maja 2026 r. Wielkopolskie Centrum Medyczne REMEDIUM wykryło nieuprawniony dostęp do danych przechowywanych w systemach informatycznych placówki. Naruszenie objęło dane zawierające imiona i nazwiska, numery PESEL, numery dowodów osobistych oraz informacje o stanie zdrowia. Placówka natychmiast odizolowała zaatakowane systemy od sieci, zabezpieczyła logi i dowody, a o incydencie poinformowała organy ścigania oraz Prezesa UODO. W lipcu, także z pomocą ransomware, doszło do incydentu w PaKK-MED, sieci czterech placówek podstawowej opieki zdrowotnej w województwie zachodniopomorskim. Po wykryciu ataku systemy zostały wyłączone, a placówki przeszły na dokumentację papierową. W komunikacie wskazano, że przestępcy przejęli dane osobowe.

Atak na MyDr z 10 sierpnia 2026 r. to największy ujawniony do tej pory wyciek danych w polskiej ochronie zdrowia. Okoliczności zdarzenia nadal wyjaśnia Policja i Centralne Biuro Walki z Cyberprzestępczością. Osoby podające się za sprawców poinformowały, że uzyskały dostęp do prawie 19 mln unikatowych numerów PESEL powiązanych z informacjami o lekach i wizytach. O tej sprawie piszemy szczegółowo **na blogu OSOZ**. W drugiej połowie września 2026 roku na jaw wyszły kolejne dwa cyberataki – na oprogramowanie Medyc oraz sieć medyczną Enel-Med.

Według danych CSIRT Centrum e-Zdrowia, w 2025 roku odnotowano 1441 incydentów bezpieczeństwa danych w sektorze zdrowia. W 2024 roku było ich 1028, a w 2023 roku – 435. ●

» Według raportu Comparitech, w pierwszych sześciu miesiącach 2026 r. liczba ataków na placówki zdrowia na całym świecie wzrosła o 14%. «

reklama

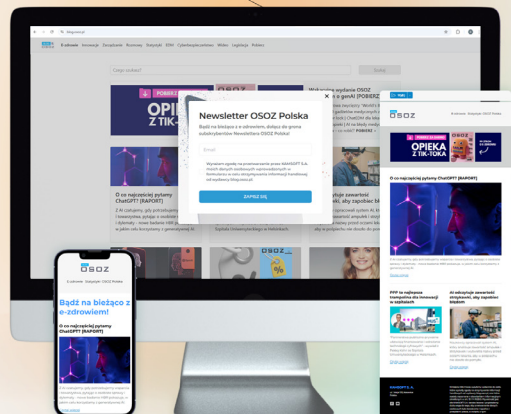
Newsletter OSOZ Polska

BLOG
OSOZ

Nie przegap nowości z [blog.OSOZ.pl](https://blog.osoz.pl)!

Bądź na bieżąco z e-zdrowiem. Dołącz do grona subskrybentów i dowiedz się, co ważnego dzieje się w cyfryzacji ochrony zdrowia w Polsce.

DOŁĄCZ DO NAS!



blog.osoz.pl

Nawigator²⁰²⁶ e-Zdrowia

**KONFERENCJA, KTÓRA POMAGA OBRAĆ
WŁAŚCIWY KURS W DYNAMICZNIE
ZMIENIAJĄCYM SIĘ ŚWIECIE E-ZDROWIA.**

Dowiedz się, jak skutecznie wykorzystać możliwości e-Zdrowia w codziennej pracy. Przygotuj się na nadchodzące zmiany i działaj z wyprzedzeniem.

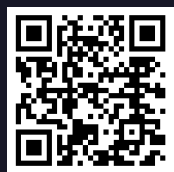
W programie XI edycji konferencji m.in. :

- Cyberbezpieczeństwo
- Centralna e-Rejestracja
- Koordynacja opieki nad pacjentem
- e-Orzeczenia w Medycynie Pracy

Wydarzenie online

14-16
października

Dołącz do nas!
www.osoz.pl/nawigator



AI GENERATED



„Nie karzemy, nie wręczamy mandatów. Naszym zadaniem jest pomoc placówce zdrowia w obsłudze incydentu”

– Odpowiednia infrastruktura teleinformatyczna i budżet na jej zakup to tylko jeden z kilku filarów skutecznej obrony przed cyberatakami. Ta wymaga spojrzenia horyzontalnego – mówi Jeremi Olechnowicz, dyrektor Pionu Eksploatacji Systemów Teleinformatycznych w Centrum e-Zdrowia.

Atak na MyDr to największy w historii Polski wyciek danych medycznych. Co Pana zdaniem trzeba zrobić, aby podobny incydent nie powtórzył się w przyszłości?

Ataki i włamania zdarzają się nieustannie na świecie, także w Polsce, i nie wyeliminujemy ich całkowicie. To, co musi się zmienić, to cyberodporność firm i placówek.

Choć RODO funkcjonuje od wielu lat, wszystko wskazuje na to, że niektóre firmy nie w pełni wdrażają jego wymogi. Być może konieczne będzie skuteczniejsze egzekwowanie odpowiedniego poziomu bezpieczeństwa danych za pomocą regulacji prawnych. Zmiany powinny dotyczyć wdrażania standardów i dobrych praktyk, o których pisaliśmy choćby w naszych niedawnych zaleceniach dla dostawców.

Można jednak odnieść wrażenie, że niezależnie od zabezpieczeń hakerzy i tak są o krok do przodu.

Zapewnienie cyberbezpieczeństwa to zadanie bardzo trudne, obejmujące wiele aspektów. To także nieustający wyścig. Hakerzy stale dostosowują się do zmieniających się realiów i niestety często mają przewagę, ponieważ sami wybierają dogodny dla siebie czas i miejsce ataku. Tymczasem dostawcy czy placówki muszą być gotowi 24/7.

Niezmiennie, bardzo często najsłabszym ogniwem wciąż pozostaje człowiek. Wiele osób nie przekonało się jeszcze do uwierzytelniania dwuskładnikowego, do szyfrowania swoich danych czy dbania o poufność swoich haseł, a nawet do używania różnych haseł do różnych systemów.

W 2025 roku CSIRT CeZ obsłużył o 60% więcej incydentów bezpieczeństwa danych niż rok wcześniej. Jak wyglądają statystyki za ten rok?

W dalszym ciągu odnotowujemy systematyczny wzrost liczby incydentów – w okresie styczeń–sierpień o prawie 30% w ujęciu do tego samego okresu w poprzednim roku.

» Spotykamy się często z przypadkami powtarzających się błędów konfiguracyjnych, np. publicznie dostępnych paneli logowania. «

Jednocześnie poprawia się skuteczność wykrywania. W 2022 roku odnotowano 251 incydentów, podczas gdy w 2025 roku było ich już 1441. Oznacza to niemal sześciokrotny wzrost w ciągu trzech lat. Trend ten utrzymuje się również w 2026 roku. Do końca września CSIRT CeZ wykrył i obsłużył 1379 incydentów, co wskazuje, że bieżący rok może zakończyć się kolejnym rekordowym wynikiem.

Najczęściej rejestrowanymi zagrożeniami w 2025 roku były oszustwa komputerowe, w tym phishing (580 przypadków), podatne usługi (344), wycieki poświadczeń (148), szkodliwe oprogramowanie (146).

Oszustwa komputerowe i podatne usługi odpowiadały łącznie za około 64 proc. wszystkich obsługiwanych zdarzeń. Dane te pokazują, że skuteczna ochrona organizacji zależy nie tylko od technologii, lecz także od świadomości użytkowników, wdrożonych procedur bezpieczeństwa oraz regularnej oceny ryzyka.

Jakie zmiany w metodach działania hakerów rzucają się w oczy?

Po pierwsze, ma miejsce automatyzacja ataków, czyli wykorzystywanie sztucznej inteligencji do ich przeprowadzenia. Skrócenie czasu od ataku do przełamania barier to też efekt automatyzacji. Można więc powiedzieć, że ataki są bardziej zmasowane, szybsze i lepiej zorganizowane. Cyberprzestępcy wykorzystują sztuczną inteligencję do podrabiania głosu i wizerunku rzeczywistych osób. Metody manipulacji są coraz bardziej wyrafinowane i trudniejsze do zdemaskowania.

Weźmy taki przykład: doszło do cyberataku i podmiot zdaje sobie sprawę, że przez lata zaniedbywał ochronę danych. Jak przekonałby Pan mimo to do zgłoszenia incydentu do CSIRT CeZ?

Przede wszystkim należy podkreślić faktyczną rolę CSIRT CeZ. Nie jesteśmy organem, którego celem jest karanie podmiotów. Nie jesteśmy organem, który wręcza mandaty. Naszym zadaniem

niem jest przede wszystkim wspieranie podmiotów w procesie obsługi incydentów. Mamy w swoim katalogu usług szereg rozwiązań, które jesteśmy w stanie zaoferować zaatakowanym podmiotom zupełnie bezpłatnie, np. usługę cyberkaretki. W tej sytuacji uważam, że jak najszybsze zgłoszenie incydentu, oprócz tego, że wynika z obowiązującego prawa, leży w interesie każdego zaatakowanego podmiotu.

Phishing, czyli oszustwa komputerowe, pozostaje najczęstszą metodą ataku. Hakerzy podszywają się pod NFZ, MZ, dostawców IT. Na co zwracać uwagę, aby nie dać się nabrać?

Atakujący bardzo często próbują wywierać presję celem podjęcia szybkich, nieprzemyślanych działań. Używają do tego wielu metod, np. budują poczucie, że konieczne jest działanie w pośpiechu, błyskawiczne podejmowanie decyzji czy też próbują podszywać się pod przełożonych. Podstawą jest wyrobienie nawyku sprawdzania adresu, z którego przychodzi wiadomość, oraz zwracanie uwagi na wykorzystywany kanał komunikacji.

Ponadto atakujący zawsze będzie próbował zmusić nas do pewnej aktywności, udostępnienia danych, pobrania pliku i jego instalacji czy też kliknięcia w przesłany link. Nigdy nie należy wykonywać takich działań. Jeżeli komunikuje się z nami osoba podająca się za pracownika placówki medycznej, z której usług korzystamy, zawsze przed wykonaniem jakiegokolwiek czynności warto wykorzystać dotychczas sprawdzony kanał komunikacji i potwierdzić, że wcześniejszy kontakt faktycznie był ze strony pracownika placówki.

Z badania poziomu cyfryzacji przeprowadzonego przez CeZ wynika, że placówki mają ogromne niezaspokojone potrzeby m.in. w zakresie szkoleń z cyberbezpieczeństwa. Zgłasza je prawie 80% placówek. Czy Centrum e-Zdrowia oferuje w tej kwestii jakieś wsparcie?

Tak, Akademia CeZ regularnie organizuje szkolenia, podczas których specjaliści z CSIRT CeZ dzielą się swoją wiedzą.

Informacje o kolejnych terminach publikujemy na naszych stronach internetowych.

CSIRT CeZ opracował też zalecenia bezpieczeństwa dla dostawców rozwiązań IT dla ochrony zdrowia. Obejmują one m.in. obszary zarządzania bezpieczeństwem, ochrony danych, architektury systemów, zarządzania dostępami oraz monitorowania i reagowania na incydenty. Materiał został rozpowszechniony za pośrednictwem organizacji zrzeszających dostawców i producentów oprogramowania.

Od początku 2026 roku eksperci CSIRT CeZ przeszkolili blisko 2 tys. osób, wysłali 117 ostrzeżeń dotyczących podatności, zaleceń i kampanii phishingowych, opisali 285 podatności wraz z rekomendacjami działań, a także wykryli 70 podatności

Centrum Operacji Bezpieczeństwa w ramach Centrum e-Zdrowia



w infrastrukturze podmiotów sektora zdrowia i wsparli ich usuwanie.

Przejdźmy do tego, co robić, gdy dojdzie do skutecznego ataku hakerów. Pierwszym odruchem, gdy na ekranie pojawia się wiadomość od hakerów, jest wyłączenie komputera albo odcięcie dostępu do internetu. To prawidłowa reakcja?

Tak, to właściwa reakcja. Najważniejsze jest szybkie odłączenie zainfekowanej stacji od sieci, tak aby atak nie rozprzestrzenił się na inne urządzenia. Jeśli to możliwe, lepiej odłączyć sam kabel sieciowy lub Wi-Fi, nie wyłączając przy tym komputera. Dzięki tej praktyce łatwiej ustalić przebieg ataku, ponieważ część danych potrzebnych do analizy po wyłączeniu urządzenia zostaje bezpowrotnie utracona.

Czego nie należy robić?

Nie odpisywać przestępcom, nie płacić okupu oraz nie próbować samodzielnie niczego naprawiać ani usuwać. Należy zawiadomić właściwe osoby w placówce. Zalecam też kontakt z CSIRT CeZ, który pomaga podmiotom ochrony zdrowia w takich sytuacjach.

Jeśli istnieje podejrzenie naruszenia ochrony danych osobowych, incydent trzeba zgłosić także do UODO w ciągu 72h.

CSIRT CeZ podkreśla, że ważne jest zabezpieczenie dowodów cyberataku. Po co i jak to zrobić?

Zabezpieczenie dowodów cyberataku jest kluczowe nie tylko po to, aby ustalić sprawcę, ale przede wszystkim, żeby zrozumieć, jak doszło do incydentu, jakie dane zostały naruszone oraz jak zapobiec podobnym zdarzeniom w przyszłości.

Sposób zabezpieczenia dowodów powinien wynikać z wcześniej przyjętych procedur wewnętrznych w ramach organizacji. Niemniej kluczowym jest, by zachować integralność, czyli

» Nie odpisuj przestępcom, nie płac okupu oraz nie próbuj samodzielnie niczego naprawiać ani usuwać. «

nie modyfikować dowodów, ponieważ każda zmiana może zacierać ślady pozostawione przez cyberprzestępców.

Drugi element to odpowiednie dokumentowanie działań wraz ze wskazaniem dat, osób oraz opisu poszczególnych czynności. Często w trakcie prowadzonych działań i pod presją czasu nie jest to zadaniem łatwym, niemniej jednak warto dokumentować wszystkie czynności nawet w sposób skrótowy, który umożliwi odtworzenie całego procesu na późniejszym etapie, kiedy sytuacja będzie na to pozwalać.

Musimy również pamiętać o obowiązkach regulacyjnych i prawnych nałożonych chociażby na podmioty kluczowe i ważne – zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa.

Na co menedżerowie placówek zdrowia powinni szczególnie zwrócić uwagę w kwestii ochrony danych? Czy CeZ zauważa powtarzające się nagminne zaniedbania?

Menedżerowie placówek medycznych powinni przede wszystkim spojrzeć na problem zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w sposób horyzontalny. Bardzo często spotykamy się z postrzeganiem cyberbezpieczeństwa przez pryzmat zapewnienia odpowiedniej infrastruktury teleinformatycznej, a co za tym idzie, odpowiednich zasobów finansowych na jej zakup oraz utrzymanie. Jest to ważny, ale jedynie jeden z kilku filarów skutecznej obrony przed cyberatakami.

Tak samo ważne jest wypracowanie rozwiązań organizacyjnych, skutecznych procedur reagowania na wypadek incydentu, przygotowanie i respektowanie zasad tworzenia kopii zapasowych oraz ich regularne sprawdzanie, tworzenie polityki bezpiecznych hasel, cykliczne szkolenia z obszaru cyberbezpieczeństwa, monitorowanie podatności i ich systematyczne łatanie. W pracy CSIRT CeZ często spotykamy się z przypadkami powtarzających się błędów konfiguracyjnych, np. publicznie dostępnych paneli logowania. Z pozoru wydaje

»Sposób zabezpieczenia dowodów cyberataku powinien wynikać z wcześniej przyjętych procedur wewnętrznych.«

się to blahym problemem, niemniej nawet to może nieść dla podmiotu bardzo przykre konsekwencje.

Wiemy, że rośnie liczba ataków. A czy mamy jakieś statystyki pokazujące, że rośnie też skuteczność ochrony?

Do prowadzenia bieżących statystyk podjętych prób ataków niezbędne byłoby posiadanie tzw. Centralnego SOCa (red.: Security Operations Center, czyli Centrum Operacji Zabezpieczeń), w ramach którego byłyby zbierane dane z całego sektora. Jest to rozwiązanie pożądanе, niemniej z uwagi na skalę niezbędnych do uruchomienia takiej usługi zasobów, zarówno finansowych, jak również organizacyjnych, sprzętowych i kadrowych, raczej trudne do osiągnięcia w najbliższej przyszłości.

Czy są jakieś nowe metody lub narzędzia, które poprawiają poziom cyberbezpieczeństwa?

Jest ich bardzo dużo, niemniej podstawową zasadą jest potraktowanie w każdej organizacji cyberbezpieczeństwa jako procesu wymagającego ustawicznego działania.

Dotyczy to wszystkich pracowników organizacji, jak również łańcucha dostaw. Zdajemy sobie sprawę, że placówki borykają się z problemami finansowymi, a zakup infrastruktury informatycznej bywa bardzo obciążający dla budżetu, niemniej jednak można wdrożyć szereg rozwiązań open-source oraz podnosić świadomość kadr w obszarze cyberbezpieczeństwa, np. organizując cykliczne szkolenia z obszaru security-awareness.

Należy pamiętać – co ponownie podkreślam – że przy atakach najczęściej tym najsłabszym ogniwiem jest człowiek. W związku z tym, podnoszenie wiedzy na temat cyberbezpieczeństwa może stanowić kluczowy element w budowaniu skutecznej obrony, przynajmniej przed podstawowymi rodzajami cyberataków, takimi jak phishing. ●



Przy tych zabezpieczeniach to cud, że jest tak mało cyberataków

– Ochrona danych jest jak zamek z tysiącem okien. Hakerowi wystarczy jedno niezabezpieczone, aby dostać się do środka – mówi Adam Haertle, założyciel serwisu ZaufanaTrzeciaStrona.pl i ekspert ds. cyberbezpieczeństwa. Rozmawiamy o kulisach ataku na MyDr, metodach działania grup cyberprzestępców, płaceniu okupu i tym, czy można się jeszcze obronić przed coraz bardziej wyrafinowanymi cyberatakami.

Dlaczego po wykradzeniu danych 19 mln osób z MyDr hakerzy skontaktowali się z Zaufaną Trzecią Stroną, aby nagłośnić sprawę?

Sprawcy, według mojej najlepszej wiedzy, próbowali skontaktować się z zaatakowaną firmą trzy dni wcześniej. Wysyłali e-maile i SMS-y na numery telefonów kierownictwa, ale przez co najmniej trzy doby nie otrzymali żadnej odpowiedzi. Pomyśleli więc, że przez dziennikarza będzie szybciej i odezwali się do mnie.

I osiągnęli cel, bo sprawa szybko została nagłośniona. Na razie cały czas toczy się śledztwo i nie wiemy, co dokładnie się stało. Po co jednak hakerzy kradną tak ogromne bazy danych, skoro raczej już z doświadczenia wiedzą, że prawdopodobieństwo, że poszkodowany zapłaci okup, jest małe?

Nasza ocena prawdopodobieństwa otrzymania okupu jest mocno zaburzona przez prosty fakt: kiedy hakerzy otrzymują okup, nie dowiadujemy się o tym.

Słyszymy przede wszystkim o przypadkach, w których płatność nie dochodzi do skutku, dochodzi do konfliktu pomiędzy włamywaczami a zaatakowaną firmą, nie osiągają porozumienia i informacja trafia do mediów.

Zgaduję – częściowo też w oparciu o swoją wiedzę – ale mogę powiedzieć, że wielokrotnie płatność okupu jednak następuje.

W przypadku MyDr, przestępcy w specyficzny sposób komunikowali się z ofiarą i mediami. Najpierw twierdzili, że nie chcą okupu. A w kolejnym zdaniu napisali, że chcą opłaty za niezamówione testy bezpieczeństwa, które przeprowadzili, i przy okazji wykradli bazę danych. De facto były to więc żądania finansowe.

Nie wiem, jakie one były i czy zostały zrealizowane. Na koniec sprawcy podkreślili jednak dobrą współpracę z zaatakowaną firmą, a dane do tej pory nie wyciekły.

To, że nie wyciekły, nie znaczy, że nie wyciekną. Mogły być przecież sprzedane służbom państw nieprzyjaznych Polsce.

Z doświadczenia stawiałbym na to, że raczej tak się nie stało. Gdyby ktoś chciał te dane skomercjalizować, nie informowałby o tym mediów. W momencie, gdy wiadomo, jakie dane wyciekły, ich wartość spada. Fakt posiadania danych bez wiedzy właściciela zwiększa ich wartość.

Fakt, że media zostały o tym poinformowane i teraz wszyscy o tym wiemy, można z jednej strony potraktować jako reklamę takiej oferty, bo potencjalnie zwiększa rynek. Ale gdyby ktoś faktycznie chciał tymi danymi handlować, to w zasadzie w każdym znanym mi przypadku taki handel odbywa się bez upubliczniania faktu ich wykradzenia.

Są liczne kanały prywatne, z których włamywacze korzystają, przedstawiając ofertę sprzedaży potencjalnym zainteresowanym. Często takie transakcje odbywają się bez światła publicznego.

Czy hakerzy mają w ogóle jakikolwiek kręgosłup etyczny? Jeżeli żądają okupu i ktoś go zapłaci, czy dane są wtedy faktycznie odblokowywane i nie są dalej sprzedawane?

Trudno podejrzewać przestępców o szczególnie kręgosłup etyczny, zwłaszcza jeżeli atakują firmy ochrony zdrowia. Kierują się przede wszystkim interesem komercyjnym, który jednak nakłada konieczność posiadania pewnej „wiarygodności” na rynku.

Jeżeli mówimy o organizacjach przestępczych szyfrujących dane i żądających okupu za ich odzyskanie oraz nieopublikowanie, albo jedno i drugie, to są one dosyć dużym ewenementem. Z reguły grupy przestępcze starają się regularnie zmieniać swoją tożsamość, żeby w razie identyfikacji nie przypisywać im więcej czynów niż to konieczne.

Tymczasem grupy szyfrujące dane działają pod określonymi markami, które same promują. Prowadzą nawet serwisy online

» Gdyby ktoś chciał te dane skomercjalizować, nie informowałby o tym mediów. «

z informacjami o swoich klientach, poradnikami, jak kupować kryptowaluty i jak zachowywać się w momencie ataku.

Liczą na to, że jeżeli będą zachowywać się rzetelnie i po otrzymaniu płatności udostępnią narzędzia do odszyfrowania danych, kolejne osoby też zapłacą. Jeżeli jednak wcześniejsze ofiary skarżą się w internecie, że po uiszczeniu zapłaty w kryptowalucie kontakt się urwał i nie otrzymały kluczy deszyfrujących, rośnie szansa, że kolejne ofiary też nie zapłacą.

Można więc mówić o czymś w rodzaju rankingu takich grup pod względem rzetelności i wiarygodności. Oczywiście nie znaczy to, że każda płatność oznacza udaną transakcję i otrzymanie tego, za co się zapłaciło.

W przypadku grup szyfrujących dane, w wielu przypadkach faktycznie starają się dostarczyć narzędzia pozwalające na odszyfrowanie danych. Nie zawsze są one dobrej jakości, ale pod względem technicznym starają się zapewnić możliwość odszyfrowania.

Czy za takimi cyberatakami stoi wyłącznie interes finansowy, czy czasami są one także motywowane, na przykład, chęcią destabilizacji sytuacji politycznej?

To zależy od kraju pochodzenia napastników. Napastnicy z Białorusi, Rosji czy byłych republik radzieckich często działają pod pewnego rodzaju opieką służb danego kraju, choć niekoniecznie bezpośrednio pod ich kierownictwem.

Wiemy z licznych wycieków, że posiadają jakiś kanał komunikacji z kimś po stronie lokalnego wywiadu czy kontrwywiadu, cywilnego albo wojskowego. Jeżeli wykradną ciekawe dane albo zdobędą interesujące informacje, może się zdarzyć, że ktoś „na górze” będzie nimi zainteresowany i takie informacje zostaną przekazane w ramach współpracy. Nie mam na to bezpośrednich dowodów, ale prawdopodobieństwo, że główne grupy cyberprzestępcze działające na terenie byłego Związku Radzieckiego oddają jakąś część dochodu komuś, kto się nimi opiekuje i dba o to, żeby nie trafiły do więzienia, oceniam raczej wysoko.

» Hakerzy z Białorusi, Rosji czy byłych republik radzieckich często działają pod pewnego rodzaju opieką służb danego kraju. «

Może się też zdarzyć, że takie grupy dostają zadania w określonym kierunku. Albo nawet nie dostają ich wprost, ale domyślają się, co ich opiekunom by się podobało. Rosyjskie grupy cyberprzestępcze mają też – podobnie jak zwykli przestępcy – potrzebę znalezienia jakiegoś uzasadnienia moralnego dla swoich działań. Jeżeli ktoś pobije drugą osobę, bo uzna, że tamta jest gorszym przestępcą, może sobie wmówić: „Ja będę teraz tym lepszym”.

Rosjanie zajmujący się włamaniami faktycznie dążą więc do tego, żeby pogrążyć te „złe” kraje Zachodu, które ich tak bardzo nie lubią. Jest w tym coś w rodzaju specyficznie rozumianego patriotyzmu.

Natomiast znakomita większość grup komercyjnych skupia się po prostu na osiąganiu dochodu. Niewykluczone jednak, że oprócz takich działań zakłócających i komercyjnych mamy też do czynienia z działaniami szpiegowskimi. To jest ta trzecia grupa, w której dane są po prostu kradzione i nikt nigdy się o tym nie dowiaduje, a kradzież odbywa się na zlecenie jakiejś instytucji państwowej.

O kradzieżach często słyszymy, ale rzadziej o tym, że udało się złapać cyberprzestępców. Jaka jest skuteczność ścigania hakerów?

Nie dysponujemy rzetelnymi statystykami, które odpowiadałyby na to pytanie. Po stronie polskich organów ścigania mamy liczbę zgłoszonych przestępstw w danej kategorii, ale ta kategoria jest bardzo pojemna. To, że coś jest przestępstwem komputerowym, wcale nie oznacza, że było włamaniem czy kradzieżą. Dzisiaj większość przestępstw ma też komponent komputerowy, bo technologia jest już obecna prawie wszędzie.

Natomiast wiemy, że takie kradzieże, małe czy duże, mają wykrywalność raczej jednocyfrową niż dwucyfrową.

Z wielu różnych powodów. Po pierwsze, są to sprawy skomplikowane technicznie, a przy niskim poziomie strat – są prowadzone przez lokalnych policjantów, którzy często nie

mają odpowiednich narzędzi, szkoleń ani kompetencji, żeby ścigać sprawców.

W przypadku większych spraw, kompetencje i narzędzia są, ale z drugiej strony śledztwa są bardzo trudne, bo ślady cyfrowe łatwo jest sfalszować. Trudno jest zostawić na miejscu przestępstwa cudze DNA, ale jest to możliwe. Natomiast ukryć się za cudzym adresem IP w internecie jest trywialnie prosto. To są trzy kliknięcia, nie trzeba do tego doktoratu.

Do tego dochodzi transgraniczność tych przestępstw. Wielu sprawców działa poza terytorium Polski i nie ma polskiego obywatelstwa. Więc nawet jeżeli uda się ich zidentyfikować, zatrzymanie poza granicami Polski są rzadkością.

W przypadku MyDr mamy do czynienia z wyciekami danych z chmury. Wcześniej zawsze krążyła opinia, że chmura jest bezpieczniejsza niż baza lokalna. Czy to przekonanie jest błędne?

Myślę, że chmura jest tak samo bezpieczna jak lokalna baza danych. Wszystko zależy od tego, kto ją skonfigurował i w jaki sposób.

Ta baza mogła równie dobrze znajdować się na komputerze lokalnego programisty i zostać stamtąd pobrana. Nie ma znaczenia, czy link do niej jest serwowany z chmury czy z lokalnego komputera. Główny problem polegał na tym, że była to jakaś kopia danych sprzed paru lat – i że była dostępna dla kogoś, komu udało się uzyskać dostęp do systemów.

Ważnym elementem bezpieczeństwa chmury jest to, że przekazujemy troskę o zabezpieczenie infrastruktury w ręce zawodowców pracujących u dostawcy chmury. Jeżeli postawimy wszystko na własnych serwerach, musimy mieć ekspertów od zabezpieczenia infrastruktury. Pamiętajmy, że oprócz warstwy bazy danych, mamy kolejne warstwy IT, takie jak aplikacje i interfejsy. Ich bezpieczeństwo zależy już od naszych programistów, bazodanowców i administratorów. Możemy znowu wynająć te usługi od dostawcy chmury, ale aplikacje nadal ktoś musi napisać.

Nie ma znaczenia, czy dany program działa lokalnie, czy w chmurze. To od jakości kodu zależy, czy będą w nim błędy, jakie i ile ich będzie. Tego, że nie będzie ich wcale, raczej nie możemy oczekiwać. Samo przechowywanie danych w chmurze rzadko jest przesłanką ich bezpieczeństwa.

Czy mamy jakieś nowe metody, żeby chronić się przed cyberatakami? Phishing jest coraz skuteczniejszy, ponieważ hakerzy korzystają ze sztucznej inteligencji. Nie popełniają już rzucających się w oczy błędów językowych. W przypadku ochrony zdrowia mogą na przykład podszywać się pod strony Ministerstwa Zdrowia czy dostawców oprogramowania.

Niestety nie widzę takiej symetrii między metodami hakerów a metodami ochrony danych. Skala zagrożeń jest duża, bo narzędzia popełniania przestępstw są powszechnie dostępne, w zasięgu kilku kliknięć.

Kiedyś, żeby zostać przestępcą, trzeba było być bardziej zdeteminowanym, mieć odwagę wyjść na ulicę, wyrwać komuś torebkę, narażając się na pościg. Dzisiaj można to bardzo prosto zrobić przed ekranem komputera. Wielu, głównie młodych, ale nie tylko, ludzi decyduje się spróbować. Jeżeli kilka razy im się uda, zostają przestępcami.

Drugi problem to transgraniczność. Kiedyś, nie chodząc po danych dzielnicach, szansa, że dostaniemy w zęby, była relatywnie niższa. Dzisiaj ten strzał w zęby możemy dostać od kogokolwiek, skądkolwiek. To może być ktoś siedzący kilka tysięcy kilometrów dalej, kto natrafił na jakiś serwer i przez przypadek jest w stanie się do niego dostać. To powoduje również masowość tych ataków. Łatwość i masowość generują skalę. Po drugiej stronie mamy ludzi, którzy próbują się przed tym zabezpieczyć. I tutaj niestety obrona się nie skaluje.

W branży mówimy o problemie zamku z tysiącem okien. Żeby skutecznie obronić zamek, potrzebujemy tysiąca strażników. Przy tysiącu okien napastnik potrzebuje tylko tego, żeby jeden strażnik się zdrzemnął. Oczywiście wiemy o tym po stronie obrony. Wiemy, że oprócz strażnika przy każdym oknie trzeba

» Skala zagrożeń jest duża, bo narzędzia popełniania przestępstw są powszechnie dostępne, w zasięgu kilku kliknięć. «

jeszcze postawić strażników patrolujących korytarze, żeby sprawdzić, czy ktoś nie prześliznął się przez okno. Budowanie obrony polega więc na tworzeniu wielu różnych warstw zabezpieczeń.

Możemy stosować również pułapki wewnątrz organizacji. W analogii do zamku, nawet dotknięcie skrzyni ze skarbem powinno aktywować alarm, bo wszyscy jego mieszkańcy wiedzą, że dotykać jej nie wolno.

Budowanie systemu obrony naszego cyfrowego zamku, opartego na wielu warstwach, zakłada, że komuś zawsze uda się włamać i dostać do środka. Mając ograniczone zasoby, musimy skupić się na wykrywaniu włamań, a nie tylko na ich zapobieganiu.

Wiemy, że stuprocentowe zabezpieczenie przed atakami kosztowałoby nas bardzo dużo i niszczyłoby większość modeli biznesowych. Inny problem ze skalowalnością obrony polega na tym, że napastnik nie ma żadnych ograniczeń technicznych. Może przeprowadzać nieudane ataki, może je wielokrotnie powtarzać, może atakować tysiąc podmiotów naraz. Obrońcy nie mogą sobie pozwolić na tyle błędów, obrona musi być bardziej precyzyjna.

A czy AI pozwala lepiej chronić dane?

Jeżeli mówimy o zastosowaniu sztucznej inteligencji w ataku, to jeżeli napastnikowi coś nie zadziała, problem dla niego jest niewielki. Natomiast z punktu widzenia obrony, jeżeli zastosujemy systemy AI i damy im autonomię w obronie, nie mogą się one pomylić. Jeżeli tak się stanie, mogą nam wyłączyć nasze usługi i serwisy.

Automatyzacja ataku jest dużo prostsza niż automatyzacja obrony, bo napastnik po prostu nie przejmuje się skutkami. Najwyżej atak się nie uda – wtedy haker próbuje dalej gdzie indziej. Z kolei obrońca musi przejmować się skutkami swojej obrony; nie może pozwolić, żeby obrona na przykład pogorszyła sytuację albo doprowadziła do przerw w ciągłości działania.

Automat broniący może powiedzieć: „Ten atak jest tak niebezpieczny, że musimy wyłączyć usługę”. Może się okazać, że ta usługa jest potrzebna, żeby na przykład szpital mógł funkcjonować.

Defensywa jest więc dużo trudniejsza niż ofensywa, ale mądra obrona pozwala nam dzisiaj równoważyć sprawność napastników. Pamiętajmy, że po stronie napastników często spotykamy się z osobami mniej wykwalifikowanymi; jest ich dużo, ale ich średni poziom umiejętności jest dużo niższy niż po stronie obrońców.

Placówki zdrowia najczęściej nie mają dużych budżetów na inwestycje w cyberbezpieczeństwo. Czy są jakieś podstawowe zabezpieczenia, które można wdrożyć stosunkowo niskim kosztem, a które zapewniałyby, powiedzmy, ponad 90-procentowe bezpieczeństwo?

Rozmawiam czasem z ludźmi odpowiedzialnymi za bezpieczeństwo w szpitalach i jest mi smutno po tych rozmowach. Pieniądze są, czy to środki z programu „Wsparcie cyberbezpieczeństwa w placówkach medycznych”, czy z KPO. Problem w tym, że często nie można ich wydać tam, gdzie najbardziej by się przydały.

A najbardziej przydałoby się zatrudnić albo lepiej wynagrodzić ludzi, którzy wiedzą, co w danej organizacji jest potrzebne. Najbardziej brakuje kompetencji.

Długofalowo, zakup urządzeń czy oprogramowania nie podnosi poziomu bezpieczeństwa. Bezpieczeństwo jest w stanie podnieść mądry człowiek, który będzie wiedział, co warto zrobić, kiedy i w jaki sposób, a potem będzie pilnował, żeby to faktycznie działało.

Zakup jednego urządzenia, którego dostawca obiecuje, że rozwiąże problemy, żadnych problemów nie rozwiąże. To, że urządzenie wykryje włamanie, wcale nie oznacza, że ktoś będzie wiedział, co z takim alertem zrobić. Po pierwsze, nie oznacza to, że ktoś ten alert przeczyta. Po drugie, jeżeli go przeczyta, nie oznacza to, że go zrozumie. Po trzecie, jeżeli zrozumie, to nie znaczy, że podejmie właściwe działania.

»Hakerów jest dużo, ale ich średni poziom umiejętności jest dużo niższy niż po stronie obrońców danych.«

Dla mnie głównym problemem ochrony zdrowia są więc kompetencje ludzi, którzy za bezpieczeństwo bardzo ważnych danych otrzymują śmiesznie niskie wynagrodzenia. Cudem można nazwać to, że tych ataków jest tak niewiele przy skali problemu, z jakim mamy do czynienia.

Nie ma uniwersalnego rozwiązania w rodzaju: kupimy coś, postawimy i będzie działało. Dla mnie uniwersalnym rozwiązaniem byłoby: zatrudnimy człowieka, który popatrzy, co mamy a czego nie mamy, jak wyglądają najczęstsze ataki i jak za przykładowo 20 procent kosztów pokryć 80 procent problemów.

Z informacji CSIRT Centrum Zdrowia wynika, że do sierpnia 2026 roku zgłoszono już prawie 1400 incydentów bezpieczeństwa danych w ochronie zdrowia. Wiemy, że te liczby są niedoszacowane, bo nie wszystkie incydenty są zgłaszane. Czym ryzykuje placówka, gdy pada ofiarą hakera i nie zgłasza tego?

Nie wiem, jakie w tej chwili są przewidziane sankcje wynikające ze wszystkich możliwych regulacji, ale jest ich sporo. Na pewno mamy sankcje z ustawy o ochronie danych osobowych wdrożonego w Polsce. Po kontroli, Urząd Ochrony Danych Osobowych może wydać rekomendacje albo nałożyć kary finansowe.

W zależności od klasyfikacji placówki z punktu widzenia krajowego systemu cyberbezpieczeństwa, po wdrożeniu NIS2 mamy również kary dla zarządów za niezastosowanie właściwych procedur bezpieczeństwa.

Nie ma w Polsce czegoś takiego jak kara za to, że ktoś padł ofiarą hakera. Jest kara za to, że nie zrobił tego, czego wymagały przepisy. Na przykład nie zareagowano na czas na żądanie organu nadzorczego, nie powiadomiono ofiar wycieku, nie podjęto właściwych działań naprawczych albo okaże się, że włamanie nastąpiło przez lukę wskazaną w audycie z zeszłego roku i nikt jej nie usunął. To są najczęstsze przyczyny, dla których instytucje są karane.

CSIRT CeZ podkreśla, że dane najczęściej wyciekają w wyniku ataku typu phishing. Każdy z nas niemal codziennie dostaje e-mail o tym, że coś wygrał albo że kurier nie mógł dostarczyć przesyłki i trzeba coś kliknąć. Nauczyliśmy się rozpoznawać niektóre metody hakerów. Ale część osób nadal daje się nabrać, a metody ataków są coraz bardziej wyrafinowane. Czy są jakieś sposoby, żeby lepiej się przed nimi bronić, oprócz oczywiście szkoleń?

Najprostszą metodą obrony przed phishingiem jest wdrożenie uwierzytelniania dwuskładnikowego. To rozwiązanie, którego w ochronie zdrowia bardzo często brakuje. Choć wymaga wykonania dodatkowego kroku przy logowaniu, zapewnia o wiele większe bezpieczeństwo niż tylko podanie loginu i hasła. Biorąc pod uwagę masowość ataków phishingowych i łatwość, z jaką można je dzisiaj przeprowadzić, to jest konieczność.

Od strony technicznej uwierzytelnianie dwuskładnikowe polega na tym, że użytkownik otrzymuje SMS, kod z aplikacji, który dodatkowo trzeba wpisać przy logowaniu. To może też być kluczyk sprzętowy przypominający pendrive, który podłącza się do komputera.

Tych technik jest sporo. Niektóre są darmowe, niektóre płatne, ale każda jest dodatkową przeszkodą dla włamywacza. Nawet jeżeli haker wyludzi od nas login i hasło, polegnie na etapie uwierzytelniania. Jasne, kod z SMS-a też można uzyskać, ale większość atakujących tego nie próbuje. Z prostego powodu – to skomplikowane, a nadal jest wystarczająco dużo systemów, które nie wymagają dodatkowego zabezpieczenia.

Nie musimy więc być superzabezpieczeni. Wystarczy, że będziemy zabezpieczeni lepiej niż przeciętna instytucja.

Dużo mówi się o nowych niebezpieczeństwach związanych z AI. Teoretycznie haker może użyć AI, aby podszyć się pod dyrektora szpitala, sklonować jego głos i zadzwonić do pracownika, prosząc o podanie hasła. Czy powinniśmy się bać takich zagrożeń ze strony AI?

Już od 2019 roku wiemy, że można podrabiać cudzy głos z pomocą AI. Do tej pory nie znalazłem żadnego dowodu, że takie narzędzie zostało użyte w ataku polegającym na podszyciu się pod kogoś – a staram się uważnie monitorować wszystkie zagrożenia w sieci.

W rzeczywistości nie trzeba podrabiać głosu wnuczka, prezesa czy kogokolwiek innego. Wystarczy, że ktoś będzie wektorem wymuszenia i przekona nas do zrobienia czegoś głupiego. W stresie, kiedy dzwoni do nas sam prezes albo dyrektor, albo słyszymy, że nasz wnuczek miał wypadek, tracimy zdolność logicznego myślenia. Zamiast tego działamy impulsywnie, reagując na zagrożenie. Staramy się jak najszybciej rozwiązać problem i nie zastanawiamy się, czy to na pewno jest głos osoby, która do nas dzwoni.

Oczywiście, ataki polegające na podszywaniu się są popularne i faktycznie widzimy ich sporo zarówno w sektorze biznesowym, jak i prywatnym. Przestępcy bardzo często podszywają się pod bank, który rzekomo dzwoni, żeby ostrzec nas, że ktoś kradnie nasze pieniądze, a potem proponuje, jak je odzyskać.

Ataki polegające na podszywaniu się pod kogoś, z pomocą czy bez AI, nie osiągają skali zwykłego phishingu, który wygląda niemal identycznie od 20 lat i nadal działa. Dlaczego? Między innymi dlatego, że ponad 95 procent osób nie ma dwuskładnikowego uwierzytelnienia.

Co jeszcze może stanowić zagrożenie dla danych medycznych, a o czym często zapominamy?

Dużym problemem jest instalowanie urządzeń i systemów i zapominanie o nich. Firewall zaktualizowany w czerwcu działa świetnie do września. Potem ktoś odkrywa w nim błąd, który sprawia, że zamiast być strażnikiem naszej sieci, staje się furtką do niej i wpuszcza włamywaczy do środka.

A wystarczy śledzić informacje od producenta i zaktualizować oprogramowanie, kiedy pojawi się aktualizacja. I to natychmiast.

»Nie ma uniwersalnego rozwiązania w rodzaju: kupimy coś, postawimy i będzie działało.«

Druga rzecz to wszelkie zdalne dostępy. Jeżeli można zdalnie zalogować się do pulpitu, wejść przez VPN i nie ma tam dwuskładnikowego uwierzytelnienia, to jest to sposób, który najczęściej stosują włamywacze zajmujący się szyfrowaniem danych.

Po ataku na MyDr można odnieść wrażenie, że hakerzy są o krok do przodu, że są w stanie włamać się do każdej bazy danych. Czy mamy powody do optymizmu, jeśli chodzi o ochronę danych?

Myślę, że tak. Co parę lat widzimy katastroficzne nagłówki, kiedy pojawia się jakaś nowa technologia, o której niewiele jeszcze wiemy i trochę boimy się tego, jakie będą jej skutki.

O tym, że maszyny wszystko zhakuja, czytam od 20 lat i nadal jakoś funkcjonujemy. Jak się okazuje, inwestujemy w ochronę danych na tyle, że nadal jakoś funkcjonujemy bez większych zakłóceń.

Takie incydenty jak w przypadku MyDR na pewno będą się w przyszłości powtarzać. Myślę jednak, że z czasem po prostu się do tego przyzwyczaimy, nauczymy się z tym żyć i znajdziemy jakieś rozwiązania. Na razie apokalipsy się nie spodziewam. ●

Rośnie nie tylko liczba cyberataków na ochronę zdrowia, ale także skala kra-
dzionych danych

Cyberatak sparaliżował system szpitala. Placówka przeszła na dokumentację papierową

Seria cyberataków na sektor zdrowia. Wyciekły dane milionów osób

Cyberatak na szpital w Szczecinie. Prokuratura wszczęła śledztwo

Trzy groźne wycieki danych medycznych Polaków w kilka tygodni. Służby wchodzą do akcji



Szpital kontra hakerzy. Jak GCM chroni dane pacjentów?

– Nie ma jednej szczelnej bariery chroniącej przed atakiem hakerów, a cyberbezpieczeństwo szpitala wymaga ciągłego doskonalenia – mówi Norbert Przemyk, Główny Specjalista ds. Technologii Informacyjnych w Górnośląskim Centrum Medycznym im Prof. Leszka Gieca Śląskiego Uniwersytetu Medycznego w Katowicach.

Statystyki pokazują, że z roku na rok rośnie liczba ataków na placówki zdrowia. Czy zauważa Pan to też w swojej pracy?

Zdecydowanie tak. Obserwujemy wyraźny wzrost liczby prób cyberataków wymierzonych w podmioty ochrony zdrowia. Obejmują one zarówno klasyczne metody, takie jak phishing i próby wyludzenia danych uwierzytelniających, jak i bardziej zaawansowane ataki ransomware, których celem jest zablokowanie dostępu do systemów informatycznych, a następnie wymuszenie okupu.

Coraz częściej mamy również do czynienia z atakami, które nie są przypadkowe, lecz stanowią element wcześniej przygotowanych i ukierunkowanych działań wymierzonych w konkretną placówkę.

Sektor ochrony zdrowia jest szczególnie atrakcyjnym celem dla cyberprzestępców z kilku powodów. Placówki medyczne przetwarzają duże ilości wrażliwych danych, w tym danych dotyczących pacjentów, a jednocześnie ich działalność wymaga zachowania ciągłości i dostępności systemów. W przypadku incydentu cyberbezpieczeństwa konsekwencje mogą więc dotyczyć nie tylko bezpieczeństwa danych, ale również bieżącego funkcjonowania placówki i zapewnienia ciągłości udzielania świadczeń.

Jak najczęściej hakerzy próbują złamać zabezpieczenia?

Najczęściej atak rozpoczyna się od phishingu, czyli próby nakłonienia pracownika do określonego działania za pomocą odpowiednio przygotowanej, fałszywej wiadomości e-mail lub SMS. Współczesne ataki coraz rzadziej polegają na bezpośrednim, siłowym przełamaniu zabezpieczeń technicznych. Cyberprzestępcy częściej wykorzystują czynnik ludzki, w szczególności nieuwagę lub brak ostrożności użytkownika.

Uzyskanie dostępu do systemu może następnie umożliwić kradzież danych albo uruchomienie ataku ransomware, którego skutkiem jest zablokowanie dostępu do systemów i utrudnienie bieżącego funkcjonowania placówki.

Dlatego bezpieczeństwo cyfrowe wymaga odpowiednich rozwiązań technologicznych, ale również odpowiedniej świadomości i czujności osób korzystających z systemów informatycznych.

Jak działa komórka ds. cyberbezpieczeństwa w GCM?

Obecnie komórka ds. cyberbezpieczeństwa w GCM jest w trakcie przebudowy. Bezpośrednio podlega mi, a jej działania koncentrują się przede wszystkim na budowaniu bezpieczeństwa biernego w obszarze cyberbezpieczeństwa.

Do najważniejszych zadań należy opracowywanie i doskonalenie procedur bezpieczeństwa, prowadzenie szkoleń oraz systematyczne budowanie świadomości pracowników w zakresie występujących zagrożeń cybernetycznych.

Celem tych działań jest stworzenie odpowiednich mechanizmów organizacyjnych i zwiększanie odporności placówki na potencjalne zagrożenia.

Które metody zabezpieczeń danych są dla Pana absolutnym priorytetem?

Na pierwszym miejscu jest podejście wielowarstwowe. Nie ma obecnie jednego rozwiązania, które mogłoby zagwarantować pełne bezpieczeństwo danych. Kluczowe jest połączenie kilku wzajemnie uzupełniających się elementów, takich jak stałe monitorowanie infrastruktury IT, uwierzytelnianie wieloskładnikowe MFA, bieżące aktualizowanie systemów oraz wykonywanie regularnych kopii zapasowych, które powinny być również cyklicznie testowane.

Szczególne znaczenie w ochronie zdrowia mają kopie zapasowe, ponieważ pozwalają na szybkie przywrócenie działania systemów nawet w sytuacji, gdy atak ransomware zakończy się powodzeniem.

Nie można również pomijać czynnika ludzkiego. Nawet najbardziej zaawansowane zabezpieczenia techniczne nie

» To właśnie ludzie, którzy potrafią rozpoznać zagrożenie i odpowiednio zareagować, stanowią dziś najskuteczniejszą linię obrony przed cyberatakami. «

będą w pełni skuteczne, jeśli użytkownik nie rozpozna próby phishingu lub nie będzie przestrzegał podstawowych zasad bezpieczeństwa. Dlatego regularne szkolenia oraz systematyczne budowanie świadomości personelu traktuję jako istotny element ochrony danych.

Krótko mówiąc, priorytetem jest nie tylko zapobieganie atakom, ale również zdolność do ich szybkiego wykrycia, ograniczenia skutków incydentu oraz sprawnego odtworzenia danych i usług.

Jak wygląda Pana dzień pracy?

Pracując w tak dużej organizacji, trudno mówić o dwóch identycznych dniach pracy. Znaczna część moich obowiązków jest planowana z wyprzedzeniem i obejmuje koordynację projektów informatycznych, rozwój systemów, wdrażanie nowych rozwiązań oraz nadzór nad przestrzeganiem przyjętych standardów bezpieczeństwa.

Jednocześnie każdego dnia pojawiają się sytuacje wymagające bieżącej analizy, szybkiej reakcji i podejmowania decyzji operacyjnych. W obszarze cyberbezpieczeństwa istotna jest więc zarówno praca planowa, jak i gotowość do reagowania na pojawiające się zdarzenia.

Moja rola nie polega na bezpośrednim monitorowaniu zagrożeń cyberbezpieczeństwa. Sprawuję natomiast nadzór nad procesem monitorowania, który realizują wyspecjalizowani pracownicy i zespoły. Odpowiadam za zapewnienie, aby odpowiednie mechanizmy kontroli funkcjonowały skutecznie, a wykryte incydenty były właściwie analizowane i obsługiwane.

Czy cyberbezpieczeństwo placówki zdrowia kosztuje dużo?

Cyberbezpieczeństwo wymaga inwestycji, jednak zdecydowanie bardziej kosztowny może okazać się brak odpowiednich zabezpieczeń. Skutki skutecznego cyberataku to koszty techniczne związane z odtworzeniem systemów, przestoje

w funkcjonowaniu placówki, ryzyko utraty danych oraz naruszenia bezpieczeństwa danych pacjentów.

Nie oznacza to jednak, że skuteczna ochrona zawsze wymaga bardzo dużych nakładów finansowych. Wiele kluczowych działań można wdrożyć przy stosunkowo niewielkich kosztach. W pierwszej kolejności inwestowałbym w regularne wykonywanie kopii zapasowych, zapewnienie bieżącej aktualizacji systemów i oprogramowania, podnoszenie kwalifikacji zespołów IT, wdrożenie segmentacji sieci, przygotowanie procedur zwiększających odporność organizacji i ograniczających ryzyko oraz regularne szkolenia personelu. Są to rozwiązania, które mogą zapewnić wysoki poziom ochrony w stosunku do ponoszonych nakładów.

Dopiero kolejnym etapem powinno być wdrażanie bardziej zaawansowanych systemów monitorowania bezpieczeństwa, wykrywania zagrożeń czy ochrony sieci. Najważniejsze jest jednak zbudowanie solidnych podstaw, ponieważ nawet najbardziej zaawansowane i kosztowne technologie nie zastąpią wykwalifikowanego personelu oraz świadomych i odpowiedzialnych przeszkolonych użytkowników.

W ochronie zdrowia warto postrzegać cyberbezpieczeństwo jako inwestycję w ciągłość działania placówki i bezpieczeństwo pacjentów. Nakłady przeznaczone na zapobieganie incydentom mogą być wielokrotnie niższe niż koszty usuwania skutków poważnego cyberataku.

Każdy system IT czy urządzenie medyczne podłączone do sieci, a tych mogą być dziesiątki, jest potencjalną furtką dla hakerów. Jak zapanować nad szczelnością tak zawiętej infrastruktury?

To jedno z największych wyzwań współczesnej ochrony zdrowia. Rzeczywiście, każda stacja robocza, serwer, urządzenie medyczne czy aplikacja podłączona do sieci może stać się potencjalnym punktem wejścia dla atakującego. Nie da się jednak osiągnąć pełnego bezpieczeństwa poprzez zabezpie-

czenie każdego elementu osobno. Kluczowe jest systemowe podejście do zarządzania bezpieczeństwem.

W praktyce podstawą jest dokładna inwentaryzacja wszystkich zasobów, ponieważ nie można chronić czegoś, o czym nie wiemy, że istnieje. Następnie konieczne są regularne aktualizacje, segmentacja sieci, kontrola dostępu oraz ciągłe monitorowanie środowiska IT.

Coraz częściej stosujemy również zasadę „zero trust”, czyli założenie, że nie należy automatycznie ufać żadnemu użytkownikowi ani urządzeniu, nawet jeśli znajduje się wewnątrz sieci placówki. Każdy dostęp powinien być weryfikowany i nadawany wyłącznie w zakresie niezbędnym do wykonywania obowiązków.

Cyberbezpieczeństwo w tak rozbudowanym środowisku nie polega więc na stworzeniu jednej szczelnej bariery, ale na budowaniu wielu warstw ochrony. Jeżeli jedna z nich zostanie przełamana, kolejne powinny zatrzymać lub ograniczyć skutki ataku. Dzięki temu nawet rozległa infrastruktura może pozostać bezpieczna i odporna na zagrożenia.

GCM jako podmiot kluczowy też wdraża NIS2. Na jakim etapie przygotowań jest szpital?

Górnośląskie Centrum Medyczne prowadzi intensywne działania związane z dostosowaniem organizacji do wymagań dyrektywy NIS2 oraz przepisów Krajowego Systemu Cyberbezpieczeństwa. Obecnie znajdujemy się na końcowym etapie wdrożenia, obejmującym dopracowanie procedur, weryfikację

» Wdrożenie NIS2 jest szansą na uporządkowanie procesów, zwiększenie odporności organizacji na współczesne zagrożenia oraz podniesienie poziomu bezpieczeństwa danych i usług. «

przyjętych rozwiązań organizacyjnych i technicznych oraz zapewnienie pełnej zgodności z obowiązującymi wymaganiami.

NIS2 to – oprócz wdrożenia nowych narzędzi i dokumentacji – przede wszystkim zmiana podejścia do zarządzania cyberbezpieczeństwem i budowania odporności organizacji na incydenty. W praktyce oznacza to konieczność ciągłej analizy ryzyka, rozwijania procedur reagowania, podnoszenia kompetencji pracowników oraz monitorowania skuteczności wdrożonych mechanizmów ochronnych.

Największym wyzwaniem jest skala i złożoność środowiska szpitalnego. Placówka medyczna to systemy informatyczne, rozbudowana infrastruktura medyczna, liczne urządzenia diagnostyczne, systemy administracyjne oraz szerokie grono użytkowników. Wszystkie te elementy muszą współpracować w sposób bezpieczny, a jednocześnie nie mogą ograniczać podstawowej misji szpitala, jaką jest zapewnienie ciągłości świadczeń medycznych i bezpieczeństwa pacjentów.

Trudnym obszarem jest także budowanie świadomości cyberbezpieczeństwa w całej organizacji. Nawet najlepsze rozwiązania technologiczne nie zapewnią pełnej ochrony bez zaangażowania pracowników i przestrzegania przez nich przyjętych zasad. Dlatego tak duży nacisk kładziemy na szkolenia, rozwój kompetencji oraz budowanie kultury bezpieczeństwa.

W mojej ocenie wdrożenie NIS2 jest szansą na uporządkowanie procesów, zwiększenie odporności organizacji na współczesne zagrożenia oraz podniesienie poziomu bezpieczeństwa danych i usług, od których zależy funkcjonowanie szpitala i bezpieczeństwo pacjentów.

Wdrożenie jakich elementów NIS2 zalecałby Pan placówkom, których dyrektywa nie obejmuje?

Rekomendowałbym wprowadzenie przede wszystkim analizy ryzyka, regularnych kopii zapasowych, uwierzytelniania wieloskładnikowego w kluczowych systemach, procedur reagowania na incydenty oraz szkoleń pracowników. To elementy,

które znacząco zwiększają poziom bezpieczeństwa i odporność na cyberataki. Najważniejsza lekcja płynąca z NIS2 jest jednak taka, że cyberbezpieczeństwo powinno być traktowane jako stały proces zarządzania ryzykiem, a nie wyłącznie obowiązek wynikający z przepisów.

Często mówi się, że najsłabszym ogniwem ochrony danych są ludzie. Co zrobić, aby stali się najmocniejszym elementem?

Kluczem jest ciągle podnoszenie świadomości pracowników oraz budowanie kultury bezpieczeństwa w całej organizacji.

W szpitalu prowadzimy regularne szkolenia i działania edukacyjne, które pomagają pracownikom rozpoznawać zagrożenia, takie jak phishing, próby wyludzenia danych czy inne formy socjotechniki. Staramy się również uświadamiać, że cyberbezpieczeństwo nie jest wyłącznie zadaniem działu IT, ale wspólną odpowiedzialnością wszystkich osób korzystających z systemów i przetwarzających dane.

Bardzo duży nacisk kładziemy także na zgłaszanie nawet najmniejszych nieprawidłowości. W obszarze cyberbezpieczeństwa nie ma błahych incydentów. Podejrzana wiadomość e-mail, nietypowe zachowanie systemu czy próba uzyskania nieautoryzowanego dostępu mogą być pierwszym sygnałem poważniejszego zagrożenia. Dlatego zachęcamy pracowników do szybkiej eskalacji wszelkich wątpliwości i potencjalnych incydentów.

Naszym celem jest stworzenie środowiska, w którym pracownik nie obawia się zgłaszać problemów, lecz traktuje to jako naturalny element dbania o bezpieczeństwo organizacji. Dzięki temu jesteśmy w stanie szybciej identyfikować zagrożenia i skuteczniej na nie reagować.

Ostatecznie nawet najlepsze technologie nie zastąpią świadomego i zaangażowanego personelu. To właśnie ludzie, którzy potrafią rozpoznać zagrożenie i odpowiednio zareagować, stanowią dziś najskuteczniejszą linię obrony przed cyberatakami.

Czego z pracy w GCM nauczył się Pan o cyberbezpieczeństwie, hakerach?

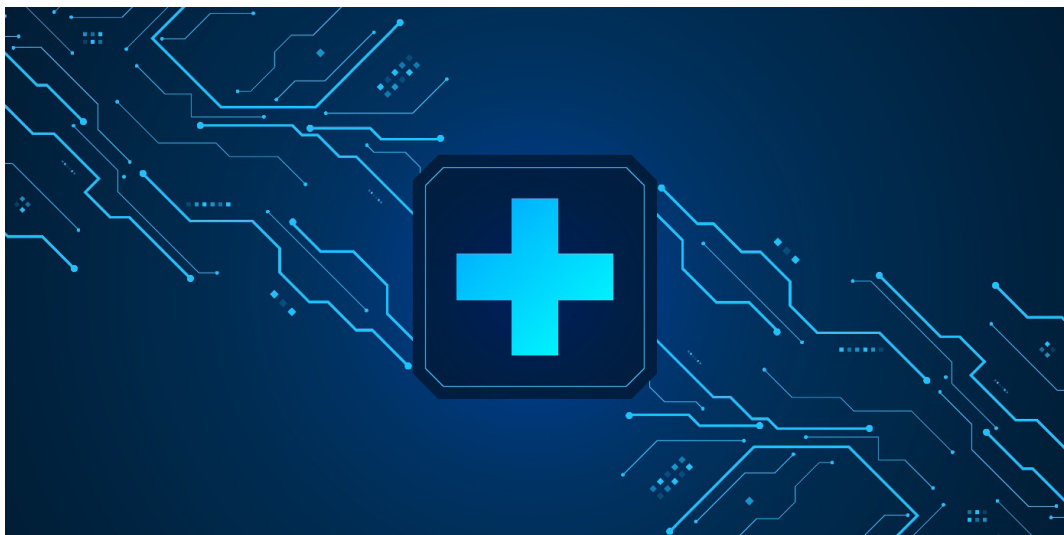
Praca w Górnośląskim Centrum Medycznym nauczyła mnie przede wszystkim, że w obszarze cyberbezpieczeństwa nie można opierać się wyłącznie na przekonaniu, że obecne zabezpieczenia są wystarczające.

Zagrożenia nieustannie ewoluują, dlatego kluczowe jest ciągle przygotowywanie się na różne scenariusze, regularne wdrażanie nowych rozwiązań oraz testowanie skuteczności istniejących mechanizmów ochrony.

Doświadczenie pokazuje również, że cyberbezpieczeństwo nie jest wyłącznie kwestią technologii. Równie ważni są ludzie, ich wiedza, doświadczenie i umiejętność współpracy. Zarządzając bezpieczeństwem tak złożonej organizacji, nauczyłem się, że warto korzystać z wiedzy i kompetencji specjalistów oraz budować kulturę otwartej wymiany informacji. Żadna osoba nie jest w stanie samodzielnie przewidzieć wszystkich zagrożeń, dlatego skuteczne działania wymagają pracy zespołowej i zaufania do ekspertów w poszczególnych obszarach.

Praca w ochronie zdrowia uświadomiła mi również, że cyberprzestępcy są coraz bardziej zorganizowani, cierpliwi i konsekwentni. Dlatego sukces w cyberbezpieczeństwie opiera się na budowaniu odporności organizacji, szybkim wykrywaniu zagrożeń i skutecznym reagowaniu na potencjalne incydenty. Nie da się całkowicie wyeliminować ryzyka – dlatego najważniejszy jest proces ciągłego doskonalenia. Jednorazowo wdrożone zabezpieczenia to za mało. ●

»Cyberbezpieczeństwo trzeba traktować
jako stały proces zarządzania ryzykiem.«



Cyberbezpieczeństwo danych. Jaka jest rola placówki zdrowia, a co zapewnia KAMSOF?



GRZEGORZ MRÓDŹ,
Prezes Zarządu KAMSOF S.A.

Nowe przepisy o cyberbezpieczeństwie – dyrektywa NIS2 i ustawa o Krajowym Systemie Cyberbezpieczeństwa – jasno pokazują jedno: bezpieczeństwo danych nie można po prostu „kupić” razem z oprogramowaniem. To wspólne zadanie, w którym producent systemu ma swoją rolę, ale kluczowa odpowiedzialność pozostaje po stronie organizacji, która na co dzień świadczy usługi medyczne, prowadzi aptekę i odpowiada za dane swoich pacjentów.

Kto odpowiada za bezpieczeństwo danych?

Obowiązki wynikające z nowych przepisów nie zależą od tego, jaki system został wybrany. Wynikają przede wszystkim z charakteru prowadzonej działalności – udzielania świadczeń zdrowotnych, prowadzenia apteki czy innej działalności objętej ustawą.

To placówka świadczy usługę pacjentowi. System informatyczny jest narzędziem, które pomaga ją realizować.

Dlatego samo korzystanie z oprogramowania, nawet bardzo dobrze zabezpieczonego, nie oznacza automatycznie spełnienia wszystkich wymagań. Tych obowiązków nie przejmie dostawca systemu ani fakt, że sam podlega podobnym regulacjom. Odpowiedzialność za zgodność organizacji z prawem pozostaje po stronie podmiotu prowadzącego działalność.

Dobra wiadomość jest taka, że nie trzeba robić tego samemu. Poniżej wyjaśniamy, jakie obowiązki w zakresie bezpieczeństwa danych są po stronie placówki, a w których obszarach może pomóc dostawca IT, czyli KAMSOFT.

Jakie obowiązki ma placówka zdrowia albo apteka?

Nadrzędne są zawsze ustawy i przepisy dotyczące ochrony danych i prowadzenia działalności leczniczej, a także wytyczne Ministerstwa Cyfryzacji czy CSIRT CeZ. Dlatego ich znajomość jest kluczowa. Ze swojej strony zalecamy następujące działania:

1. Sprawdź, jakie przepisy Cię dotyczą.

Trzeba samodzielnie ustalić, czy placówka jest tzw. podmiotem kluczowym albo ważnym. Sama działalność prowadzona w sektorze ochrony zdrowia czy farmacji tego nie przesądza – decydują o tym konkretne kryteria określone w ustawie. Tej oceny nikt nie wykona za placówkę.

2. Zgłoś placówkę i aktualizuj dane.

Jeżeli przepisy o Krajowym Systemie Cyberbezpieczeństwa KSC (adaptujące dyrektywę NIS2) mają zastosowanie, trzeba

» Dane w systemie IT placówki zdrowia są tak bezpieczne, jak dobrze zbudowany jest cały system ochrony. «

dokonać samodzielnego wpisu do Wykazu KSC i na bieżąco aktualizować zawarte w nim informacje.

3. Uporządkuj bezpieczeństwo.

Ustawa oczekuje nie pojedynczych zabezpieczeń, ale spójnego systemu zarządzania bezpieczeństwem informacji – zestawu zasad, procedur i odpowiedzialności, które działają razem.

4. Oceniaj ryzyko i dobieraj zabezpieczenia.

Trzeba regularnie sprawdzać, co może pójść nie tak, i dobierać ochronę do rzeczywistych zagrożeń oraz wielkości i charakteru placówki. Bezpieczeństwo powinno wynikać z oceny ryzyka, a nie z kopiowania rozwiązań stosowanych gdzie indziej.

5. Zadbaj o ludzi i dostęp do systemu.

Duża część bezpieczeństwa „ma miejsce” każdego dnia: przy nadawaniu i odbieraniu uprawnień, szkoleniu pracowników czy reagowaniu na podejrzone wiadomości i załączniki. Nawet najlepsze zabezpieczenia techniczne nie zastąpią czujnego zespołu.

6. Włącz i właściwie skonfiguruj dostępne zabezpieczenia.

Systemy KAMSOFT udostępniają gotowe mechanizmy ochrony, które opisujemy poniżej. Ich wykorzystanie i konfiguracja pozostają jednak po stronie placówki. Jeśli z któregoś zabezpieczenia świadomie się rezygnuje, warto to udokumentować wraz z uzasadnieniem.

7. Reaguj na incydenty i zgłaszaj je na czas.

Poważne zdarzenia trzeba odpowiednio obsłużyć i – jeśli wymagają tego przepisy – zgłosić właściwym organom w określonych terminach. Dobrze jest wcześniej wyznaczyć osobę odpowiedzialną za koordynację takich działań.

8. Instaluj aktualizacje i kontroluj dostawców.

Aktualizacje producenta należy wdrażać zgodnie z jego zaleceniami. Ważny jest także dobór i ocena pozostałych dostawców rozwiązań informatycznych.

9. Przygotuj się na audyt, jeśli jest wymagany.

Niektóre podmioty mają obowiązek okresowego audytu bezpieczeństwa swojego systemu informatycznego.

Dla placówek, które spełniały warunki w dniu wejścia w życie nowych przepisów, czyli 3 kwietnia 2026 r., orientacyjne terminy to około pół roku na wpis do wykazu, około roku na wdrożenie uporządkowanego systemu bezpieczeństwa, a w przypadku podmiotów kluczowych – do dwóch lat na pierwszy audyt. Placówki, które spełnią warunki później, liczą te terminy od swojej daty.

To wystarczająco dużo czasu, żeby spokojnie się przygotować. Nie jest go jednak na tyle dużo, żeby odkładać temat na później.

Czego KAMSOFТ nie załatwi za Państwa? Częste nieporozumienia

W rozmowach z placówkami regularnie wracają te same pytania. Odpowiadamy na nie wprost, żeby uniknąć kosztownych nieporozumień.

„Skoro mamy system KAMSOFТ, jesteście zgodni z przepisami”. Nie. Oprogramowanie jest narzędziem, które pomaga spełnić wymagania, ale samo ich nie spełnia.

„KAMSOFТ podlega tym przepisom, więc nas to nie dotyczy”. To, że KAMSOFТ jest firmą regulowaną, odnosi się do działalności KAMSOFТ. Nie znosi obowiązków wynikających z działalności placówki.

„Czy system KAMSOFТ jest certyfikowany jako zgodny z NIS2?” Nie ma takiego certyfikatu. Zgodność ocenia się w odniesieniu do całej organizacji – jej ludzi, procesów, sprzętu i sposobu korzystania z systemów – a nie samego programu.

„Dostaliśmy komplet dokumentów, więc dokumentację mamy gotową”. Udostępniane przez nas materiały stanowią punkt wyjścia. Trzeba je przeanalizować, dopasować do konkretnej placówki i włączyć do własnej dokumentacji. Samo

ich posiadanie, nawet po opatrzeniu pieczętą, nie oznacza wykonania obowiązku.

W czym KAMSOFIT może pomóc?

Odpowiedzialność placówki jest kluczowa, ale nie oznacza, że zostaje ona z tym zadaniem sama. Jako producent i dostawca wnosimy do wspólnego systemu bezpieczeństwa konkretne rozwiązania.

Bezpieczeństwo od pierwszego etapu projektowania. Nasze systemy projektujemy z myślą o bezpieczeństwie od początku. Analizujemy sposób logowania, zarządzanie uprawnieniami i potencjalne zagrożenia, zanim rozwiązanie trafi do placówki.

Gotowe mechanizmy ochrony. Systemy udostępniają m.in. logowanie dwuskładnikowe, zarządzanie uprawnieniami, rejestrowanie zdarzeń, szyfrowanie przesyłanych danych, kopie zapasowe oraz ochronę przed nieuprawnioną zmianą danych. Placówka decyduje, które mechanizmy wykorzystać i jak je skonfigurować. My dbamy o to, żeby były dostępne, aktualne i sprawdzone.

Aktualizacje i wsparcie. Regularnie wydajemy aktualizacje, informujemy o wspieranych wersjach i – w zakresie zawartej umowy – pomagamy w ich wdrożeniu. Zapewniamy również kanały zgłoszeń, w tym system MRK.

Większy zakres odpowiedzialności po naszej stronie

w chmurze. Przy korzystaniu z oprogramowania jako usługi utrzymujemy infrastrukturę, serwery, kopie zapasowe środowiska i ich monitorowanie. Po stronie placówki pozostają m.in. konta, uprawnienia, konfiguracja oraz obowiązki związane z usługą świadczoną pacjentom.

Materiały ułatwiające przygotowanie dokumentacji.

Udostępniamy wzorcowe opisy, przykładowe elementy oceny ryzyka i wytyczne, które można wykorzystać jako punkt wyjścia do własnej dokumentacji. Wymagają one jednak dopasowania do realiów konkretnej organizacji.

» To placówka zdrowia decyduje, które mechanizmy bezpieczeństwa dostawcy IT wykorzystać i jak je skonfigurować. «

Bezpieczeństwo potwierdzone również po naszej stronie.

Utrzymujemy certyfikowany system zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001. To jeden z elementów, które można uwzględnić przy ocenie dostawcy.

Jedno zastrzeżenie jest ważne: wszystkie te rozwiązania wspierają obowiązki placówki, ale ich nie zastępują. Jeśli potrzebne są zabezpieczenia wykraczające poza standardowe możliwości systemu, warto się z nami skontaktować. Pomożemy dobrać odpowiednie rozwiązanie.

Bezpieczeństwo to wspólne dzieło

W cyberbezpieczeństwie od lat funkcjonuje zasada „szwajcarskiego sera”. Każda pojedyncza warstwa ochrony ma swoje słabości. Im więcej dobrze zaprojektowanych warstw, tym mniejsze prawdopodobieństwo, że hakerowi uda się przebić przez wszystkie.

Część tych warstw budujemy my – projektując, rozwijając i zabezpieczając system. Kolejne powstają w placówce: poprzez właściwą konfigurację, szkolenie zespołu, zarządzanie dostępami i codzienne przestrzeganie procedur. Dopiero wszystkie te elementy razem tworzą skuteczną ochronę.

Żaden system nie daje stuprocentowej gwarancji. Ataki dotyczą nawet dobrze chronionych instytucji. Nie oznacza to jednak, że ochrona zdrowia jest bezbronna. Każdego dnia wiele ataków jest skutecznie wykrywanych i odpieranych dzięki technologii, procedurom i ludziom, którzy wiedzą, jak reagować.

Bezpieczeństwo cyfrowej ochrony zdrowia nie jest zadaniem jednego dostawcy ani jednej placówki. To wspólna odpowiedzialność.

My odpowiadamy za swoją część. Placówki za swoją. A najważniejszy cel pozostaje ten sam: żeby cyfrowa ochrona zdrowia była nie tylko sprawna i dostępna, ale także bezpieczna dla pacjentów i ich danych. ●



W tym szpitalu cyberatak zabił pacjenta. Lekcje z kryzysu

Londyński szpital NHS King's College od lat jest jednym z głównych celów cyberataków. W 2025 roku, paraliż spowodowany atakiem ransomware na współpracujące laboratorium doprowadził do śmierci pacjenta. W jaki sposób placówka walczy z hakerami i przygotowuje się na podobne sytuacje kryzysowe?

Pierwsza potwierdzona ofiara cyberataku. Takich przypadków jest więcej

Joe Harper, dyrektor IT w NHS King's College Hospital, z doświadczenia wie, że każdy poważny incydent cybernetyczny w szpitalu może w kilka minut stać się zagrożeniem dla zdrowia i życia pacjentów. I nawet jeśli atak nie dotyczy bezpośrednio placówki, może poważnie zakłócić jej działanie – mówi ekspert ds. bezpieczeństwa, którego spotkaliśmy podczas konferencji HIMSS Europe 2026 w maju br.

Najbardziej pamiętny dla Joe Harpera jest cyberatak z czerwca 2024 r., gdy ofiarą ransomware padła firma Synnovis, dostawca usług laboratoryjnych współpracujący właśnie m.in. z King's College Hospital. Cyberatak sparaliżował systemy diagnostyczne, doprowadził do odwołania ponad 10 tys. wizyt ambulatoryjnych i ponad 1,7 tys. zabiegów planowych.

Konsekwencje okazały się dramatyczne. W 2025 r. King's College Hospital NHS Foundation Trust potwierdził, że śmierć jednego z pacjentów była częściowo związana z opóźnieniem otrzymania wyniku badania krwi spowodowanym cyberatakiem. Był to pierwszy w Wielkiej Brytanii przypadek incydentu ransomware oficjalnie powiązany ze śmiercią pacjenta.

King's College Hospital należy do największych organizacji medycznych w Wielkiej Brytanii. To razem siedem szpitali, dwa oddziały ratunkowe oraz kilkadziesiąt placówek ambulatoryjnych i społecznościowych w południowo-wschodnim Londynie. Szpital korzysta z systemu Epic jako centralnego elektronicznego rekordu pacjenta, ale jednocześnie – podobnie jak większość europejskich placówek – zmagają się z ogromną liczbą starych aplikacji i urządzeń medycznych, których nie można tak łatwo wymienić, a które szybko mogą zostać wykorzystane przez hakerów, aby włamać się do systemu IT placówki i ukraść dane pacjentów.

Zasada nr 1: jeden system centralny zamiast dziesiątków małych aplikacji

Joe Harper zwraca uwagę, że największym problemem wielu szpitali są wieloletnie zaniedbania infrastrukturalne

»Przewieziony do innego szpitala pacjent zmarł po tym, jak w 2020 roku w Klinice Uniwersyteckiej w Düsseldorfie doszło do ataku ransomware.«

– przestarzałe aplikacje, niewspierane systemy operacyjne i urządzenia medyczne, które nadal działają, mimo że nie spełniają wymaganych standardów bezpieczeństwa.

To efekt wieloletniej ewolucji systemów IT w szpitalach. Poszczególne oddziały przez lata kupowały pojedyncze rozwiązania cyfrowe, które później próbowano integrować z centralnym systemem elektronicznej dokumentacji medycznej. W efekcie w szpitalach nadal działają pojedyncze aplikacje używane np. tylko w kardiologii czy diagnostyce obrazowej, często oparte na bardzo starych technologiach. Problem polega na tym, że tych systemów nie da się po prostu wyłączyć ani wymienić z dnia na dzień.

Harper podkreśla, że każdy taki system zwiększa „powierzchnię ataku”, czyli liczbę wrażliwych punktów, które mogą wykorzystać hakerzy. I wówczas nie pomogą nawet nowoczesne narzędzia cyberbezpieczeństwa. Część komputerów lub urządzeń medycznych pozostaje niezalutana i podatna na ataki. Dotyczy to szczególnie urządzeń medycznych, których producenci już nie wspierają, ale które nadal są wykorzystywane w praktyce klinicznej, ponieważ szpitali nie stać na ich wymianę. Najlepszym rozwiązaniem jest wdrożenie jednego zintegrowanego systemu, który wyeliminuje małe aplikacje i zapewni większą przejrzystość infrastruktury IT, a tym samym – wyższy poziom cyberbezpieczeństwa. Łatwiej nadzorować jeden system niż kilka lub dziesiątki małych aplikacji.

Brytyjska służba zdrowia NHS traktuje cyberbezpieczeństwo jako element zarządzania ryzykiem klinicznym. Priorytetem jest utrzymanie zdolności szpitala do leczenia pacjentów nawet podczas incydentu oraz wzmacnianie odporności operacyjnej, czyli tego, aby placówka mogła funkcjonować bez systemów cyfrowych i szybko wrócić do normalnego trybu pracy po ataku hakerów.

Dane w chmurze? Tak, ale ważne jest w której

Harper przypomina też o kwestii, która będzie coraz ważniejsza, czyli niezależności cyfrowej i danych. Każda placówka zdrowia musi zadać sobie pytanie, kto ma dostęp do danych

i w jaki sposób są one wykorzystywane. Dotyczy to zwłaszcza rozwiązań AI rozwijanych w środowiskach chmurowych należących do globalnych dostawców technologii, takich jak AWS lub Microsoft Azure. Coraz częściej pojawiają się obawy m.in. o dostęp do danych szpitali przez koncerny AI, które potrzebują danych z EDM do trenowania modeli AI. Harper wskazuje, że szpitale muszą dokładnie wiedzieć, gdzie trafiają dane pacjentów i jakie ryzyko wiąże się z ich przetwarzaniem poza organizacją.

Wielka Brytania ma w tym obszarze negatywne doświadczenia. W 2017 r. Royal Free London NHS Foundation Trust nawiązał współpracę z należącym do Google DeepMind. W efekcie DeepMind uzyskał dostęp do danych ok. 1,6 mln pacjentów. W 2025 r., po protestach lekarzy rodzinnych i pytaniach o zgodę pacjentów, NHS England czasowo wstrzymał projekt *Foresight*, który zakładał wykorzystanie zanonimizowanych danych 57 mln pacjentów do trenowania modelu generatywnej AI. Duży sprzeciw wywołał projekt *Federated Data Platform* realizowany przez Palantir. Stało się to po doniesieniach, że pracownicy zewnętrznych firm mogli uzyskać dostęp do identyfikowalnych danych pacjentów NHS przed ich pseudonimizacją.

Jak mówi Joe Harper, NHS coraz większy nacisk kładzie na zaangażowanie osób ze szczebla kierownictwa w cyberbezpieczeństwo. Regularne rozmowy z zarządem są często trudne i wymagają tłumaczenia technicznych zagadnień osobom nietechnicznym, ale właśnie to pozwala budować realne zrozumienie ryzyka. Dzięki temu cyberbezpieczeństwo przestaje być wyłącznie „problemem IT”.

Ważnym elementem jest również jasne określenie poziomu akceptowalnego ryzyka. Zarząd szpitala musi wiedzieć, które ryzyka zostały ograniczone, które zaakceptowane, a które przeniesione na dostawców. Według Harpera tylko wtedy zespoły IT mogą przestać „gasić pożary” i skupić się na realnym wzmacnianiu odporności organizacji.

» Szpital wdrożył podejście „command and control” pozwalające szybko podejmować decyzje w sytuacjach kryzysowych. «

Szpital musi działać po cyberataku – i to za wszelką cenę

Każdy szpital musi mieć dobrze przygotowane procedury funkcjonowania w warunkach ograniczonej dostępności systemów cyfrowych. Jak zaznacza Harper, prędzej czy później trzeba będzie do nich sięgnąć, bo cyberatak to kwestia czasu. King’s College Hospital musiał przejść na procedury awaryjne podczas wspomnianego wcześniej ataku ransomware na zewnętrznego dostawcę usług laboratoryjnych Synnovis. Choć sama placówka nie została bezpośrednio zhakowana, konieczna była reorganizacja opieki, przepływu pacjentów oraz diagnostyki. Szpitalowi udało się utrzymać ciągłość świadczeń, ale musiał działać w zupełnie innym modelu operacyjnym.

Szpitalom muszą regularnie ćwiczyć scenariusze kryzysowe – podkreśla Harper. W NHS funkcjonują struktury *command and control* wzorowane częściowo na procedurach stosowanych podczas pandemii COVID-19. Chodzi o scentralizowany model zarządzania kryzysowego, który ma na celu szybkie podejmowanie decyzji w trakcie kryzysu. W przypadku ataku hakerów to np. automatyczne przejście na pracę z papierową dokumentacją oraz uruchomienie alternatywnych ścieżek pracy klinicznej. Wówczas nie ma czasu na procedury stosowane codziennie, trzeba działać szybko na podstawie wcześniej przygotowanych planów awaryjnych.

NHS kładzie też duży nacisk na szkolenia personelu. Podczas jednego z ćwiczeń phishingowych, aż 6 proc. pracowników kliknęło w fałszywe wiadomości i przekazało hakerom hasła dostępu. Jak podkreśla Harper, czynnik ludzki jest i będzie najsłabszym ogniwem. Dlatego jego celem jako szefa IT w szpitalu King’s College nie jest wcale stworzenie idealnego systemu odpornego na każdy atak – to jest po prostu nierealne. Dużo ważniejsze jest zbudowanie organizacji zdolnej do utrzymania ciągłości leczenia pacjentów nawet podczas poważnego incydentu cyfrowego oraz szybkie przywrócenie normalnego trybu działania. ●



KAMSOFT

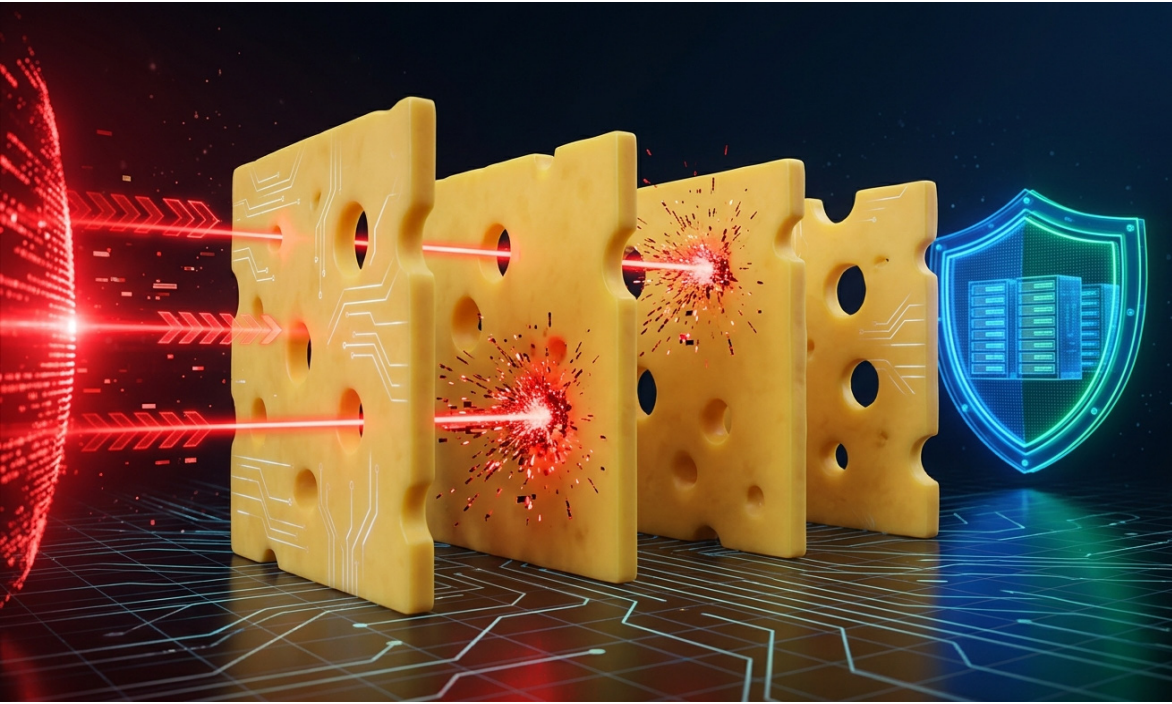
Doświadczenie. Zastosowane.

Od ponad 40 lat tworzymy rozwiązania dla ochrony zdrowia, które każdego dnia wspierają placówki medyczne, apteki i cały ekosystem rynku zdrowia.

Łączymy doświadczenie z nowoczesnymi technologiami, dbając o bezpieczeństwo danych, ciągłość działania i zgodność z wymaganiami sektora ochrony zdrowia.

KAMSOFT | Technologia, której można zaufać.





Ochrona danych w modelu sera szwajcarskiego

Nie ma jednego narzędzia lub procedury zapewniającej 100% ochrony przed cyberatakami. Ale im więcej warstw zabezpieczeń, tym większa szczelność systemu. Nawet, jeśli hakerzy przedostaną się przez jedną zaporę techniczno-organizacyjną, zatrzymać ich może kolejny poziom ochrony.

Ochrona danych opiera się na systemie różnych zabezpieczeń

Hakerzy wykorzystują różne metody, aby wykraść dane medyczne – to może być złośliwe oprogramowanie ransomware, phishing mający skłonić nieświadome ofiary do przekazania danych logowania albo atak cybernetyczny polegający na znalezieniu słabego ogniwa w zabezpieczeniach technicznych. Dlatego nie ma jednej, uniwersalnej metody ochrony danych, której implementacja gwarantuje, że można spać spokojnie. Zamiast tego eksperci zalecają stworzenie wielowarstwowego systemu zabezpieczeń składającego się z technicznych środków ochrony (oprogramowanie chroniące przed cyberatakami) i organizacyjnych (procedury pracy).

» W modelu sera szwajcarskiego, nigdy nie wiadomo, które dziury w systemie znajdują i wykorzystają hakerzy. «

Każdy z elementów takiego systemu ma swoje zalety, ale też swoje słabe punkty i ograniczenia. Nawet jeśli podmiot leczniczy stosuje oprogramowanie antywirusowe i filtry antyspamowe, złośliwe oprogramowanie może przedostać się do sieci placówki po tym, jak pracownik kliknie w link znajdujący się w zainfekowanej wiadomości e-mail. Jednak w takim przypadku, przed dużymi stratami może uchronić kolejna warstwa systemu bezpieczeństwa, przykładowo zgłoszenie incydentu i zmiana hasel.

Koncepcja ochrony wielowarstwowej podobna jest do „siera szwajcarskiego”. Każdy plaster (metoda zabezpieczenia danych) posiada dziury (słabe punkty). Ale kiedy stworzymy system stworzony z wielu plastrów, szczelność całości znacznie wzrośnie. Taki ekosystem ochrony powinien być mieszaną technologii, procedur postępowania, zasobów kadrowych (osoby odpowiedzialne za cyberbezpieczeństwo, inspektor ochrony danych), szkoleń dla pracowników, fizycznych systemów zabezpieczeń itd.

W zakresie bezpieczeństwa danych, wyróżnia się trzy główne kategorie barier (grup plastrów):

- **Technologia.** Wszystkie zabezpieczenia na poziomie systemów: aktualne systemy operacyjne i antywirusowe, automatyczne tworzenie kopii zapasowych, filtry anty-

spamowe, odpowiednia konfiguracja systemu uprawnień w systemach IT, mocne hasła dostępu, wirtualne sieci prywatne VPN, serwery i chmury danych itd.;

- **Ludzie.** Umiejętność identyfikacji zagrożenia i reagowania na nie: zdolność rozpoznania wiadomości typu phishing, usuwanie i zgłaszanie podejrzanych maili, zabezpieczenie nośników danych i sprzętu przenośnego, wiedza na temat procedur ochrony danych, znajomość procedur w przypadku ataku cybernetycznego;
- **Procedury.** Polityka ochrony danych, plany postępowania z ryzykiem, identyfikacja podatności systemów, procedury na wypadek ataków cybernetycznych, audyty bezpieczeństwa danych, monitorowanie zasobów, procedury onboarding pracowników i plany szkoleń itd. W tworzeniu systemu zabezpieczeń trzeba pamiętać, że nie wszystkie dane mają taką samą wartość i priorytet ochrony. Każda placówka musi przeprowadzić weryfikację gromadzonych i przetwarzanych danych, aby skoncentrować się na ochronie tych najbardziej wrażliwych.

Z kolei kategoryzacja funkcjonalna zabezpieczeń zawiera takie warstwy jak:

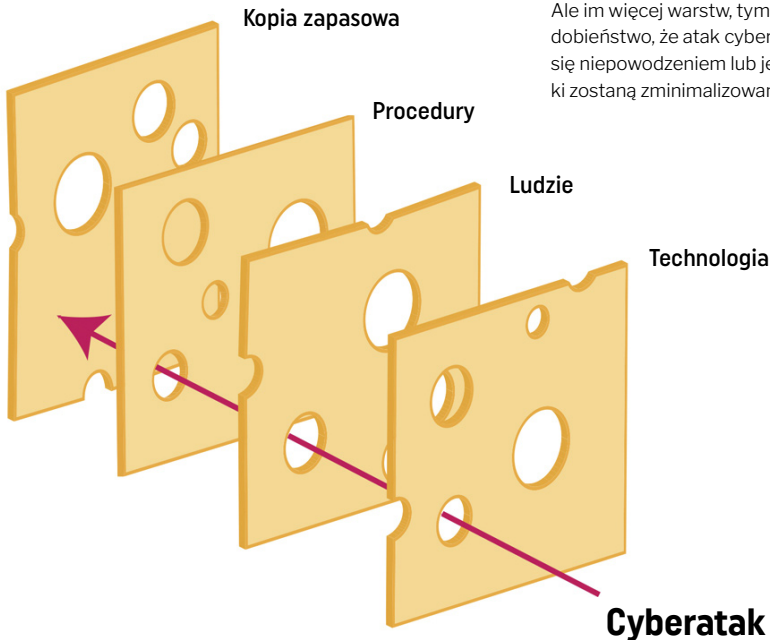
- **Bezpieczeństwo obwodowe** (infrastruktura techniczna): bariery fizyczne, cyfrowe systemy zabezpieczeń, kontrola dostępu, mechanizmy uwierzytelniania;
- **Bezpieczeństwo sieci** (infrastruktura sieciowa): firewall, VPN, kontrola dostępu;
- **Szkolenia dla pracowników** (wiedza i know-how): jak rozpoznać i reagować na zagrożenia, symulacje phishingu, procedury raportowania zdarzeń związanych z atakami cybernetycznymi, polityka IT i bezpieczeństwa;
- **Ochrona punktów końcowych** (infrastruktura IT): oprogramowanie antywirusowe, filtr antyspamowy, uwierzytelnienie wielopoziomowe, zarządzanie słabymi punktami zabezpieczeń;
- **Monitoring w czasie rzeczywistym:** kontrola i wykrywanie zagrożeń, usuwanie ich skutków;

- **Odzyskiwanie danych w sytuacjach awaryjnych:** kopie zapasowe, plan ciągłości działania, ubezpieczenie od cyberataków.

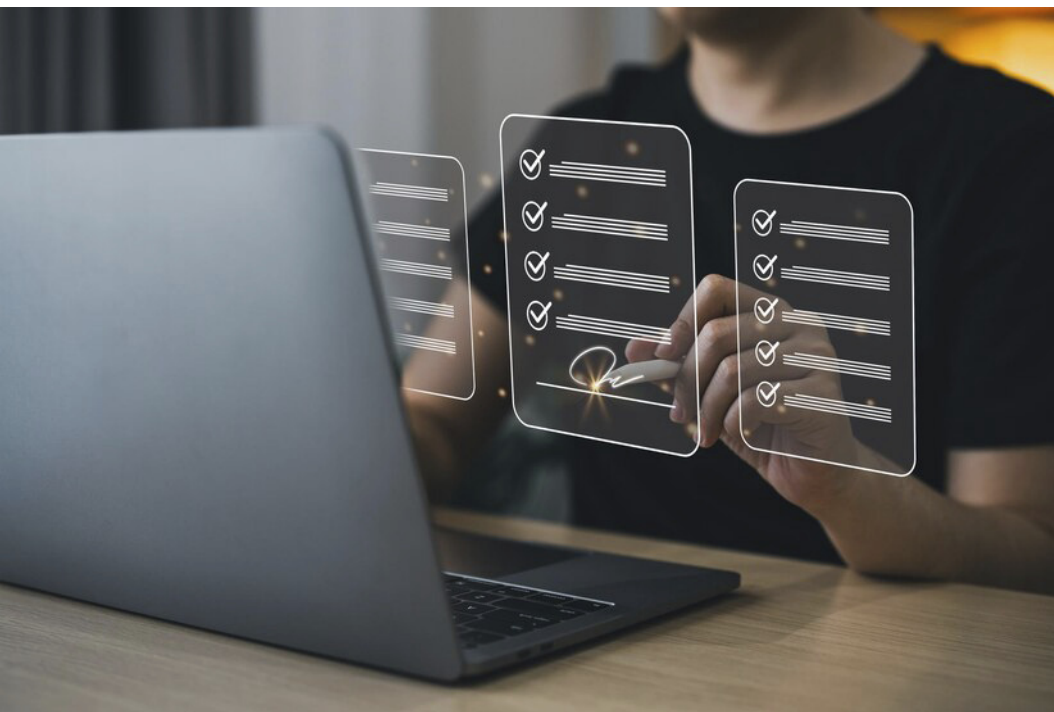
Opcja awaryjna, czyli kopia danych

Tworzenie szczelnej zapory z plasterków różnych rozwiązań i procedur to proces ciągły. Taki system trzeba na bieżąco pielęgnować organizując cykliczne szkolenia dla pracowników, aktualizując zabezpieczenia techniczne oraz dokładając nowe warstwy w odpowiedzi na nowe metody działania hakerów.

W schemacie sera szwajcarskiego ostatnim plasterkiem jest bezpieczna i aktualna kopia zapasowa i plan ciągłości działania, który pozwoli nieprzerwanie świadczyć usługi medyczne podczas przywracania sprawności systemu IT, gwarantując bezpieczeństwo pacjenta. ●



Model „sera szwajcarskiego”. Każdy system i procedura ochrony danych mają słabe punkty. Ale im więcej warstw, tym większe prawdopodobieństwo, że atak cybernetyczny zakończy się niepowodzeniem lub jego negatywne skutki zostaną zminimalizowane.



Za 80% poziomu bezpieczeństwa odpowiada 20% bazowych zabezpieczeń

Zaniedbania cyberbezpieczeństwa w ochronie zdrowia nie wynikają ze złej woli, ale z przekonania, że ochrona danych jest skomplikowana, droga i czasochłonna.

Hakerzy rzadko kiedy atakują celowo. Raczej liczą na łut szczęścia

Ochrona danych zaczyna się od zrozumienia, że to wspólny wysilek całej organizacji. Dział IT dba o zabezpieczenia techniczne, a pracownicy znający tricki cyberprzestępców zapewniają ochronę na pierwszej linii. Ich rola jest kluczowa, bo zdecydowana większość ataków ma charakter masowy. Ale to nie oznacza, że szpital albo małe placówki zdrowia nigdy nie staną się celem ataku celowanego.

W pozostałych przypadkach hakerzy zarzucają na ślepo sieci, licząc, że wpadnie w nie przypadkowa ofiara. A dokładnie – wysyłają masowo wiadomości phishingowe i czekają, aż nieświadomy pracownik kliknie na zainfekowany załącznik albo link i tym samym otworzy szczelne bramy do danych. Gdy tak się stanie, cyberprzestępcy błyskawicznie kradną dane i opcjonalnie blokują system. Jeszcze kilka lat temu kończyli na zablokowaniu komputera. Jednak odkąd coraz więcej podmiotów leczniczych tworzy kopie zapasowe pozwalające na szybkie przywrócenie ciągłości działania, zmienili swoją strategię. Teraz szantażują upublicznieniem wykradzionych danych pacjentów, licząc, że to skłoni podmiot do zapłaty okupu.

Ochrona danych wszyta w kulturę organizacyjną

Większość skutecznych cyberataków wykorzystuje proste luki i karygodne zaniedbania w zabezpieczeniach technicznych albo niewiedzę pracowników na temat działania ransomware oraz phishingu. Problemem nie jest to, że szpitale i przychodnie nie mają zaawansowanych zabezpieczeń technicznych, ale niedociągnięcia w podstawowych kwestiach jak szkolenia personelu albo aktualizacje systemów.

Ochrona danych nie zawsze wymaga od razu zatrudnienia ekspertów cyberbezpieczeństwa i dużych inwestycji finansowych. Małe placówki, które z reguły nie są na celowniku hakerów, powinny skupić się na prostych zasadach cyberhigieny, jak oddzielenie sieci do zadań prywatnych od sieci gromadzenia i przetwarzania danych pacjentów,

» Małe placówki, które z reguły nie są na celowniku hakerów, powinny skupić się na prostych zasadach cyberhigieny. «

nieinstalowania na komputerach do gromadzenia EDM innych systemów (przeglądarki internetowej, poczta e-mail), szkoleniach z cyberbezpieczeństwa (poprawa świadomości ochrony danych), logowanie wieloskładnikowe do krytycznych zasobów, kopie danych w czasie rzeczywistym.

Są to pasywne elementy bezpieczeństwa, czyli stałe zabezpieczenia zapewniające ochronę niezależnie od metod działania hakerów. Na wyższym poziomie znajduje się aktywne podejście obejmujące monitorowanie zagrożeń ze strony hakerów oraz zarządzanie ryzykiem.

Oto checklista, która pozwoli ci sprawdzić, czy dobrze chronisz dane.

Zarządzanie ryzykiem. Czy znasz wszystkie punkty końcowe zbierania danych? Czy są one odpowiednio chronione? Czy przeprowadziłeś ocenę ryzyka dotyczącą zasobów IT i ustaliłeś priorytety ochrony? Czy wdrożyłeś zabezpieczenia adekwatne do przeprowadzonej analizy ryzyka?

RODO i audyty. Czy pracownicy znają i stosują zasady ochrony danych pacjentów? Czy przeprowadzane są audyty RODO i wewnętrzne/zewnętrzne audyty bezpieczeństwa? Czy wdrożono kodeksy postępowania RODO zatwierdzone przez UODO?

Kontrola dostępu do danych. Czy dane pacjentów są dobrze chronione przed dostępem osób nieuprawnionych? Czy personel stosuje silne, systematycznie zmieniane hasła? Czy odpowiednio nadano role w systemie IT, aby zarządzać dostępem do danych? Czy są one regularnie aktualizowane?

Ustawienia prywatności. Czy komputery, na których gromadzona jest EDM, mają włączone autowylgowywanie się? Czy zablokowano porty USB? Czy lokalizacja komputerów i opcje blokowania ekranu zapewniają prywatność danych?

Ochrona sprzętu i zasobów. Czy serwery oraz komputery są odpowiednio chronione? Czy stosowane są systemy monitoringu zagrożeń, oprogramowanie antywirusowe i filtry antyspamowe? Czy dane są szyfrowane? Czy lekarze

pracujący zdalnie łączą się z bazą danych poprzez VPN (wirtualną sieć prywatną)?

Procedury. Czy wdrożono zarządzanie dostawcami? Czy monitorujesz dostawców i usługodawców pod względem przestrzegania praktyk bezpieczeństwa? Czy umowy z dostawcami zawierają klauzule bezpieczeństwa danych?

Zarządzanie bezpieczeństwem sieciowym. Czy sieć placówki medycznej została podzielona na część obsługującą wrażliwe dane i systemy (system elektronicznej dokumentacji medycznej) i inne zadania (np. korzystanie ze stron internetowych przez pracowników, sieć WiFi dla pacjentów)? Czy dostęp pracowników do skrzynki e-mail jest bezpieczny?

Szkolenia pracowników. Czy istnieje plan szkoleń z cyberbezpieczeństwa? Czy przygotowano instrukcje onboardingu dla nowych pracowników z uwzględnieniem zasad ochrony danych? Czy pracownicy są regularnie informowani o nowych rodzajach zagrożeń? Czy pracownicy są świadomi swojej roli w systemie cyberbezpieczeństwa? Czy prowadzone są kontrolowane testy bezpieczeństwa?

Monitoring ataków cybernetycznych. Czy posiadasz rozwiązanie techniczne do monitoringu ataków hakerskich? Czy w razie ataku zostaniesz o nim poinformowany, abyś mógł niezwłocznie zareagować? Czy monitorujesz ruch sieciowy i niebezpieczne zachowania użytkowników?

Usuwanie luk w systemie bezpieczeństwa. Czy istnieje procedura regularnego sprawdzania, czy oprogramowanie i sprzęt są zaktualizowane do najnowszych wersji? Czy otrzymujesz informacje o nowych latkach bezpieczeństwa w systemach IT i sprzęcie?

Reagowanie na incydenty. Czy posiadasz procedurę na wypadek ataku hakerów? Czy organizacja ćwiczy regularnie scenariusze ataków i usuwania ich skutków? Czy wiesz jak powstrzymać lub wyeliminować zagrożenie, odzyskać sprawność działania organizacji i przyjąć pacjentów? Czy pracownicy wiedzą, co robić w przypadku wykrycia zagrożenia?

Plan komunikacji. Czy istnieje plan komunikacji z pracownikami w razie skutecznego ataku cybernetycznego? Czy istnieją procedury komunikacji z pacjentami? Czy pracownicy wiedzą jak bezpiecznie kontynuować opiekę nad pacjentem w przypadku incydentów cybernetycznych?

Wiedza o zagrożeniach. Czy znasz aktualne ostrzeżenia instytucji odpowiedzialnych za bezpieczeństwo danych, jak np. NASK. Czy wiesz, gdzie zgłosić atak hakerski i wyciek danych? Czy gromadzisz informacje o udanych atakach i na ich podstawie zwiększasz własne kompetencje?

Inwestycje w ochronę techniczną. Czy placówka medyczna ma wydzielony budżet celowy na ochronę danych? Czy monitorowane są aktualne oferty szkoleń dla ochrony zdrowia oraz programy dofinansowania cyberbezpieczeństwa? ●

 reklama

BLOG

OSOZ

„MEDYCyna ROZWIJA SIĘ DZIĘKI INNOWACJAM. WIEMY, KTÓRE Z NICH SĄ WAŻNE”


 blog.osoz.pl



Jaki program antywirusowy? I czy Windows wystarczy, aby dobrze chronić dane?

Program antywirusowy i aktualny system operacyjny to absolutne minimum ochrony danych. Tłumaczymy, jak szybko zadbać o wysoki poziom cyberbezpieczeństwa bez zawracania sobie głowy informatyką.

Łatwy łup dla hakerów

„Informatyka jest skomplikowana i nie mam na nią czasu” – wielu lekarzy, którzy często są menedżerami indywidualnych praktyk nie korzysta nawet z podstawowych zabezpieczeń danych medycznych.

Dlaczego? Bo albo są zapracowani, nie wiedzą, jak się do tego zabrać, albo myślą, że hakerzy interesują się tylko dużymi placówkami. Prawdą jest, że hakerzy rzadko kiedy wybierają za cel ataku konkretną indywidualną praktykę, bo potencjalny zysk jest za mały w stosunku do czasu potrzebnego na włamanie się do systemu. Ale małe placówki powinny bać się ataków „na ślepo”, czyli masowo wysyłanego spamu ze złośliwym oprogramowaniem albo zainfekowanych stron w Internecie.

Brakuje dokładnych badań pokazujących skalę stosowania programów antywirusowych na komputerach u lekarzy, w przychodniach i szpitalach. Ale można się domyślać, że dobrze nie jest. Z najnowszego badania przeprowadzonego na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych wynika, że tylko 35 proc. mikroprzedsiębiorców ma zainstalowane na firmowych komputerach pełne wersje programów antywirusowych. W przypadku indywidualnych praktyk lekarskich skala może być podobna. A to oznacza, że w większości mikro-placówek zdrowia, dane są zagrożone.

Przekonanie, że ochrona danych medycznych to jakaś wyższa szkoła jazdy, jest błędne. Dobry system ochrony można zredukować do pięciu elementów:

- aktualnego systemu operacyjnego i systemu gabinetowego,
- programu antywirusowego,
- mocnego i systematycznie zmienianego hasła,
- podwójnej autentyfikacji,
- kopii zapasowej bazy danych.

Słowo kluczowe w filozofii ochrony danych to „aktualny” – aktualny system i antywirus, aktualna wiedza i kopia zapasowa. Skupmy się na pierwszych dwóch elementach – systemie operacyjnym i oprogramowaniu antywirusowym.

» Aktualna wersja Windowsa 11 całkiem dobrze chroni komputer. Ale do łatwego serwisowania komputera, przyda się płatny antywirus. «

Czy wystarczy sam Windows?

Zdecydowana większość placówek medycznych i lekarzy korzysta z systemu operacyjnego Windows. Jeśli jest aktualny, zyskujemy już bardzo mocną ochronę danych. Statystyki z 2026 roku pokazują, że nadal prawie **30–50% komputerów w Polsce korzysta z Windows 10**, podczas gdy najnowszy Windows 11 jest już dostępny od 5 lat. Nie wspominając o 2% osób mających jeszcze archaicznego Windowsa 7.

Pamiętajmy, że wsparcie techniczne dla systemu Windows 10 oficjalnie zakończyło się w październiku 2025 roku, a więc korzystanie z niego jest po prostu niebezpieczne.

Dlaczego Windows 11? Bo daje solidną ochronę, nawet jeśli na komputerze nie ma antywirusa. W systemie jest zaszyty Microsoft Defender, czyli mocne rozwiązanie antywirusowe, które jest aktualizowane na bieżąco. Jeśli użytkownik nie wyłączył automatycznych aktualizacji Windows – czego nie powinno się robić w żadnym wypadku – komputer jest chroniony. Windows ma też zaporę ogniową, która uniemożliwia hakerom lub złośliwemu oprogramowaniu uzyskanie dostępu do komputera za pośrednictwem Internetu lub sieci.

W przypadku pracy zdalnej (wizyty domowe), w Win 11 łatwo zainstalować VPN do szyfrowania danych. Windows ma też system zabezpieczeń hasel i zarządzania nimi. Według danych Microsoft, **w każdej sekundzie dochodzi do ponad 920 ataków na hasła**. Nowe komputery umożliwiają logowanie się odciskiem palca albo na podstawie skanowania twarzy.

Jaki antywirus wybrać?

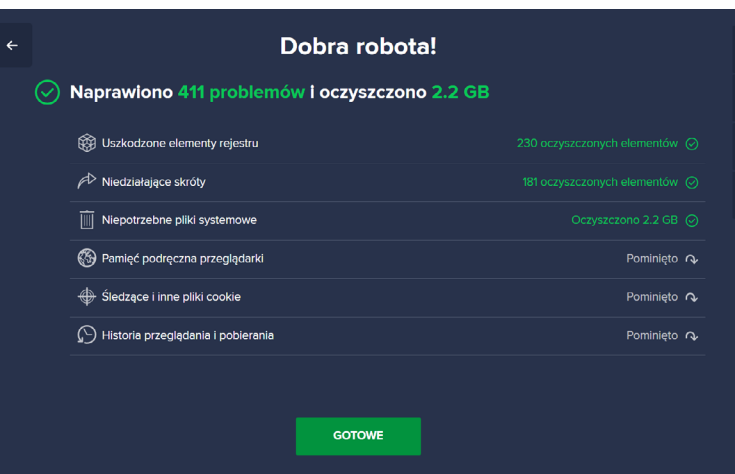
Microsoft zrobił ogromny postęp w ochronie danych użytkowników Windowsa. Osobom, które nie mają na komputerach wrażliwych danych, nowy system może wystarczyć. Ale w ochronie danych medycznych zalecana jest dodatkowa warstwa w postaci programu antywirusowego. Najlepiej takiego, który będzie automatycznie wykonywał konserwację komputera, pełniąc rolę cyfrowego mini-informatyka.

Najważniejsza informacja jest taka, że każdy z najpopularniejszych antywirusów gwarantuje dobry poziom ochrony. Z kilkoma wyjątkami. Jednym z nich jest system Kaspersky, z którego korzysta ok. 400 mln osób na świecie. Jednak nie dlatego, że źle chroni dane, ale ze względu na to, że firma ma siedzibę w Rosji. Administracja Prezydenta USA Joe Bidena nałożyła na Kaspersky'ego sankcje, w wyniku czego w lipcu 2024 r. firma rozpoczęła wychodzenie z amerykańskiego rynku. Ze względów etycznych, z recenzowania i reklamowania antywirusa wycofało się wiele portali internetowych. Dlatego także w naszej analizie nie będziemy brać pod uwagę tego programu.

W najnowszym teście portalu Komputer Świat najlepiej wypadły trzy płatne systemy:

- Norton 360 Advanced,
- Bitdefender Premium Security,
- Avast One.

Koszt zakupu mieści się pomiędzy 60 a 200 zł w licencji rocznej, najczęściej na 1 komputer. Alternatywą są bezpłatne systemy, które też oferują całkiem dobrą ochronę. Według portalu Antyweb.pl, najlepsze to Avast Free Antivirus, AVG



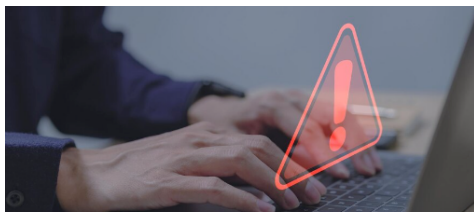
Komunikat z Avast o przeprowadzonej konserwacji. Obsługa systemu jest maksymalnie prosta

AntiVirus Free oraz Avira Free Security – wykrywają one złośliwe oprogramowanie, zagrożenia sieciowe, analizują podejrzaną pliki, skanują pocztę e-mail, sprawdzają i blokują w razie zagrożenia niebezpieczne strony internetowe. Ale brakuje im wielu funkcji jak VPN, ukrywanie adresu IP albo wsparcie techniczne.

Przewagą antywirusów dostawców zewnętrznych nad Microsoft Defender wbudowanym w Windows jest przejrzysty interfejs użytkownika. Oferują też dodatkowe opcje jak ochrona tożsamości, menedżer haseł oraz funkcje serwisowe. Przykładowo, Avast Cleanup (dodatkowa płatna licencja) oferuje wsparcie techniczne, automatycznie serwisując komputer, naprawiając uszkodzone rejestry, usuwając niepotrzebne pliki systemowe albo pliki śledzące cookie.

Zwycięzca testu Komputer Świata, czyli Norton 360 Advanced, posiada wiele dodatkowych zalet jak np. nie spowalnia komputera, oferuje dobry VPN zwiększający bezpieczeństwo przesyłania danych.

Jaki program antywirusowy ostatecznie wybrać? Różnice pomiędzy liderami rankingów – czyli Norton 360 Advanced, Bitdefender Premium Security, Avast One, Avira Premium – są niewielkie. Każdy zwiększy bezpieczeństwo danych przy maksymalnej prostocie obsługi. ●



Aktualne informacje o bezpieczeństwie danych w placówkach ochrony zdrowia znajdziesz na blog.osoz.pl.

UODO nakłada karę 1,5 mln zł na American Heart of Poland

To pokłosie ataku hakerów, w wyniku którego wyciekły dane 21 tys. osób. UODO zarzuca AHP niski poziom bezpieczeństwa danych i zaniedbania w analizie ryzyka.



Ochrona danych w indywidualnej praktyce lekarskiej. „Już za ok. 1400 zł rocznie można uchronić się przed 90 proc. ataków”

Kiedy duże szpitale nadrabiają zaległości w cyberbezpieczeństwie, między innymi dzięki środkom z KPO, małe, indywidualne praktyki lekarskie stają się łatwym łupem dla hakerów. Ale dobra ochrona danych to kwestia prostych zabezpieczeń za ok. 116 zł miesięcznie.

1400 zł – tyle biorą hakerzy za ukradzioną kartotekę medyczną pacjenta

Szacuje się, że 8 na 10 lekarzy doświadczyło próby ataku hakerskiego. Złamanie zabezpieczeń jest znacznie łatwiejsze niż w przypadku coraz lepiej chronionych dużych placówek, przy czym wartość danych i obietnica szybkiego zarobku – takie same albo większe. Lekarz, który przez lata pracował na zaufanie swoich pacjentów, może je stracić w ułamku sekundy. Hakerzy o tym dobrze wiedzą.

Nawet 1400 zł kosztuje w darknecie skradziona kartoteka medyczna. To znacznie więcej niż dane karty kredytowej, które można zdobyć już za 25 zł. Chętnych, żeby je kupić, nie brakuje, bo to łatwe narzędzie wywierania przez przestępców presji okupu na lekarzy. W przypadku ataku ransomware, w panice wiele osób woli przelać w bitcoina kilka tysięcy złotych, aby szybko odblokować komputer. Według statystyk, robi to ok. 20–50% ofiar. Zapłata nie gwarantuje jednak, że haker nie wykradł dodatkowo danych, potem ktoś je kupi i w krótkim czasie pojawiają się kolejne szantaże i groźby. Ataków phishingowych przybywa, a hakerzy coraz lepiej podszywają się pod NFZ i ZUS, aby przekonać do kliknięcia w zainfekowany link.

Brak zabezpieczeń przed hakerami to ryzykowna gra, która może źle się skończyć. A wystarczy nieco ponad 100 złotych miesięcznie, aby spać spokojniej.

Menedżer haseł dla całego gabinetu

Najczęstszą przyczyną włamania do komputera, a następnie do systemu gabinetowego, są słabe hasła. Eksperti zalecają stosowanie menedżerów haseł, które generują długie, unikalne hasła złożone z różnych kombinacji liter, cyfr i znaków specjalnych oraz przechowują je w zaszyfrowanej bazie. Menedżer haseł jest dostępny za darmo m.in. w przeglądarce internetowej Chrome od Google i Edge od Microsoft. Mają go też popularne systemy antywirusowe w wersjach premium, jak np. Avast. Użytkownik musi pamiętać tylko hasło główne do menedżera.

Dwuskładnikowe uwierzytelnianie

Nawet jeśli haker zdobędzie hasło, nie dostanie się do systemu zabezpieczonego tzw. 2FA, czyli metodą dwuetapowego uwierzytelniania. Logowanie trzeba wówczas potwierdzić kodem wysłanym na aplikację w telefonie. 2FA znacząco redukuje ryzyko skutecznego ataku i stało się standardem zabezpieczenia danych.

2FA można włączyć za darmo m.in. w poczcie internetowej. Jest też wymagane podczas logowania do platform ZUS i NFZ. Wspierają go np. bezpłatny Microsoft Authenticator albo Google Authenticator oraz niektóre aplikacje mobilne dla lekarzy i pielęgniarek.

Chmurowe kopie zapasowe z wersjonowaniem

Kiedy lekarz kliknie przez nieuwagę na link albo załącznik w wiadomości phishingowej, na komputerze zostanie zainstalowane złośliwe oprogramowanie ransomware. Szyfruje ono dane, a na ekranie pojawia się żądanie okupu. Komputer zostaje zablokowany. Jeśli nie utworzono kopii zapasowej, często oznacza to bezpowrotną utratę bazy danych. W tym czarnym scenariuszu lekarz traci w jednej chwili dostęp do wszystkich kartotek swoich pacjentów, terminów, kontaktów – danych zbieranych przez kilka, kilkanaście lat.

Jedynym ratunkiem jest kopia zapasowa na innym nośniku danych, a najlepiej w innej lokalizacji, bo dane można stracić też w wyniku np. poważnej awarii komputera, pożaru, kradzieży itd. Najwygodniejszą i niewymagającą żadnych dodatkowych czynności (oprócz jednorazowej konfiguracji) jest kopia w chmurze danych. Taki backup jest coraz tańszy.

» Lekarz może w jednej chwili stracić dostęp do wszystkich kartotek swoich pacjentów, terminów, kontaktów – danych zbieranych przez kilka, kilkanaście lat. «

Przykładowo, w systemie KS-PPS firmy KAMSOFIT kosztuje ok. 611 zł netto rocznie za jeden serwer. Systemy gabinetowe mają też inne opcje bezpieczeństwa danych, jak np. moduł ułatwiający spełnienie wymagań RODO (cena także ok. 640 zł za pierwszy rok).

Szyfrowanie dysków i urządzeń mobilnych

System Windows 11 Pro oraz macOS oferują wbudowane szyfrowanie dysku, tzw. BitLocker (Windows) oraz FileVault (Apple). Jego aktywacja jest bezpłatna.

Po co szyfrować dyski? Jeśli urządzenie zostanie skradzione lub zgubione, dostęp do danych pacjentów – w przypadku lokalnej bazy danych – będzie znacznie utrudniony. Szyfrowanie jest też kluczowe w kontekście RODO. W przypadku urządzeń mobilnych, jak smartfon albo tablet, szyfrowanie najczęściej aktywowane jest automatycznie, np. poprzez FaceID (rozpoznawanie twarzy) lub TouchID (odcisk palca).

Szkolenie z cyberbezpieczeństwa i phishingu

Lekarze regularnie uczestniczą w konferencjach oraz szkoleniach, aby zaktualizować swoją wiedzę medyczną. Warto je uzupełnić o przynajmniej jedno szkolenie rocznie na temat bezpieczeństwa danych. Te organizowane przez Akademię Centrum e-Zdrowia są bezpłatne. Aby być na bieżąco, polecamy newsletter ezdrowie.gov.pl. Wielu dostawców IT organizuje też własne kursy albo webinary on-line, za które nie trzeba płacić.

Powyższe opcje powinny wystarczyć, aby być na bieżąco z cyberzagrożeniami. Zainteresowani wiedzą na poziomie zaawansowanym, łatwo znajdą szkolenia z cyberbezpieczeństwa za ok. 200–1000 zł od osoby. Te z NIS2 – które choć nie dotyczą gabinetów lekarskich, ale mogą okazać się pomocne – kosztują od 2000 zł w górę.

Antywirus i firewall

Kiedyś to komputery Apple uchodziły za dużo bezpieczniejsze niż Windows, ale najnowsze wersje systemu firmy Microsoft

też mają bardzo dobre zabezpieczenia przed wirusami. Ochrona zdrowia wymaga aktualnego systemu operacyjnego, bo hakerzy często wykorzystują luki w zabezpieczeniach w nieaktualnym oprogramowaniu. Dlatego pod żadnym pozorem nie można wyłączać automatycznych aktualizacji systemów operacyjnych. Update trzeba przeprowadzić natychmiast po tym, jak na ekranie pojawi się informacja o nowej wersji i prośba o restart komputera.

W systemie iOS oraz w usłudze Windows 365 dane są gromadzone w chmurze (tylko dane systemowe i tworzone przez użytkownika pliki, teksty i obrazy, ale nie baza danych systemu gabinetowego), co ułatwia ich odzyskanie po awarii lub blokadzie systemu przez cyberprzestępców.

Antywirus nadal warto mieć, gdy w grę wchodzi dane medyczne. Programy takie jak Avast, Norton 360 czy Bitdefender, oprócz firewalla mają też wbudowane narzędzia rozpoznawania zagrożeń w czasie rzeczywistym (np. podczas odwiedzania stron www), zarządzania hasłami, wykonywania skanowania dysków albo konserwacji komputera. Roczna licencja kosztuje ok. 150–250 zł.

Na koniec jeszcze jedna rada: na komputerze z systemem gabinetowym nie powinno się instalować żadnych innych programów albo, co gorsza, korzystać z prywatnej poczty, odwiedzać prywatnie strony internetowe, robić zakupy online. To idealne okazje dla hakerów, aby wykraść nasze dane.

Zestawienie rocznych kosztów podstawowych zabezpieczeń

Rodzaj zabezpieczenia	Zakres	Koszt roczny (zł netto)
Chmurowa kopia zapasowa (np. system KS-PPS – KAMSOF)	Backup w chmurze	ok. 611
Moduł zgodności z RODO	Wsparcie spełnienia wymagań ochrony danych osobowych	ok. 640 za pierwszy rok i 400 zł za kolejny
Oprogramowanie antywirusowe + firewall (wersja premium)	Ochrona w czasie rzeczywistym	150–250
Szkolenie z cyberbezpieczeństwa	W ramach Akademii Centrum e-Zdrowia	0
Menedżer haseł (np. Chrome – Google/Edge – Microsoft)	Generowanie i przechowywanie haseł	0
Dwuskładnikowe uwierzytelnianie 2FA (np. Microsoft Authenticator/Google Authenticator)	Dodatkowa warstwa logowania	0
Szyfrowanie dysku (BitLocker/FileVault)	Ochrona danych w przypadku kradzieży sprzętu	0
Razem (rocznie)		1400–1501 zł

OCHRONA DANYCH W GABINECIE LEKARSKIM

Używaj menedżera haseł.

Generuj długie i unikalne hasła zamiast powtarzać te same w różnych systemach.



Włącz uwierzytelnianie dwuskładnikowe 2FA.

Kod wysyłany na telefon znacznie utrudnia kradzież danych, nawet jeśli haker zna hasło.



Twórz automatycznie kopie zapasowe w chmurze.

Szybko odzyskasz dane po ataku ransomware. Nie musisz myśleć o codziennym robieniu back-upów.



Szyfruj dyski i urządzenia mobilne.

W przypadku kradzieży sprzętu dane pacjentów pozostaną niedostępne.



Szkol się z cyberbezpieczeństwa.

Znajomość socjotechnik i nowych metod hakerów zmniejsza ryzyko kliknięcia w zainfekowany link albo nabrania się na ataki z wykorzystaniem AI.

WWW

Włącz automatyczne aktualizacje systemu operacyjnego.

Luki w Windows są częstą drogą ataku.



6 zasad ochrony przed ransomware i reguła 3-2-1

Kilka wskazówek, dzięki którym poprawisz poziom bezpieczeństwa danych placówki medycznej lub szybko odzyskasz dane i przywrócisz działanie systemów IT w przypadku ataku hakerów.

Mała luka bezpieczeństwa, duża szkoda

Nawet ataki na największe i – wydawałoby się – najlepiej zabezpieczone placówki ochrony zdrowia mają zazwyczaj ten sam schemat: złośliwe oprogramowanie ransomware dostaje się do sieci i zaraża kolejne urządzenia. Dzieje się to z reguły albo w wyniku złamania słabych haseł, albo uruchomienia złośliwego pliku przesłanego e-mailem.

» Pracownicy szpitali klikają na zarażony załącznik w co siódmej wiadomości e-mail – pokazują przeprowadzone badania. «

Człowiek jest najsłabszym ogniwem systemu zabezpieczeń – aż w ok. 80–90% przypadków incydentów bezpieczeństwa to pracownicy stają się nieświadomymi wrotami do danych i systemów IT.

Badania pokazują, że w symulowanych atakach phishingowych, pracownicy szpitali klikają na zarażony załącznik w co siódmej wiadomości e-mail. Dlatego należy się skupić właśnie na tym, aby bezpieczeństwo informacji było wszyte w używane systemy i procedury. To jest zadanie dla administratorów systemów IT i ochrony danych.

Absolutnym minimum w systemie bezpieczeństwa przed cyberatakami są:

- **Bieżąca aktualizacja wszystkich zasobów IT**, w tym przeglądarek internetowych, systemów operacyjnych, systemów antywirusowych itd. Wiele podmiotów medycznych nadal korzysta – ze względu na koszty – ze starych systemów operacyjnych bardzo podatnych na włamania;
- **Używanie silnych haseł** i ich regularna zmiana;
- **Silne filtry antyspamowe** i uczulanie pracowników, aby nie otwierać żadnych podejrzanych załączników (szkolenia i symulacje ataków);
- W przypadku pracy zdalnej, należy upewnić się, że pracownicy ochrony zdrowia korzystają z **bezpiecznej usługi VPN**;
- Wykonywanie kilku **kopii bezpieczeństwa**, w tym jednej w chmurze danych;
- Opracowanie i przegląd **systemu bezpieczeństwa informacji**, który obejmuje regularne szkolenia i sposób reagowania w przypadku ataku cybernetycznego.

Warto pamiętać, że ataki phishingowe dokonywane są najczęściej za pośrednictwem poczty elektronicznej, telefonu i wiadomości tekstowych. Przykładowo, hakerzy mogą zadzwonić podszywając się pod pracownika placówki i poprosić o otworzenie załącznika w przesłanym mailu, podanie hasła albo przekazanie kartoteki pacjenta. Metody są coraz bardziej

wyrafinowane. Hakerzy mogą wybrać sobie za cel konkretnego pracownika szpitala i zmusić go do udostępnienia danych albo kliknięcie załącznika, powołując się na stan pacjenta zagrażający jego życiu.

3–2–1: Kopie, kopie i jeszcze raz kopie

Jak podkreślają eksperci, bezpieczna i aktualna kopia zapasowa to najlepsza polisa w przypadku ataku cyberprzestępców. Kopia pozwoli przywrócić normalne funkcjonowanie placówki i odzyskać wszystkie dane medyczne pacjentów, które są krytyczne z punktu widzenia leczenia. I nawet jeśli hakerzy opublikują dane w darknecie, co ma poważne konsekwencje dla prywatności pacjentów, placówka zapewni ciągłość leczenia i bezpieczeństwo chorych.

Zaleca się, aby przechowywać kilka kopii zapasowych w różnych lokalizacjach z różnym stopniem aktualności. Jedną z zasad jest „3–2–1”: tworzenie trzech oddzielnych kopii zapasowych danych, dwóch na różnych nośnikach i jedną poza siedzibą firmy, najlepiej w chmurze. Kopia w chmurze powinna być aktualizowana w czasie rzeczywistym. Z kolei kopie na nośnikach zewnętrznych, które przydadzą się w awaryjnych sytuacjach, mogą być tworzone w większych odstępach czasu.

Archiwizacja w chmurze jest najwygodniejszą metodą, bo realizowana jest automatycznie, a do tego kopia przechowywana jest poza siecią placówki ochrony zdrowia. Jest też coraz tańszym sposobem ze względu na rosnącą ofertę chmur danych. Niektóre usługi oparte na chmurze pozwalają tworzyć nieedytowalne kopie – nie mogą być one ani usunięte, ani zmienione przez cały okres przechowywania, co jeszcze bardziej zwiększa poziom ochrony.

» Chmura jest z reguły postrzegana za bezpieczniejszą formę przechowywania danych, ale też nie zapewnia 100-proc. ochrony. «

Chmura ma też jeszcze jedną zaletę – usługa bezpieczeństwa danych i tworzenia kopii jest outsourcingowana. A przy trudnościach, jakie placówki lecznicze mają z zatrudnieniem pracowników IT i ich rotacją, może to być decydujący argument.

Silna kultura cyberbezpieczeństwa powinna być zadaniem nr 1 dla wszystkich podmiotów ochrony zdrowia. A na nią składa się dobrze opracowana strategia, aktualne systemy IT, bezpieczne kopie baz w chmurze, systematyczne szkolenia i regularne symulacje ataków. ●

reklama



CO NOWEGO W E-ZDROWIU?

Porady | Wywiady | Polityka | Systemy IT | Dane z rynku

Czytaj blog OSOZ.
Pobierz bezpłatne poradniki o cyfryzacji i cyberbezpieczeństwie w ochronie zdrowia.

blog.osoz.pl



KS-BDO RODO

RODO pod kontrolą



- Analiza ryzyka
- Dokumentacja i procedury
- Obsługa incydentów
- **Wsparcie w realizacji obowiązków wynikających z RODO, NIS2 i KSC**
- Integracja z systemami **KAMSOFT** (KS-SOMED, KS-PPS, KS-AOW)





Podstępny phishing. Jak go rozpoznać i nie dać żadnej szansy hakerom?

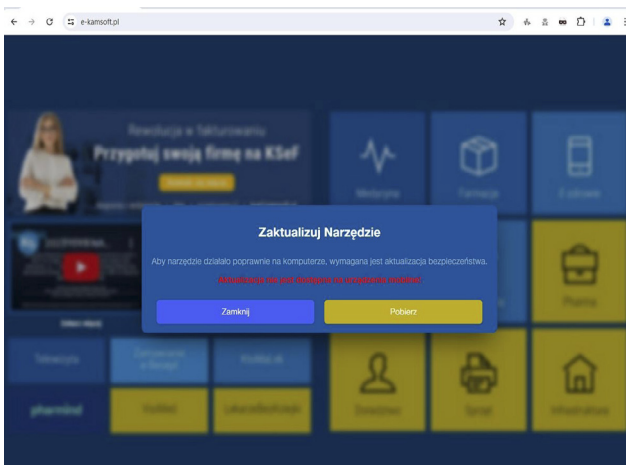
Wielokrotnie hakerzy dokonali próby ataku phishingowego, podszywając się pod dostawcę oprogramowania dla ochrony zdrowia KAMSOFT. Dzięki szybkiej reakcji udało się go udaremnić. Przedstawiamy kulisy cyberataku, aby uczulić na tego typu działania hakerów.

Kradzież nazwy firmy i sfałszowana strona

To już nie tylko informacja o przesyłce kurierskiej albo spadku – hakerzy przygotowują wyrafinowane ataki budując wierną kopię strony internetowej, aby zwabić na nią potencjalne ofiary. Jeśli im się to uda, zyskują dostęp do komputera.

Taka metoda działania cyberprzestępców oparta na socjotechnice nazywana jest *pharmingiem* (przekierowanie użytkownika na fałszywą stronę), a jej celem jest kradzież danych. Najczęściej była stosowana w sektorze finansowym, ale odkąd banki zaczęły stosować bardzo silne zabezpieczenia, hakerzy na cel wzięli słabiej chronione placówki medyczne. Nie zawsze chodzi im o dane medyczne, ale także np. hasła do bankowości elektronicznej. Jak wyglądał jeden z takich ataków?

Przykładem jest incydent z maja 2024 roku, kiedy to placówki medyczne zaczęły otrzymywać wiadomości SMS z informacją o konieczności pobrania aktualizacji systemu informatycznego KAMSOFT. Kliknięcie linku powodowało przekierowanie na stronę internetową przypominającą do złudzenia stronę firmy. Hakerzy nawet posłużyli się podobnym adresem www, różniącym się jedynie przedrostkiem e-.



Fałszywa kopia strony internetowej KAMSOFT, która tłem i kolorami odpowiada stronie oryginalnej. Adres www jest podobny, ale powinien wzbudzić podejrzenie

Falszywa strona zachęcała do pobrania aktualizacji. Tak naprawdę, po kliknięciu na przycisk *Pobierz*, pobierane było złośliwe oprogramowanie. Po jego uruchomieniu, hakerzy mogli uzyskać dostęp do danych na komputerze.

» Średnio 2,9% wiadomości phishingowych jest klikanych. «

Jak uniknąć ataku phishingowego?

Atak szybko udaremniono, bo został zdemaskowany przez m.in. CERT oraz klientów firmy, którzy poinformowali o podejrzanych SMS-ach. Dzięki temu fałszywy portal został zablokowany, a firma szybko ostrzegła o próbie ataku.

Ale nie zawsze udaje się zdemaskować cyberataki na czas, dlatego najlepszą ochroną jest wiedza użytkowników na temat metod działania przestępców internetowych. Co powinno wzbudzić podejrzenie i jak się zachować?

- **Ufaj tylko tym kanałom komunikacji z dostawcą IT, z których korzystałeś dotychczas.** W przypadku opisanego ataku, cyberprzestępcy wysłali SMS-a z informacją o aktualizacji systemu. KAMSOFIT nigdy nie informuje o upgrade'ach w ten sposób wiedząc, że mogliby to wykozystać hakerzy;
- **Weryfikuj wiarygodność niespodziewanych wiadomości.** Jeśli informacja przychodzi z nowego adresu albo za pomocą nowego kanału komunikacji, potwierdź jej autentyczność kontaktując się z nadawcą. Sprawdź, czy adres nadawcy zgadza się z tym, od którego dotychczas dochodziły wiadomości;
- **Samodzielnie wpisuj adres www w wyszukiwarce internetowej jeśli chcesz wejść na dany portal.** Podobnie jak w przypadku bankowości elektronicznej, zawsze korzystaj z adresu, który wpisujesz sam lub masz zapamiętany w wyszukiwarce. W przypadku opisanego sprawy, pojawiłaby się oryginalna strona www, na której nie było żadnego komunikatu o aktualizacji.
- **Regularnie aktualizuj oprogramowanie antywirusowe i firewall.** Dobre i aktualne systemy były w stanie

stosunkowo szybko wykryć, że strona jest zafalszowana, ostrzegając przed wejściem na nią.

- **Pobieraj aktualizacje** ze sprawdzonych źródeł, za pomocą oprogramowania gabinetowego, tak jak robiłeś to dotychczas. Nie klikaj na żadne linki przesłane mailem albo SMS-em jeśli nie masz pewności, że pochodzą z zaufanego źródła.

W przypadku otwarcia wiadomości i pobrania złośliwego oprogramowania, zaleca się wyłączenie komputera, kontakt z opiekunem IT lub serwisem, który sprawdzi komputer. Warto też zmienić wszystkie hasła, w pierwszej kolejności do bankowości elektronicznej i oprogramowania gabinetowego. Do tego atak należy zgłosić do CERT Polska (CSIRT NASK), aby instytucje odpowiedzialne za cyberbezpieczeństwo mogły podjąć odpowiednie kroki.

Ataki phishing będą się nasilały

Phishing jest główną przyczyną naruszeń danych w służbie zdrowia. Podczas pandemii COVID-19, ich liczba się podwoiła. Według raportu Phishing Statistics z 2026 roku, średnio 2,7% wiadomości phishingowych jest klikanych.

Atak SMS-owy jest kilkukrotnie rzadziej przeprowadzany niż e-mailowy (stosunek 10:1), bo wymaga zdobycia numerów telefonów komórkowych placówek zdrowia. Ale jest skuteczniejszy, bo w przypadku cyberataku liczy się skłonienie ofiary do emocjonalnego, szybkiego działania. Do tego większość skrzynek e-mailowych posiada filtry antyspamowe podczas gdy SMS-y nie są weryfikowane.

Nie istnieje jedna, uniwersalna metoda obrony przed atakami phishingowymi. Zabezpieczenia techniczne są tak samo ważne jak regularne szkolenia. Świadomi metod działania hakerów użytkownicy systemów IT – a tymi dzisiaj jest każdy pracownik ochrony zdrowia – mogą udaremnić nawet najlepiej zaplanowany cyberatak. Wiele prób phishingu można rozpoznać dzięki odpowiedniej czujności i przestrzeganiu zasad cyberhigieny. ●



Hakerzy nie mają skrupułów, ale może ich zatrzymać „firewall z ludzi”

Naruszenia bezpieczeństwa danych często zaczynają się od chwili słabości, którą każdy doświadcza pod presją czasu albo z poczucia władzy – twierdzi Mark T. Hofmann, profiler kryminalny i wywiadowczy oraz psycholog biznesowy. Jego zdaniem ochrona danych to przede wszystkim wyzwanie psychologiczne.

Jest Pan profilerem kryminalnym zajmującym się cyberprzestępczością. Co to oznacza?

Zaglądam tam, gdzie inni nie zagląдают – do *Darknetu*, forów dla hakerów; analizuję rozmowy na Telegramie albo logi czatów, które wyciekły. Łącząc analizę behawioralną z bezpośrednimi badaniami w Darknecie, badam zachowania hakerów: Kim są? Jak myślą? Co ich motywuje? Jak się organizują? Cel jest zawsze ten sam: uczyć się od „złych aktorów”, aby pokazać organizacjom i władzom, jak się chronić.

Na pierwszy rzut oka można pomyśleć, że cyberprzestępczość jest problemem technicznym. Jednak największe znaczenie mają aspekty psychologiczne, zarówno te po stronie ofiar ataków jak i hakerów.

Co powinniśmy wiedzieć o współczesnych hakerach?

Hakerzy są często młodzi, bardzo inteligentni i dobrze wykształceni. Kieruje nimi silna chęć rzucenia wyzwania systemowi. Wielu z nich określiłbym mianem „cyfrowych anarchistów” – lubią grę w kotka i myszkę z władzami i są dumni ze swoich umiejętności. Pieniądze są często tylko jednym z motywatorów; równie ważne są dreszczyk emocji, wyzwanie, chęć rozwiązania „zagadki” i prestiż. Nawet ci hakerzy, którzy już się wzbogacili, kontynuują swoją działalność cyberprzestępczą. Nie chodzi tylko o pieniądze, ale o status, przyciągnięcie uwagi i panowanie nad systemami IT.

Od lat wiemy, jak działa phishing i mimo to dajemy się na niego nabierać. Dlaczego?

Atakujący zawsze wykorzystują te same czynniki wyzwalające: emocje, presję czasu i nietypowe prośby. Najważniejsze są emocje. I ten schemat działania sprawdza się, ponieważ ludzie reagują odruchowo, zanim zaczną myśleć.

Sama świadomość często nie wystarcza, gdy w grę wchodzi stres, rutyna lub zaskoczenie. Nawet doświadczeni eksperci

» Pozostawienie komputera bez nadzoru na kilka minut to jak otwarte drzwi do danych. «

mogą dać się oszukać, zwłaszcza gdy haker wzbudza zaufanie, wykorzystuje emocje, autorytet lub presję czasu. Wyobraź sobie, że otrzymujesz dramatyczny telefon od córki, słysząc jej prawdziwy głos. Dzięki technologii deepfake jest to możliwe.

Hakerzy chętnie podszywają się pod autorytety: „Tu policja”, „Jest problem z Twoim kontem bankowym, musimy działać szybko”. Zawsze, gdy ktoś próbuje wyrzucić na nas presję, abyśmy zrobili coś nietypowego, na przykład ujawnili hasło lub przelali pieniądze na nieznane konto, powinniśmy wziąć głęboki oddech, zatrzymać się i pomyśleć: Czy mój bank zadzwoniłby do mnie i poprosił o hasło? Czy zadzwoniłby do mnie urząd skarbowy? Czy mój syn poprosiłby mnie o pieniądze przez telefon? Zastanów się, zanim zaczniesz działać, i słuchaj swojego doświadczenia.

Z psychologicznego punktu widzenia, co sprawia, że pracownicy służby zdrowia są szczególnie podatni na socjotechnikę?

Lekarze, pielęgniarki czy osoby na rejestracji pracują w warunkach dużego stresu i odpowiedzialności. Muszą działać szybko i pod presją. Atakujący wykorzystują to za pomocą socjotechniki: krótki telefon, e-mail lub wiadomość, które wywołują poczucie pilności i wyłączają racjonalne myślenie.

Ale są też inne często występujące luki bezpieczeństwa danych generowane przez ludzi: pozostawianie włączonych laptopów bez nadzoru, udostępnianie hasel przez telefon lub zapisywanie ich na karteczkach, otwieranie załączników bez weryfikacji lub głośne omawianie informacji o pacjentach w miejscach publicznych.

Każdy drobny, rutynowy błąd może stać się furtką dla atakujących. Pewnej nocy spacerowałem korytarzami jednego ze szpitali. Liczba odblokowanych i pozostawionych bez nadzoru komputerów mnie zaszokowała. Jeśli zalogowany użytkownik oddala się na chwilę, otwiera szeroko drzwi każdemu, kto chce wykraść dane.

» Techniczne środki bezpieczeństwa nie zawsze są w stanie zniwelować ryzyko wynikające z niebezpiecznych zachowań ludzi. «

Czyli szkolenia z ochrony zdrowia powinny obejmować także profilowanie behawioralne.

Tak, główna zasada bezpieczeństwa danych to „poznaj swojego wroga”. Lubię opisywać cyberprzestępczość jako grę w szachy behawioralne. Im lepiej zrozumiemy motyw i metody hakerów oraz wnिकniemy w ich umysły, tym lepiej możemy się bronić i przygotować. Jeśli zrozumiemy, w jaki sposób hakerzy wykorzystują sztuczną inteligencję i deepfake'i oraz jak ten trend się rozwija, będziemy mogli się odpowiednio przygotować.

Techniczne środki bezpieczeństwa nie zawsze są w stanie zniwelować ryzyko wynikające z niebezpiecznych zachowań ludzi. Jeśli ujawnisz hasło przez telefon, ponieważ ktoś podaje się za „wsparcie IT” i twierdzi, że ma miejsce sytuacja awaryjna, nawet najlepsza zaporę sieciową lub zespół ds. bezpieczeństwa nie pomogą. Nie jestem przeciwny technicznym środkom bezpieczeństwa. Długie, zróżnicowane hasła, firewall'e, zabezpieczenia sieciowe i uwierzytelnianie wieloskładnikowe są niezbędne. Potrzebujemy jednak zarówno technicznej, jak i ludzkiej zapory sieciowej. A to wymaga ciągłego szkolenia pracowników.

Jak stworzyć taką zaporę sieciową z ludzi?

Pod pojęciem „zapory sieciowej z ludzi” rozumiem sytuację, w której pracownicy organizacji nie są słabym punktem, ale stanowią pierwszą linię obrony przed hakerami. Chodzi o świadomość, krytyczne myślenie, rutynowe czynności i kulturę bezpieczeństwa.

Moim zdaniem cyberbezpieczeństwo musi stać się atrakcyjne i ciekawe. Zbyt często szkolenia z ochrony danych są nudne. W efekcie postrzegamy je jako przykry obowiązek i szybko zapominamy, o czym były. Ale nie musi tak być. Możemy zabrać uczestników w podróż do Darknetu, co jest tak samo fascynujące jak najlepszy serial na Netflixie. Możemy sprawić, że obrona przed hakerami będzie zabawna.

Zabawna?

Tak. Pod koniec mojego pierwszego wykładu TEDx „*Psychologia cyberprzestępczości*”, podeszła do mnie osoba z publiczności i zapytała: „To było zabawne, ale czy naprawdę uważasz, że tak poważny temat jak cyberprzestępczość powinien być zabawny?”. Nie, nie powinien być zabawny, ale musi być zabawny. To jedyny sposób, aby dotrzeć do osób, które nie interesują się tematami związanymi z IT i cyberbezpieczeństwem.

Dzięki AI, ataki phishingowe są coraz doskonalsze.

Wspomniał Pan jak hakerzy klonują głos, a nawet wizerunek zaufanej osoby. Co zrobić, żeby w takich sytuacjach zadziałały odpowiednie procedury ochrony danych?

Sztuczna inteligencja i deepfake'i przenoszą inżynierię społeczną na nowy, dużo wyższy poziom, a podszywanie się pod znane osoby pracujące w organizacji i ataki na tożsamość stają się znacznie skuteczniejsze.

W służbie zdrowia mieszanka presji czasu, stresu i wielozadaniowości sprawia, że łatwiej jest manipulować ludźmi, aby dostać się do systemu IT. Do tego trzeba stworzyć odpowiednią kulturę ochrony danych, personel musi wiedzieć, kiedy powinno się zapalić czerwone światło, jak działają strategie „zatrzymywania się i weryfikacji” oraz jakie są procedury w przypadku nietypowych sytuacji. Każdy pracownik musi mieć świadomość, że przykładowo najpierw należy zadzwonić pod numer wybrany z telefonu, a nie oddzwaniać, zadawać pytania weryfikujące tożsamość lub używać wcześniej uzgodnione hasła. Świadomość w połączeniu z kulturą i rutyną pozostaje najskuteczniejszą formą obrony.

Pracownicy muszą wiedzieć, że każdy człowiek reaguje odruchowo pod wpływem emocji i stresu. Atakujący systematycznie to wykorzystują, a sztuczna inteligencja zwiększa zarówno ilość, jak i jakość tych ataków. Po drugie, autorytet i poczucie pilności są potężnymi narzędziami oddziaływania

na zachowania i nawet osoby dobrze wyszkolone mogą dać się oszukać. I po trzecie, większość cyberataków zaczyna się od błędu ludzkiego, ale ludzie mogą być również najsilniejszą obroną, jeśli są przeszkoleni, zmotywowani i mają odpowiednie uprawnienia.

Co o cyberbezpieczeństwie powinien wiedzieć każdy menedżer szpitala?

Moim zdaniem trzeba skończyć z traktowaniem cyberbezpieczeństwa w charakterze wyzwania czysto technicznego i zacząć postrzegać ludzi jako najważniejszy element pierwszej linii obrony przed hakerami. Jasne procedury, podnoszenie świadomości w tematach związanych z ochroną danych – to elementy, które muszą wniknąć w codzienną pracę. Szkolenie organizowane raz na jakiś czas nie wystarczy.

Drugim priorytetem jest normalizacja procedur weryfikacji. Personel powinien czuć się zachęcany do sprawdzenia źródła informacji przed podjęciem działania, nawet pod presją.

Zabezpieczenia jak podwójna autoryzacja muszą być postrzegane jako pomoc, a nie wyraz nieufności lub biurokracji.

I wreszcie, zachęcam do szkoleń, podczas których omawiane są elementy psychologii. Kiedy ludzie dowiadują się, dlaczego ataki są skuteczne, w jaki sposób celowo wykorzystuje się poczucie pilności, autorytet i strach oraz jakie błędy poznawcze są słabymi punktami każdej osoby, znacznie lepiej rozpoznają wczesne sygnały ostrzegawcze i nie dają się tak łatwo zmanipulować. ●

Hakerzy czasami kradną dane, aby się popisać i wzbudzić respekt u innych hakerów.





Ochrona danych polega na budowaniu procedur bezpieczeństwa wokół pracownika

– Każdy ma prawo się pomylić i kliknąć w zainfekowany link. Decyduje to, co dzieje się później – mówi Patryk Kuchta, Data Privacy Manager w Medcover. Rozmawiamy o tym, jak stworzyć silny, wielowarstwowy system ochrony przez cyberatakami.

Jakie ataki hakerów najbardziej zagrażają danym medycznym?

Nie zaskoczę, jeśli powiem, że cały czas najbardziej powszechną próbą cyberataku jest stary, dobry, klasyczny phishing. Najpopularniejszy jest phishing mailowy, ale także ten przez komunikatory internetowe, z których pracownicy korzystają czasem prywatnie. Do tego dochodzi jeszcze coraz częściej stosowany phishing głosowy, czyli telefoniczny.

Niestety, jest on coraz bardziej wyrafinowany i przybiera coraz trudniejsze do rozpoznania formy. A wszystko dzięki AI. Do niedawna, pisane przez hakerów i masowo wysyłane wiadomości phishingowe, były stosunkowo łatwe do wykrycia. Zawierały błędy językowe, dziwne czcionki i podejrzane grafiki. Dzisiaj narzędzia oparte na sztucznej inteligencji są w stanie przygotować wiarygodne teksty w każdym języku, podszywające się pod różne instytucje. Trudno je odróżnić od prawdziwych wiadomości.

Drugą podatnością są luki w wykorzystywanym oprogramowaniu. Cyberprzestępcy cały czas monitorują dziury w systemach IT, by z ich pomocą dostać się do infrastruktury IT, zanim jeszcze producent wypuści odpowiednią łatkę, a użytkownik ją zainstaluje. Pomocne w monitorowaniu takich aktywności są narzędzia typu Cyberthreat Intelligence. Jak tylko zauważymy w raportach z monitoringu kampanii hakerskich, że jakiś system IT jest wykorzystywany w atakach, musimy tak szybko jak to możliwe zainstalować łatkę.

Wspomniał Pan o wiadomościach phishingowych, które mogą być trudne do rozpoznania. Nie wszystkie zostaną odsiane jako SPAM. I wtedy ostatnim ogniwem obrony jest personel. I tu kłaniają się regularne szkolenia z cyberbezpieczeństwa.

Proponuję, aby nie nazywać tego szkoleniami, ale kampanią budowania świadomości i edukacją pracowników. Szkolenie

za bardzo kojarzy się z jednorazowym wydarzeniem, czymś co ma początek i koniec. W Medcover podchodzimy do wzmacniania cyberbezpieczeństwa jako do ciągłego procesu.

Oprócz tego, że organizujemy klasyczne szkolenia dla pracowników – wymagane przepisami prawa albo naszymi wewnętrznymi standardami – prowadzimy regularne treningi phishingowe. Korzystamy ze specjalnych platform generujących kontrolowane wiadomości phishingowe. Sprawdzamy reakcje pracowników: nie tylko to, czy klikają w niechciane linki lub załączniki, ale przede wszystkim to, czy zgłaszają phishing. Do tego publikujemy w intranecie aktualne materiały dotyczące bezpieczeństwa danych.

Zgłaszanie zagrożeń jest kluczowe. To, co często obserwujemy w zarządzaniu incydentami cyberbezpieczeństwa, to nie tyle fakt, że użytkownicy dają się złapać na phishing – bo świadomość jest coraz większa – ale to, że ignorują phishing. Dostają wiadomość, rozpoznają, że to phishing i ją kasują. Tymczasem takie wiadomości powinny być zgłaszane, bo dzięki temu wewnętrzny zespół IT jest w stanie skorelować informacje i wykryć, że przykładowo prowadzona jest kampania wymierzona w naszych pracowników. Wtedy możemy podnieść alarm i uruchomić dedykowaną kampanię informacyjną.

Jeśli chodzi o budowanie świadomości i kultury organizacyjnej, edukacja jest kluczowa. Ale nie oszukujmy się: edukacja bez odpowiednich zabezpieczeń technologicznych nie będzie w stanie sprostać współczesnym zagrożeniom. Dlatego konieczne jest budowanie wielowarstwowego ekosystemu bezpieczeństwa zawierającego m.in. zapory sieciowe, kontrolę ruchu w sieci placówki, zaawansowane narzędzia ochrony poczty, ochronę stacji końcowych, systemy klasy EDR (red.: Endpoint Detection and Response, narzędzia do wykrywania i reagowania na podejrzaną aktywność na urządzeniach końcowych). Ochrona cybernetyczna jest ochroną wielowarstwową. Edukacja jest fundamentalna, ale musi być wsparta technologią.

Co zrobić, aby pracownicy nie bali się zgłaszać incydentów, również wtedy, gdy kliknęli w niebezpieczny link i myślą, że to ich wina?

To jest bardzo dobre pytanie i odpowiedź wcale nie jest prosta. Bardzo trudno jest zbudować kulturę organizacyjną w obszarze bezpieczeństwa, w której pracownicy wiedzą, że nawet jeśli kliknęli dziwny link nieumyślnie, to powinni to zgłosić. Oczywiście nie mówimy o sytuacjach, gdy ktoś klika na wiadomość phishing celowo – to zupełnie inny problem.

W ramach prowadzonych kampanii edukacyjnych stosujemy wewnętrzny system walidacji. Każda symulacja phishingu jest podsumowywana, a pracownik dostaje informację zwrotną – jak mu poszło, jak często klikał w wiadomości phishingowe albo czy je zgłaszał, jak radził sobie z quizami dotyczącymi bezpieczeństwa. Oprócz szkoleń prowadzimy regularne krótkie quizy, oparte na bardzo konkretnych sytuacjach związanych z cyberzagrożeniami, z prostymi pytaniami i dwoma wariantami odpowiedzi. Często są one wsparte formą graficzną, np. komiksem, żeby lepiej dotrzeć do pracownika.

Podczas każdego szkolenia jasno podkreślam, że każdy ma prawo się pomylić. Po to zarządzamy ryzykiem. Każdy może mieć swój słabszy dzień albo chwilę nieuwagi. Błąd popełniony nieumyślnie nie jest podstawą do karania pracownika. Wręcz przeciwnie – sytuacje, w których ktoś zgłasza, że zrobił coś nie tak, traktujemy jako zachowanie pożądane. Konsekwencje mogą pojawić się wtedy, gdy ktoś wie, że zrobił coś złe, i świadomie tego nie zgłasza. W takim przypadku dochodzi do złamania procedur.

Rozmawialiśmy o wielowarstwowej ochronie złożonej z zabezpieczeń technicznych i organizacyjnych. Czy cyberbezpieczeństwo w ochronie zdrowia jest drogą?

I tak, i nie. Na pewno jest to koszt – nie da się tego zrobić zupełnie bezkosztowo. Trzeba jednak mierzyć siły na zamiary.

» Chmura może być bardzo opłacalna, także pod względem bezpieczeństwa. «

Jeśli jesteśmy małą, jedno- czy kilkugabinetową placówką, prawdopodobieństwo ukierunkowanego ataku jest dużo mniejsze niż w przypadku dużej grupy kapitałowej działającej w ochronie zdrowia.

Nie każda placówka musi mieć etatowego specjalistę ds. cyberbezpieczeństwa. W mniejszych podmiotach często wystarczy dostęp do eksperta zewnętrznego, z którym można się konsultować. Dużą część bezpieczeństwa można też przenieść na usługodawcę. Coraz więcej usług IT jest świadczonych w modelu usługowym, bez konieczności utrzymywania własnej infrastruktury. Wtedy to dostawca odpowiada za jej zabezpieczenie.

Do tego dochodzi edukacja personelu, śledzenie portali branżowych, komunikatów CSIRT i zapisanie się do sektorewego CSIRT, aby otrzymywać ostrzeżenia o zagrożeniach. To wszystko można zrobić niskim kosztem lub bezpłatnie.

Wspomniał Pan o scedowaniu odpowiedzialności na zewnątrz. Czy dotyczy to też wyboru między serwerem lokalnym a chmurą?

Oczywiście, że tak. Chmura może być bardzo opłacalna, także pod względem bezpieczeństwa. Odpowiedzialności prawnej nie da się przenieść na dostawcę, ale można się nią w dużym stopniu podzielić, jeśli zadamy o odpowiednie umowy, certyfikaty i analizę ryzyka. Dla mniejszych podmiotów chmura bywa bardzo rozsądnym rozwiązaniem.

Parlament i Senat przyjęły już ustawę o Krajowym Systemie Cyberbezpieczeństwa adaptującą dyrektywę NIS2. Prezydent ją podpisał, ale jednocześnie skierował do Trybunału Konstytucyjnego. Czy Medicover już przygotowuje się na obowiązki z niej wynikające?

Nie tylko się przygotowujemy, ale w niektórych podmiotach już wdrożyliśmy wymagania wynikające z NIS2. Proszę pamiętać, że działamy również na rynkach zagranicznych,

jak w Rumunii czy Niemczech, gdzie NIS2 już obowiązuje. Wiemy od dawna, które podmioty w naszej grupie będą objęte nowymi przepisami, a dzięki centralizacji standardów bezpieczeństwa łatwiej jest nam nimi zarządzać. Od 2014 roku funkcjonujemy w oparciu o system zarządzania bezpieczeństwem informacji zgodny z ISO 27001 i te standardy przenosimy na kolejne spółki.

Jak wygląda typowy dzień pracy osoby, która odpowiada za bezpieczeństwo danych?

Bardzo rzadko ma on swój wyraźny początek i koniec. Oczywiście są pewne godziny pracy, w których intensywność i dyspozycyjność są największe, ale cyberprzestępcy nie patrzą ani na zegarek, ani na kalendarz. W sytuacji, w której pojawia się poważny incydent lub naruszenie bezpieczeństwa, inne zadania schodzą na dalszy plan i wszystkie ręce są na pokładzie, żeby zająć się tym, co jest w danym momencie najważniejsze.

Na co dzień odpowiadam również za tzw. governance w obszarze cyberbezpieczeństwa. Sprawdzam, jak wyglądamy pod kątem wskaźników bezpieczeństwa, ponieważ bardzo wiele obszarów monitorujemy na bieżąco. Analizuję, czy w którymś miejscu nie trzeba podjąć dodatkowych działań, z kimś się skontaktować albo zainicjować konkretną akcję.

Regularnie sprawdzam też, jak przebiegają projekty z zakresu cyberbezpieczeństwa, jak wdrażanie nowych standardów, technologii czy rozwiązań. Bardzo często trafiają do nas również umowy, wnioski i projekty do zaopiniowania, więc dużą częścią mojej pracy jest decydowanie i planowanie, w jaki sposób dany projekt lub system wdrożyć tak, aby był bezpieczny i zgodny z obowiązującymi wymaganiami.

Istotnym elementem mojej pracy jest także monitorowanie zmian, w szczególności legislacyjnych. Zajmuję się formalną i prawną stroną bezpieczeństwa informacji, a w ostatnich miesiącach – zwłaszcza na poziomie unijnym – zmian w przepisach jest bardzo dużo. To wymaga stałej uwagi.

Jeśli dzień jest spokojny i nie ma żadnych „pożarów”, staram się wygospodarować czas na przeglądanie komunikatów z instytucji branżowych, portali i źródeł, które subskrybuję, żeby sprawdzić, czy nie pojawiły się nowe zagrożenia, ostrzeżenia albo informacje, które mogłyby wymagać naszej reakcji w Medicover.

Ma Pan jedną główną dewizę dotyczącą cyberbezpieczeństwa?

Tak. Edukacja i budowanie świadomości wśród pracowników. Wierzę, że bezpieczeństwem trzeba pracowników zarazić. Jeśli zrozumieją, że bezpieczeństwo ich chroni, a nie tylko utrudnia pracę, to naturalnie będą je stosować. Chodzi o budowanie kultury bezpieczeństwa wokół pracownika. ●

reklama



SZTUCZNA INTELIGENCJA W OCHRONIE ZDROWIA AI

242 STRONY
Z PORADAMI
I NOWOŚCIAMI

↓ POBIERZ ZA DARMO



BLOG.OSOZ.PL



Mikro-wycieki danych to plaga. „Wystarczy poczekać kilka minut przy drukarce”

Szpitala walczą z cyberatakami, ale zapominają, że dane mogą wyciekać w błahy sposób. Automatyczne blokowanie ekranu po 1–2 minutach bezczynności na wszystkich urządzeniach czy odwracanie dokumentów niezapisaną stroną do góry to metody ochrony danych, które warto sobie przypomnieć.

Cyberzagrożenie czai się wewnątrz organizacji

Liczba cyberataków na ochronę zdrowia wzrosła w 2025 roku o ponad 40% – wynika z nowego raportu CSIRT CeZ. Ale do oficjalnych statystyk trafia tylko mała część wycieków danych spowodowanych włamaniami hakerów do komputerów, phishingiem, złośliwym oprogramowaniem typu ransomware.

Gdy lupem padają setki, tysiące kartotek, sprawa robi się głośna. Mało kiedy mówi się o naruszeniach bezpieczeństwa, które dotyczą pojedynczych kartotek pacjentów i zaczynają się wewnątrz organizacji – od komputera pozostawionego bez nadzoru, wydruków wyników badań leżących na drukarce przez kilkadziesiąt minut, czy kartoteki pacjenta widocznej dla każdego zza lady rejestracji.

W badaniu z 2025 roku naukowcy ze szpitala St Michael's i Uniwersytetu w Toronto znaleźli w pojemnikach na makulaturę pięciu różnych szpitali ok. 600 kg papieru oraz 2500 arkuszy zawierających dane osobowe chronione przepisami o ochronie danych medycznych.

Skala tzw. insider threats jest ogromna – szacuje się, że odpowiedzialność za ok. 30% wszystkich wycieków danych ponoszą osoby z wewnątrz organizacji. W połowie przypadków wynikają one z błędów pracowników. Podczas szkoleń mówi się dużo o tym, jak rozpoznać phishing, zapominając o takich metodach ochrony jak prawidłowe niszczenie dokumentów.

Nowoczesne firewalle nic nie dają, gdy pacjent zostaje sam na sam z komputerem

Szpitala inwestują miliony złotych w nowoczesne systemy bezpieczeństwa, centra monitorowania sieci i rozwiązania wykorzystujące sztuczną inteligencję do wykrywania cyberataków. Tymczasem organizacje zajmujące się cyberbezpieczeństwem, takie jak amerykański *Department of Health and Human Services* (HHS), alarmują, że wiele incydentów zaczyna się od prostych błędów popełnianych przez personel.

Jednym z nich jest pozostawienie odblokowanego komputera po odejściu ze stanowiska pracy. Lekarze i pielęgniarki wielokrotnie w ciągu dnia przerywają pracę przy komputerze, aby zająć się pacjentem, odpowiedzieć na telefon i skonsultować wyniki badań. Jeśli komputer zablokuje się dopiero po 5 minutach, te momenty, gdy komputer stoi otworem dla osób postronnych, sumują się w kilkadziesiąt minut dziennie. W tym czasie osoba nieuprawniona może z łatwością uzyskać dostęp do elektronicznej dokumentacji medycznej.

Eksperti od IT zalecają ustawienie automatycznego blokowania ekranu już po 1–2 minutach bezczynności. To może irytować, bo lekarz musi kilkanaście razy w ciągu dnia wprowadzać hasło, ale jest to konieczne. Dodatkowym zabezpieczeniem są filtry i przesłony montowane na monitorach, ograniczające możliwość odczytania danych przez osoby stojące obok. Powinny być standardem w rejestracji, bo skutecznie chronią przed tzw. *shoulder surfingiem*, czyli podglądaniem informacji wyświetlanych na ekranie przez osoby postronne.

Jeszcze innym błędem jest brak pełnego szyfrowania dysku. Jeśli lekarz korzystający z laptopa albo smartfona zgubi swoje urządzenie, zapisane dane można bez problemu odczytać. HHS od lat zaleca szyfrowanie urządzeń jako jedno z podstawowych zabezpieczeń danych medycznych.

Wydruki, kopie, notatki na papierze poniewierają się na biurku i w koszach

Mimo digitalizacji dokumentacji medycznej, w każdej przychodni albo szpitalu nadal w obiegu są wydruki wyników badań, listy wizyt na dany dzień, książeczki zdrowia i szczepień, upoważnienia, karty anestezyjologiczne. Leżą na biurkach, w niezamkniętych szafach, w koszach.

Eksperti zalecają stosowanie zasady „czystego biurka”. Przy dłuższej nieobecności na stanowisku pracy nie powinny pozostawać żadne wydruki z danymi pacjentów ani odręczne notatki. Dokumentację pozostawioną na biurku zaleca się odwracać tekstem do dołu.

» W koszach na śmieci szpitali często można bez problemu znaleźć dane osobowe. «

Jeśli placówka korzysta z centralnej drukarki w osobnym pomieszczeniu, wydruki trzeba odebrać natychmiast po ich wydrukowaniu. Robocze notatki, harmonogramy, karteczki samoprzylepne czy wydruki z systemów informatycznych powinny trafiać do niszczarek, zgodnie z procedurami obowiązującymi w placówce.

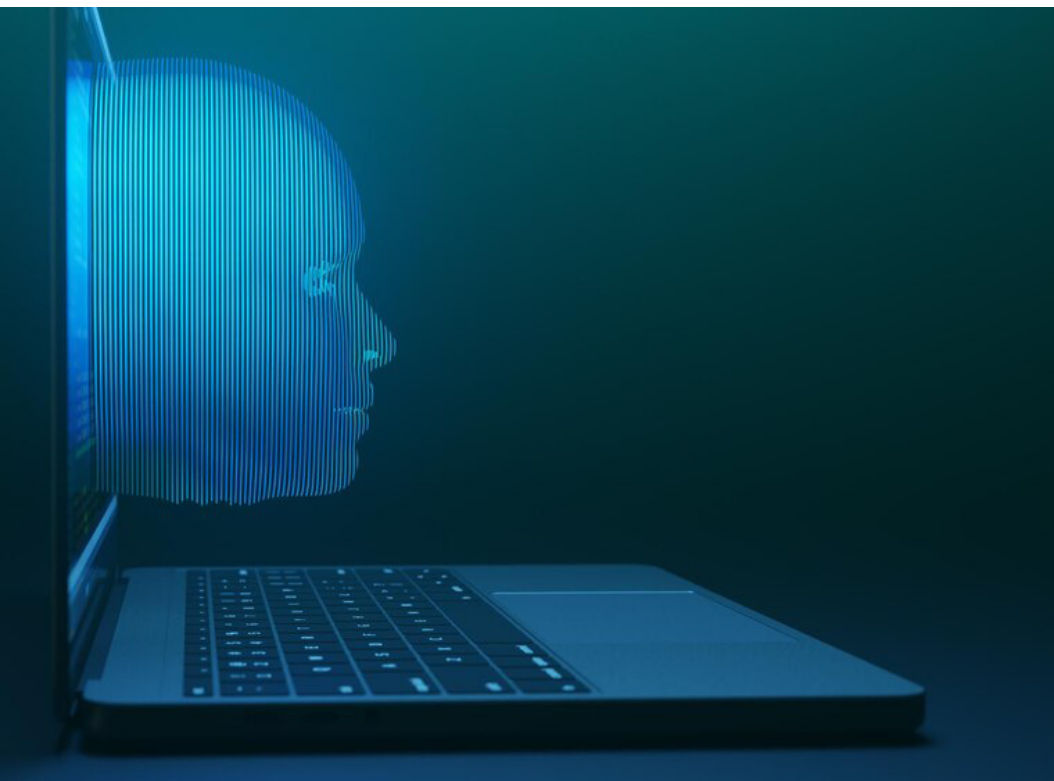
Zakres dostępu do danych powinien odpowiadać kompetencjom

W dużych organizacjach standardem jest dostęp do danych oparty na rolach. Lekarz, pielęgniarka, rejestratorka czy pracownik administracyjny powinni widzieć wyłącznie te dane, które są niezbędne do wykonywania ich obowiązków. Jest to dodatkowa warstwa ochrony przed hakerami – nawet w przypadku przejęcia hasła do jednego konta, zakres danych możliwych do wykradzenia jest mocno ograniczony.

Standardem powinno być uwierzytelnianie wieloskładnikowe (MFA). Korzystając z krytycznych systemów, potwierdzenie tożsamości za pomocą aplikacji mobilnej, klucza sprzętowego lub danych biometrycznych skutecznie chroni dane, nawet jeśli doszło do złamania hasła dostępu.

Punktów nieuprawnionego dostępu do danych jest więcej: otwarte drzwi na zaplecze, gdzie pracownicy wychodzą na papierosa, zasada nieograniczonego zaufania do kurierów i wpuszczanie osób ubranych jak serwisanci bez przepustek. Może to być też skrzynka pocztowa pracownika, jak w przypadku Szpitala Uniwersyteckiego w Krakowie, gdy w marcu 2026 roku przestępcy włamali się na skrzynkę mailową jednego z pracowników szpitala. Używając jego legalnej tożsamości, byli w stanie poruszać się wewnątrz sieci i prowadzić korespondencję.

Przestroga powinien być też incydent w szpitalu im. Króla Edwarda VII w Londynie. W 2012 roku dwoje prezenterów radiowych zadzwoniło do szpitala, podszywając się pod Królową Elżbietę II oraz Księcia Karola, pytając o stan zdrowia hospitalizowanej tam księżnej Kate. Pielęgniarka uwierzyła oszustom i bez weryfikacji wydała przez telefon ściśle poufne, szczegółowe informacje o stanie zdrowia członkini rodziny królewskiej. ●



Cyberpsychologia. Nowe narzędzie do walki z hakerami

To nie pracownicy są najsłabszym ogniwem ochrony danych, ale nieprawidłowo wyszkoleni pracownicy. Znając zasady cyberpsychologii, można zapobiec wielu błędom prowadzącym do incydentów bezpieczeństwa informacji.

Hakerzy manipulują pracownikami

Według badań przeprowadzonych przez Uniwersytet Stanforda, 88% naruszeń bezpieczeństwa danych zaczyna się od błędu człowieka. Cyberprzestępcy wiedzą, że o wiele łatwiej jest wprowadzić w błąd człowieka i w ten sposób uzyskać dostęp do danych niż łamać zabezpieczenia techniczne. Stosują w tym celu wyrafinowane metody socjotechniki, aby pracownik kliknął na wysłany link albo otworzył załącznik, wpuszczając do systemu złośliwe oprogramowanie.

Szacuje się, że co 11 sekund dochodzi do skutecznego ataku ransomware. Aktywowany przez nieuwagę albo niewiedzę wirus przejmuje kontrolę nad siecią i komputerem, a w zamian za jego odblokowanie hakerzy żądają okupu. Każdy może paść ofiarą coraz sprytniejszych metod hakerów wysyłających maile podszywające się pod wiadomości od zaufanej instytucji, banku, kuriera.

Jak może pomóc psychologia?

Szkolenia z cyberbezpieczeństwa są najlepszą metodą ochrony przed hakerami. Mimo to, nie zawsze są tak skuteczne, jak by tego oczekiwano. W natłoku obowiązków i stresie ludzie szybko zapominają, czego się nauczyli i popełniają błędy.

Dlatego inżynierowie i psycholodzy starają się poznać interakcje człowieka z technologią, zidentyfikować niewralgiczne sytuacje i zmniejszyć liczbę błędów. Na bazie ich badań powstaje nowa koncepcja „zorientowanego na człowieka cyberbezpieczeństwa”, polegająca na zrozumieniu, jak pracownicy wykorzystują komputery. Cyberpsychologia łączy wiedzę o cyberbezpieczeństwie z wiedzą o zachowaniu człowieka, tworząc nowe zasady bezpiecznej pracy z nowymi technologiami.

Zgodnie z nią, budując skuteczną politykę ochrony danych, trzeba zwrócić uwagę na kilka elementów:

Zmień podejście pracowników do technologii. Ludzie mają tendencję do cedowania swojej odpowiedzialności na

» Ćwiczenie:
Grupa pracowników wciela się w rolę hakerów i ma za zadanie stworzenie podstępnej wiadomości phishingowej. «

technologię: „Komputer powinien działać zawsze dobrze, a za bezpieczeństwo odpowiadają informatycy, dlatego nie muszą sobie zawracać głowy hakerami”. W takim nastawieniu, cyberbezpieczeństwo postrzegane jest jako obciążenie, bo wymaga uwagi, a nie rutynowego korzystania z technologii w trybie autopilota.

W szkoleniach należy podkreślać inne podejście, np. zerowego zaufania do otrzymywanych wiadomości, wśród których może znaleźć się phishing. Nie wyłącza to oczywiście odpowiedzialności działu IT, aby stosować zabezpieczenia techniczne. Jeśli stetoskop działa wadliwie, lekarz nie zrzuci winy na sprzęt, bo wie, jak funkcjonuje ten sprawny i jest w stanie korygować swoje decyzje. Taka sama świadomość powinna dotyczyć sprzętu i systemów IT.

Spraw, aby pracownicy identyfikowali się z infrastrukturą IT. Ryzykowne cybernetycznie zachowania pracowników mogą wynikać z tego, że traktują oni komputery jako sprzęt firmy, a nie swój. Eksperymenty przeprowadzone przez Profesora Phila Morgana i jego zespół z Uniwersytetu New Castle wykazały, że personalizacja urządzenia zwiększa poczucie odpowiedzialności. Profesor Morgan przez trzy lata pracował dla giganta przemysłu lotniczego Airbusa, badając przyczyny ryzykownych zachowań w cyberprzestrzeni. W licznych badaniach doszedł on do wniosku, że wychodzenie z założenia, że „komputer to sprzęt firmy”, powoduje automatyczne przerzucenie obowiązku ochrony danych na organizację i brak poczucia współodpowiedzialności.

Zbuduj zorientowane na człowieka podejście do cyberbezpieczeństwa oparte na triadzie wiedzy, świadomości i zrozumienia. Wiedzę zdobywa się podczas systematycznych szkoleń z ochrony danych i nowych metod działania hakerów. Aby wzmocnić element zrozumienia, należy stworzyć kulturę uczenia się na błędach. Organizacja musi jasno komunikować, że pomyłka pracownika, który prowadzi do ataku hakerów, nie będzie powodem do zwolnienia albo kary, ale jest częścią kultury doskonalenia procesów.

Takie podejście sprawia, że pracownicy szybciej przyznają się do ewentualnych błędów, co pozwala błyskawicznie zareagować na atak i zminimalizować jego skutki. I odwrotnie – ukrywanie incydentu prowadzi do narastania wyrządzonych szkód proporcjonalnie do upływającego czasu. Profesor Morgan twierdzi, że zamiast postrzegać błąd w zabezpieczeniach jako powód do wstydu, powinniśmy postrzegać go jako coś, co się zdarza ludziom i jest normalne. Kultura zachęcająca do zgłaszania błędów pozwala dodatkowo budować zaufanie w organizacji. Analogicznie jak zgłaszanie błędów medycznych jest niezbędne do poprawy standardów leczenia, raportowanie incydentów bezpieczeństwa ułatwia wzmocnienie ochrony przed hakerami.

Personalizuj interfejs użytkownika, aby komputer był traktowany jak przyjazne narzędzie pracy. Osoby, które padły ofiarą cyberataków często twierdzą, że wcześniej zdawały sobie doskonale sprawę z zagrożenia i nie wiedzą, jak mogły popełnić taki błąd.

Problemem może być nieprawidłowa konfiguracja systemu. Ludzie zapominają o procedurach, bo z czasem powtarzalne czynności wykonują mechanicznie. Dlatego systemy powinny im przypominać np. o konieczności wylogowania się (albo robić to automatycznie po określonym czasie), zmianie hasła itd. To tzw. twarde ograniczenia, czyli hamulce na poziomie systemowym. Drugą grupą są ograniczenia miękkie. Jednym z nich jest wprowadzenie kilkusekundowego opóźnienia w dostępie do danych albo konieczność dodatkowej weryfikacji poprzez skorzystanie z uwierzytelniania wieloskładnikowego. Tak, aby pracownik nie działał w afekcie, ale miał czas na dokładne przemyślenie, czy naprawdę chce otworzyć załącznik albo udostępnić dane.

Od czego zacząć wdrażać zasady cyberpsychologii?

Szkolenia z cyberbezpieczeństwa dla wszystkich to za mało – twierdzą eksperci cyberpsychologii – bo ochrona danych jest procesem, nad którym trzeba pracować codziennie. Dbłość o bezpieczeństwo danych zaczyna się na etapie

zatrudnienia nowego pracownika i onboardingu. Ludzie muszą wiedzieć, że są odpowiedzialni za komputery, na których pracują, ale nie mogą być straszeni konsekwencjami związanymi z wyciekiem danych.

Szkolenia należy prowadzić w grupach według ról w organizacji, bo obszar interakcji personelu medycznego i administracyjnego z komputerem jest różny. Należy analizować i komunikować zagrożenia identyfikowane przez dział IT. Warto włączyć czynnik emocjonalny, który pozwala



lepiej zapamiętać przekazywane informacje, przykładowo pokazując case study z wycieku danych oraz ich konsekwencji, przytaczając dane z aktualnych raportów itd. To nie mogą być tylko suche dane, ale przykłady pokazujące, co dzieje się, gdy dojdzie do ataku, jak cierpią na tym pacjenci, personel, cała placówka zdrowia; ile stresu może kosztować powrót do normalnej działalności itd.

Poziom cyberbezpieczeństwa trzeba też monitorować organizując symulowane ataki. Jednym z pomysłów jest wprowadzanie elementu gamifikacji. Przykładowo, grupa pracowników wciela się w rolę hakerów i ma za zadanie stworzenie podstępnej wiadomości phishingowej. Ta następnie jest wysyłana w sposób kontrolowalny i z zaskoczenia przez dział IT, po czym sprawdza się, na jakich komputerach mail został otwarty.

Nowe standardy cyberbezpieczeństwa

Do przeszłości odchodzi podejście do cyberbezpieczeństwa oparte na szkoleniach organizowanych co kilka miesięcy oraz polityce bezpieczeństwa, której pracownicy często nie znają albo nie rozumieją. Jednym z powodów oporu przed RODO jest stopień skomplikowania przepisów i języka, którym posługują się eksperci cyberbezpieczeństwa.

Krytyczne dla ochrony danych incydenty wynikające z ludzkich błędów mają najczęściej źródło w stresie, rutynie, negatywnym nastawieniu do informatyzacji, deficytach w identyfikowaniu się pracowników z placówką ochrony zdrowia. Pierwszą linią ochrony zawsze powinna być technologia – systemy antywirusowe, aktualizacja oprogramowania, wykonywane w czasie rzeczywistym kopie bezpieczeństwa. Drugim – człowiek świadomy zagrożeń i swojej roli w obronie przed hakerami. ●

Zarządzaj kompleksowo swoją placówką



Wybierz **oprogramowanie**
dla medycyny od **KAMSOFT**
i zyskaj:

- wsparcie w komunikacji i obsłudze pacjenta,
- profesjonalną pomoc działu obsługi Klienta,
- aplikacje mobilne dla lekarzy, pielęgniarek i położnych,
- system IT dostosowany do Twojej placówki oraz zmieniających się przepisów prawa,
- kompleksowe narzędzia pracy dla personelu medycznego, administracji i kadry zarządzającej.





Co dzieje się z danymi, które lekarz wpisuje do czatbotów jak ChatGPT?

Nigdy nie wprowadzaj danych pacjenta do ChatGPT i podobnych chatbotów – radzą eksperci od ochrony danych osobowych. Jak w takim razie bez obaw korzystać ze sztucznej inteligencji? Które narzędzia generatywnej AI są najbezpieczniejsze, a których unikać?

Popularność AI w ochronie zdrowia rośnie

Szacuje się, że ok. 25% Polaków już korzysta z generatywnej AI w życiu prywatnym i do celów zawodowych. Narzędzia takie jak ChatGPT, Perplexity, Copilot albo Gemini mają swoich zwolenników, którymi są zwłaszcza osoby młode i wykształcone, ale i równie dużą grupę sceptyków obawiających się o swoją prywatność i ryzyko bycia wprowadzonym w błąd (halucynacje AI). Duża część osób nadal nie wie, jak w ogóle rozpocząć pracę z AI.

Według badania American Medical Association z 2026 r. już 81% lekarzy deklaruje korzystanie z AI lub znajomość narzędzi AI dostępnych w ich praktyce. Najczęściej technologie te służą do podsumowywania badań naukowych i standardów opieki – korzysta z nich niemal 40% lekarzy. AI jest także wykorzystywana do tworzenia zaleceń dotyczących wypisu, planów opieki i notatek z wizyt, dokumentowania wizyt oraz przygotowywania podsumowań dokumentacji.

Jeszcze wyższy poziom wykorzystania pokazuje badanie Doximity obejmujące 3151 lekarzy w USA: 54% respondentów deklarowało korzystanie z AI w praktyce klinicznej, a wśród lekarzy rodzinnych, którzy już wdrożyli AI, 88% używało jej codziennie.

Tymczasem mało osób wie, że część zapytań wpisywanych do czatbota jest zapamiętywanych i przechowywanych na serwerach, najczęściej poza Unią Europejską. A to może prowadzić nie tylko do łamania przepisów RODO, ale także grozi wyciekiem wrażliwych danych. ChatGPT, Copilot, a może DeepSeek – które narzędzia oferują największą prywatność?

DeepSeek na czarnej liście

Zacznijmy od sensacji ostatnich tygodni, czyli chińskiego modelu DeepSeek R1. Po jego premierze, był on najchętniej pobieraną aplikacją na świecie – w okresie dwóch pierwszych tygodni oprogramowanie ściągnęło 3,6 mln osób. DeepSeek obiecuje wysoką wydajność modelu i precyzję odpowiedzi, a do tego jest całkowicie bezpłatny. Ale czy bezpieczny?

Nie do końca. Przed stosowaniem DeepSeek ostrzega Urząd Ochrony Danych Osobowych (UODO). Z polityki prywatności aplikacji wynika, że dane użytkowników mogą być przechowywane na serwerach zlokalizowanych w Chinach.

– Zgodnie z obowiązującymi przepisami rząd chiński posiada szerokie uprawnienia związane z dostępem do danych osobowych bez gwarancji ochrony przewidzianej w europejskim porządku prawnym – czytamy w oświadczeniu UODO. Do tego duży model językowy z Chin może wykorzystywać przekazywane przez użytkowników dane do dalszego trenowania modelu albo celów marketingowych.

Co-Pilot, ChatGPT, Gemini, Perplexity też pod znakiem zapytania

Nie tylko chiński model zapisuje dane z zapytań do dalszego trenowania AI. Robi to tak samo amerykański ChatGPT i Perplexity albo francuski Vibe (wcześniej LeChat) od Mistral AI. Wszystko zależy od tego, czy to model konsumencki czy biznesowy, oraz czy użytkownik zastrzegł taką możliwość w ustawieniach systemu.

Z kolei Microsoft 365 Copilot przechowuje dane dotyczące interakcji, w tym polecenia i odpowiedzi, jako część historii aktywności Copilot użytkownika. Jak deklaruje firma w warunkach użytkowania, dane te pozostają w usłudze chmurowej

Ulepszanie modelu

Ulepsz model dla wszystkich



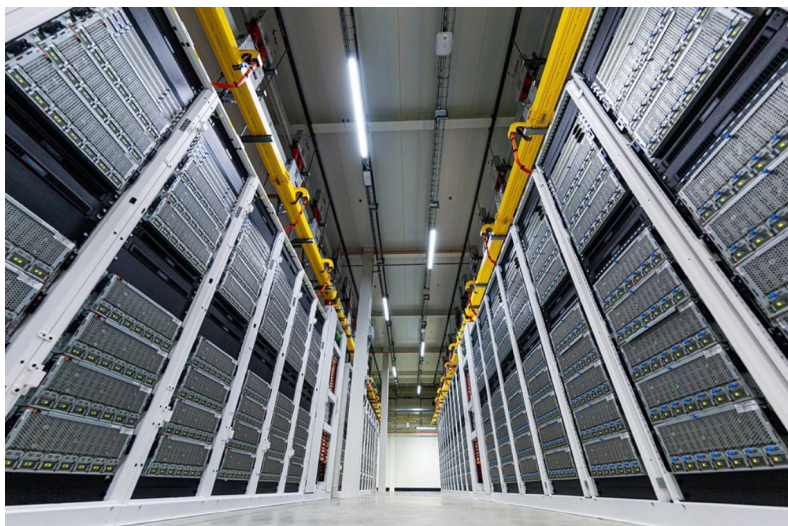
Zezwól na używanie Twoich treści do trenowania naszych modeli, co pozwoli ulepszyć czatbota ChatGPT dla Ciebie i wszystkich innych korzystających z niego osób. Podejmiemy działania w celu ochrony Twojej prywatności. [Dowiedz się więcej](#)

W ChatGPT można włączyć opcję, dzięki której wpisywane polecenia (prompty) nie będą używane do dalszego trenowania modelu AI

Microsoft 365 i są szyfrowane podczas przechowywania. Nie są one wykorzystywane do dalszego trenowania modelu AI, a użytkownicy mogą usunąć historię aktywności Copilot. Firma twierdzi także, że Copilot spełnia wymagania ogólnego rozporządzenia o ochronie danych (RODO).

Nawet jeśli czatbot nie przetwarza promptów wprowadzanych przez użytkownika – a te mogą czasami zawierać wrażliwe dane – pozostaje kolejny problem: większość popularnych dużych modeli językowych AI działa w chmurze danych, a niektóre serwery zlokalizowane są w USA. Przykładowo, jeśli korzystamy z bezpłatnego ChatGPT, dane z reguły trafiają do centrum danych Microsoft Azure w Teksasie. Wersje płatne i biznesowe ChatGPT opierają się na serwerach zlokalizowanych w granicach Europejskiego Obszaru Gospodarczego, ale to i tak nie sprawia, że można wpisywać dane medyczne pacjentów.

Trzeba także pamiętać, że firmy tworzące duże modele językowe też są narażone na ataki hackerów albo wycieki



Centrum danych Microsoft Azure. To tutaj przetwarzane są dane, które wpisujemy do ChatGPT (zdjęcie: Microsoft)

danych spowodowane błędami oprogramowania. Takie miały miejsce np. w przypadku ChatGPT, choć żadne dane z rozmów nie zostały dotąd naruszone.

Czy są modele LLM, z których można korzystać bez obaw?

Odpowiedź jest prosta: modele open-weight/source. Mogą być instalowane lokalnie i nie przesyłają danych na serwery zewnętrzne. Tylko takie modele – jeśli zostaną odpowiednio skonfigurowane z naciskiem na zarządzanie ryzykiem – mogą być stosowane bez obaw przez europejskie placówki medyczne. Niestety, ich stosowanie nie jest tak łatwe jak ChatGPT – wymagają instalacji na lokalnych serwerach przez osoby, które mają przynajmniej bazową wiedzę informatyczną. Ich obsługą i trenowaniem są w stanie zająć się tylko wykwalifikowani informatycy albo inżynierowie danych. Zaletą jest to, że można je dalej trenować na własnych bazach danych, tworząc czatboty przystosowane do różnych zadań, np. wyszukiwania danych w elektronicznej dokumentacji medycznej.

Do najbardziej znanych modeli open-weight należą m.in. Llama 3 firmy Meta oraz modele rozwijane przez francuską firmę Mistral AI. Wśród nowszych konstrukcji Mistral są Mistral Large 3, Mistral Small 4 i seria Ministral 3.

Alternatywą są funkcje AI wprowadzane przez dostawców oprogramowania IT do programów gabinetowych. Opierają się one na bezpiecznych lokalnych modelach, a do tego są zintegrowane z systemem IT dzięki czemu nie trzeba się przełączać pomiędzy różnymi aplikacjami. Z czasem będzie ich przybywać, bo oferują duże ułatwienia w m.in. wyszukiwaniu danych.

Podsumowanie

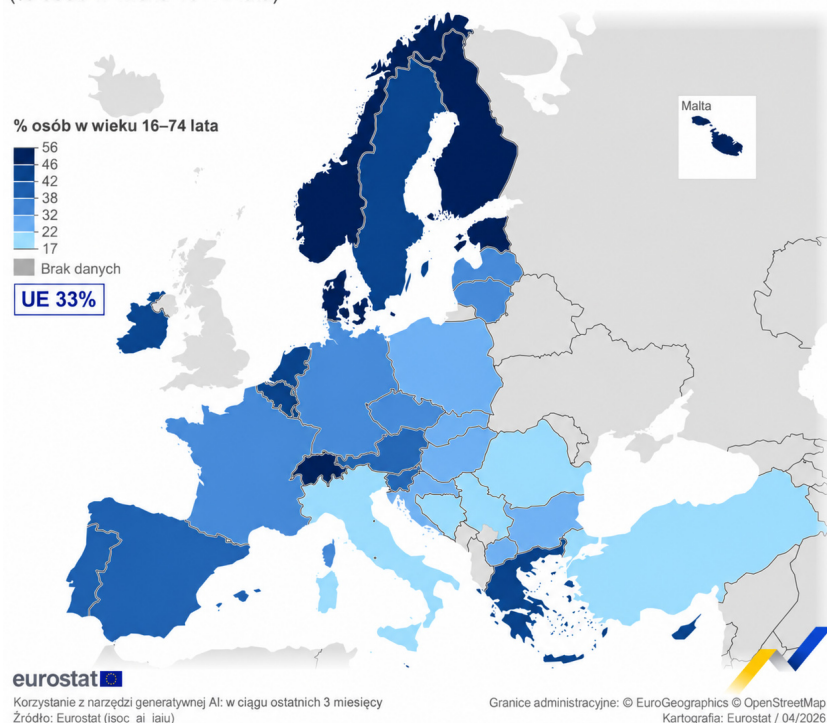
Żaden z modeli generatywnej sztucznej inteligencji działających w chmurze danych nie powinien być wykorzystywany do analizy wrażliwych danych pacjentów. Dlatego zasadą nr 1 jest unikanie w promptach danych osobowych albo informacji mogących posłużyć do identyfikacji konkretnej osoby (np. na

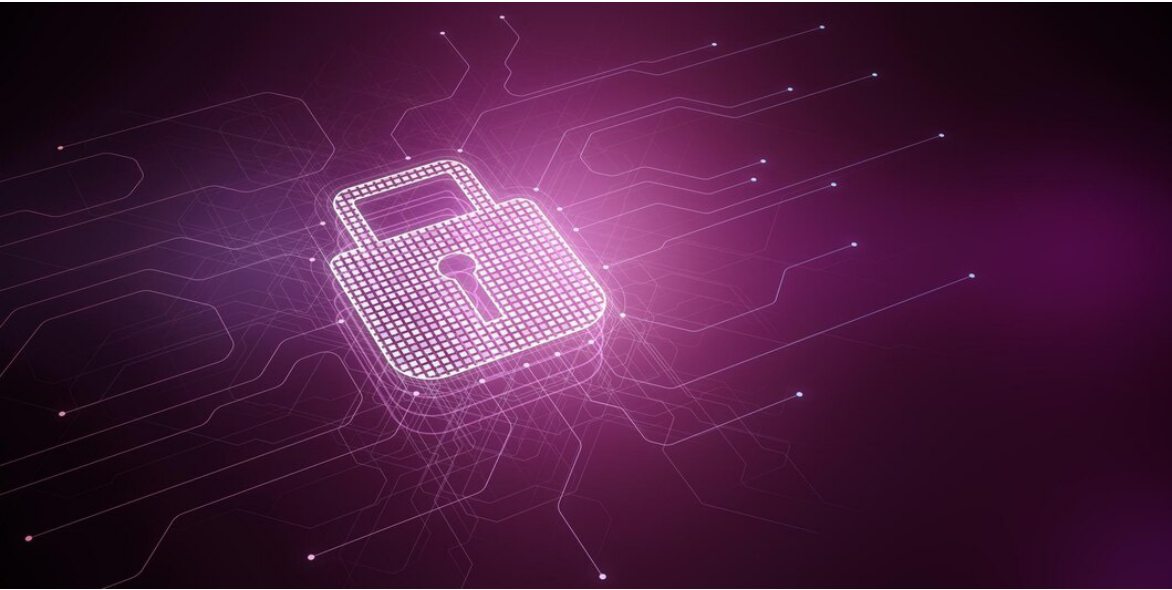
podstawie kilku znaczników jak wiek, miejsce zamieszkania, cechy charakterystyczne). Lekarz może ogólnie zapytać o diagnozę na podstawie objawów, ostatnie badania naukowe albo rekomendacje medyczne. Zaleca się przy tym wyłączenie pozwolenia stosowania zapytań do dalszego trenowania modelu.

Największe korzyści i gwarancję bezpieczeństwa danych dają modele open source, choć ich wdrożenie wiąże się ze stworzeniem mocnego zaplecza bazowo-serwerowego. Najprostszym rozwiązaniem jest testowanie funkcji AI wprowadzanych do systemów IT. ●

Korzystanie z narzędzi generatywnej AI przez osoby fizyczne, 2025

(% osób w wieku 16–74 lata)





Co to jest i jak wdrożyć strategię „zerowego zaufania”?

Jeśli infrastruktura cyfrowa wspierająca opiekę nad pacjentem nie gwarantuje ochrony danych, to narażone jest także zdrowie i życie pacjenta – tak radykalne i szczere spojrzenie na bezpieczeństwo danych to konieczność, bo liczba ataków hakerów szybko rośnie. Najwyższy poziom ochrony to cel tzw. polityki zerowego zaufania. Na czym polega?

Ochrona zdrowia pozostaje jednym z głównych celów cyberprzestępców. W 2025 r. CSIRT CeZ odnotował w polskim sektorze ochrony zdrowia 1441 incydentów bezpieczeństwa – o ponad 60 proc. więcej niż w 2024 r. Wśród nich było



Liczba ataków hakerów (tygodniowo) z podziałem na branże (źródło: World Economic Forum)

pięć incydentów poważnych i osiem ataków ransomware. Hakerzy obrali sobie za cel placówki zdrowia nie dlatego, że przetwarzają one wrażliwe dane medyczne, ale ze względu na wyjątkowo niski poziom cyberbezpieczeństwa. Wiele podmiotów nadal posiada stare systemy zawierające luki w zabezpieczeniach, a kwestie ochrony danych – ze względów finansowych i organizacyjnych – są często bagatelizowane.

9 filarów twierdzy danych

Zasady zerowego zaufania dotyczące ochrony danych zostały wypracowane w ramach Forrester And National Institute of Standards and Technology (NIST). Filozofię można streścić w jednym zdaniu: „nigdy nie ufaj, zawsze weryfikuj, dynamicznie rozwijaj politykę bezpieczeństwa”. Zakłada ona dodatkowo, że organizacja już stała się ofiarą ataku hakerów lub, że wkrótce on nastąpi, a więc dostęp do zasobów nie jest bezpieczny.

Pierwsze pięć fundamentów podejścia „zero trust” skupia się na:

- **Użytkownikach:** wiedza o sposobach działania hakerów i zasadach ochrony danych;
- **Urządzeniach:** zabezpieczenia techniczne, jak oprogramowanie antywirusowe, zapory sieciowe, ochrona urządzeń medycznych i innych elementów infrastruktury (kamery, drukarki wpięte w sieć itd.)
- **Sieciach:** oddzielenie sieci wewnętrznej od ogólnodostępnej sieci internetowej, stworzenie tzw. mikro-sieci;

- **Obciążeniach:** specyficzne elementy narażone na ataki jak np. rozwiązania chmurowe;
- **Danych:** klasyfikacja danych, ich szyfrowanie oraz bezpieczne przechowywanie kopii zapasowych.

Na tym poziomie organizacja przyjmuje zasadę restrykcyjnego uwierzytelniania dostępu użytkowników do zasobów organizacji. Przykładowo, wymagając regularnej zmiany haseł, wprowadzając domyślne wylogowanie po odejściu od stacji roboczej (ochrona na poziomie sesji korzystania z systemu, a nie użytkownika). Żadna osoba pracująca z infrastrukturą IT, od informatyków po lekarzy, nie ma przywilejów i objęta jest takim samym rygiem w ramach polityki bezpieczeństwa.

Większość filarów na tym poziomie ma charakter techniczny i leży w kompetencji informatyków i ekspertów bezpieczeństwa danych. Elementem organizacyjnym odgrywającym największą rolę, jest filar zerowego zaufania do ludzi. Kradzież lub złamanie danych uwierzytelniających oraz zainfekowanie sieci złośliwym oprogramowaniem są głównymi przyczynami naruszeń danych. Dlatego wymaga się m.in. uwierzytelniania wieloskładnikowego oraz intensywnych testów wiedzy i czujności użytkowników.

Pozostałe cztery filary to strategiczne elementy ochrony kluczowe w przypadku naruszenia bezpieczeństwa:

- **Widoczność.** Podejmowanie świadomych decyzji dotyczących dostępu do danych przez pracowników oraz podmioty zewnętrzne (brak domyślności zaufania). Wszystkie działania realizowane przez pracowników na urządzeniach i sieciach firmowych muszą być widoczne dla informatyków i specjalistów bezpieczeństwa danych;
- **Analityka.** Monitorowanie zasobów sieciowych oraz danych, analiza przepływów informacji w całym ekosystemie placówki medycznej;
- **Automatyzacja i zarządzanie.** Możliwość szybkiej identyfikacji nieautoryzowanego dostępu do danych i potencjalnie złośliwych działań. Wbudowane mechanizmy

automatycznego reagowania na sytuacje, audyty bezpieczeństwa i aktywne wyszukiwanie potencjalnych zagrożeń.

- **Administrowanie.** Każdy użytkownik, urządzenie, aplikacja i transakcja wymiany danych muszą być stale weryfikowane a środowisko danych – testowane i nadzorowane. Strategia bezpieczeństwa danych staje się nieustannym procesem, a nie działaniem podejmowanym od czasu do czasu i ograniczającym się do aktualizacji oprogramowania antywirusowego, prowadzenia szkoleń z ochrony danych co kilka miesięcy, czy – co gorsza – przeprowadzenia kontrolowanych ataków lub audytów raz w roku.

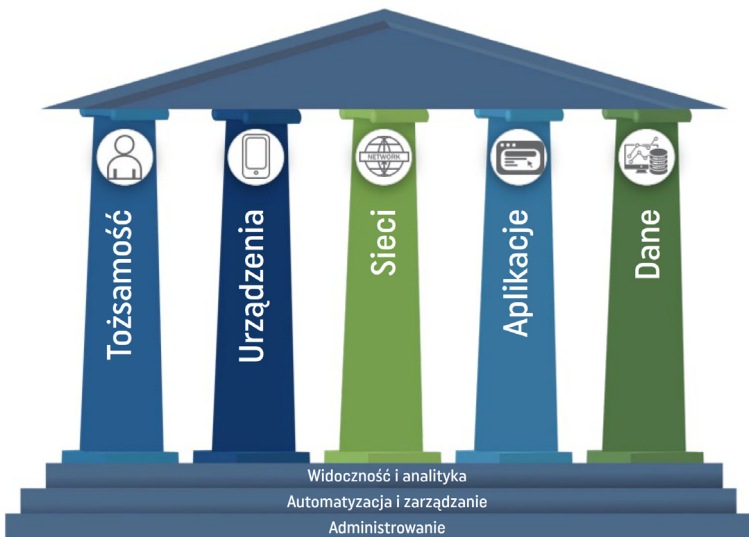
Wdrożenie filozofii „zero trust” nie jest łatwe i może trwać kilka lat, wymagając opracowania bardzo szczegółowych i dynamicznych procedur oraz wdrożenia kosztownych rozwiązań technicznych – wiąże się z większymi kosztami cyberbezpieczeństwa, bo konieczne staje się zatrudnienie specjalistów ochrony danych czy korzystanie z zewnętrznych audytów systemów bezpieczeństwa. Dlatego podejście „zero zaufania” zalecane jest dużym podmiotom, które z reguły narażone są na celowane ataki hakerów mające na celu kompromitację danych, ich kradzież i uzyskanie dużego okupu.

Ale warto ją również stosować nawet w częściowej formie, np. w odniesieniu do zasobów ludzkich, bo pozwala ustrzec się przed najczęściej popełnianymi błędami bezpieczeństwa danych. Oto kilka przykładów:

- **Skupianie się na podejściu nastawionym na niwelowanie skutków ataku, a nie zapobieganie.** Bezpieczna kopia zapasowa to podstawa w procedurze ochrony danych, ale cyberataki można śledzić i zapobiegać nim, zanim się wydarzą poprzez np. monitoring anomalii w ruchu sieciowym oraz analizę zagrożeń w czasie rzeczywistym;
- **Płaskie sieci.** W miarę rozwoju infrastruktury IT i podłączania kolejnych punktów sieciowych (urządzeń) rośnie sieć informatyczna, z czasem tworząc jeden rozbudowany ekosystem danych. Eksperci zalecają segmentację i podział sieci na łatwiejsze w zarządzaniu mikro-sieci, w których zapory ogniowe stosowane są już na poziomie urządzenia;

- **Braki w ochronie urządzeń końcowych.** Duży szpital może mieć ich kilkaset a nawet kilka tysięcy – to systemy do monitorowania parametrów życiowych pacjenta, urządzenia telemedyczne, systemy przywoławcze itd. Pierwszym krokiem jest identyfikacja wszystkich punktów końcowych i opracowanie dla nich polityki dostępu i ochrony.
- **Wdrażanie zdezaktualizowanych mechanizmów kontroli bezpieczeństwa.** Nie wystarczy kontynuować wdrożoną kilka lat temu politykę ochrony danych – trzeba ją na bieżąco udoskonalać wraz z postępem technologicznym. Organizacje ochrony zdrowia powinny też pamiętać, że bezpieczeństwo danych zaczyna się na długo przed zakupem systemu IT. Na tym etapie można zdefiniować rodzaj potrzebnych mechanizmów, np. autoryzacji albo uprawnień użytkowników.

Podejście zerowego zaufania wprowadza duży reżim ochrony. Poczucie zagrożenia nie ma jednak w tym wypadku straszyć, ale zwiększać czujność. Częstotliwość cyberataków rośnie, hakerzy sięgają do coraz bardziej wyrafinowanych sposobów. Statyczna polityka bezpieczeństwa wystarczyła kilka lat temu, ale dziś musi być stale aktualizowana, bo od niej zależy zdrowie i życie pacjentów. ●



Filary
systemu
zerowego
zaufania



Tak ChatGPT pomocze wzmocnić poziom cyberbezpieczeństwa

Jak zaprojektować testy odporności, przygotować cykliczne szkolenia z bezpieczeństwa danych i regularnie informować o nowych zagrożeniach? Zrób to we własnym zakresie z pomocą AI.

Dostępny od września 2026 roku nowy model GPT-6 Astra dorównuje albo przewyższa poziom wiedzy eksperckiej człowieka – tak przynajmniej twierdzi szef OpenAI. Czy także w zakresie cyberbezpieczeństwa? Na pytanie o to, jak wzmocnić ochronę danych, otrzymamy praktyczne wskazówki. ChatGPT zasugeruje zabezpieczenia techniczne, szkolenia personelu, tworzenie kopii zapasowych. Ale jego największą zaletą jest możliwość wzmocnienia wiedzy pracowników o tym, jak chronić dane – a wiemy ze statystyk, że za 80% skutecznych ataków hakerów odpowiada właśnie czynnik ludzki. Tę umiejętność ChatGPT można inteligentnie, ale ostrożnie, wykorzystać do poprawy poziomu cyberbezpieczeństwa.

Symulacje phishingu

Ataki z wykorzystaniem metod socjotechnicznych, czyli najczęściej phishing, są najczęstszą metodą wykorzystywaną przez hakerów. To od nich zaczyna się 90% skutecznych cyberataków. Wystarczy nieuważnie kliknąć na link w wiadomości e-mail albo SMS i hacker zyskuje dostęp do komputerów, blokuje je i żąda okupu. Jeszcze gorzej, gdy wykrada dane i upublicznia je w darknetcie.

Dlatego każda organizacja powinna systematycznie badać, czy pracownicy potrafią rozpoznać fałszywe wiadomości. Do tego służą tzw. ataki symulowane. Taką wiadomość z łańcuchem przygotuje ChatGPT. Wystarczy poprosić o napisanie „maila typu phishing z NFZ albo dostawcy oprogramowania z informacją o zablokowaniu konta i prośbą o weryfikację tożsamości”. Mamy treść, teraz trzeba odpowiednio zaprojektować wysyłkę. Najlepiej sięgnąć do jednego z wielu dostępnych na rynku narzędzi do symulacji phishingu jak np. Microsoft Attack Simulator. Takich rozwiązań jest dużo i nie kosztują dużo. Narzędzia do symulacji ataków phishingowych od razu raportują, osoby z jakimi adresami e-mail kliknęły w link albo otwarły załącznik w mailu. Taką symulację można przeprowadzać regularnie traktując to w charakterze zabawy, aby pracownicy nie czuli niepotrzebnej presji kontroli.

» ChatGPT wygeneruje pytania otwarte albo testy jedno- i wielkokrotnego wyboru na temat cyberbezpieczeństwa. «

Wirtualny trener dla pracowników

ChatGPT świetnie się sprawdza w charakterze interaktywnego trenera. Zalecany rozwiązaniem jest stworzenie własnego modelu wytrenowanego na danych placówki, ale to już wyższa szkoła jazdy dla dużych podmiotów, które rozwijają modele działające lokalnie.

W przypadku małych placówek wystarczy uruchomienie bezpłatnego ChatGPT i poproszenie go o wcielenie się w rolę eksperta cyberbezpieczeństwa w placówce medycznej i zadawanie pytań pracownikowi na np. podstawowym poziomie. W prompcie należy sprecyzować, że każda błędna odpowiedź powinna być korygowana i zadawana w podobny sposób ponownie i aby czat składał się z np. 10 sesji o długości 15 minut każda. W ten sposób ChatGPT sam planuje cały kurs.

Testy i system certyfikacji dla pracowników

Testowanie wiedzy pracowników trzeba dobrze przemyśleć, aby zachować równowagę. Tak, bezpieczeństwo danych jest kluczowe i będzie coraz ważniejsze, ale musi działać w tle. ChatGPT jest źródłem pomysłów, jak stworzyć wewnętrzny, zabawny i oryginalny system certyfikatów traktowanych mniej poważnie. Wszystko zależy od kultury organizacyjnej i hierarchii – w większej organizacji lepiej sprawdzi się sformalizowany system, który pozwoli śledzić postępy wzmocniania poziomu wiedzy z cyberbezpieczeństwa w dużej grupie pracowników; w mniejszej – nieformalne podejście.

ChatGPT jest wprost idealny do tworzenia testów z wiedzy o bezpieczeństwie danych. Wygeneruje pytania otwarte albo testy jedno- i wielkokrotnego wyboru. Przygotuje krótkie studia przypadków i pytania kontekstowe dopasowane do różnych ról w organizacji – od lekarzy i pielęgniarek do rejestratorek i księgowych. Przeprowadzane np. co kwartał testy mogą zawierać przykłady najbardziej aktualnych metod działania hakerów. Testy należy ocenić, przygotować raport słabych i mocnych stron pracownika i na koniec zaproponować indywidualny plan szkoleń.

» ChatGPT wygeneruje w kilka sekund politykę cyberbezpieczeństwa, ale najlepsza jest ta tworzona samodzielnie. «

Weryfikacja i aktualizacja procedur bezpieczeństwa i polityk reagowania na incydenty

Każda placówka powinna mieć – choć w praktyce jest zupełnie inaczej – politykę ochrony danych i reagowania na incydenty. Najczęściej trafia ona na dno szuflady, bo nikt nie ma czasu, aby ją regularnie przeglądać i aktualizować. Ale i tutaj świetnie sprawdzi się ChatGPT. Po wczytaniu dokumentu opisującego politykę bezpieczeństwa (bez podawania danych placówki), AI sprawdzi, czy zawiera on wszystkie niezbędne punkty i podpowie, jak ją udoskonalić. Jeśli w międzyczasie pojawiły się nowe wytyczne, można wprost poprosić ChatGPT o odpowiednie zaktualizowanie procedur.

To samo dotyczy polityki reagowania na incydenty – ta zmienia się w raz z rozwojem placówki i dojrzewaniem cyfrowym. Przykładowo, jeśli podmiot przeszedł na pełną elektroniczną dokumentację medyczną, za tym muszą iść odpowiednie korekty w dokumentach opisujących, co robić w przypadku ataku. Kiedyś to zadanie było żmudne i wymagało przeglądu całych dokumentów. Dzisiaj w kilka sekund zrobi to za nas ChatGPT.

Co więcej, ChatGPT może wykryć niespójności z RODO, EU AI Act a nawet z dyrektywą NIS2 i interpretacjami, które opublikowano już w tym zakresie. Po wczytaniu Ustawy o Krajowym Systemie Cyberbezpieczeństwa i dostępnych wytycznych, ChatGPT podpowie, jak i kiedy przygotować się do audytów zewnętrznych.

Symulator sytuacji kryzysowej

Scenariuszy ataków hakerskich może być wiele: zablokowanie systemów kontrahenta, przykładowo laboratorium wykonującego badania albo firmy cateringowej, groźba publikacji wrażliwych danych pacjentów itd. Jak reagować w takiej sytuacji? Udany atak hakerski to duży stres dla organizacji i w takim przypadku trzeba działać szybko i zgodnie z góry zaplanowanym harmonogramem. Każdy musi wiedzieć co robić, musi być jasne, kto za co odpowiada, aby atak nie

» CeZ: 30 proc. podmiotów zdrowia nigdy nie opublikowało dokumentu polityki cyberbezpieczeństwa. «

stał się zagrożeniem dla zdrowia i życia pacjentów. Do tego służą symulacje sytuacji kryzysowych. Może je wygenerować ChatGPT, testując opcje, których czasami nawet nie możemy sobie wyobrazić, a przez które przeszły inne placówki zdrowia.

ChatGPT jako doradca strategiczny ds. bezpieczeństwa i twórca newslettera

Według statystyk Centrum e-Zdrowia, tylko co trzecia placówka posiada wewnętrzną komórkę ds. bezpieczeństwa danych. Rzeczywistość jest taka, że zadania z tym związane są delegowane do działu IT (jeśli jest) albo osoby z działu organizacji. Z kolei 28 procent podmiotów nigdy nie opublikowało dokumentu polityki cyberbezpieczeństwa.

Cyberochrona nie jest wyłączną kompetencją i często tonie w masie innych obowiązków. Dlatego ChatGPT może być tymczasową pomocą – cyfrowym doradcą. Potrafi naprawdę wiele – zaplanuje harmonogram wdrażania wymagań związanych z dyrektywą NIS2, streści długie raporty i rekomendacje, stworzy plan szkoleń. Od czego zacząć? Od eksperymentowania z wymienionymi zadaniami.

Jeszcze kilka lat temu samodzielne przygotowanie newslettera wewnętrznego o nowych zagrożeniach i z krótkimi praktycznymi radami dla personelu wymagałoby przynajmniej jednego dnia pracy. Dziś robi to AI.

Ale w pracy z ChatGPT obowiązuje ważna zasada: AI nie może uzyskać dostępu do danych pacjentów. Wszystkie wczytywane do modelu dokumenty należy pozbawić danych adresowych (optymalne są modele działające lokalnie). Nowy model GPT-6 nadal, choć rzadziej, halucynuje, dlatego w kwestii cyberbezpieczeństwa najlepiej stosować go do mniej strategicznych zadań jak wspomniane testy czy symulacje phishingu, a kwestie technicznych i organizacyjnych zabezpieczeń pozostawić ekspertom. ●

Zwiększ bezpieczeństwo danych w swojej aptece



włącz **RepoCloud**
i **CopyCloud** już dziś!

- Zminimalizuj ryzyko utraty danych
- Zapewnij ciągłość działania apteki
- Odzyskaj dane po awarii bez straty



Zobacz prezentację



Crash testy bezpieczeństwa danych w szpitalach. Jak się je przeprowadza?

Coraz częściej mówi się o konieczności regularnego testowania odporności systemów IT – od sprawdzania podatności i zabezpieczeń po symulacje cyberataków i testowanie procedur reagowania. Jak wygląda taki „crash test” infrastruktury bezpieczeństwa danych i co może powiedzieć placówce o jej rzeczywistej odporności?

Testowanie bezpieczeństwa systemów IT powinno być stałym elementem zarządzania bezpieczeństwem danych w placówkach medycznych. Samo posiadanie zabezpieczeń nie oznacza bowiem, że są one skuteczne w sytuacji rzeczywistego zagrożenia.

Określenie „crash test” nie oznacza jednego, ściśle zdefiniowanego badania. W praktyce może obejmować różne formy testowania odporności – od analizy podatności i testów penetracyjnych po symulacje ataków oraz sprawdzenie procedur reagowania i odtwarzania systemów po awarii. Ich celem jest sprawdzenie, czy cała organizacja potrafi zareagować, gdy zabezpieczenia zostaną przełamane.

Ocena podatności (analiza ryzyka)

To podstawowe narzędzie, którego celem jest wykrycie słabych punktów zabezpieczeń w infrastrukturze IT szpitala – takich, które mogą wykorzystać hakerzy, aby włamać się do sieci placówki. Ocena podatności wykonywana jest przez informatyków i obejmuje m.in. skanowanie sieci, testowanie sprzętu i systemów. Szpital musi na bieżąco kontrolować, czy posiadane oprogramowanie jest aktualne, a wszystkie systemy zabezpieczeń – np. zapora sieciowa – są odpowiednio skonfigurowane.

Testy penetracyjne

Kontrolowane hakowanie polega na przeprowadzeniu symulacji cyberataku w celu zidentyfikowania słabych punktów ochrony. Dobrze zrealizowane testy penetracyjne mogą otworzyć oczy na wcześniej przeoczone słabe ogniwa systemu zabezpieczeń. Przeprowadza je firma zewnętrzna lub pracownik szpitala. Testy penetracyjne powinny być realizowane nie tylko na systemach IT, ale także na procedurach ochrony danych oraz urządzeniach medycznych wpiętych w sieć szpitalną. Można sprawdzić, czy przykładowo pracownicy mogą potencjalnie nadużyć uprawnień dostępu do danych.

Audyty bezpieczeństwa baz danych

Jednym z głównych celów ataków na placówki zdrowia są dane pacjentów. Hakerzy starają się albo wykraść dane, albo je zaszyfrować, a coraz częściej wykonują obydwie operacje (tzw. podwójne wymuszenie). Ich celem jest zazwyczaj wymuszenie okupu, a skradzione dane mogą być dodatkowo publikowane w darknecie. Dlatego audyt bezpieczeństwa danych – wykonywany przez wyspecjalizowaną firmę – powinien być standardem w dużych placówkach, bo jest podstawą do dalszych inwestycji w cyberbezpieczeństwo. Audytorzy sprawdzają skrupulatnie każdy poziom ochrony danych, ale także procedury reagowania na incydenty bezpieczeństwa.

Jednym z elementów audytów bezpieczeństwa jest audyt zgodności z przepisami dotyczącymi ochrony danych, czyli RODO. To na ich podstawie budowane są strategie ograniczania ryzyka wystąpienia incydentów bezpieczeństwa danych.

Testy reagowania na incydenty

Celem jest sprawdzenie, czy plan reagowania na incydenty bezpieczeństwa danych jest aktualny i zapewnia szybkie odzyskanie danych po awarii i kontynuację działalności, czyli przyjęć, leczenia (z dostępem do krytycznych danych) i planowania wizyt pacjentów. W języku fachowym mówi się o tzw. ćwiczeniach TableTop. Uczestnicy w grupie osób decyzyjnych omawiają dokładnie plan reagowania, a obserwatorzy – eksperci ochrony danych – analizują stopień przygotowania. Oprócz tego sprawdzana jest zdolność do przywracania danych oraz znajomość procedur zgłaszania incydentów naruszenia danych przez pracowników.

Testy phishingowe

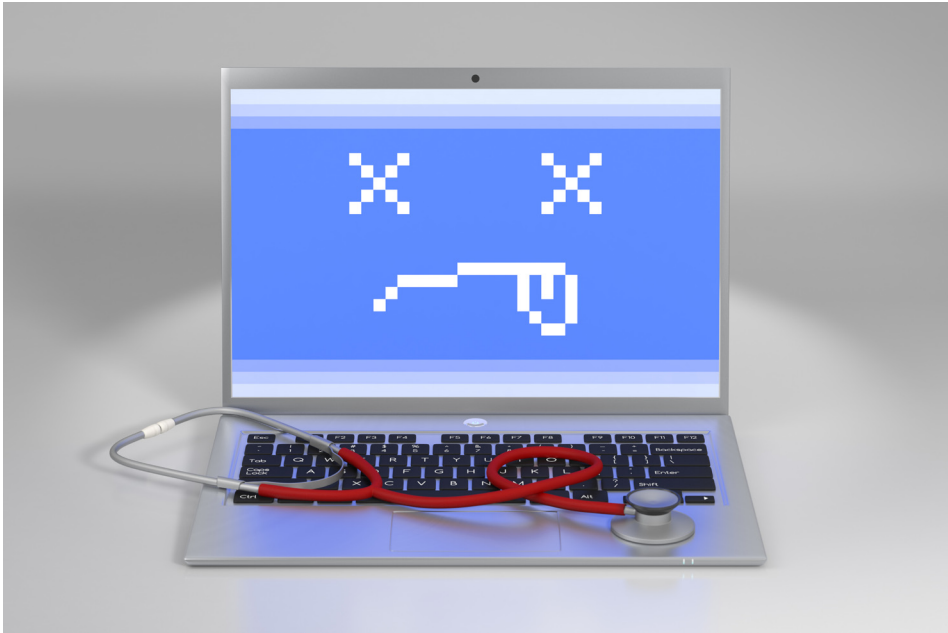
W 2025 roku na całym świecie odnotowano ponad 7,4 tys. publicznie ujawnionych ataków ransomware, o 32 proc. więcej niż rok wcześniej. Ransomware to złośliwe oprogramowanie, które zostaje zainstalowane na komputerze lub sieci placówki. Aby wprowadzić takiego wirusa do sieci szpitala, hakerzy często sięgają do phishingu. Polega on na zachęceniu

» Wyższe wersje systemu Microsoft posiadają opcję symulacji ataków phishingowych. Pozwala ona w łatwy sposób testować reakcję pracowników na podejrzone maile. «

użytkownika do kliknięcia w zainfekowany link albo załącznik, który powoduje instalację wirusa. W tym przypadku „crash-test” polega na przeprowadzeniu symulowanych ataków phishingowych. Na skrzynki poczty elektronicznej pracowników placówki medycznej wysyłana jest wiadomość z podejrzanego e-maila, w której prosi się o np. zainstalowanie nowej wersji systemu albo weryfikację konta. Taki mail powinien zawierać narzędzie trackingowe, aby wiadomo było, ilu pracowników kliknęło na link. ●

Jak przeprowadzić crash test cyberbezpieczeństwa?

1. Zidentyfikuj najważniejsze systemy, urządzenia i dane. Ustal, które zasoby są kluczowe dla leczenia pacjentów i funkcjonowania placówki.
2. Sprawdź aktualność oprogramowania i zabezpieczeń. Zweryfikuj, czy systemy, aplikacje i urządzenia mają aktualne poprawki bezpieczeństwa.
3. Zweryfikuj hasła, MFA i uprawnienia. Sprawdź, czy dostęp do danych mają tylko właściwe osoby i czy konta są odpowiednio zabezpieczone.
4. Sprawdź bezpieczeństwo sieci i dostępu zdalnego. Oceń ochronę połączeń, segmentację sieci oraz zabezpieczenie dostępu spoza placówki.
5. Wykonaj test podatności. Sprawdź, czy w systemach znajdują się luki, które mogłyby zostać wykorzystane przez napastnika.
6. Zasymuluj cyberatak. Przeprowadź kontrolowane ćwiczenie, aby sprawdzić, jak szybko placówka wykryje zagrożenie i zareaguje na nie.
7. Przetestuj kopie zapasowe. Wykonaj rzeczywiste odtworzenie danych i sprawdź, jak szybko można przywrócić kluczowe systemy.
8. Sprawdź działanie podczas awarii. Zweryfikuj, czy personel potrafi kontynuować najważniejsze procesy medyczne bez dostępu do systemów IT.
9. Zweryfikuj procedury reagowania. Sprawdź, czy wiadomo, kto podejmuje decyzje, komu zgłosić incydent i jak przebiega komunikacja.
10. Usuń wykryte słabości. Przygotuj plan naprawczy z określeniem priorytetów, odpowiedzialnych osób i terminów realizacji.



Placówka medyczna padła ofiarą hakerów. Co robić?

Co roku rośnie liczba ataków hakerów na placówki medyczne. Co robić, kiedy na ekranie pojawi się żądanie zapłaty okupu, a komputery są zablokowane?

Cyberataki na placówki medyczne nie zawsze mają spektakularny przebieg, jak w przypadku Szpitala Wojewódzkiego w Szczecinie czy Bonifraterskiego Centrum Medycznego w marcu 2026 r. Częściej są efektem automatycznych kampanii, phishingu lub wykorzystania niezalatanych luk w systemach.

» Jeśli pracownik dopuścił do ataku hakerów, może próbować na własną rękę rozwiązać problem. To najniebezpieczniejszy scenariusz. «

Prawdopodobieństwo wystąpienia cyberataku w okresie kolejnych 12 miesięcy szacuje się na ok. 75%. Na przestrzeni 2 lat rośnie do ok. 85%. Funkcjonowanie bez dobrego planu reagowania na incydenty ochrony danych jest nie tylko ryzykowne, ale nieodpowiedzialne. Jego przygotowanie i testowanie jest czasochłonne, ale wartość podczas ataku – bezcenna. Gdy komputery nie działają, a pacjenci czekają w poczekalni, placówka szybko może pogrążyć się w chaosie. Co wtedy zrobić?

Uruchom procedury z planu reagowania na incydenty

Atak hakerów to sytuacja kryzysowa. Kiedy został zidentyfikowany, trzeba działać zgodnie z *Planem Reagowania na Incydenty (PRI)*. Dobrze przygotowany pozwoli ograniczyć straty – finansowe, wizerunkowe i organizacyjne – i szybko przywrócić placówce płynność funkcjonowania.

Jeśli istnieje podejrzenie ataku cybernetycznego, od razu należy poinformować o tym kierownictwo. Ten oczywisty krok jest jednocześnie najsłabszym ogniwem. Jeśli atak wykryje osoba, która potencjalnie do niego dopuściła, może starać się go ukryć, próbując rozwiązać problem na własną rękę. To jeden z najgorszych scenariuszy, bo z każdą minutą straty mogą być coraz większe. Dlatego pracownicy nie mogą się bać zgłaszania ataków.

Menedżer placówki aktywuje zespół zarządzania kryzysowego, gdzie każda osoba ma z góry przydzielone zadania. Przykładowo, menedżer zgłasza atak do odpowiedzialnych organów, informatyk zabezpiecza infrastrukturę IT, dział komunikacji przygotowuje informację dla mediów, a dział prawny – koordynuje wszystkie kroki, aby były zgodne z przepisami. Każde działanie musi być udokumentowane – dla własnego interesu, aby mieć dowody na podjęcie działań zgodnych z wymaganiami przed Urzędem Ochrony Danych Osobowych (UODO).

Izolacja zagrożenia i komunikacja

Dział IT natychmiast odłącza podejrzane urządzenia od sieci informatycznej i blokuje podejrzane adresy IT i domeny. Zaatakowane lub podejrzane systemy są izolowane zgodnie

» Pierwszym punktem kontaktowym powinien być CSIRT Centrum e-Zdrowia. «

z planem reagowania, a dalsza komunikacja między zespołem kryzysowym oraz pracownikami odbywa się alternatywnymi kanałami informacyjnymi, aby hakerzy nie mogli śledzić działań placówki. To może być np. zaufany i bezpieczny komunikator internetowy. PRI powinien także określać, co zrobić w sytuacji, gdy trwa atak cybernetyczny, a w tym samym czasie chirurdzy wykonują operację pacjenta. To samo dotyczy przekierowania pacjentów do innych placówek oraz procedur odwołania (jeśli to możliwe) wizyt.

O ataku powinni zostać poinformowani wszyscy pracownicy, aby zapobiec rozpowszechnianiu nieprawdziwych informacji albo chaosowi. Osoby z rejestracji muszą wiedzieć, terminy których pacjentów mogą zmienić i jak; lekarze – w jaki sposób zapewnić ciągłość dokumentacji medycznej, gdy nie działa system IT; a wszyscy pracownicy – jak odpowiadać na pytania zaniepokojonych pacjentów albo mediów.

Pierwszym punktem kontaktowym powinien być CSIRT Centrum e-Zdrowia. Incydent można zgłosić albo z pomocą formularza kontaktowego albo telefonicznie. CSIRT CeZ pomoże w dalszych działaniach, które obejmują m.in. zgłoszenie do UODO oraz na Policję. Aby organy te mogły szybko działać, placówka musi zebrać możliwie szerokie informacje o ataku: zapisać logi systemowe albo wyniki skanowania systemu, wykonać kopie zainfekowanych systemów w bezpiecznym środowisku, nie usuwać podejrzanych plików albo e-maili, które posłużą jako materiał dowodowy. Jeśli placówka ma polisę od zagrożeń cybernetycznych, zgłasza natychmiast incydent ubezpieczycielowi. Pod żadnym pozorem nie należy najpierw próbować zapłacić okupu, aby pozbyć się problemu. Atak cybernetyczny to przestępstwo, którym zajmuje się Policja.

Ocena wpływu i przywracanie działania

Obowiązkiem podmiotu jest też ocena skali ataku i jego konsekwencji. Jakie systemy zostały naruszone? Czy doszło do kradzieży danych? Jeśli tak – jakich dokładnie? Czy zagrożone są systemy i dane stron trzecich (kontrahentów)? Te informacje także będą wymagane przez organy jak np. UODO.

Jak pokazuje praktyka, UODO nakłada kary finansowe na placówki, które nie współpracują z urzędem albo nie miały prawidłowo opracowanego planu reagowania na incydenty bezpieczeństwa. Z kolei dobra współpraca zazwyczaj kończy się tylko upomnieniem.

Po etapie oceny, następuje przywracanie płynności działania. Jeśli systemy zostały zaszyfrowane przez np. ransomware, placówka korzysta z bezpiecznej kopii zapasowej (offline albo w chmurze). To właśnie automatyczne kopie z wersjonowaniem znacznie ograniczają ryzyko utraty danych i powinny być elementem strategii backupu. Po przetestowaniu nowej instalacji, można przywrócić działanie systemu.

Zwiększenie poziomu bezpieczeństwa

Nowy start systemu wymaga zmiany wszystkich haseł dostępu użytkowników w każdym, nawet najmniejszym systemie. Wydział IT sprawdza funkcjonowanie systemu antywirusowego i aktualizuje go, instaluje wszystkie dostępne poprawki dla systemów i wprowadza – jeśli jeszcze nie ma – uwierzytelnianie dwuskładnikowe (MFA). Niektóre rygorystyczne zabezpieczenia mogą być uciążliwe dla użytkowników wymuszając np. silne i unikalne hasła albo potwierdzanie logowania kodem MFA, ale cel bezpieczeństwa uświęca środki.

Zgodnie z przepisami ochrony danych osobowych, placówka musi ocenić, czy i jakie dane osobowe zostały naruszone albo wykradzione oraz poinformować o tym poszkodowane osoby. Ten element działania musi być dokładnie skonsultowany z działem prawnym.

Po tym, jak udało się zażegnać kryzys i systemy IT działają poprawnie, czas na analizę, co można zrobić, aby podobny atak się nie powtórzył. Nie chodzi o szukanie winnych, bo nawet dobrze zabezpieczone placówki mogą zostać skutecznie zaatakowane przez hakerów, ale aktualizację planu reagowania na incydenty, ulepszenie procedur oraz rewizję inwestycji w cyberbezpieczeństwo, w tym szkolenia personelu. ●



5 sposobów, jak uniknąć kary Urzędu Ochrony Danych Osobowych

W 2025 roku UODO nałożył rekordowe kary za naruszenie ochrony danych osobowych. Ich wysokość była prawie 5-krotnie wyższa niż w 2024 roku i przekroczyła 64 mln zł. Wśród nich była też grzywna dla podmiotu medycznego w kwocie 1,1 mln zł. Paradoksalnie, większości z nich można było uniknąć.

» Trudno w to uwierzyć, ale część podmiotów nadal nie spełniła podstawowego obowiązku RODO, jakim jest wyznaczenie Inspektora Ochrony Danych. «

Nie jest tajemnicą, za co można dostać karę od UODO, bo wszystkie sprawy podawane są do opinii publicznej na stronie www organu nadzorczego. Najważniejszy wniosek jest taki, że jeszcze nigdy UODO nie nałożył grzywny za to, że hakerzy wykradli dane – to może zdarzyć się każdej firmie posiadającej nawet najlepsze zabezpieczenia. Po kary sięga się wtedy, gdy uchybienia są rażące albo gdy podmiot odmawia współpracy lub utrudnia wyjaśnienie sprawy.

– Kary Prezesa UODO często mają związek z naruszeniami ochrony danych osobowych, ale są nakładane nie za to, że doszło do konkretnego incydentu, ale za nieprzestrzeganie przepisów o ochronie danych osobowych – mówi w rozmowie z OSOZ Mirosław Wróblewski, Prezes UODO.

Przeanalizowaliśmy wszystkie administracyjne kary pieniężne nałożone w ostatnich 5 lat. Które powtarzają się najczęściej?

Liczba i wysokość kar nakładanych przez UODO w latach 2020–2025

Rok	Liczba decyzji	Kwota kar
2020	10 decyzji	3,5 mln zł
2021	14 decyzji	2,2 mln zł
2022	13 decyzji	6,1 mln zł
2023	30 decyzji	1,2 mln zł
2024	20 decyzji	13,9 mln zł
2025	20 decyzji	64 mln*

* dane do listopada 2025

Wysokość kary w zależności od naruszenia (średnia dla lat 2020–2025)

Kategoria naruszenia	Przedział kar (PLN)
Brak zgłoszenia naruszenia	20 000 – 250 000
Niedostateczne zabezpieczenia	30 000 – 500 000+
Brak współpracy z UODO	10 000 – 150 000
Brak / błędy IOD	10 000 – 50 000
Transfery danych niezgodne z prawem	100 000 – kilka mln

Niezgłoszenie naruszenia ochrony danych i niepowiadomienie poszkodowanych osób

Jedna z najczęstszych kar (około 25% wszystkich) dotyczy sytuacji, w której administratorzy nie zgłosili naruszenia organowi nadzorcemu „bez zbędnej zwłoki”, czyli do 72 godzin od zidentyfikowania problemu, albo nie powiadomili osób poszkodowanych w sytuacji, gdy naruszenie miało wysokie ryzyko. To twarda zasada, w przypadku której rzadko kiedy udało się uniknąć kary poprzez odwołanie decyzji do sądu administracyjnego.

A można się przed nią ustrzec w banalnie prosty sposób, wdrażając procedurę wykrywania i raportowania incydentów (*Incident Response*), określając, kto jest odpowiedzialny za zgłoszenie naruszenia i kontakt z osobami poszkodowanymi, przygotowując gotowe szablony zgłoszeń i komunikatów dla osób, których dane dotyczą.

Za takie niedociągnięcia dotąd nałożone kary były bolesne i sięgały 250 tys. zł, nawet w przypadku podmiotów publicznych.

Niedostateczne środki techniczne i organizacyjne w zakresie bezpieczeństwa danych

RODO obowiązuje w Polsce już od 2018 roku i pomimo to nadal wiele podmiotów nie wprowadziło podstawowych jego zapisów. Na początku UODO pobłażliwie traktowało uchybienia, ale teraz twardo karze za brak zabezpieczeń, takich jak niezaszyfrowane bazy danych, brak regularnego testowania mechanizmów bezpieczeństwa danych, nieodpowiednie zabezpieczenia urządzeń mobilnych. Kary w tym obszarze dotyczą ok. 35% wszystkich nałożonych kar administracyjnych, a ich wysokość przekraczała nawet 500 000 zł.

Pierwszym krokiem jest przeprowadzenie rzetelnej oceny ryzyka, wdrożenie polityki szyfrowania danych w spoczynku i w transzycie, zarządzanie aktualizacjami, segmentacja sieci (różne sieci dla różnych systemów), wielopoziomowe logowanie i regularne zmiany haseł, tworzenie i testowanie kopii zapasowych oraz przygotowanie procedur odzyskiwania danych.

Brak współpracy z organem nadzorczym i nieprzekazywanie informacji

Ukrywanie naruszenia i liczenie na to, że „nikt nie zauważy”, to wysoce ryzykowna strategia, bo UODO najczęściej dowiaduje się o sprawach od samych poszkodowanych. UODO karze też wtedy, gdy administrator danych osobowych odmawia udostępnienia dokumentów lub danych niezbędnych do kontroli albo opóźnia realizację analizy sprawy. Ten powód nałożenia kary dotyczy co dziesiątej sprawy, a można byłoby go zminimalizować do zera. Jak?

Stwórz kulturę kładącą nacisk na jawne komunikowanie incydentów w zakresie ochrony danych osobowych, wyznacz dedykowaną do kontaktu osobę, przeprowadź szkolenia dla pracowników ze współpracy z UODO i innymi organami, jak CSIRT CeZ i Policją. Na ukrywaniu można stracić podwójnie, bo takie sprawy najczęściej odbijają się szerokim echem w mediach.

Nieprawidłowości w wyznaczaniu lub brak Inspektora Ochrony Danych (IOD)

Trudno w to uwierzyć, ale część podmiotów nadal nie spełniła podstawowego obowiązku RODO, jakim jest wyznaczenie Inspektora Ochrony Danych. W tym przypadku kara jest jednoznaczna, a odwołanie się do sądu administracyjnego – bezskuteczne. To uchybienie najczęściej dotyczy jednostek publicznych. Przy dobrej współpracy z UODO sprawa kończy się upomnieniem, ale w przeszłości były i kary wynoszące od 10 do 150 tys. zł.

Niwelowanie ryzyka otrzymania tej kary też jest proste: sprawdź obowiązki w zakresie IOD w przepisach RODO, wyznacz jego obowiązki, opublikuj dane kontaktowe.

Uchybienia w przekazywaniu danych poza EOG

Statystycznie co szósta kara UODO dotyczy przekazywania danych do krajów znajdujących się poza Europejskim Obszarem Gospodarczym bez wymaganych umów powierzenia. Należy dokładnie przeanalizować ryzyko po stronie dostaw-

ców i to czy dane osobowe lub medyczne nie są przetwarzane na serwerach w np. USA (wiele e-usług koncernów zagranicznych jest opartych na chmurach danych znajdujących się właśnie w USA, np. call center).

Co zrobić, aby zminimalizować ryzyko kary od UODO?

Odpowiadaj na każde pismo UODO

Brak odpowiedzi na pisma organu nadzorczego jest najkrótszą drogą do otrzymania kary. Niezależnie od oceny zasadności zarzutów, każda korespondencja z UODO wymaga reakcji w wyznaczonym terminie.

Szyfruj nośniki danych i stosuj kontrolę dostępu

Zagubiony niezasyfrowany laptop czy pendrive z danymi pacjentów – za to już UODO nakładał kary. Szyfrowanie dysków twardych i nośników przenośnych, polityka czystego biurka, kontrola dostępu do systemów IT to minimum wymagań wynikających z art. 32 RODO.

Wdrożenie procedury 72 godzin

Każda organizacja musi mieć procedurę zgłaszania naruszeń, regularnie ją testować i komunikować pracownikom. Obejmuje m.in. metody identyfikacji naruszenia, szablon zgłoszenia do UODO oraz kryteria oceny, czy konieczne jest również powiadomienie osób fizycznych.

Weryfikuj podmioty przetwarzające

Wiele kar wynikało z faktu, że administrator nie sprawdził, czy jego podwykonawcy – przykładowo firma IT, dostawca systemu HIS, operatorzy call center – zapewniają właściwy poziom bezpieczeństwa. Umowa powierzenia przetwarzania to absolutne minimum.

Wyznacz IOD

W 2024 roku jedną z kar nałożono na podmiot, który nie wyznaczył Inspektora Ochrony Danych po 6 latach od wejścia w życie RODO. To obowiązek ustawowy.

Kary dla podmiotów medycznych

Choć kary na podmioty medyczne nadal stanowią tylko niewielką część wszystkich kar UODO, to czasami są one bardzo wysokie i rzucają się cieniem na zaufaniu pacjentów do placówki zdrowia.

Oto kilka przykładów. W 2025 roku Centrum Medyczne Ujastek zostało ukarane kwotą ponad 1,1 mln zł za niezgodny z prawem monitoring na salach neonatologii oraz brak odpowiednich zabezpieczeń technicznych i organizacyjnych danych osobowych. W 2024 roku spółka American Heart of Poland otrzymała karę 1,5 mln zł za naruszenie bezpieczeństwa danych około 21 000 osób. Powodem był atak hakerów, będący następstwem błędnej oceny ryzyka i nieprzestrzegania polityki bezpieczeństwa.

Również w 2024 roku SPZOZ w Pajęcznie dostał karę 40 000 zł za niewystarczające środki ochrony danych po ataku ransomware oraz niewypełnienie obowiązku powiadomienia osób dotkniętych incydem. W 2025 roku Uniwersytecki Dziecięcy Szpital Kliniczny w Białymstoku otrzymał karę 66 500 zł za nieprawidłową analizę ryzyka oraz brak odpowiednich technicznych i organizacyjnych środków po ataku ransomware. Z kolei Gyncentrum otrzymało karę 40 000 zł za niepowiadomienie o naruszeniu danych pacjentów po wysłaniu dokumentu zawierającego dane do niewłaściwej osoby.

Na koniec warto zaznaczyć, że polityka bezpieczeństwa danych w podmiocie medycznym nie powinna mieć na celu uniknięcia kary UODO albo innego organu nadzorczego, ale ochronę danych pacjentów. Jeśli to będzie priorytetem, o kary nie trzeba się martwić. ●



NIS2 w placówce zdrowia. Od czego zacząć?

Szacuje się, że 38 000 podmiotów w Polsce musi wprowadzić nowe procedury cyberbezpieczeństwa. Wśród nich jest ok. 1500 placówek zdrowia. To efekt dyrektywy NIS2, którą wprowadza znowelizowana ustawa o krajowym systemie cyberbezpieczeństwa (KSC).

NIS2 to konieczna zmiana

Zapewnienie ciągłości dostępu do usług zdrowotnych jest dziś elementem bezpieczeństwa zarówno pacjentów, jak i państwa. Dlatego sektor ochrony zdrowia został uznany

w dyrektywie NIS2 za sektor kluczowy, tym bardziej że skala cyberataków stale rośnie – według danych Centrum e-Zdrowia, liczba incydentów cyberbezpieczeństwa w latach 2021–2025 zwiększyła się aż 12-krotnie.

W marcu 2025 roku ransomware sparaliżował Szpital MSWiA w Krakowie, powodując niedostępność systemu EDM, wstrzymanie planowych przyjęć i przekierowywanie karettek do innych placówek. W ostatnich miesiącach cyberprzestępcy zaatakowali też Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie, Bonifratskie Centrum Medyczne, Centrum Medyczne Eskulap oraz Świętokrzyskie Centrum Rehabilitacji.

NIS2 ma wzmocnić sektor zdrowia przed skutkami ataków hakerów, co jednak wiąże się z koniecznością wprowadzenia dodatkowych procedur ochrony danych. Nowe przepisy dotyczą szpitali publicznych i prywatnych, większych przychodni, laboratoriów diagnostycznych, operatorów usług medycznych, części dostawców IT dla zdrowia oraz podmiotów zarządzających infrastrukturą cyfrową wykorzystywaną przez ochronę zdrowia.

Nowe obowiązki, terminy i kary

W podmiotach objętych NIS2, cyberbezpieczeństwo staje się obowiązkiem regulacyjnym, a nie jak dotychczas – luźnymi rekomendacjami. Pierwszym podstawowym krokiem, jaki powinna wykonać każda placówka zdrowia, jest wypełnienie ankiety, która pozwoli ocenić, czy podmiot musi spełnić obowiązki wynikające z ustawy o KSC i dyrektywy NIS2. Tzw. pre-weryfikację zgodności z zaleceniami NIS2 można przeprowadzić na udostępnionej przez rząd stronie [www](#) (kliknij tutaj).

Nawet jeśli z ankiety wyjdzie, że NIS2 nie dotyczy twojej placówki, nie oznacza to, że nie zmieni się to w przyszłości (np. w wyniku fuzji, zwiększenia skali działania itd.). Druga ważna wiadomość: otrzymanie wyniku weryfikacji „NIS 2 nie ma zastosowania do twojej działalności” nie zwalnia z obowiązków dokonania rejestracji w Wykazie KSC (kliknij tutaj).

» Duży szpital i mała przychodnia będą miały inne wymagania związane z NIS2. «

Tę trzeba przeprowadzić do 3 października. Niektóre podmioty zostaną wpisane do KSC z urzędu i otrzymają odpowiednie zawiadomienie.

Wdrożenie pełnego systemu zarządzania cyberbezpieczeństwem trzeba zamknąć do 3 kwietnia 2027 roku. Po 24 miesiącach od momentu spełnienia przesłanek uznania za podmiot kluczowy należy przeprowadzić pierwszy audyt zgodności z przepisami, aby potwierdzić realizację obowiązków i przygotować się do kontroli organów państwowych. A kary za niedociągnięcia – przykładowo za brak Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) lub niezgłoszenie incydentu albo lekceważenie obowiązków technicznych i organizacyjnych – mogą być dotkliwe (nawet do 10 mln euro lub 2% rocznego obrotu, a dla podmiotów ważnych: do 7 mln euro lub 1,4% przychodu).

Dobra wiadomość jest taka, że regulacja opiera się na zasadzie proporcjonalności – wymagania dla dużego szpitala są dużo wyższe niż dla małej przychodni. Jest i zła – zbudowanie modelu bezpieczeństwa zgodnego z NIS2 wymaga wdrożenia nowego modelu zarządzania ryzykiem, co trwa kilka miesięcy i kosztuje. Niektóre szpitale otrzymały na wzmocnienie cyberbezpieczeństwa pieniądze z KPO. Pozostałe będą musiały sfinansować proces dostosowawczy z własnych środków.

Najważniejsze terminy związane z NIS2

Termin	Obowiązek
7 maja – 3 października 2026	Samorejestracja w wykazie KSC
do 3 października 2026	Obowiązkowy wpis do wykazu
do 3 kwietnia 2027	Wdrożenie systemu zarządzania cyberbezpieczeństwem
2027–2029 (24 miesiące od uznania za podmiot kluczowy)	Audyty i kontrole zgodności
co 3 lata	Powtórzenie audytu
3 dni od otrzymania raportu z audytu	Przekazanie raportu organowi ds. cyberbezpieczeństwa w formie elektronicznej

Samoidentyfikacja zakończona. Czas na inwentaryzację

Błędem jest myślenie, że wystarczy oddelegować wdrożenie obowiązków NIS2 do działu IT. Przepisy wymagają zaangażowania zarządu i odpowiedzialności kierownictwa. Dlatego kolejnym krokiem jest stworzenie zespołu odpowiedzialnego za cyberbezpieczeństwo. W jego skład powinny wejść:

- dział IT,
- dyrekcja,
- inspektor ochrony danych,
- dział prawny,
- administracja,
- przedstawiciele pionów klinicznych,
- osoby odpowiedzialne za ciągłość działania.

NIS2 wychodzi z logicznego założenia, że skoro cyberatak dotyka każdej komórki organizacyjnej i w każdej może się zacząć, to strategią ochrony musi być objęty każdy element szpitala.

7 kroków wdrożenia NIS2



» Audyt trzeba prowadzić co 3 lata i to na własny koszt. «

Kolejnym elementem jest inwentaryzacja, która polega na odpowiedzi na kilka pytań:

- Które systemy są krytyczne dla bezpieczeństwa działania placówki?
- Jakie procesy mogą zostać zakłócone w wyniku cyberataku?
- Jakie dane są najbardziej wrażliwe?
- Które urządzenia stanowią największe zagrożenie dla bezpieczeństwa informacyjnego?

Hakerzy najczęściej wkradają się do systemu szpitala za pomocą phishingu, ale także wykorzystując luki ochrony w postaci nieaktualnych systemów operacyjnych albo urządzeń medycznych wpiętych do internetu (np. systemów, urządzeń medycznych).

Jeśli już wiemy, jakie zasoby IT mamy, przechodzimy do budowania zabezpieczeń. Pierwszym i najważniejszym jest stworzenie mechanizmu automatycznego tworzenia kopii zapasowych i procedur odtwarzania danych na wypadek ataku hakerów. Następnie przeprowadza się segmentację sieci, czyli podział infrastruktury IT na mniejsze, odseparowane od siebie części. W efekcie, szpitalny system IT musi działać w innej sieci niż np. sieć Wi-Fi dla pacjentów. Każdy pracownik musi mieć tylko niezbędne uprawnienia dostępu do zasobów IT, podzielone zgodnie z rolami.

Już po stronie działu IT pozostają regularna aktualizacja infrastruktury IT, monitoring incydentów bezpieczeństwa danych i ich raportowanie, ochrona poczty elektronicznej oraz stworzenie procedur awaryjnych – działań, które szpital lub placówka medyczna uruchamia w sytuacji kryzysowej, np. podczas cyberataku.

Procedury są bezcenne, aby uniknąć jeszcze większego chaosu

Procedury awaryjne precyzują, kto podejmuje decyzje w sytuacji kryzysowej, jak personel ma pracować bez systemów cyfrowych, w jaki sposób zabezpieczyć dane i sprzęt, jak utrzymać ciągłość leczenia pacjentów oraz kiedy i komu

zgłosić incydent. W praktyce chodzi m.in. o przejście na dokumentację papierową, alternatywne sposoby komunikacji między oddziałami (np. telefon), manualne przyjmowanie pacjentów bez komputera, odłączanie zainfekowanych komputerów od sieci, procedury odwoływania lub przekierowywania wizyt i karetek, a także kontakt z CERT, policją i UODO.

Wraz z procedurami trzeba też dokładnie określić, kto za co odpowiada: kto podejmuje decyzję o odłączeniu systemów w przypadku ataku hakerów, kto komunikuje się z mediami, kto przejmuje proces przejścia na dokumentację papierową oraz przywracania działania kluczowych usług.

RODO chroni dane osobowe,
a NIS2 wzmacnia odporność organizacji na cyberataki

	RODO	NIS2
Główny cel	Ochrona danych osobowych	Cyberodporność organizacji
Maksymalna kara	20 mln EUR lub 4% obrotu	10 mln EUR lub 2% obrotu
Dotyczy	Prywatności	Ciągłości działania
Odpowiedzialność zarządu	Ograniczona	Bezpośrednia
Raportowanie incydentów	Tak	Tak
Audyty bezpieczeństwa	Częściowo	Obowiązkowe

Co powinien zawierać plan reakcji na incydent bezpieczeństwa informacji?

Obszar	Co powinno być przygotowane?
Detekcja	Monitoring i alerty
Eskalacja	Lista kontaktów i odpowiedzialności
Backup	Regularne testy odtwarzania
Komunikacja	Procedury dla personelu i pacjentów
Izolacja systemów	Możliwość odłączenia segmentów
Praca awaryjna	Procedury offline
Raportowanie	Zgłoszenie do CSIRT CeZ
Analiza po incydencie	Wnioski i aktualizacja procedur

» Szkolenia dla personelu medycznego z bezpieczeństwa danych należy prowadzić co 6 miesięcy. «

Wcześniej było zaleceniem, a w NIS2 jest obowiązkiem – chodzi o zarządzanie łańcuchem dostaw. Większe placówki zdrowia powinny już znać zasady w tym obszarze. Podmiot musi sprawdzić, czy dostawcy IT posiadają procedury bezpieczeństwa dotyczące przechowywania danych, kto ma zdalny dostęp do systemów oraz czy umowy zawierają wymagania cyberbezpieczeństwa.

Szkolenia są często ważniejsze niż najlepsze zabezpieczenia technologiczne

90% wszystkich udanych ataków hakerów zaczyna się od phishingu, czyli maila albo wiadomości na telefon, w którym hakerzy podszywają się pod zaufane instytucje i osoby, nakłaniając odbiorcę do kliknięcia zainfekowanego linku lub otwarcia załącznika. W przypadku placówek ochrony mieliśmy już do czynienia z sytuacjami, gdy hakerzy podszywali się pod NFZ albo dostawcę IT, prosząc o zalogowanie się celem pobrania nowej wersji oprogramowania gabinetowego albo wyjaśnienia problemów z rozliczeniem.

Phishingu nie da się zatrzymać zabezpieczeniami technicznymi, dlatego pracownicy muszą wiedzieć, jak go zdementować. Dlatego NIS2 kładzie nacisk na cykliczne szkolenia. W przypadku lekarzy, pielęgniarek i pracowników rejestracji powinny się one odbywać co 6 miesięcy (zalecane). W ramach

Plan szkoleń pozwalający zapewnić zgodność z NIS2

Grupa	Zakres szkolenia	Częstotliwość
Zarząd	Zarządzanie bezpieczeństwem danych (governance)	co 12 miesięcy
Lekarze i pielęgniarki	Phishing i bezpieczeństwo danych, bezpieczne hasła, bezpieczeństwo urządzeń	co 6 miesięcy (zalecane)
Rejestracja	Ochrona danych pacjentów	co 6 miesięcy (zalecane)
IT	Monitoring i reagowanie na incydenty bezpieczeństwa danych	ciągłe
Nowi pracownicy	Podstawy higieny cybernetycznej	W ramach procedury zatrudnienia

planu szkoleń można przygotować symulacje phishingu, testować procedury bezpieczeństwa, ćwiczyć przejście na pracę offline.

Każdy pracownik musi wiedzieć, kogo informować o incydentach i nie bać się tego robić w obawie o konsekwencje personalne. W przypadku poważnego incydentu cyberbezpieczeństwa podmiot zdrowia musi zgłosić go do CSIRT Centrum e-Zdrowia, ocenić możliwy wpływ oraz poinformować użytkowników o zagrożeniu i działaniach ochronnych.

Procedura obejmuje trzy etapy: wczesne ostrzeżenie w ciągu 24 godzin (informacja do CSIRT CeZ; ocena, czy to działanie celowe i określenie, czy dotyczy także innych państw UE), szczegółowe zgłoszenie incydentu w ciągu 72 godzin

Obowiązki raportowania incydentów bezpieczeństwa danych

Obowiązek po incydencie	Czas	Zakres działań
Wczesne ostrzeżenie do CSIRT	Do 24 godzin	Poinformowanie o incydencie CSIRT CeZ, wskazanie, czy działanie było celowe oraz ocena potencjalnego wpływu na inne państwa UE
Szczegółowe zgłoszenie incydentu	Do 72 godzin	Formalne zgłoszenie do CSIRT CeZ, przekazanie opisu wpływu incydentu na usługi, przyczyn, przebiegu, skutków oraz działań zapobiegawczych
Zgłoszenie dla dostawców usług zaufania	Do 24 godzin	Obowiązek szybszego zgłaszania incydentów przez dostawców usług zaufania (usługi regulowane unijnym rozporządzeniem eIDAS)
Sprawozdanie okresowe	Na żądanie CSIRT	Aktualizacja informacji o przebiegu i obsłudze incydentu
Sprawozdanie końcowe	Do miesiąca od zgłoszenia	Podsumowanie incydentu, jego skutków, przyczyn, działań naprawczych i wpływu transgranicznego
Sprawozdanie z postępu	Jeśli incydent nadal trwa	Informacja o aktualnym statusie incydentu do czasu zakończenia obsługi
Informowanie użytkowników	Niezwłocznie	Powiadomienie odbiorców usług o zagrożeniu i możliwych działaniach ochronnych
Dodatkowe raportowanie	W razie potrzeby	Przekazywanie informacji o podatnościach, ryzykach, cyberzagrożeniach i wykorzystywanych technologiach

(zgłoszenie formalne do CSIRT CeZ) oraz sprawozdanie końcowe maksymalnie miesiąc po zgłoszeniu. Raporty muszą zawierać m.in. opis incydentu, jego przyczyn, skutków oraz zastosowanych działań naprawczych. Podmioty mogą także przekazywać informacje o podatnościach, ryzykach i cyberzagrożeniach przez system S46 lub inne kanały komunikacji, pamiętając o oznaczeniu danych objętych tajemnicą przedsiębiorstwa. ●



Cyberbezpieczeństwo w ochronie zdrowia

Wiedza o cyberbezpieczeństwie dla placówek medycznych i aptek w jednym miejscu.

SPRAWDŹ, CO MUSISZ WIEDZIEĆ

Praktyczne porady | Aktualne przepisy | Dobre praktyki.

OTWARTY SYSTEM OCHRONY ZDROWIA

OSOZ

Wydawca:
KAMSOF T S.A.
40-235 Katowice, ul. 1 Maja 133
tel. +48 32 209-07-05
fax +48 32 209-07-15
e-mail: czasopismo@osoz.pl

Redaktor naczelny: Artur Olesch



Jesteśmy partnerem
European Connected Health Alliance

Zespół redakcyjny:
Zygmunt Kamiński,
Agnieszka Golec,
Aleksandra Kurowska,
Katarzyna Płoskonka,
Bożena Wojnarowicz-Głuszek.

Współpracownicy:
Adam Haertle,
Patrik Kuchta,
Grzegorz Mródź,
Jeremi Olechnowicz,
Norbert Przemyk.

Skład i łamanie: Piotr Chamera

Przedruk, kopiowanie, skracanie, wykorzystanie
tekstów (lub ich fragmentów) publikowanych
w czasopiśmie OSOZ bez zgody wydawcy
KAMSOF T S.A. jest zabronione.

Redakcja nie odpowiada za treść reklam,
ogłoszeń i artykułów sponsorowanych.