CZASOPISMO O CYFRYZACJI OCHRONY ZDROWIA

BLOG.OSOZ.PL

OSOZ

ISSN 1897-5828

RAPORT SPECJALNY

CYBER OCHRONA

Poradnik bezpieczeństwa danych dla podmiotów leczniczych.

Nowe metody hakerów
Phishing i ransomware
Cyberpsychologia
Powtórka z RODO
Chmura danych
Onboarding IT
Insider threats
Fake newsy

129 STRON
z wytycznymi dla małych i dużych podmiotów
+
AKTUALNE ZALECENIA CSIRT CeZ

Wzmocnij ochronę danych

ARTUR OLESCH
Redakcja Czasopisma
OSOZ Polska
OSOZ Statystyki

✉ redakcja@osoz.pl

Jak udaremnić atak hakerów, zapobiec wyciekowi danych lub zmniejszyć jego negatywne skutki? W naszym poradniku znajdziesz porady ekspertów i esencję wiedzy z cyberbezpieczeństwa w ochronie zdrowia.

Zmień sposób myślenia o cyberbezpieczeństwie

Liczba cyberataków na placówki ochrony zdrowia rośnie z roku na roku. Ofiarą mogą paść duże podmioty posiadające działy IT i indywidualne praktyki lekarskie wyposażone jedynie w standardowe zabezpieczenia techniczne. Ale w walce z hakerami każda organizacja może zbudować wielowarstwowy, szczelny system ochrony.

Z analizy incydentów bezpieczeństwa danych w ochronie zdrowia wynika, że to **wiedza pracowników i procedury** są najskuteczniejszą metodą ochrony przez atakiem cyberprzestępców i minimalizacji jego negatywnych efektów.

W praktyce bywa różnie – podmioty lecznicze gubią się w przepisach, a ochrona danych medycznych jest postrzegana jako dodatkowe obciążenie i koszt. Nasz przewodnik udowadnia, że dobrze zorganizowany i systematycznie aktualizowany system bezpieczeństwa informacyjnego nie musi być skomplikowany, działa niezauważalnie w tle, a do tego wspiera długofalowo cyfrowe dojrzewanie podmiotu medycznego.

Wskazówki dla małych i dużych podmiotów

Poradnik bezpieczeństwa danych w ochronie zdrowia zawiera porady pozwalające zwiększyć poziom ochrony informacji, wywiady z ekspertami, najlepsze praktyki z Polski i zza granicy oraz pomysły dopasowane do możliwości każdego podmiotu leczniczego.

Dowiedz się jak:

- Spełnić wymagania RODO;
- Chronić dane pacjentów przed nowymi zagrożeniami cybernetycznymi;
- Nie dać się nabrać na phishing i ataki ransomware;
- Zabezpieczyć bazy danych;
- Stosować zasady cyberpsychologii;
- Wdrażać AI bez obaw o ochronę danych;
- Uniknąć kar UODO.

Poradnik polecamy placówkom medycznym jako materiał do szkoleń oraz osobom, które indywidualnie chcą podnieść swoje kompetencje w zakresie ochrony danych.

Bezpłatny webinar „Cyberbezpieczeństwo i RODO w ochronie zdrowia”

Szybki kurs z podstaw ochrony danych.
Czas trwania: 21 minut

Kliknij na grafikę lub zeskanuj kod QR.

OCHRONA DANYCH

Poradnik dla podmiotów leczniczych

RODO I CYBERBEZPIECZEŃSTWO
Co trzeba wiedzieć?

7 Większość podmiotów leczniczych deklaruje, że chroni dane pacjentów. Ale czy skutecznie?

12 Ochrona danych w modelu sera szwajcarskiego

16 Powtórka z RODO

23 Obowiązki Inspektora Ochrony Danych Osobowych

27 Kary pieniężne za naruszenie RODO. Czy można oszacować ich wysokość?

32 20 zaleceń ochrony danych medycznych z USA

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

NOWE METODY HAKERÓW
Zaktualizuj politykę bezpieczeństwa danych

45 Ekspert CSIRT CeZ: Cyberbezpieczeństwo to system naczyń połączonych

53 Jak wzmocnić cyberbezpieczeństwo w roku 2024/2025?

57 Co każdy lekarz może zrobić, aby lepiej chronić dane pacjentów?

62 Bezpieczne logowanie do usług on-line

REWOLUCJA SZTUCZNEJ INTELIGENCJI
Przygotuj się na narzędzia AI

66 Przewodnik, jak wdrażać AI zgodnie z przepisami

LUDZIE NA PIERWSZEJ LINII OCHRONY DANYCH
Jak wzmocnić umiejętności cyfrowe personelu?

75 Jak przeprowadzić onboarding IT nowych pracowników?

80 Cyberpsychologia. Nowe narzędzie do walki z hakerami

86 Phishing najczęstszą przyczyną kradzieży danych. Jak się bronić?

91 Insider threats, czyli jak chronić dane przed zagrożeniami wewnętrznymi

97 6 zasad ochrony przed ransomware i reguła 3-2-1

CIEMNE STRONY SZTUCZNEJ INTELIGENCJI
Uwaga na fake newsy

102 Raport: AI i dezinformacja na liście największych zagrożeń dla świata

106 Nowe zagrożenia cybernetyczne oparte na sztucznej inteligencji

111 Fake newsy tworzone przez AI zalewają internet. Infodemia jest śmiertelnie niebezpieczna

TRENDY CYBERBEZPIECZEŃSTWA
Strategie liderów

115 Kim jest i dlaczego placówki medyczne potrzebują CMIO/CDO?

119 Dane w chmurze: bezpieczniej, wygodniej, perspektywicznie

125 Chmura w aptekach. Automatyczna ochrona przed utratą danych

Buduj **relacje** z pacjentami dzięki **aplikacji**

VisiMed

- ✓ Ułatwiasz pacjentom rezerwację wizyt
- ✓ Zmniejszasz kolejki i liczbę telefonów do rejestracji
- ✓ Realizujesz porady on-line i zamówienia na e-Recepty
- ✓ Redukujesz liczbę niezrealizowanych wizyt
- ✓ Dbasz o dyskrecję obsługi pacjenta

pomoc@osoz.pl | tel. (+48) 32 209 07 05

visimed.osoz.pl

Większość podmiotów leczniczych deklaruje, że chroni dane pacjentów. Ale czy skutecznie?

Jakie nowe metody stosują cyberprzestępcy? Jak się przed nimi bronić? Rozmowa z Jakubem Betka, Prezesem Zarządu Ogólnopolskiego Stowarzyszenia Ochrony Danych Osobowych w Sektorze Medycznym oraz inspektorem ochrony danych, konsultantem ds. cyberbezpieczeństwa.

Jak wyglądają statystyki dotyczące ataków hakerów na placówki zdrowia?

Skalę ataków hakerskich na polskie placówki medyczne można podzielić na trzy etapy. Pierwszy to okres do 2020 roku, kiedy ataków było stosunkowo niewiele. Oczywiście takie ataki występowały, natomiast rok 2020 wszystko zmienił. Skutkiem pandemii COVID-19 była wzmożona cyfryzacja w sektorze medycznym, co zachęciło cyberprzestępców do coraz częstszych ataków. Ten stan trwał do 2022 roku i rozpoczęcia przez Rosję wojny z Ukrainą – od tego czasu skala cyberataków znacznie znaczenie wzrosła.

O ile?

Porównując pierwszy kwartał 2022 roku i pierwszy kwartał 2023 roku, obserwujemy wzrost ataków hakerskich na podmioty z sektora medycznego o 24%. Podmioty medyczne, które wdrożyły mechanizmy monitorowania swoich systemów teleinformatycznych, wprost wskazują, że do prób ataków dochodzi kilkadziesiąt, a często kilkaset razy dziennie.

Czy podmioty lecznicze dobrze chronią dane pacjentów?

Większość placówek na pewno sądzi, że dobrze chroni dane pacjentów. Pytanie, czy na pewno skutecznie? Ochrona danych i cyberbezpieczeństwo to ciągła walka z cyberprzestępcami. Dlatego do tematu ochrony danych pacjentów trzeba podchodzić jak do procesu ciągłego doskonalenia i poprawiania systemu. W ramach stowarzyszenia OSODO w Sektorze Medycznym, prowadzimy regularne spotkania,

» W dalszym ciągu RODO w sektorze zdrowia jest postrzegane przez pryzmat absurdalnych sytuacji. «

podczas których członkowie, czyli Inspektorzy Ochrony Danych, wskazują, gdzie widzą największe zagrożenia. To daje możliwość reakcji innym członkom w ich placówkach.

Co jest w takim razie najsłabszym ogniwem? Jak najczęściej dochodzi do wycieku danych?

Utrwaliło się stwierdzenie, że najsłabszym ogniwem w systemie bezpieczeństwa danych jest człowiek. Trudno nie zgodzić się z tym stwierdzeniem. Placówka medyczna, może dysponować najnowszymi rozwiązaniami technicznymi, ale bez odpowiedniej wiedzy i świadomości personelu nie będzie można ich w pełni wykorzystać. Jednak w ostatnim czasie, bardzo często dochodzi do ataków typu DDoS (ang.: Distributed Denial of Service), które mają na celu zakłócenie lub całkowite wyłączenie danej usługi czy systemu. Ryzyko tego typu ataku można ograniczyć najlepiej poprzez wprowadzenie odpowiednich rozwiązań technicznych.

Czy oprócz DDoS są jeszcze jakieś inne, nowe metody działania cyberprzestępców?

Najwięcej w ostatnim czasie w zakresie cyfryzacji mówi się o sztucznej inteligencji. Po rozwiązania oparte na AI sięgają również cyberprzestępcy, wykorzystując je go szybszych i sprawniejszych ataków. Sztuczna inteligencja jest wykorzystywana do łamania haseł, w analizach najsłabszych punktów placówki, w zbieraniu informacji do przeprowadzenia ataków phishingowych oraz do tworzenia wiadomości phishingowych.

Hakerzy korzystający ze sztucznej inteligencji są w stanie wygenerować wiadomość np. dyrektora szpitala do działu IT, używając w wiadomości stwierdzeń, powiedzeń, słów, szyku zdań, które zazwyczaj stosuje nadawca.

» W ostatnim czasie, bardzo często dochodzi do ataków typu DDoS. «

Trzeba także pamiętać, że sztuczna inteligencja jest coraz częściej wykorzystywana w ochronie zdrowia. Takie rozwiązania mają wspomóc personel medyczny w analizie i podejmowaniu decyzji. Jednak w przypadku wykorzystania AI, kwestia bezpieczeństwa danych zyskuje jeszcze bardziej na znaczeniu. Nie chodzi tutaj już o wycieki danych. Atak hakerski może bowiem polegać na nieautoryzowanej manipulacji danymi służącymi do nauki lub testowania algorytmu. Skutkiem mogą być zafałszowane wyniki, które mogą prowadzić do błędnych analiz, błędnych decyzji, zastosowania błędnego leczenia, a w najgorszych przypadkach – nawet do śmierci pacjenta.

Wiele kwestii związanych z ochroną danych reguluje RODO, które obowiązuje w Polsce już od 6 lat. Czy w ochronie zdrowia jest ono przestrzegane?

Z RODO jest dokładnie jak z cyberbezpieczeństwem – zapewnienie zgodności z przepisami tego unijnego rozporządzenia to ciągły proces. Każda nowa usługa, nowy proces, nowy system informatyczny lub aparatura medyczna, może generować nowe ryzyko dla bezpieczeństwa danych pacjentów.

Mimo upływu 6 lat, w dalszym ciągu RODO w sektorze zdrowia jest postrzegane przez pryzmat absurdalnych sytuacji, do których dochodziło przy początkach jego stosowania. W niektórych jednostkach można nadal spotkać niepotrzebne zgody pacjentów na przetwarzanie ich danych osobowych w celu prowadzenia procesu leczenia.

Część placówek skupiła się na stworzeniu dokumentacji, która ma „zapewnić zgodność z RODO". Po tym, jak zostały opracowane, często trafiały do szuflady, w której czekają na kontrolę. Niestety, nie tędy droga.

RODO opiera się na analizie ryzyka, czyli na analizie, która ma wykazać, jakie sytuacje mogą skutkować utratą bezpieczeństwa dla danych i jakie zabezpieczenia placówka wdrożyła lub wdroży, aby zmniejszyć skutki takich sytuacji

lub prawdopodobieństwo ich wystąpienia. Taka analiza powinna być prowadzona cyklicznie, choćby ze względu na to, że zmieniają się metody działania cyberprzestępców.

Podmioty lecznicze z reguły nie mają dużych budżetów na ochronę danych. Jak mimo to zwiększyć poziom cyberbezpieczeństwa?

Bez wystarczających środków finansowych, cyberprzestępcy zawsze będą o krok przed placówkami medycznymi.

Można oczywiście zwiększać świadomość personelu. Takie szkolenia może, wręcz powinien, prowadzić Inspektor Ochrony Danych, który posiada odpowiednią wiedzę i cały czas ją aktualizuje. A to z kolei oznacza koszt dla placówki medycznej.

Innym aspektem bezpieczeństwa, który nie wymaga dużych nakładów finansowych, jest wyegzekwowania bezpieczeństwa danych u dostawców. Placówki medyczne coraz częściej korzystają z rozwiązań zewnętrznych (np. chmura, oprogramowanie medyczne, zdalny serwis aparatury medycznej), jednak nie stawiają przed dostawcami żadnych wymogów związanych z zapewnieniem bezpieczeństwa danych podczas korzystania z tych rozwiązań.

Polecam też uczyć się na cudzych błędach. Placówki powinny przeanalizować przypadki ataków hakerskich na inne jednostki, jak przykładowo ostatni głośny atak na Laboratoria ALAB, i sprawdzić, czy są gotowe na takie sytuacje. Jeżeli nie, to kolejnym krokiem jest wprowadzenie mechanizmów, które zminimalizują prawdopodobieństwo wystąpienia podobnego ataku „u Nas".

Jednak obawiam się, że bez wystarczających środków finansowych, placówki medyczne nie będą gotowe na coraz intensywniejszą wojnę w cyberprzestrzeni.

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 znajdą 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 haseł.

Koncepcja ochrony wielowarstwowej podobna jest do „sera 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 mieszanką 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:

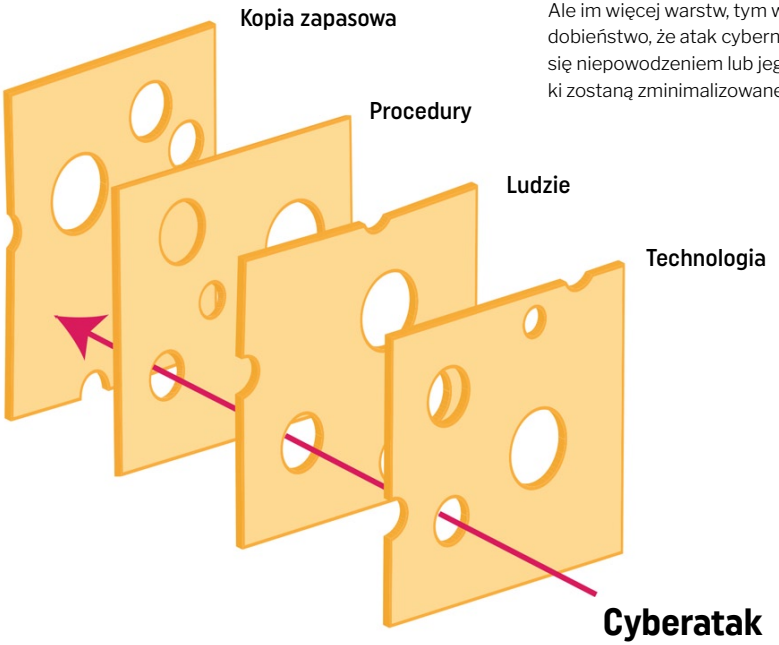
- **Bezpieczeństwo obwodowe** (infrastruktura techniczna): bariery fizyczne, cyfrowe systemy zabezpieczeń, kontrola dostępu, mechanizmy uwierzytelniania;
- **Bezpieczeństwo sieci** (infrastruktura sieciowa): firewall, VPN, kontrola dostępu;
- **Szkolenia dla pracowników** (wiedza i know-how): jak rozpoznać 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.

Powtórka z RODO

Sprawdź, czy chronisz dane pacjentów zgodnie z RODO. Dzięki temu uchronisz się przed przykrymi konsekwencjami: karami finansowymi, szantażem cyberprzestępców i kłopotami związanymi z usuwaniem skutków naruszenia prywatności danych.

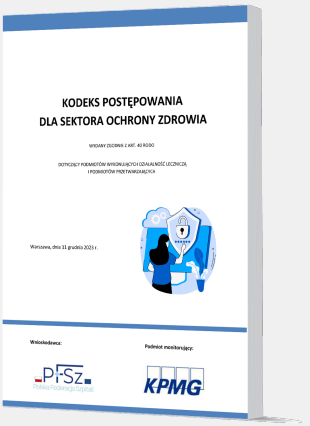
Rekordowe kary UODO

W maju 2023 roku minęła 5 rocznica obowiązywania RODO w Polsce. Do Rozporządzenia o Ochronie Danych Osobowych jedni zdążyli się już przyzwyczaić, u niektórych samo pojęcie nadal wzbudza strach.

Jednak z danych Urzędu Ochrony Danych Osobowych (UODO) wynika, że zaniedbania są nadal ogromne. W 2022 roku UODO nałożył rekordową karę administracyjną w kwocie 5 mln zł. 63% wszystkich kar nałożonych od 2018

Kodeks postępowania dla sektora ochrony zdrowia

Polska Federacja Szpitali



Kliknij tutaj,
aby pobrać plik

Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych

Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie

Kliknij tutaj,
aby pobrać plik

roku przez europejskie urzędy ochrony danych (2,9 mld euro) przypada na 2022 rok (1,83 mld euro). W rankingu kar w Europie, Polska znalazła się na 15. miejscu z 13 karami w kwocie prawie 12 mln zł.

Na liście jest jedna placówka medyczna – Warszawski Uniwersytet Medyczny, który ukarano kwotą 10 000 zł za niezgłoszenie w wymaganym czasie 72 godzin naruszenia ochrony danych osobowych. Jeden z pacjentów otrzymał skierowanie zawierające dane innej osoby, a administrator nie zgłosił tego incydentu do UODO. Do historii przejdzie jednak kara w wysokości 100 000 tys. zł, jaką w 2023 roku UODO nałożył na byłego ministra zdrowia Adama Niedzielskiego za ujawnienie danych lekarza i wystawionej recepty. To najwyższa z możliwych kar, jaką można było nałożyć.

Podstawy RODO w ochronie zdrowia

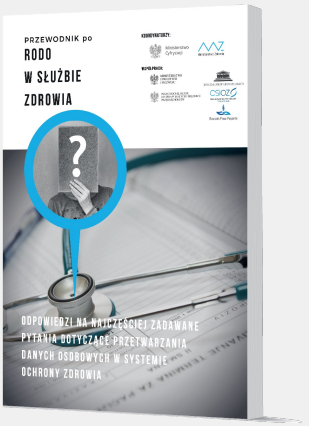
Z zagwarantowaniem bezpieczeństwa informacji problem mają nawet doświadczeni administratorzy systemów IT podmiotów medycznych. A co dopiero lekarze prowadzący indywidualne praktyki lekarskie, którym brakuje czasu na zajmowanie się sprawami administracyjnymi. Efekt jest taki, że w wielu podmiotach wymagania RODO nie są spełniane. Do tego szybko rosnąca skala cyberataków na szpitale wymusza systematyczną aktualizację i wzmacnianie zabezpieczeń.

Najważniejsze informacje o RODO w ochronie zdrowia można znaleźć w trzech dokumentach, które uzyskały pozytywną opinię Prezesa Urzędu Ochrony Danych Osobowych:

- **Kodeks postępowania dla sektora ochrony zdrowia** przygotowany przez Polską Federację Szpitali (grudzień 2023),
- **Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych** opracowany przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie (grudzień 2022)

Przewodnik po RODO w służbie zdrowia

Ministerstwo Zdrowia
i Rzecznik Praw Pacjenta



Kliknij tutaj,
aby pobrać plik

- **Przewodnik po RODO w służbie zdrowia** wydany przez Ministerstwo Zdrowia we współpracy z Rzecznikiem Praw Pacjenta (wrzesień 2018)

Podsumujmy zasady, które stanowią absolutne minimum w każdym podmiocie przetwarzającym dane medyczne.

Zapewnienie rozliczalności

Zapewnienie rozliczalności przestrzegania obowiązujących przepisów realizowane jest m.in. poprzez prowadzenie dokumentacji ochrony danych osobowych zawierającej procedury, instrukcje, wytyczne oraz inne uregulowania związane z bezpieczeństwem informacji.

Na dokumentację ochrony danych osobowych w placówce medycznej powinny się składać przynajmniej następujące elementy:

- rejestr czynności przetwarzania;
- ewidencja naruszeń ochrony danych osobowych;
- sposób postępowania z naruszeniami ochrony danych osobowych;
- procedura rozpatrywania wniosków osób, których dane dotyczą np. w sprawie dostępu do danych, żądania usunięcia danych, kopii danych;
- procedura udostępniania dokumentacji lub informacji medycznych;
- zasady pracy w systemach informatycznych.

Umowy powierzenia

Jednym z obowiązków nakładanych przez RODO jest zawieranie umów powierzenia przetwarzania danych w trybie udostępniania danych podmiotom zewnętrznym będących Podmiotami Przetwarzającymi.

W takich umowach mamy dwie strony: *Administratora Danych Osobowych* określającego cele i sposoby wykorzystania danych osobowych oraz *Podmiot Przetwarzający* realizujący zlecenie Administratora i przetwarzający dane wyłącznie w celach wskazanych przez Administratora.

Obowiązek informacyjny

Klauzule zawierające informacje o przetwarzaniu danych, które powinny być udostępnione w taki sposób, aby pacjenci mieli możliwość się z nimi zapoznać. W praktyce wystarczy wywiesić obowiązek informacyjny w widocznym miejscu placówki medycznej (np. na tablicy przy rejestracji) oraz na stronie www placówki.

Poszanowanie intymności i godności pacjentów

O poszanowaniu intymności i godności pacjentów należy pamiętać na każdym etapie wizyty. Najbardziej newralgicznym punktem jest rejestracja i wywoływanie do gabinetu pacjentów oczekujących w poczekalni. Musi się to odbywać się w sposób, który gwarantuje, że osoby postronne nie będą w stanie wejść w posiadanie informacji, które nie są dla nich przeznaczone. Przykładowo, inni pacjenci nie mogą dowiedzieć się, że pacjent A – wywołany z imienia i nazwiska – leczy się u lekarza danej specjalności. Oto kilka prostych sposobów jak to zrobić:

- umieszczenie przy rejestracji informacji „Przy stanowisku rejestracji może przebywać tylko jedna osoba";
- umieszczenie na podłodze przed rejestracją linii określającej strefę, poza którą czekają na swoją kolej inni pacjenci (strefa intymna);
- stworzenie bezpiecznego systemu przywoławczego, np. poprzez system numerów, elektroniczne systemy kolejkowe;
- rozdzielenie ściankami stanowisk rejestracji (jeśli jest kilka).

Zabezpieczenie danych przechowywanych w formie elektronicznej

Już prawie wszystkie dane gromadzone są w formie elektronicznej, a to oznacza, że system informatyczny musi zostać objęty szczególną ochroną. Tak, aby osoby nieupoważnione (to nie zawsze muszą być hakerzy żądający okupu) nie zyskały

» RODO to także poszanowanie intymności i godności pacjentów ważne na każdym etapie wizyty. «

do nich dostępu. Oto najważniejsze zalecenia, które powinny być przestrzegane zawsze:

- Przestrzeganie polityki mocnych haseł – skomplikowane, długie hasła dostępu składające się z małych i dużych liter, cyfr i znaków specjalnych;
- Wprowadzenie polityki czystego pulpitu (żaden dokument z danymi pacjenta nie może być zapisany poza zabezpieczonym systemem IT) oraz blokowanie stacji po określonym czasie bezczynności;
- Wykonywanie i zabezpieczanie kopii zapasowych zbiorów danych (zaleca się co najmniej dwie kopie w różnych lokalizacjach, w tym w chmurze danych);
- Stosowanie kryptograficznych środków ochrony przetwarzanych danych osobowych przez osoby użytkujące komputer przenośny zawierający dane osobowe podczas transportu, przechowywania;
- Zabezpieczenie kluczowej infrastruktury (np. zamki do serwerów);
- Wykorzystanie agregatów prądotwórczych, urządzeń UPS;
- Zabezpieczanie elektronicznych nośników informacji;
- Stosowanie i aktualizacja systemów antywirusowych;
- Używanie aktualnych wersji oprogramowania do tworzenia EDM i systemu operacyjnego;
- Prowadzenie systematycznych szkoleń pracowników w zakresie zapobiegania atakom socjotechnicznym;
- Przeprowadzanie testów bezpieczeństwa systemu w tym testów penetracyjnych.

Należy pamiętać, że zabezpieczenia powinny wynikać z przeprowadzonej oceny ryzyka.

Zabezpieczenie papierowej dokumentacji medycznej

Mimo postępującej digitalizacji, w wielu placówkach nadal istnieją archiwa kartotek papierowych. Te również należy objąć odpowiednią ochroną przed:

- kradzieżą. Można minimalizować jej ryzyko wprowadzając rolety, kraty, systemy antywłamaniowe i alarmowe;
- nieuprawnionym dostępem z wewnątrz osób spoza personelu medycznego. Wśród najprostszych sposobów zabezpieczenia można wymienić przechowywanie kartotek w szafach zamykanych na klucz, a także zarządzanie kluczami do pomieszczeń;
- brakiem dostępu do gromadzonej dokumentacji. Aby zapobiec zniszczeniu dokumentów, warto zapewnić odpowiednie warunki środowiskowe, takie jak odpowiednia temperatura, wilgotność, wentylacja, systemy alarmujące zagrożenia takie jak zalanie albo pożar.

Szkolenia osób zatrudnionych

» Mocna ochrona danych wymaga regularnych szkoleń i onbo-ardingu nowych pracowników. «

Zastosowanie wyłącznie środków technicznych i organizacyjnych to dopiero pierwszy krok. Drugim jest dostarczenie personelowi wiedzy o tym, jak pracować z danymi osobowymi, z jakimi zagrożeniami mogą się spotkać, jak na nie reagować. Personel musi być szkolony z obowiązujących w placówce zasad bezpieczeństwa i ochrony danych osobowych. Powinien wiedzieć, jakimi sztuczkami posługują się cyberprzestępcy próbujący wykraść dane lub zainfekować system IT. Generalna zasada brzmi: system zabezpieczeń danych osobowych w placówce medycznej jak tak mocny, jak jego najsłabsze ogniwo.

Szkolenia dotyczą zarówno nowych pracowników (boarding), jak i obecnych (systematyczne kursy aktualizujące wiedzę).

Upoważnienia osób zatrudnionych

Każda osoba zatrudniona w placówce medycznej powinna mieć ściśle określony dostęp do danych osobowych. Zakres upoważnień powinien uwzględniać obowiązki osoby

zatrudnionej. Warto pamiętać, aby nie nadawać uprawnień personelowi „na zapas", w sposób nadmiarowy. Istotne jest także prawidłowe ewidencjonowanie osób upoważnionych do przetwarzania danych osobowych.

Procedury na wypadek naruszenia danych

Mimo najlepszych zabezpieczeń, wyciek danych lub naruszenie przepisów RODO może się przytrafić. Każda placówka musi posiadać procedury postępowania w takich przypadkach. Wśród nich jest zgłoszenie przypadku do UODO w czasie 72 godzi od identyfikacji naruszenia, a w przypadku podmiotów medycznych – także do CSIRT Centrum e-Zdrowia.

Nie tylko administratorzy, ale też pracownicy muszą wiedzieć, jak się zachować, bo to oni najczęściej są pierwszymi świadkami ataku cybernetycznego albo naruszenia danych. A szybka reakcja decyduje o wielkości szkód.

» System zabezpieczeń danych w placówce medycznej jak tak mocny, jak jego najsłabsze ogniwo. «

Obowiązki Inspektora Ochrony Danych Osobowych

Francuski organ regulacyjny ds. ochrony danych osobowych (CNIL) wydał przewodnik inspektora ochrony danych osobowych (IOD). To zbiór pogłębionych podpowiedzi, jak zapewnić zgodność z RODO, które mogą się przydać IOD w polskich podmiotach leczniczych.

Po wejściu w życie RODO, rola IOD – w stosunku do jego poprzednika, czyli ABI (Administrator Bezpieczeństwa Informacji) – jest dla każdej organizacji kluczowa. W szczególności, ze względu na jego czynny udział we wszystkich procesach przetwarzania danych osobowych. Jednak IOD nie jest osobiście odpowiedzialny za naruszenia obowiązków określonych w RODO. W przypadku zaistnienia naruszeń, odpowiedzialność ponosi organizacja powołująca IOD, czyli w praktyce administrator lub podmiot przetwarzający.

Organizacje często zapominają, że IOD pełni rolę o charakterze nadzorczym, doradczym, informacyjnym i jego głównym zadaniem jest wsparcie kierownictwa w wypełnianiu obowiązków w zakresie danych osobowych.

Z pewnością rola IOD nie ma charakteru wyłącznie wykonawczego. IOD udziela kierownictwu oraz innym osobom uczestniczącym w procesach przetwarzania danych osobowych eksperckich wskazówek, aby zapewnić zgodność z obowiązującymi przepisami prawa. Co więcej, IOD jest źródłem wiedzy w zakresie ochrony danych osobowych, która powinna być cyklicznie przekazywana osobom zainteresowanym podczas szkoleń i konsultacji.

Oto zakresy działań, w które w szczególności powinien być zaangażowany IOD:

- **Monitorowanie przestrzegania RODO.** Przykładem tych działań będzie realizowanie wewnętrznych weryfikacji procesów przetwarzania danych osobowych, zlecanie audytów zewnętrznych w tym zakresie oraz monitorowanie działań korygujących i naprawczych w następstwie zidentyfikowania nieprawidłowości.
- **Kontakty z organem nadzorczym.** IOD jest punktem kontaktowym pomiędzy organizacją, a organem nadzorczym. Do jego zadań należy odpowiadanie na pytania i wezwania organu. Powiadamia on organ nadzorczy o zaistniałych naruszeniach ochrony danych w organizacji. Kierunek komunikacji nie jest jednak jednostronny, należy pamiętać,

że IOD może zwracać się z pytaniami dotyczącymi danych osobowych do organu nadzorczego.

- **Kontakty z osobami, których dane dotyczą.** Bardzo ważnym aspektem pracy IOD są kontakty z osobami, których dane dotyczą. Osoby te mogą zwracać się z wszelkimi pytaniami oraz żądaniami dotyczącymi ich praw, np. żądaniem usunięcia danych, prawem dostępu do danych, prawem do sprostowania danych.
- **Zapewnienie rozliczalności m.in. poprzez prowadzenie dokumentacji przetwarzania danych osobowych.** Podstawowymi dokumentami dotyczącymi przetwarzania danych osobowych są m.in. rejestr czynności przetwarzania, rejestr naruszeń, DPIA (ocena skutków), umowy powierzenia, ewidencja zgód. Są to podstawowe narzędzia pracy IOD, które przede wszystkim pozwalają na pozyskiwanie wiedzy na temat procesów przetwarzania danych w organizacji i ich prawidłowe monitorowanie.

Należy pamiętać, że nie w każdym przypadku wyznaczenie IOD jest obowiązkowe. Przepisy regulujące tę kwestię to art. 37 RODO. Jako ciekawostka – CNIL zaprezentował statystykę dotyczącą wykształcenia osób zajmujących stanowisko IOD:

- 28% posiada wykształcenie IT;
- 28% wykształcenie prawnicze;
- w pozostałej części to osoby o profilu administracyjnym, finansowym, compliance, audytowym.

» IOD jest punktem kontaktowym pomiędzy organizacją, a organem nadzorczym. «

KAMSOFT S.A.

Zarządzaj

kompleksowo swoją placówką medyczną

Wsparcie
w realizacji opieki
koordynowanej

Wybierz oprogramowanie dla medycyny od KAMSOFT i zyskaj:

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

medycyna@kamsoft.pl | tel. (+48) 32 209 07 05

kamsoft.pl

Kary pieniężne za naruszenie RODO. Czy można oszacować ich wysokość?

Kary nakładane przez UODO mogą być dotkliwe: 100 000 zł za ujawnienie danych o recepcie przez byłego ministra zdrowia, 10 000 zł za niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych przez Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego. Od czego zależy ich wysokość i jak ich uniknąć?

Co o karach mówi RODO?

W przypadku stwierdzenia naruszeń przepisów o ochronie danych osobowych, Prezes Urzędu Ochrony Danych Osobowych jest uprawniony do nakładania kar pieniężnych. RODO, w zależności od tego, który przepis prawa został naruszony, przewiduje co do zasady dwa progi w zakresie wysokości kar administracyjnych:

- do 10 mln EUR, a w przypadku przedsiębiorstwa, w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa;
- do 20 mln EUR, a w przypadku przedsiębiorstwa, w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

W Polsce obowiązują dodatkowe progi. W zakresie jednostek sektora finansów publicznych górny próg to 100 000 złotych kary, a w zakresie państwowych i samorządowych instytucji kultury – do 10 000 zł. Kara nałożona przez UODO na byłego ministra zdrowia Adama Niedzielskiego była więc maksymalną ze względu na rodzaj ukaranego podmiotu (w tym przypadku nie prywatnie minister, ale Ministerstwo Zdrowia).

Jak ustalana jest wysokość kary?

RODO wskazuje, iż nakładane kary powinny być skuteczne, proporcjonalne i odstraszające, a ustalając ich wysokość w każdym indywidualnym przypadku należy zwrócić uwagę na kilkanaście szczegółowo opisanych kryteriów.

Proces dochodzenia do konkretnej kwoty jest dosyć skomplikowany. Konkretnych wskazówek dostarczyć mogą wybrane Wytyczne Grupy Roboczej Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych. Jakie kryteria oceny organ weźmie pod uwagę?

Charakter, waga i czas trwania naruszenia. Wyszczególnione dwa progi wysokości kar wskazują, iż istnieje różnicowanie

stopnia istotności naruszenia. Co więcej, motyw 148 RODO wprowadza pojęcie tzw. „niewielkich naruszeń", które nie stanowią poważnego zagrożenia dla praw osób, których dane dotyczą. Za tego typu naruszenie, zgodnie z Wytycznymi, karę pieniężną można zastąpić upomnieniem. Zastąpienie kary pieniężnej upomnieniem jest także możliwe w przypadku, gdy administratorem danych jest osoba fizyczna, a grożąca kara pieniężna stanowiłaby dla niej nieproporcjonalne obciążenie. Organ oceni również czas trwania naruszenia, co bez wątpienia będzie miało wpływ na wysokość nałożonej kary.

Kategorie danych osobowych, których dotyczyło naruszenie. Jest to bardzo istotne kryterium. W tym zakresie organ ustali, czy naruszenie dotyczy przetwarzania szczególnych kategorii danych, czy na podstawie tych danych jest możliwa bezpośrednia identyfikacja osoby, np. czy dane są zaszyfrowane oraz czy naruszenie może spowodować negatywny skutek dla osoby, której dane dotyczą.

Wdrożone przez podmiot zabezpieczenia. Każda osoba zajmująca się bezpieczeństwem wie, że niełatwo jest zapewnić w sposób ciągły najwyższy poziom zabezpieczeń. Szczególnie, że naruszenia mogą wynikać z nieumyślnego błędu człowieka lub mogą być celowym działaniem grup cyberprzestępczych. Dlatego są sytuacje, w których trudno uniknąć incydentów bezpieczeństwa danych, pomimo zastosowania wielu środków ostrożności. Z tego względu, organ dokonując oceny będzie brał pod uwagę m.in. jakie narzędzia techniczne i procedury organizacyjne wdrożył podmiot w celu zabezpieczenia danych, czy wdrożone rozwiązania są zgodne z zasadą uwzględniania ochrony danych w fazie projektowania lub z zasadą domyślnej ochrony danych, czy w jego organizacji są znane i stosowane właściwe procedury ochrony danych itd. Innymi słowy, zgodnie z Wytycznymi, organ nadzorczy musi ocenić, w jakim stopniu podmiot wdrożył zabezpieczenia, których można było oczekiwać w zakresie systemu zabezpieczeń.

» Za nieumyślne naruszenie można uznać np. omyłkowe otwarcie załącznika łudząco podobnego do prawidłowego, a zawierającego złośliwe oprogramowane. «

Nieumyślny lub umyślny charakter naruszenia. Zgodnie z Wytycznymi, za umyślne naruszenie uznamy niezgodne

z prawem przetwarzanie danych, np. działanie niezgodne z RODO, a świadomie zatwierdzone przez najwyższe kierownictwo. Za nieumyślne naruszenie można uznać np. omyłkowe otwarcie załącznika łudząco podobnego do prawidłowego, a zawierającego złośliwe oprogramowane. Mimo szkoleń w zakresie phishingu, takie przypadki mają miejsce, gdyż atakujący wciąż doskonaloną techniki ataków cybernetycznych. Oczywistym jest to, że celowe naruszenie przepisów będzie wiązało się z zaostrzeniem odpowiedzialności.

Działania podjęte w celu zminimalizowania negatywnych skutków naruszenia. Wobec administratorów, którzy sami zgłosili naruszenie, a następnie podjęli działania zmierzające do ograniczenia negatywnych skutków naruszenia, możemy spodziewać się łagodniejszego podejścia ze strony organu. Dlatego tak ważne jest wykazanie się sumiennością i aktywną postawą po stwierdzeniu naruszenia.

Wcześniejsze istotne naruszenia. Organ musi ocenić, jak wyglądała dotychczasowa działalność podmiotu, u którego stwierdzono naruszenie m.in. czy stwierdzono wcześniej takie samo naruszenie i czy dopuszczono się go w ten sam sposób. Okoliczności te mogą istotnie wpłynąć na ostateczną wysokość nałożonej kary.

Stosowanie zatwierdzonych kodeksów postępowania. Zgodnie z Wytycznymi, w przypadku, gdy podmiot zastosował się do zatwierdzonego kodeksu postępowania, organ nadzorczy może ocenić, że wdrożył on odpowiednie zabezpieczenia i jest zaangażowany w ochronę danych osobowych, które przetwarza. To kolejny argument za stosowaniem kodeksów, które zostały opracowane dla ochrony zdrowia.

» Placówka zdrowia stosująca Kodeks postępowania RODO dla sektora ochrony zdrowia ma większe szanse uniknąć kary UODO. «

Podsumowanie

Organ nadzorczy weźmie pod uwagę wszystkie wymienione wyżej okoliczności mogące mieć znaczenie dla sprawy. Wysokość kary za naruszenie przepisów RODO jest zawsze wyliczana po bardzo szczegółowej analizie stanu faktycznego w każdym indywidualnym przypadku. Warto pamiętać, że proaktywna postawa podmiotu, u którego miało miejsce

naruszenie danych, zwykle oceniana jest z korzyścią dla samego podmiotu i może pozytywnie wpływać na ostateczną wysokość kary.

Dlatego nawet w przypadku naruszeń, w których wina ewidentnie leży po stronie podmiotu, zawsze należy współpracować z organem nadzorczym m.in. poprzez zgłoszenie naruszenia zgodnie z wymaganiami określonymi w art. 33 RODO oraz w zakresie pomocy w ustaleniu stanu faktycznego sprawy i prawidłowym jej rozstrzygnięciu.

Elementy brane pod uwagę przez UODO przy określaniu wysokości kar i grzywien nakładanych za naruszenie danych osobowych. Każde dodatkowe zabezpieczenie zwiększa szansę na to, że sprawa zakończy się upomnieniem, a nie karą pieniężną

20 zaleceń ochrony danych medycznych z USA

Amerykański Departament Zdrowia i Usług Społecznych (The U.S. Department of Health & Human Services, DHHS) przygotował listę 20 wskazówek dotyczących bezpieczeństwa informacji, które mają pomóc szpitalom lepiej chronić wrażliwe dane pacjentów.

Zagrożenia cyberbezpieczeństwa są takie same na całym świecie, bo dla hakerów granice nie istnieją. Wirusy i złośliwe oprogramowanie ransomware mogą wniknąć do każdego systemu IT i komputera; wielu ataków nie jesteśmy świadomi, bo są udaremniane przez systemy antywirusowe lub wtedy, gdy zdecydujemy się usunąć podejrzany e-mail.

» Aktualne informacje o ochronie danych publikujemy na blog.osoz.pl w zakładce „Cyberbezpieczeństwo”. «

Zalecenia DHHS – choć opracowane w USA – są uniwersalne i mogą znaleźć zastosowanie we wszystkich organizacjach opieki zdrowotnej. Uświadamiają przy okazji, że skuteczna polityka bezpieczeństwa opiera się na przewidywaniu potencjalnych zagrożeń, znajomości sposobów działania hakerów i aktywnej profilaktyce cyberzagrożeń.

Cyberprzestępcy stosują coraz to nowsze metody socjotechniczne, aby wykraść dane. Ich celem jest najczęściej wyłudzenie okupu albo kompromitacja placówki. Czasami dane od razu trafiają do darknetu i to bez ostrzeżenia. Niezależnie od motywu, placówki ochrony zdrowia nie są bezbronne i mogą zbudować odporny system zabezpieczeń i reagowania na kryzysy bezpieczeństwa danych.

1. Stwórz kulturę bezpieczeństwa

Żadna polityka bezpieczeństwa nie będzie skuteczna, jeśli pracownicy nie będą znali i przestrzegali najlepszych praktyk ochrony danych. Kierownictwo musi dawać dobry przykład i prowadzić szkolenia pracowników. Tak samo ważna jest zaufana kultura pracy – tylko od tego zależy, czy w przypadku błędu prowadzącego do wycieku danych, pracownicy poinformują o tym kierownictwo i w ten sposób można będzie szybko zareagować.

2. Chroń szczególnie urządzenia mobilne

Coraz częściej elektroniczna dokumentacja medyczna (EDM) jest gromadzona z pomocą urządzeń przenośnych, jak tablety czy smartfony. Warto pamiętać, że są one bardziej narażone na kradzież i nieautoryzowany dostęp niż urządzenia stacjonarne.

3. Utrzymuj wysoką higienę cybernetyczną

Ustal twarde zasady polityki bezpieczeństwa i pilnuj, aby były przestrzegane. Nie zapomnij o takich często pomijanych szczegółach jak zmiana domyślnych haseł w komputerach i systemach albo dokładne czyszczenie danych z utylizowanych urządzeń.

4. Skonfiguruj zapory sieciowe

Polegaj na przeszkolonym personelu w zakresie konfiguracji zapór sieciowych, aby chronić systemy szpitalne przed atakami z zewnątrz. Zapory mogą być oparte na sprzęcie lub oprogramowaniu w zależności od wielkości systemu szpitalnego. Unikaj zatrudniania ekspertów bezpieczeństwa na pół etatu lub korzystania z usług osób o niezweryfikowanych kwalifikacjach.

5. Zainstaluj i konserwuj oprogramowanie antywirusowe

Dobre oprogramowanie antywirusowe to podstawa w każdym podmiocie leczniczym. Musi ono być automatycznie aktualizowane, bo hakerzy często próbują wykorzystać istniejące luki bezpieczeństwa, które na bieżąco są łatane przez dostawców antywirusów.

6. Wykonuj kopie zapasowe danych

Regularne tworzenie kopii zapasowych danych i bezpieczne przechowywanie tych kopii jest kluczem do odzyskania sprawności po ataku hakerów. Zaleca się minimum dwie kopie przechowywane w różnych lokalizacjach, np. w chmurze danych i na zewnętrznym nośniku danych niepodłączonym do sieci komputerowej.

7. Kontroluj dostęp do chronionych informacji zdrowotnych

Przemyśl dokładnie, kto potrzebuje dostępu do dokumentacji pacjenta, ustal poziomy uprawnień dla poszczególnych grup pracowników. Stosuj audyty, aby na bieżąco kontrolować stan dostępu do danych. Nie zapomnij o usuwaniu uprawnień pracowników, którzy zakończyli pracę.

8. Używaj silnych haseł i zmieniaj je regularnie

Stosuj najlepsze praktyki bezpiecznych haseł, takie jak:

– Do każdego systemu używaj innego hasła;

– Regularnie zmieniaj hasła;

– Używaj skomplikowanych haseł, które nie są łatwe do odgadnięcia (litery, cyfry, znaki specjalne oraz odpowiednia długość);
– Używaj uwierzytelniania wieloskładnikowego, zawsze gdy to możliwe;
– Wprowadź możliwość łatwego resetowania haseł, gdy pracownik go nie pamięta. W ten sposób zapobiegasz zapisywaniu haseł na kartkach naklejanych na komputer czy zostawianych w szufladach.

9. Ogranicz dostęp do sieci

Sieci bezprzewodowe mogą być łatwe do skonfigurowania, ale są podatne na nieautoryzowany dostęp, jeśli nie używa się w nich szyfrowania. Najlepiej skonfiguruj wirtualną sieć prywatną, czyli VPN.

10. Kontroluj dostęp fizyczny do danych

Wraz z postępującą cyfryzacją, większość incydentów bezpieczeństwa dotyczy danych w formie elektronicznej. Ale to nie oznacza, że można zignorować zagrożenia fizyczne. Przenośne urządzenia powinny być przechowywane w bezpiecznych miejscach, do których mają dostęp tylko uprawnione osoby. Polityka bezpieczeństwa powinna ograniczać ich użycie poza placówkami. Dostęp do pomieszczeń placówek należy tak zorganizować, aby mogli się po nich poruszać tylko pracownicy. Przy każdym odejściu od stacji roboczej, należy wylogować się z systemu.

11. Prowadź regularne szkolenia personelu

Pracownicy są najsłabszym ogniwem w systemie bezpieczeństwie informacji. Dlatego muszą oni znać i rozumieć aktualnie stosowane protokoły bezpieczeństwa oraz być świadomi konsekwencji ich nieprzestrzegania.

Oceń poziom wiedzy swoich pracowników i opracuj programy szkoleniowe, które wypełnią zidentyfikowane luki.

12. Realizuj kontrole wykorzystania danych

Wykorzystaj narzędzia do wykrywania i klasyfikacji danych, aby zidentyfikować wrażliwe dane dotyczące zdrowia, monitorować dostęp do nich i chronić je. Tego typu systemy kontroli wykorzystania danych mogą np. uniemożliwić pracownikom wysyłanie danych wrażliwych pocztą elektroniczną, umieszczanie na nieautoryzowanych stronach lub kopiowanie na urządzeniach pamięci masowej.

13. Monitoruj dostęp do danych

Śledzenie, którzy użytkownicy mają dostęp do danych i zasobów opieki zdrowotnej, pomaga zidentyfikować wrażliwe punkty systemu informacji i wdrożyć działania ochronne. Monitorowanie umożliwia tworzenie ścieżek audytu, dzięki czemu łatwiej jest wykryć nieautoryzowane punkty dostępu.

14. Szyfruj dane

Szyfruj dane, aby utrudnić – a najlepiej uniemożliwić – hakerom odczytanie danych nawet w przypadku udanego naruszenia. Określ, jakie dane mają być szyfrowane i jakimi metodami. W przypadku korzystania z rozwiązań chmurowych, szyfrowanie danych powinien zagwarantować dostawca rozwiązania. Ponieważ dane medyczne są danymi wrażliwymi, moc kryptograficzna powinna być na bardzo wysokim poziomie.

15. Minimalizuj ryzyko związane z urządzeniami podłączonymi do sieci

Urządzenia służące do gromadzenia EDM to nie jedyny podatny na cyberzagrożenia element sieci szpitalnych. Nie można zapomnieć o urządzeniach medycznych, kamerach bezpieczeństwa i sprzęcie biurowym włączonych w sieć. Oferują one punkty dostępu, które ostatecznie mogą prowadzić do danych pacjentów. Utrzymuj tego typu urządzenia w oddzielnych sieciach i monitoruj je pod kątem nieautoryzowanego dostępu.

» Symulowane ataki hakerów pozwalają przetestować wiedzę pracowników i wdrożone procedury. «

16. Przeprowadzaj regularne oceny ryzyka

Oceny ryzyka pomogą zrozumieć podatności organizacji na zagrożenia. Tylko wtedy można przewidzieć problemy z bezpieczeństwem i odpowiednio zabezpieczyć systemy szpitalne. Przykładem jest symulacja ataków hakerów (np. wysyłka maili z podejrzanymi załącznikami) albo kontrolowana blokada komputerów z wyświetleniem informacji o wirusie.

17. Oceniaj bezpieczeństwo partnerów biznesowych

Opieka zdrowotna opiera się na dzieleniu się informacjami. Upewnij się, że systemy szpitalne są chronione przed nieautoryzowanym dostępem w przypadku wymiany danych z partnerami biznesowymi. Tego zresztą wymaga RODO.

18. Aktualizuj oprogramowanie systemowe, części białej i szarej

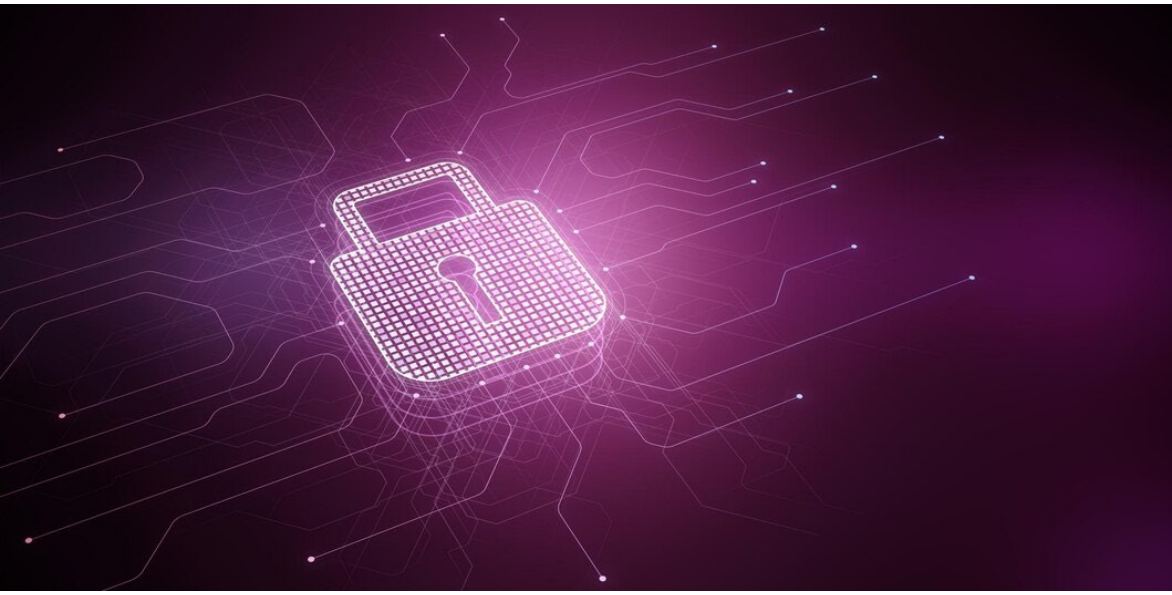
Przestarzałe oprogramowanie jest bardziej podatne na ataki. Przykładowo, hakerzy często atakują starsze wersje systemów, które nie mają najnowszych łatek bezpieczeństwa. Dotyczy to przede wszystkim systemu operacyjnego, ale również systemów szpitalnych, zarówno w części administracyjnej (np. terminarze wizyt), jak i klinicznej (EDM).

19. Stwórz plan odzyskiwania danych

Atak cybernetyczny jest tylko kwestią czasu. Pytanie brzmi nie „czy", ale „kiedy" do niego dojdzie. System bezpieczeństwa powinien mieć strukturę warstwową – nawet jeśli jedna z nich zawiedzie, potencjalny atak może zostać powstrzymany na kolejnym poziomie. Jednak nawet przy najwyższej staranności, czasami hakerom udaje się zyskać dostęp do danych. Wówczas ratunkiem są kopie bezpieczeństwa i plan przywracania systemów szpitala do normalnego funkcjonowania oraz ochrona przed kolejnym atakiem. Nieprzygotowanym placówkom grozi m.in. paraliż pracy i konieczność odwołania wizyt.

20. Ustal zasady zdalnego dostępu do informacji

W ochronie zdrowia praca zdalna jest rzadkością, ale nie wyjątkiem. To może być lekarz sprawdzający po godzinach pracy dane pacjenta lub pracownik uzupełniający informacje rozliczeniowe. Dostęp do danych poza kontrolowanym środowiskiem placówki medycznej wiąże się zawsze z dużym ryzykiem. Polityka bezpieczeństwa musi określać, kto może mieć wgląd do danych z urządzeń zewnętrznych oraz w jakich sytuacjach. Tego typu urządzenia muszą spełniać określone warunki, np. mieć odpowiednie zabezpieczenia.



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 jest w czołówce najczęściej atakowanych przez hakerów branż. Z najnowszych danych wynika, że w I kwartale 2023 liczba incydentów bezpieczeństwa wzrosła w stosunku do 2022 roku o 22%. Hakerzy obrali sobie za cel

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

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 rygorem 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.

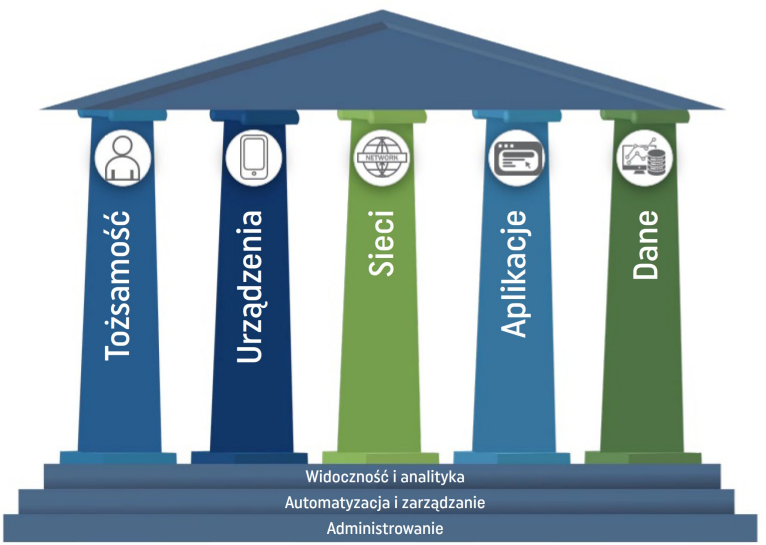
Wdrożenie filozofii „zero trust" nie jest łatwe i może trwać kilka lat, wymagając opracowania bardzo szczegółowych i dynamicznych procedur oraz wdrożenia kosztownym rozwiązań technicznych – wiąże się z większymi kosztami cyberbezpieczeństwa, bo konieczne staje się zatrudnienie specjalistów ochrony danych 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 cząstkowej 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

KAMSOFT S.A.

Zwiększ **bezpieczeństwo** danych w swojej **aptece**

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

- ✓ **Zminimalizuj** ryzyko utraty danych
- ✓ **Zapewnij** ciągłość działania apteki
- ✓ **Odzyskuj** dane po awarii bez straty

ks-omnipharm_one@kamsoft.pl | tel. (+48) 32 209 07 05

Zobacz prezentację

Ekspert CSIRT CeZ: Cyberbezpieczeństwo to system naczyń połączonych

W jaki sposób najczęściej dochodzi do wycieku danych? Co zrobić, gdy hakerzy zaatakują placówkę medyczną? Gdzie się szkolić i szukać wsparcia finansowego na inwestycje w cyberbezpieczeństwo? Na nasze pytania odpowiada Jeremi Olechnowicz, kierownik wydziału CSIRT w Centrum e-Zdrowia.

Jaka jest skala incydentów bezpieczeństwa danych w ochronie zdrowia w Polsce według danych, którymi dysponuje CeZ?

Bazując na analizach przeprowadzonych przez Centrum e-Zdrowia oraz dostępnych publicznie raportach branżowych – np. CERT PL – widzimy, że liczba ataków ciągle rośnie.

W roku 2023 miało miejsce ponad dwa razy więcej różnych incydentów niż rok wcześniej. Zakładam, że w tym roku tendencja wzrostowa się utrzyma. Tylko w styczniu Centrum e-Zdrowia zarejestrowało ponad 40 różnych incydentów w sektorze ochrony zdrowia, od prób phishingu, przez wycieki poświadczeń, aż po próby ataków na infrastrukturę podmiotów.

W jaki sposób najczęściej dochodzi do wycieku danych medycznych?

Do udanego ataku prowadzi wiele różnych czynników, które zwykle muszą wystąpić razem. Rzadko jest tak, żeby udany atak był efektem pojedynczej słabości, choć to też jest możliwe.

Najczęściej obserwowane przez nas słabości, które wykorzystują hakerzy to:

- podatności i luki w systemach i urządzeniach,
- zbyt szeroko przyznane zdalne dostępy do organizacji,
- nadużycia i nadmiarowe uprawnienia kont użytkowników, np. kont administratorów domeny lub stacji roboczej,
- błędy w konfiguracji w infrastruktury,
- brak mechanizmów uwierzytelnienia dwuskładnikowego,
- ekspozycja zasobów organizacji do sieci publicznej,
- nieaktualne i podatne wersje elementów stron internetowych np.: CMS, wtyczki.

Przykładowo, atakujący wykorzystuje jedną z popularnych podatności na publicznie dostępną usługę, np. portal

logowania do VPNa. Następnie uzyskuje dostęp do jednego z serwerów na peryferiach sieci, gdzie wykonuje tzw. eskalację uprawnień. Atakujący ma już podwyższone uprawnienia, które pozwalają na wykonanie wielu niebezpiecznych czynności. Może na przykład dalej przeczesywać sieć wewnętrzną organizacji. Finalnie atakujący uzyskuje dostęp np. do serwera plików lub baz systemów dokumentacji medycznej, które wykrada.

Media informują zazwyczaj tylko o dużych atakach hakerów. Czy małe, indywidualne praktyki lekarskie też mają się czego obawiać?

To, w jakim stopniu dany podmiot jest narażony na ryzyko, zależy m.in. od jego wielkości oraz od tego, jak oceniają je grupy atakujące. Duże, znane jednostki, o krytycznym znaczeniu dla systemu ochrony zdrowia, są oczywiście bardziej narażone na ataki, niż mniejsze placówki. Takie jednostki mogą paść ofiarą zarówno grup hakerskich nastawionych na zyski finansowe, jak i tzw. national state actors, czyli grup hakerów wspieranych przez obce rządy. Ich działania będą ukierunkowane na destabilizację ciągłości świadczenia usług, zniszczenia zasobów, manipulację danymi, czy też kradzież danych.

Nie oznacza to jednak, że mikro i małe podmioty nie są narażone na ataki. W takich placówkach względnie łatwo można ukraść login i hasło pojedynczym specjalistom np. poprzez masowe kampanie phishingowe oraz strony internetowe dystrybuujące złośliwy kod. Choć procentowa skuteczność takich kampanii jest śladowa to nakład pracy jest na tyle niski, że ta technika jest często stosowana.

Jakie są w takim razie minimalne zabezpieczenia techniczne i organizacyjne, które powinny być stosowane przez każdy podmiot leczniczy bez wyjątku?

Po pierwsze cyberbezpieczeństwo to system naczyń połączonych. Słabości lub braki pojedynczych elementów wpłyną na

odporność całego systemu. Po drugie, cyberbezpieczeństwo to nie stan zero-jedynkowy. To proces ciągły wymagający weryfikacji i doskonalenia. Po trzecie, cyberbezpieczeństwo to nie kwestia zakupu kilku systemów lub urządzeń o dziwnych skrótach np. FW, AV, SMG, NAC, PAM czy DAM. Aby osiągnąć cel, jakim jest ochrona informacji przetwarzanych w organizacji, należy zaplanować kompleksową architekturę cyberbezpieczeństwa składającą się z elementów takich jak rozwiązania techniczne, organizacyjne, formalne, a także kompetencje specjalistów z różnych dziedzin. Na koniec elementy te należy połączyć w jeden sprawnie działający system.

Często pomijany jest fakt, że pierwszym ważnym krokiem jest świadomość o zagrożeniach oraz ich konsekwencjach. A więc znajomość aspektów Security Awareness wśród pracowników organizacji, w szczególności kierownictwa, na którym spoczywa obowiązek zapewnienia bezpieczeństwa przetwarzanych informacji.

Trudno jest jednoznacznie wybrać pojedyncze elementy, które powinny być stosowane bez wyjątku. Jest ich po prostu wiele, a cel można osiągnąć różnymi sposobami.

Niezmiennie najsłabszym ogniwem w łańcuchu cyberbezpieczeństwa jest człowiek. Dlatego to właśnie działania, które mają na celu zniwelowanie błędów i słabości ludzi są niezwykle istotne. Zaimplementowanie zasad cyberhigieny znacznie podnosi odporność organizacji na zagrożenia z cyberprzestrzeni, a inwestycja w kompetencje wsparcia IT na pewno się opłaci. Więcej szczegółów na temat architektury bezpieczeństwa poruszamy w opublikowanych na stronie ezdrowie.gov.pl rekomendacjach.

» Wiele ataków dokonywanych jest przy wykorzystaniu jednej lub kilku znanych podatności. «

Oprócz cyberhigieny, co jeszcze można zrobić, aby wzmocnić ochronę danych bez ponoszenia dużych nakładów?

Po pierwsze można skorzystać z wielu rozwiązań opensource. Takie rozwiązanie będzie tańsze, jednak wymaga więcej czasu na implementację i wysokich kompetencji osób je wdrażających oraz integrujących. Systemy takie można zainstalować

na bezpłatnych dystrybucjach systemów operacyjnych z rodziny Linux. Środowisko dla takich rozwiązań także można utworzyć z pomocą usług o otwartym kodzie.

Ważnym aspektem architektury bezpieczeństwa jest nie samo wdrożenie rozwiązania technicznego, ale jego prawidłowa konfiguracja oraz integracja z innymi narzędziami. Czyli implementacja różnych dobrych praktyk, także na rozwiązaniach opensource, może skutecznie zmniejszyć powierzchnię ataku. Dla przykładu błędnie wdrożony system klasy Firewall na brzegu infrastruktury nie zapewni bezpieczeństwa nawet jak będzie bardzo drogi, a wszystkie podatności zostaną załatane.

Wiele ataków dokonywanych jest przy wykorzystaniu jednej lub kilku znanych podatności. Monitorowanie doniesień o nowych podatnościach oraz wdrożenie skutecznego procesu szybkiego ich usuwania również zmniejsza ryzyko skutecznego ataku.

Ważne części architektury bezpieczeństwa organizacji to wewnętrzne polityki bezpieczeństwa teleinformatycznego, a w idealnych warunkach cały System Zarządzania Bezpieczeństwem Informacji (SZBI). Wdrożenie SZBI może nie być proste i tanie, ale można zaimplementować – dodatkowym nakładem pracy – okrojoną wersję takich polityk, procesów oraz procedur. Dostępnych jest wiele poradników, zaleceń oraz ostrzeżeń opracowywanych m.in. przez CSIRTy poziomu krajowego, np. CERT PL oraz przez sektorowy zespół cyberbezpieczeństwa CSIRT CEZ. Można wykorzystać te informacje w organizacji także w formie np. mailowych ostrzeżeń dla pracowników lub jako cykliczne przypomnienia dobrych praktyk z zakresu cyberhigieny.

To wymaga z kolei ciągłej aktualizacji wiedzy, bo hakerzy też doskonalą swoje strategie działania.

Atakujący będą zmieniali swoje metody wraz ze zmianami rozwiązań z zakresu zabezpieczeń. Cyberataki wciąż są bardzo

» Hakerzy zaczęli nie tylko szyfrować dane, ale też je wykradać. «

dochodowe, więc grupy hakerskie na pewno nie zaprzestaną swojego procederu. Po drugie, pozyskane środki wykorzystują na dalszy rozwój swoich zasobów oraz metod.

Ewoluująca technologia ma także wpływ na stosowane przez atakujących metody. Jedną z charakterystycznych zmian w ostatnich latach jest modyfikacja modelu biznesowego ataków ransomware. Kiedyś po prostu żądano okupu za odszyfrowanie. Rynek odpowiedział na to szerszym i skuteczniejszym wdrożeniem systemów kopii zapasowych. Hakerzy zaczęli więc nie tylko szyfrować dane, ale też je wykradać. Teraz żądają okupu za odszyfrowanie i niepublikowanie wykradzionych danych. Jest to tzw. Double Extortion. Metody te są rozwijane w celu wywarcia dodatkowej presji na atakowaną organizację czyli np. Triple lub Quadruple Extortion.

Oczywiście to tylko ułamek zmian, które zachodzą w metodach stosowanych przez hakerów. Ciekawa przyszłość czeka nas w kontekście wykorzystania AI w cyberbezpieczeństwie. Nie tylko rozwiązania bezpieczeństwa będą implementować AI. Hakerzy też się dostosowują i zaczynają korzystać ze wsparcia sztucznej inteligencji.

Co robić, gdy już doszło do ataku cybernetycznego w placówce medycznej?

Gdy już dojdzie do ataku, kluczowe jest jego rozpoznanie i podjęcie działań, które mogą zminimalizować/zniwelować skutki ataku. Na przykład, jeśli zauważymy masowe wyłączanie serwerów w sieci, warto rozpocząć izolowanie całych segmentów sieci, tak żeby złośliwy kod nie miał możliwości się rozprzestrzenić. Na tym etapie nie jest zalecane natomiast fizyczne odłączanie urządzeń od zasilania. Zalecany jest natomiast pilny kontakt telefoniczny do zespołów CSIRT w celu uzyskania szybkiego wsparcia poprzez zdalną konsultację. Takim zespołem jest m.in. CERT PL ulokowany w NASK oraz sektorowy zespół cyberbezpieczeństwa w Centrum e-Zdrowia – CSIRT CEZ.

Należy pamiętać też o obowiązkach wynikających z Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Mowa o formalnym zgłoszeniu incydentu na dedykowanym formularzu. Formularz nie musi być w 100% wypełniony przy pierwszym zgłoszeniu. Zgłoszenie można zaktualizować w późniejszym czasie. Jeśli trwa incydent, zgłaszający może nie mieć kompletu informacji. Ważne jest natomiast jak najszybsze poinformowanie dedykowanych zespołów cyberbezpieczeństwa. W przypadku nieterminowego zgłoszenia podmiot może się narazić na kary finansowe.

Gdzie szukać programów wsparcia na inwestycje w bezpieczeństwo danych?

Centrum e-Zdrowia oraz Ministerstwo Zdrowia propagują informacje o różnych projektach wśród podmiotów wykonujących działalność leczniczą, w szczególności wśród szpitali.

Największy tego typu projekt to „CyberSzpitale". Jest on skierowany do szpitali w Polsce. Polega na refundacji inwestycji poniesionych przez tę grupę podmiotów na rzecz podniesienia poziomu cyberbezpieczeństwa. Pierwsza edycja zakończyła się w ubiegłym roku. Wkrótce, dzięki rządowemu wsparciu, ruszy kolejna edycja.

Poza wymienioną refundacją prowadzone są też różne przedsięwzięcia szkoleniowe. Jedno z nich to szkolenia Security Awareness realizowane przez NASK na rzecz podmiotów Podstawowej Opieki Zdrowotnej (POZ). Ministerstwo Cyfryzacji wraz z partnerami prowadzi teraz cykl szkoleń podnoszących kompetencje kadry IT w szpitalach. Szkolenia te już trwają. Na rok bieżący oraz kolejny przygotowywane są kolejne projekty szkoleniowe, o których Centrum e-Zdrowia oraz Ministerstwo Zdrowia będzie informować. Wśród nich znajdą się m.in. szkolenia Security Awareness dla kadry kierowniczej szpitali.

Jakie trzy bazowe inwestycje w bezpieczeństwo danych pozwalają znacznie poprawić ochronę danych w podmiotach medycznych?

Jak już wcześniej wspomniałem, architektura cyberbezpieczeństwa składa się z wielu elementów. Nie da się zbudować bezpiecznej infrastruktury bez zabezpieczeń technicznych: płatnych lub bezpłatnych. Każda organizacja ma już jakieś rozwiązania techniczne zaimplementowane – lepsze lub gorsze.

To, czego najczęściej brakuje, a znacząco podnosi odporność organizacji to:

- Szkolenia z Security Awareness dla całej kadry w organizacji wraz z cyklicznym przypomnieniem obowiązujących zasad bezpieczeństwa;
- Wieloskładnikowe logowanie MFA (multi factor authentication), które znacząco podniesie odporność kont na przejęcie dostępów;
- Prawidłowo zaimplementowany system kopii zapasowych z kopią offline, który – gdy zawiodą inne rozwiązania – pozwoli na odzyskanie ciągłości działania oraz utraconych danych.

csirt Centrum e-Zdrowia

CSIRT CeZ przyjmuje zgłoszenia o poważnych incydentach bezpieczeństwa danych oraz wspiera placówki medyczne w ich w obsłudze.

Kliknij tutaj, aby przejść do strony CSIRT CeZ

Jak wzmocnić cyberbezpieczeństwo w roku 2024/2025?

91% szpitali w Polsce „zgłasza zapotrzebowanie” w zakresie cyberbezpieczeństwa – wynika z badania Centrum e-Zdrowia. Za tym sformułowaniem kryją się duże niedociągnięcia infrastrukturalne, organizacyjne i bezradność, bo placówki zdrowia nie mają pieniędzy na zakup sprzętu czy zatrudnienie informatyków.

W szpitalach jest lepiej, POZ-ty dalej nieprzygotowane

Badanie CeZ przeprowadzone w 2023 roku sugeruje, że placówki skupiają się obecnie na poprawie odporności na cyberataki (25,8%), zwiększeniu ochrony danych osobowych (24,3%), poprawie ciągłości działania systemów informatycznych (16,9%) oraz szerzeniu wiedzy o zagrożeniach informatycznych wśród pracowników/kierownictwa jednostki (14%).

Niepokojąca jest jednak odpowiedź na pytanie o aktywne dbanie o bezpieczeństwo danych: tylko połowa ankietowanych placówek (51,5%) zadeklarowała, że już wcześniej (przed badaniem) podejmowała działania w zakresie cyberbezpieczeństwa. Z tego większość to szpitale (94%), a największe zaniedbania są w placówkach AOS i POZ. Badanie nie wskazuje powodów, ale można się jedynie domyślać, że jak zawsze chodzi o pieniądze oraz samą świadomość problemu.

W 70% przypadków, inwestycje w cyberbieczeństwo są finansowane ze środków własnych. Do własnych budżetów muszą sięgać najczęściej ambulatoryjne placówki medyczne, w przeciwieństwie do szpitali, gdzie aż 75% funduszy pochodzi ze wsparcia NFZ. Tylko w co 40-stej placówce udało się znaleźć pieniądze z funduszy UE lub ze środków publicznych, np. od podmiotów tworzących.

Jeśli pieniądze już są, to trafiają na monitorowanie bezpieczeństwa teleinformatycznego podmiotu (51,1% ankietowanych) i szkolenia dla pracowników z bezpieczeństwa informacji i cyberbezpieczeństwa (47,3%).

Można z dużą pewnością przyjąć, że rzeczywista ochrona danych jest na gorszym niż deklarowanym poziomie. Menedżerowie placówek medycznych powtarzają od lat, że nie mają pieniędzy na cyberbezpieczeństwo i nie stać ich na zatrudnienie deficytowych i drogich ekspertów, których i tak wchłaniają inne branże.

» Codziennie na świecie rejestruje się ok. 250 ataków hakerów na podmioty medyczne. «

Więcej ataków na małe, nieprzygotowane placówki

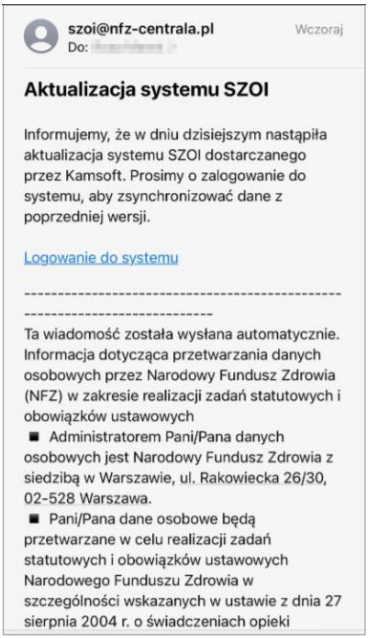
Tymczasem statystyki za rok 2023 pokazują, że nie słabnie intensywność ataków na placówki ochrony zdrowia. W Polsce

wystarczy wspomnieć o głośnej kradzieży danych w Laboratoriach ALAB. W 2021 roku polskie szpitale i przychodnie zgłosiły 13 ataków hakerów, a w 2022 roku było już ich 43. Faktyczna liczba jest kilkukrotnie większa, bo wiele podmiotów woli ukryć naruszenie bezpieczeństwa danych w obawie przed konsekwencjami.

Na całym świecie, codziennie rejestruje się ok. 250 ataków hakerów na podmioty medyczne. Według badania Check Point Research, w I półroczu 2023 r. liczba ataków na opiekę zdrowotną na świecie wzrosła o 18 proc. Z kolei według raportu IBM i Ponemon Institute z lipca 2023 r., naruszenia cyberbezpieczeństwa kosztowały organizacje opieki zdrowotnej średnio 10,1 miliona dolarów na incydent. W 2023 roku można zaobserwować zmianę taktyki hakerów. Ponieważ duże szpitale wzmocniły w ostatnich latach poziom bezpieczeństwa danych – co też wynika z ankiety CeZ – ofiarą coraz częściej padają mniejsze placówki.

Spooning, czyli maile prawie jak z NFZ

Sektor zdrowia musi się też przygotować na zwiększoną liczbę cyberataków przeprowadzanych z pomocą sztucznej inteligencji. Wśród nich są personalizowane wiadomości phishingowe wykorzystujące nieuwagę pracowników ochrony zdrowia, czy adaptacyjne złośliwe oprogramowanie wymagające nowych zabezpieczeń. Hakerzy sięgają do coraz bardziej wyrafinowanych technik socjo-technicznych, w czym pomaga im AI.



szoi@nfz-centrala.pl Wczoraj
Do:

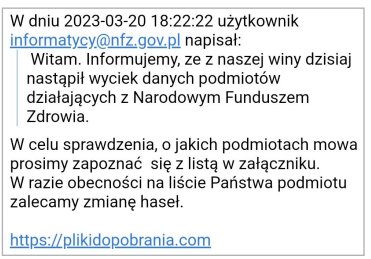
Aktualizacja systemu SZOI

Informujemy, że w dniu dzisiejszym nastąpiła aktualizacja systemu SZOI dostarczanego przez Kamsoft. Prosimy o zalogowanie do systemu, aby zsynchronizować dane z poprzedniej wersji.

Logowanie do systemu

Ta wiadomość została wysłana automatycznie. Informacja dotycząca przetwarzania danych osobowych przez Narodowy Fundusz Zdrowia (NFZ) w zakresie realizacji zadań statutowych i obowiązków ustawowych

- Administratorem Pani/Pana danych osobowych jest Narodowy Fundusz Zdrowia z siedzibą w Warszawie, ul. Rakowiecka 26/30, 02-528 Warszawa.
- Pani/Pana dane osobowe będą przetwarzane w celu realizacji zadań statutowych i obowiązków ustawowych Narodowego Funduszu Zdrowia w szczególności wskazanych w ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki



W dniu 2023-03-20 18:22:22 użytkownik informatycy@nfz.gov.pl napisał:

> Witam. Informujemy, ze z naszej winy dzisiaj nastąpił wyciek danych podmiotów działających z Narodowym Funduszem Zdrowia.

W celu sprawdzenia, o jakich podmiotach mowa prosimy zapoznać się z listą w załączniku.
W razie obecności na liście Państwa podmiotu zalecamy zmianę haseł.

https://plikidopobrania.com

W marcu 2023 roku hakerzy wysłali fałszywe wiadomości do placówek medycznych, podszywając się pod Narodowy Fundusz Zdrowia. Zawierały one link, którego kliknięcie powodowało zainstalowanie złośliwego oprogramowania. Tego typu atak, nazywany spoofingiem, polega na podszywaniu się pod zaufaną osobę lub podmiot

A to oznacza jedno: nawet te placówki, które mają już politykę bezpieczeństwa informacyjnego, muszą ją zaktualizować m.in. o element **aktywnego przewidywania i zapobiegania nowym rodzajom ryzyka cybernetycznego**. Drugi ważny element strategii 2024/2025 to **wzmocnienie zarządzania ryzykiem stron trzecich**. Każda umowa outsourcingowa, która wymaga wymiany/powierzenia danych, powinna być solidnie przygotowana pod względem cyberbezpieczeństwa. Oprócz wstępnej oceny, należy zaplanować systematyczne przeglądy poziomu bezpieczeństwa. Tak samo ważne są regularne szkolenia pracowników informujące o potencjalnych zagrożeniach związanych z interakcjami z podmiotami zewnętrznymi.

Pracownicy powinni być na bieżąco z nowymi taktykami ataków. Przykładem jest np. **spoofing e-mail albo telefoniczny**, gdy oszust podszywa się pod podmiot lub osobę. Największy atak tego rodzaju miał miejsce w marcu 2023 roku. Placówki medyczne otrzymały wówczas maila wyglądającego jak informacja z NFZ, o tytule „Nowe oprogramowanie SZOI" albo „Aktualizacja systemu SZOI". Wiadomości zostały wysłane z adresów bardzo podobnych do oficjalnych, np. informatycy@szoi-nfz.pl albo szoi@nfz-centrala.pl. Na pierwszy rzut oka mail trudno było odróżnić od prawdziwych komunikatów rozsyłanych przez NFZ. Pracownicy muszą wiedzieć, jak weryfikować maile, prośby o poufne informacje albo wezwania do zalogowania się do platform IT. W 2023 roku to właśnie phishing był najczęstszą przyczyną wycieku danych.

Nie można też zapominać o klasycznych zabezpieczeniach jak silne i regularnie zmieniane hasła, wykonywanie w czasie rzeczywistym kopii bezpieczeństwa, aktualizacja oprogramowania, zarządzanie dostępem do danych przez pracowników oraz minimalizacja zagrożeń wewnętrznych.

Wraz z tym jak szpitale stają się smart, integrując ze sobą urządzenia w ramach jednej infrastruktury IT, uwagi wymagają **zagrożenia w ramach tzw. internetu rzeczy**.

Co każdy lekarz może zrobić, aby lepiej chronić dane pacjentów?

Choć w media informują wyłącznie o atakach hakerów na duże szpitale i przychodnie, ofiarami cyberprzestępców padają też indywidualne praktyki lekarskie i małe podmioty. Jak samemu zadbać o dane pacjentów, gdy nie można liczyć na pomoc informatyka albo działu IT?

Małe praktyki ignorują zagrożenia, a hakerzy to wykorzystują

Według ostatnich danych, ponad 130 tys. lekarzy w Polsce wykonuje pracę w ramach indywidualnych praktyk lekarskich. Nie mają oni często ani zaplecza IT dbającego o bez-

pieczeństwo danych i systemów ochrony cybernetycznej, ani czasu na to, aby zajmować się informatyką. Często korzystają z tego samego komputera do prowadzenia kartotek pacjentów i czytania prywatnych maili, nie mają dużych budżetów na bezpieczeństwo danych.

Wielu lekarzy wychodzi z błędnego założenia, że hakerzy i tak nie interesują się małymi praktykami, bo duży okup można wyłudzić tylko od dużych podmiotów. Do tego chcą skupiać się na przyjmowaniu pacjentów, a nie na informatyce. Wiedzą o tym dobrze hakerzy – według raportu Critical Insight „2022 Healthcare Data Breach Report", liczba ataków cybernetycznych na małe placówki zdrowia systematycznie rośnie. W 2022 roku jedna trzecia z nich dotyczyła szpitali, a 12% – małych praktyk lekarskich. W 2019 roku było to zaledwie 2%. Skąd aż 6-krotny wzrost?

Duże placówki nadrabiają zaległości w cyberbezpieczeństwie i hakerom coraz trudniej przełamać bariery bezpieczeństwa. Ale nadal łatwą ofiarą są małe jednostki nieposiadające nawet podstawowych zabezpieczeń, ale gromadzące cenne dane medyczne pacjentów. Jeśli przyczyną ataku był masowo wysyłany phishing (hakerzy wysyłają codziennie 3,4 mld maili z phishingiem), lekarze są skłonni dużo częściej zapłacić okup, aby szybko pozbyć się problemu i ewentualnych konsekwencji.

Ochrona wbudowana w rutynową pracę

Czy można znaleźć kompromis pomiędzy wysokim poziomem bezpieczeństwa a minimalnym nakładem czasu? Tak, ale wymaga to takiego przygotowania, aby bezpieczeństwo było wbudowane domyślnie w procedury codziennej pracy. Warto poświęcić kilka dni w roku na cyberbezpieczeństwo, aby potem nie spędzać tygodni na usuwaniu skutków potencjalnego ataku i mierzyć się z konsekwencjami wizerunkowymi, prawnymi i finansowymi. Oto co radzą eksperci cyberbezpieczeństwa.

Oddziel dane prywatne od służbowych. Pierwsza i podstawowa zasada pozwalająca znacznie podwyższyć poziom cyberbezpieczeństwa to osobny komputer z zainstalowanym systemem gabinetowym. Bez dostępu do maili i możliwości przeglądania stron Internetowych. Jak wynika z analizy Deloitte, aż 91% wszystkich cyberataków zaczyna się od otwarcia wiadomości phishingowej, a według Europejskiej Agencji Cyberbezpieczeństwa, ataki z wykorzystaniem ransomare stanowią 54% wszystkich ataków hakerów na placówki ochrony zdrowia.

Archiwizuj dane. Nie od czasu do czasu na dysku zewnętrznym, ale w trybie ciągłym i najlepiej w chmurze danych. Zapytaj o takie rozwiązanie u dostawcy systemu gabinetowego. Koszt kilkuset złotych rocznie jest niewspółmiernie mały do posiadania bezpiecznej i aktualnej kopii zapasowej. Nawet jeśli twój komputer zostanie zablokowany przez złośliwe oprogramowanie, będziesz mógł szybko przywrócić wszystkie dane i oszczędzić sobie ogromnych kłopotów.

Szyfruj dane (VPN). Lekarze pracujący mobilnie czasami korzystają z sieci publicznych, a to wiąże się z dużym ryzykiem dla bezpieczeństwa danych. Aby go zminimalizować, szyfruj dane z pomocą wirtualnej sieci prywatnej (tzw. VPN). Ceny VPN-ów zaczynają się już od ok. 10–15 zł miesięcznie i to dobra inwestycja w bezpieczeństwo danych.

Przestudiuj kodeks RODO dla małych placówek medycznych. RODO może kojarzyć się z niejasnymi przepisami i dziwnymi wytycznymi. Jak praktycznie stosować zasady ochrony danych osobowych w placówkach ochrony zdrowia tłumaczy „Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych" opracowany przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie. Na 109 stronach znajdziesz najważniejsze wytyczne.

Silne hasła. Silne hasło to takie, którego nie jesteś w stanie zapamiętać, składające się z kombinacji znaków specjalnych, dużych i małych liter oraz cyfr (minimum 8). Dobre hasło

powinno chronić oprogramowanie gabinetowe, ale także sieć WiFi w miejscu wykonywania pracy. Hasło zmieniaj koniecznie przynajmniej raz w miesiącu. Nie trzymaj kartek z hasłem w portfelu albo przy komputerze. Możesz skorzystać z systemów zarządzania hasłami.

Nie oszczędzaj na oprogramowaniu. Ustaw automatyczną aktualizację systemu operacyjnego i nie zwlekaj z uruchomieniem update'u, jeśli komputer tego wymaga. Na bieżąco aktualizuj system gabinetowy. Zainstaluj i aktualizuj oprogramowanie antywirusowe. To samo dotyczy smartfonu, jeśli korzystasz na nim z mobilnych aplikacji gabinetowych np. do obsługi pacjentów czy gromadzenia danych w EDM.

Zastanów się, czy nie skorzystać z outsourcingu IT. Jeśli nie chcesz sobie zawracać głowy sprawą cyberbezpieczeństwa, skorzystaj z usług firm, które się tym zajmują. Zapytaj firmę-dostawcę systemu gabinetowego, czy oferuje takie usługi lub sprawdź oferty outsourcingu IT. Za wygodę trzeba jednak zapłacić – ceny zaczynają się ok. 500 zł miesięcznie i zależą od liczby komputerów.

Chroń swój komputer jak portfel. Nawet najsilniejsze hasła nie pomogą, gdy złodzieje ukradną twój komputer z danymi. Pamiętaj także, aby nigdy nie instalować oprogramowania z niezaufanych źródeł albo podłączać nieznanych nośników pamięci. Ta stara metoda dalej dobrze działa i według nowych danych, w pierwszym półroczu 2023 roku aż trzykrotnie zwiększyła się liczba ataków z pomocą złośliwego oprogramowania dystrybuowanego na nośnikach pamięci USB. Następnym razem gdy znajdziesz atrakcyjnie wyglądający dysk USB albo dostaniesz go od nieznajomej osoby, dla pewności zrezygnuj z prezentu. Jego otwarcie może cię drogo kosztować.

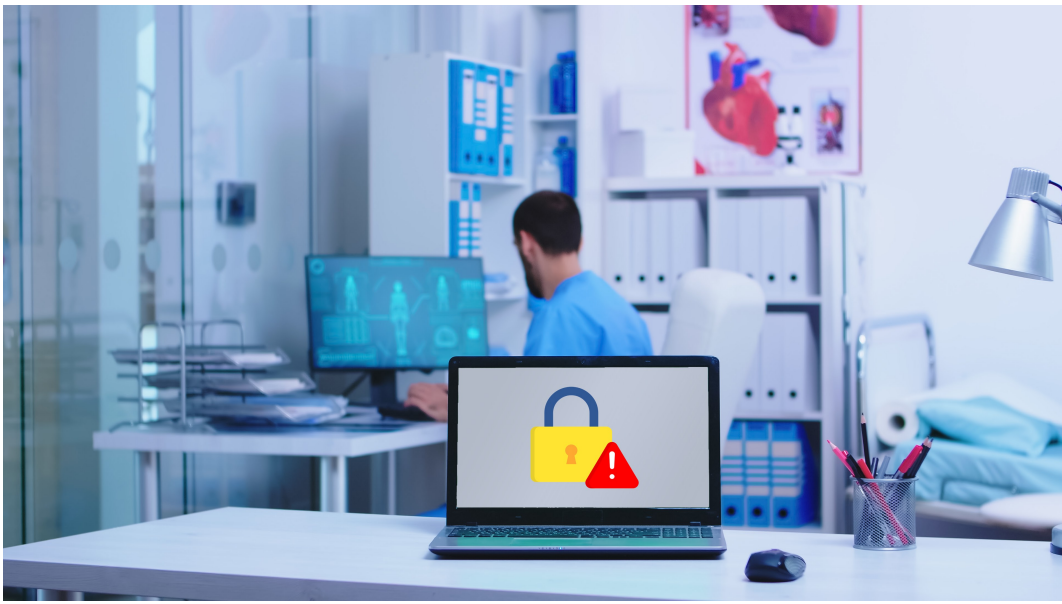
» Znalazłeś nośnik pamięci USB? Uważaj, to stara metoda hakerów. «

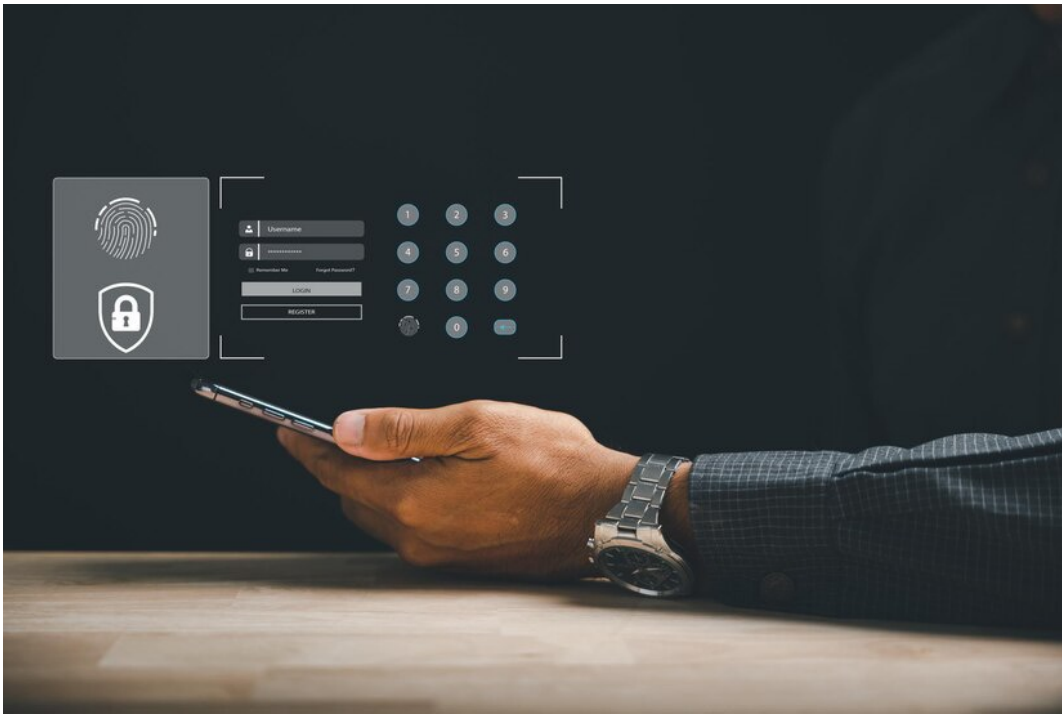
Rozważ ubezpieczenie od ryzyk cybernetycznych, jeśli chcesz dmuchać na zimne. Ale najpierw spełnij powyższe warunki. Nie jest tanie, a do tego udział własny najczęściej wynosi kilka tysięcy złotych. Należy je traktować opcjonalnie. W przypadku ataku hakerów ubezpieczeni mogą

liczyć najczęściej na przywrócenie danych i pracy systemów informatycznych (o ile mają kopię zapasową), pomoc prawną w zakresie roszczeń odszkodowawczych, pokrycie kosztów roszczeń i kosztów związanych z naprawą, a nawet wsparcie PR, jeśli reputacja firmy została naruszona w wyniku incydentu. Dostępne w Polsce ubezpieczenia raczej kierowane są do dużych placówek medycznych

Aktualizuj swoją wiedzę. Hakerzy stosują coraz bardziej wyrafinowane metody działania. Umiejętności dotyczące ochrony danych stają się częścią zawodu lekarza, odkąd praca w ochronie zdrowia to praca na danych.

Co tydzień na świecie dochodzi do ok. 1800 ataków cybernetycznych na placówki zdrowia. W 2023 roku było ich o 74% więcej w stosunku do 2022 roku. I to coraz częściej ataki na małe gabinety lekarskie, które mają spore zaległości w kwestiach ochrony danych





Bezpieczne logowanie do usług on-line

Aplikacja Wizyta Lekarska firmy KAMSOFT wspiera uwierzytelnienie wieloskładnikowe zapewniając dodatkową ochronę danych w serwisach internetowych.

Każdego dnia logujemy się do bankowości elektronicznej, poczty internetowej czy też serwisów dla specjalistów, jak np. Portal Świadczeniodawcy. Jednak nasze loginy i hasła często nie zapewniają dostatecznego poziomu bezpieczeństwa danych. Biorąc pod uwagę zwiększoną w ostatnich latach

intensywność ataków hakerskich, warto korzystać podczas procesu logowania do wybranych serwisów z dodatkowych zabezpieczeń. Jednym z nich jest uwierzytelnianie wieloskładnikowe MFA, które zapewnia jeszcze lepszą ochronę. Użytkownicy przeprowadzają dodatkową weryfikację tożsamości, np. poprzez wprowadzenie kodu otrzymanego na telefon.

Na czym to polega uwierzytelnienie wieloskładnikowe MFA?

MFA czyli *Multi-Factor Authentication* to zabezpieczenie, które zdecydowanie utrudnia przejęcie konta użytkownika przez osoby nieuprawnione, nawet jeśli hasło zostanie skradzione lub ujawnione.

Logowanie dwuetapowe wprowadza dodatkową ochronę. W trakcie uwierzytelniania zostaniesz poproszony nie tylko o hasło, ale także o dodatkowe dane, bez których nie otrzymasz dostępu do serwisu. Może być to być np. kod PIN, jednorazowy kod czy kod SMS. To ochrona przed różnymi rodzajami ataków oraz złośliwym oprogramowaniem mającym na celu przejęcie danych logowania. Korzysta z niego wiele aplikacji bankowych, sklepów oraz portale Świadczeniodawcy i Pracownika NFZ, a wkrótce także system medyczny SERUM. Jego zdecydowaną zaletą jest skuteczność oraz prosta konfiguracja.

» ENISA – Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji – zaleca uwierzytelnianie dwuskładnikowe w celu poprawy bezpieczeństwa cybernetycznego, ochrony przed phishingiem i naruszeniem danych. «

Co trzeba zrobić, aby uruchomić MFA?

Po pierwsze należy pobrać aplikację na telefon, za pomocą której zalogujesz się do internetowych kont użytkownika korzystających z dwuetapowej autentykacji. Tego typu aplikacji jest sporo, wśród nich są także aplikacje dla profesjonalistów medycznych takie jak: Wizyta Lekarska, Wizyta Pielęgniarska czy Wizyta Położnej, a także aplikacja dla farmaceutów KS-APTIX, dedykowana do pracy w aptece przy kompletacji leków z e-Recept, inwentaryzacji czy weryfikacji dostaw leków. To szybkie, proste i darmowe zabezpieczenie konta. Po pobraniu aplikacji, należy skonfigurować weryfikację dwu-

etapową MFA postępując zgodnie z instrukcją aplikacji lub usługi, do której dodajesz uwierzytelnienie wieloskładnikowe.

Jak to działa w aplikacji Wizyta Lekarska?

Aplikacja Wizyta Lekarska jest zgodna ze standardem TOTP, co oznacza, że pomoże Ci zalogować się do internetowych kont użytkownika korzystających z dwuetapowej autentyfikacji (tzw. MFA). Dzięki temu, nawet jeśli ktoś wykradnie Twoje hasło, to i tak nie uzyska dostępu do zgromadzonych danych, bo są one dodatkowo chronione jednorazowymi kodami (OTP). Do tego nie musisz instalować osobnej aplikacji uwierzytelniającej. Uwaga: aplikacja nie ma dostępu do danych, jedynie generuje kod jednorazowy.

Uwierzytelnienie wieloskładnikowe (MFA) jest szczególnie ważne w przypadku logowania do serwisów, w których przechowujemy cenne dla nas dane i informacje. Coraz częściej dochodzi do wycieków danych, kiedy loginy i hasła użytkowników portali zostają upublicznione.

Dlaczego potrzebujesz dodatkowo zabezpieczyć swoje dane?

Twoje hasło i login mogą zostać przejęte przez złośliwe oprogramowanie, lub innymi metodami jak np. socjotechnika, odgadywanie haseł czy też podglądnięcie hasła, kiedy użytkownik loguje się do portalu. Niebezpieczeństw jest wiele, dlatego warto zwiększyć bezpieczeństwo danych stosując wieloskładnikowe uwierzytelnianie.

Aplikacja **Wizyta Lekarska** z funkcjonalnością uwierzytelnienia wieloskładnikowego

Zadbaj o **bezpieczeństwo** danych osobowych w Twojej placówce medycznej z KS-BDO RODO!

- **Wsparcie** w przeprowadzeniu analizy ryzyka
- **Ankieta** umożliwiająca ocenę indywidualnej sytuacji podmiotu w obszarze przetwarzania danych osobowych
- **Wzorce** dokumentów wykorzystywanych w procesach przetwarzania danych osobowych
- **Wskaźniki** poziomu wdrożenia rekomendowanych zabezpieczeń
- Wbudowane **mechanizmy aktualizacji** dokumentacji w obszarze wynikającym ze zmian personalnych
- Wbudowane **rejestry** pozwalające dokumentować czynności związane z przetwarzaniem danych

Rozwiązanie KS-BDO RODO współpracuje z systemami produkcji KAMSOFT: KS-AOW, KS-SOMED, KS-PPS.

kontakt@osoz.pl | tel. (+48) 32 209 07 05

kamsoft.pl/KS-BDO-RODO

Przewodnik, jak wdrażać AI zgodnie z przepisami

Jak wdrażać rozwiązania oparte na AI w ochronie zdrowia? Wywiad z adwokatem Michałem Chodorkiem, partnerem w Kancelarii Prawnej KRK Kieszkowska Rutkowska Kolasiński.

Dostawca IT albo startup proponuje menedżerowi placówki medycznej wdrożenie nowego rozwiązania AI. Na jakie elementy organizacyjno-prawne powinien on zwrócić uwagę?

Decyzja o wdrożeniu nowego rozwiązania AI w placówce medycznej wymaga rozważenia wielu aspektów i powinna być poprzedzona szczegółową analizą potrzeb, a w proces definiowania wymagań placówki powinny być zaangażowane różne zespoły i specjaliści: IT, kierownictwo placówki, i oczywiście personel medyczny, który ma korzystać z tego narzędzia. Na pewno należy przeanalizować kilka podstawowych aspektów.

Pierwszy to business case. To oczywistość, ale warto zawsze podkreślać, że AI to narzędzie jak każde inne – jego celem jest zapewnienie, że praca, umiejętności i czas ludzi będą wykorzystywane lepiej, efektywniej i bezpieczniej. Każdy system AI trzeba więc ocenić pod kątem jego wartości dla placówki – czy AI wspierający ocenę zdjęć diagnostyki obrazowej przyspieszy pracę lekarzy, dzięki czemu możliwe będzie obsłużenie większej liczby pacjentów, albo rozwiązany będzie problem braku odpowiedniej ilości lekarzy? Czy AI odpowiedzialny za rekonstrukcję i post-processing obrazów generowanych w ramach diagnostyki nuklearnej (np. PET, SPECT) pozwoli zmniejszyć ilość używanych radioizotopów i promieniowania jonizującego oddziałującego na pacjenta – obniżając koszty po stronie szpitala i ryzyka po stronie pacjenta?

Kolejną kwestią do przeanalizowania jest integracja z istniejącymi systemami. Wdrożenie narzędzia AI powinno obejmować integrację z obecnym ekosystemem informatycznym placówki, w tym z systemami służącymi do prowadzenia elektronicznej dokumentacji medycznej (EDM), systemami HIS czy innymi używanymi narzędziami i platformami. Kwestia odpowiedzialności za integrację powinna być jasno określona w umowie z dostawcą.

Idąc dalej, trzeba dobrze przemyśleć model wdrożenia. To przede wszystkim kwestia wyboru między on premises vs. chmurą. Te dwa modele istotnie różnią się od siebie i każdy

z nich ma konsekwencje – w modelu on premises, AI działa na infrastrukturze szpitala. W modelu chmurowym, AI działa na zewnętrznym serwerze, udostępnianym przed dostawcę narzędzia AI albo (najczęściej) przez zewnętrznego dostawcę.

I oczywiście trzeba dobrze przeanalizować kwestie regulacyjne. Jeżeli AI jest wyrobem medycznym (AIMD) albo wyrobem medycznym do diagnostyki in vitro (AIIVD), musi spełniać odpowiednie wymogi regulacyjne – w szczególności wymogi MDR (w przypadku AIMD) albo IVDR (w przypadku AIIVD). Za spełnienie tych obowiązków odpowiada producent technologii, ale szpital musi zapewnić, że korzysta z narzędzia spełniającego te wymogi.

Szpital musi również zapewnić sobie w umowie z dostawcą odpowiednie współdziałanie dostawcy przy realizacji obowiązków, które spoczywają bezpośrednio na szpitalu. Są to np. obowiązki wynikające z RODO czy ustawy o prawach pacjenta – szpital jest administratorem danych osobowych pacjentów, prowadzi dokumentację medyczną pacjentów i musi realizować obowiązki wynikające z tych przepisów, a w wielu przypadkach wymaga to odpowiedniej współpracy dostawcy technologii.

Również unijny AI Act nakładał będzie na szpitale, jako użytkowników AI, określone obowiązki (np. zapewnienie odpowiedniego nadzoru ludzkiego nad działaniem AI czy udzielanie pacjentom informacji na temat sposobu działania AI), które trudno będzie realizować bez odpowiedniej współpracy dostawcy technologii.

» Konieczne jest np. ustalenie, czy dane pacjentów mają być wykorzystywane do dalszego trenowania algorytmu AI. «

Oprócz tego, korzystanie z AI wiąże się z wieloma specyficznymi aspektami, które nie pojawiają się przy innych technologiach. Konieczne jest np. ustalenie, czy dane pacjentów mają być wykorzystywane do dalszego trenowania algorytmu AI. Jeżeli tak, trzeba określić zasady, na jakich będzie to następować – jakie dane są potrzebne do dalszego trenowania? Czy dane będą anonimizowane w tym celu? W jaki sposób dokonywana będzie anonimizacja?

Ten wątek wiąże się oczywiście z tematem zgodności regulacyjnej wyrobu medycznego AI, o którym mówiłem wcześniej – ponieważ zasady dalszego trenowania modelu AI i wdrażania nowych wersji modelu muszą być określone w dokumentacji technicznej i systemie zarządzania jakością wyrobu.

Co z kolei prowadzi nas do kolejnego ważnego tematu, czyli: aktualizacje i wsparcie. W przypadku każdego oprogramowania istotne jest określenie warunków wsparcia technicznego, usuwania wad i aktualizacji systemu. Ale w przypadku AI aktualizacje wynikające z implementacji nowszej, re-trenowanej wersji modelu AI, wiążą się z dodatkowymi obowiązkami zarówno po stronie dostawcy technologii, jak i szpitala.

Przykładowo, nowa wersja modelu AI może zachowywać się inaczej na określonych danych wejściowych. Takie zmiany czułości i swoistości modelu są oceniane w procesie walidacji nowej wersji modelu, ale jeżeli mogą mieć przełożenie na praktykę kliniczną, muszą być odpowiednio zakomunikowane użytkownikom. W takich przypadkach dostawca technologii powinien nie tylko przekazać zaktualizowane informacje dot. działania systemu, ale też w razie konieczności przeprowadzić odpowiednie szkolenia użytkowników.

Według ostatniego badania Centrum e-Zdrowia, tylko ok. 6,4% placówek ochrony zdrowia wykorzystuje narzędzia AI. Które rozwiązania AI zaliczyłby Pan do grupy rozwiązań niskiego ryzyka, które można wdrożyć najłatwiej, a które do wysokiego ryzyka?

Te metryki oceny się krzyżują, a nie pokrywają – łatwość wdrożenia zależy np. od tego, jak głęboką zmianę dotychczasowych procesów wymusza wdrożenie określonego narzędzia AI, czy z iloma istniejącymi systemami trzeba dokonać integracji. Wyroby medyczne AI, które należą do najwyższej klasy ryzyka (np. klasy III wg. MDR) wcale nie muszą stwarzać istotnych trudności wdrożeniowych.

Z drugiej strony technologie AI, które łatwo wdrożyć w placówce i które nie różnią się między sobą z punktu widzenia

sposobu interakcji z użytkownikiem (np. pracujące w oparciu o dane wprowadzane samodzielnie przez pacjentów i informacje ekstrahowane z danych dot. sposobu korzystania z określonego urządzenia, np. smartfona, i analizujące te dane, aby wysyłać alerty lekarzowi i samemu pacjentowi) mogą diametralnie różnić się między sobą poziomem ryzyka, ponieważ służą do monitorowania i wspierania terapii bardzo różnych stanów chorobowych.

W mojej praktyce pracuję z producentami takich narzędzi AI, które należą zarówno do najniższej możliwej w praktyce MDR klasy ryzyka dla wyrobu medycznego AI, czyli klasy IIa, jak i producentami AI, które należą dla klasy najwyższej, czyli klasy III.

Wiele podmiotów deklaruje, że planuje wdrożenie rozwiązań AI. Jak się do tego przygotować z wyprzedzeniem?

Tu zastosowanie znajdzie wszystko, o czym rozmawialiśmy do tej pory. Czyli w pierwszej kolejności – zmapowanie potrzeb po stronie placówki i ocena konkretnego business case. Po drugie, zaangażowanie w proces definiowania potrzeb przedstawicieli wszystkich kluczowych grup interesariuszy w placówce, w tym pracowników, którzy będą na koniec korzystać z AI. Po trzecie, przemyślenie, w jaki sposób narzędzie AI wpisuje się w istniejące procesy w placówce, a w jakim stopniu te procesy będą musiały ulec modyfikacji.

A z jeszcze szerszej perspektywy – warto szkolić personel i pokazywać, że AI nie stanowi dla nich zagrożenia, ponieważ nie zastąpi pracy człowieka, natomiast może stanowić duże wsparcie, generujące korzyści zarówno dla pacjentów, jak i przedstawicieli zawodów medycznych.

» Większość aspektów dotyczących przetwarzania danych, które trzeba wziąć pod uwagę w projekcie AI, nie jest związana z AI. «

Czy inne sektory gospodarki mają łatwiej z wdrażaniem AI?

Zależy, o jakich sektorach mówimy! Sektory, które nie są tak regulowane, na pewno mają łatwiej, np. jeżeli jestem firmą z sektora FMCG i chcę zbudować modele predykcyjne,

prognozujące przyszłe trendy popytowe, aby optymalizować koszty produkcyjne i łańcuch dostaw, to właściwie nie ma wymogów regulacyjnych, które dotyczyłyby takiego projektu.

Ale już wykorzystanie AI w sektorze finansowym jest obudowane równie wieloma wymogami, co w sektorze Healthcare & Life Sciences.

Z drugiej strony, wiele zastosowań AI w Healthcare & Life Sciences nie jest aż tak restrykcyjnie regulowanych. Przykładowo, korzystanie z AI w fazie przedklinicznej procesu R&D leków, np. do identyfikowania kandydatów do dalszego rozwoju na podstawie predykcji dotyczącej reakcji immunologicznych na określone epitopy. Pracujemy z firmami korzystającymi z AI w fazie przedklinicznej i takie wykorzystanie AI nie jest obciążone aż tyloma wymaganiami regulacyjnymi.

Wiele podmiotów medycznych z góry przekreśla wszelkie rozwiązania oparte na sztucznej inteligencji, aby nie robić sobie kłopotu na zapas z przetwarzaniem danych. Takie podejście jest słuszne?

W mojej ocenie to zbyt rygorystyczne podejście. Po pierwsze, większość aspektów dot. przetwarzania danych, które trzeba wziąć pod uwagę w projekcie AI, nie jest związana z AI i występuje w każdym przypadku wdrażania w podmiocie leczniczym oprogramowania, które będzie służyło do przetwarzania danych medycznych czy prowadzenia dokumentacji medycznej. Tak jak w przypadku każdego innego software, tak w przypadku AI te kwestie można odpowiednio uregulować w umowie między placówką a dostawcą technologii.

Korzystanie z AI tworzy specyficzne wyzwania, np. właśnie pytanie o wykorzystywanie danych medycznych do dalszego trenowania algorytmu AI. Ale również te zagadnienia nie są nierozwiązywalne. Doradzamy w wielu projektach związanych z wdrażaniem AI w podmiotach leczniczych i wiem z doświadczenia, że kwestie przetwarzania danych są jednym

» Lekarze wykorzystujący system AI wysokiego ryzyka będą musieli stosować się do instrukcji udostępnionej przez producenta i m.in. zgłaszać incydenty nieprawidłowego funkcjonowania. «

z tych tematów, na które placówki zwracają szczególną uwagę, ale ostatecznie zawsze udaje się uzgodnić takie warunki implementacji, które są akceptowane przez podmioty lecznicze.

Czy europejski akt w sprawie sztucznej inteligencji – EU AI Act – sprawia, że regulacje dot. AI są bardziej przejrzyste? Co zmieni ta nowa regulacja?

Paradoksalnie AI Act nie będzie stanowił wielkiej rewolucji dla producentów AI w branży Healthcare & Life Sciences, ponieważ wymogi AI są w dużym stopniu wzorowane na przepisach dot. wyrobów medycznych (MDR i IVDR). Producenci AI będących wyrobami medycznymi albo wyrobami medycznymi do diagnostyki in vitro, którzy spełniają wymogi MDR/IVDR, już teraz spełniają wiele wymogów, które wprowadzi AI Act.

Powyższe ma oczywiście konsekwencje dla strategii dostosowywania się do tych nowych wymogów. AI Act przewiduje 2-letni okres przejściowy, co jest terminem bardzo krótkim, biorąc pod uwagę ilość pracy związanej z realizacją wynikających z niego obowiązków. Producenci AI będących wyrobami medycznymi albo wyrobami medycznymi do diagnostyki in vitro na pewno będą w lepszej sytuacji niż producenci AI, które do tej pory nie były regulowane.

Nawet dla producentów AIMD/AIIVD (i przede wszystkim dla użytkowników AIMD/AIIVD) pojawi się jednak kilka nowych obowiązków, np. w zakresie wytłumaczalności działania AI i nadzoru ludzkiego nad działaniem systemu AI. Ale nie będzie to aż taka rewolucja, jak w przypadku innych branż.

Zostawiam na razie na boku temat jednostek notyfikowanych, które zgodnie z AI Act będą odpowiedzialne za certyfikację systemów AI wysokiego ryzyka. W praktyce trudności z uzyskiwaniem statusu jednostki notyfikowanej pod AI Act mogą spowodować, że okresy przejściowe zostaną przesunięte, jak widzieliśmy to już w przypadku MDR i IVDR.

Z jakimi pytaniami związanymi z implementacją AI w ochronie zdrowia spotyka się Pan najczęściej?

Są chyba dwie grupy najczęściej stawianych pytań. Pierwsza dotyczy zasad rozwoju, testowania i walidacji medycznych AI: Czy trzeba przeprowadzić badanie kliniczne? Czy może walidacja z wykorzystaniem podzbioru danych treningowych jest wystarczająca? Jeżeli badanie kliniczne – co zdefiniować jako istniejący standard of care? Jak zarządzać procesem dalszego trenowania algorytmu AI po zakończeniu oceny zgodności?

Druga grupa pytań dotyczy przetwarzania danych: Jakie dane można wykorzystać do trenowania AI? Czy dane z badań klinicznych i eksperymentów medycznych można wykorzystać do trenowania AI? Czy dostawca technologii może wykorzystywać dane medyczne do dalszego trenowania AI, a jeżeli tak – pod jakimi warunkami?

Co by Pan poradził lekarzowi, który korzysta z ChatGPT w swojej pracy?

To pytanie podchwytliwe. Ale gdybym miał ograniczyć się do jednej kwestii, to radziłbym pracować na GPT-4 (a nie bezpłatnej wersji 3.5.), i korzystać z niego jak ze zwykłej wyszukiwarki internetowej, ale z rewolucyjnym interfejsem użytkownika, czyli maksymalnie wykorzystać możliwość wprowadzania długich i skomplikowanych komend, aby dobrze przedstawić sytuację (np. zmienność w czasie wyników badań krwi), i jednocześnie krytycznie podchodzić do uzyskiwanych outputów.

Metodyki promptowania AI, w tym ChatGPT, i weryfikacji outputów przez lekarzy to zresztą jeden z tematów szkoleń, które prowadzimy razem z współpracującymi analitykami danych.

I jeszcze jedno – nigdy nie należy wprowadzać do publicznie dostępnych narzędzi AI danych osobowych pacjenta.

Jak wdrażać Opiekę Koordynowaną w POZ?

- Pobierz bezpłatnie nowy poradnik
- Zobacz 55-minutowy webinar

KLIKNIJ TUTAJ
lub wejdź na blog.osoz.pl

Jak przeprowadzić onboarding IT nowych pracowników?

Dane są bezpieczne, gdy pracownicy wiedzą, jak obsługiwać system IT i znają zasady bezpieczeństwa informacyjnego. Tymczasem większość szpitali i przychodni nie ma sformalizowanego programu onboardingu. Jak go przygotować, aby nowi lekarze i pielęgniarki szybko wdrożyli się do pracy w podmiocie leczniczym i wiedzieli, jak chronić dane?

Plan onboarding IT ma na celu oswojenie nowych pracowników z oprogramowaniem. Po co? Aby zapewnić wysoką jakość gromadzonych danych, płynność procesów organizacyjnych oraz bezpieczeństwo informacyjne. Niepoprawna obsługa systemu IT może mieć poważne konsekwencje, prowadząc do błędów medycznych albo nawet wycieku danych.

Dobry onboarding powinien obejmować pakiet zagadnień IT: obsługę systemu EDM oraz bezpieczeństwo danych medycznych i procedury stosowane przez organizację. Należy pamiętać, że nawet pracownicy znający daną markę oprogramowania, muszą poznać wypracowane przez placówkę zasady przetwarzania danych: kto wprowadza jakie dane, czy stosowane są niestandardowe szablony wywiadów albo lokalne bazy danych, jak wygląda ścieżka obsługi pacjenta dla różnych grup pacjentów (np. w ramach opieki koordynowanej).

Od czego zacząć?

Potrzebne będą dwa dokumenty: przewodnik dla nowych pracowników oraz procedura wewnętrzna onboardingu:

- Kilkustronicowy **przewodnik dla pracownika** powinien zawierać informacje o rodzaju systemu, cyklu szkoleń, kontakcie do działu IT, kluczowych liderach IT w zespole klinicznym gotowych do pomocy, instrukcje obsługi systemu, procedury obsługi pacjenta (jakie dane są wymagane, jakie fakultatywne), filmy szkoleniowe i webinaria oferowane przez dostawcę IT, numery telefonów w sytuacjach krytycznych, polityka bezpieczeństwa danych. Standardowy dokument uzupełniany jest załącznikiem z informacjami o harmonogramie szkoleń oraz wytycznymi dotyczącymi ochrony danych medycznych.
- **Strategia onboardingu** zawiera ogólną politykę IT, plan szkoleń i wsparcia indywidualnego na dalszych etapach obsługi systemu (coaching IT), plan audytu poprawności wprowadzania danych będący podstawą stworzenia protokołu ze wskazówkami dla użytkownika, plan informowania o nowych funkcjach i aktualizacji systemu (obowiązujący

dla wszystkich pracowników), udział w webinariach organizowanych przez dostawcę IT.

Oswajanie z systemem najlepiej podzielić na etapy, na początku skupiając się na standardowej ścieżce wprowadzania danych. Żaden pracownik – czy to lekarz, pielęgniarka albo rejestratorka – nie musi od razu znać każdej z tysiąca funkcji systemu. Na początek wystarczy klasyczna procedura obsługi statystycznego pacjenta. Dobrze sprawdzają się graficzne arkusze postępowania w zależności od sytuacji i plansze dostępne przy komputerze nowego pracownika (koniecznie w formie zrzutów ekranu, a nie tylko opisów).

Elementy dobrego onboardingu

Zakres dokumentu zależy od tego, czy to mniejsza przychodnia czy duży szpital, ale zawsze powinien uwzględniać takie kluczowe elementy jak:

Plan wielopoziomowych szkoleń w tym podstawy obsługi oprogramowania (gotowe webinary), podstawowe funkcje (np. realizacja usługi medycznej, umówienie nowego terminu w kalendarzu), obsługa systemu przez osoby na podobnych stanowiskach (kursy organizowane przez użytkowników). Zaleca się stworzenie trzech scenariuszy szkoleń: podstawowy (dla osób mających trudności z IT i komputerami), średni (dla osób biegle posługujących się komputerem, ale nieznających systemu IT) i zaawansowany (dla osób już znających system IT, które trzeba wdrożyć w specyficzne dla placówki procedury rejestracji danych i obsługi pacjenta).

Na początek każdy pracownik musi przejść przez tzw. sesje orientacyjne pozwalające zadomowić się w otoczeniu informatycznym. Obejmują one wiedzę z infrastruktury IT, poziomu i wizji cyfryzacji, zasady ochrony i bezpieczeństwa danych.

Plan wsparcia przy biurku. Dużo ważniejsze – i często pomijane – są mikro-szkolenia w codziennej pracy. Chodzi o wyodrębnienie trenerów wśród pracowników, którzy dobrze znają system i pomogą w gorącej sytuacji, gdy pojawia się

problem albo wątpliwość, a pacjent czeka przy stanowisku rejestracji albo w gabinecie. Oprócz coachów należy stworzyć tzw. help desk – dedykowane wsparcie IT dostępne 7 dni w tygodniu, aby pracownik mógł otrzymać pomoc w krytycznych sytuacjach lub zgłosić problem.

E-learning. Każdy uczy się we własnym tempie, w czym pomagają zasoby on-line, do których pracownik może sięgnąć w czasie pracy lub w domu (często nie doceniamy zaangażowania pracowników i chęci samodzielnego podnoszenia kwalifikacji).

Szkolenia scenariuszowe. W każdej placówce medycznej można wyodrębnić kilka najczęściej występujących ścieżek obsługi pacjenta i na ich podstawie przygotować plan szkoleń. Przykładowo: obsługa osoby w ramach Opieki Koordynowanej, proste przypadki, skierowania na badania, pacjent przewlekły itd. W zakresie bezpieczeństwa danych, pracownik musi orientować się w sposobach działania hakerów i potrafić rozpoznać atak cybernetyczny i na niego prawidłowo zareagować.

Personalizacja miejsca pracy. O wygodzie pracy z infrastrukturą IT mogą decydować błahe szczegóły: podobna myszka jak ta używana prywatnie, personalizacja systemu IT (wstępna konfiguracja) itd. W dopasowaniu stanowiska pracy pomoże ankieta potrzeb informatycznych będąca częścią procedury onboardingu. Przy każdym stanowisku pracy powinien znajdować się kontakt do działu IT, ułatwiający szybkie zgłoszenie problemu technicznego z komputerem, który czasami może być pierwszym sygnałem cyberataku.

Ocena i certyfikacja. Nikt nie lubi być ocenianym, ale oceny są niezbędne, aby monitorować umiejętność obsługi systemu. Można to zrobić w formie obserwacji, ankiet, testów. Weryfikację wiedzy należy zorganizować tak, aby motywować, a nie straszyć pracowników, zastępując szkolne oceny poziomami biegłości IT, nagradzając za zaangażowanie w naukę obsługi oprogramowania, a nawet przygotowując certyfikaty, które przydadzą się w przypadku zmiany miejsca pracy.

» Pracownicy powinni wiedzieć, jak rozpoznać atak cybernetyczny i jak na niego zareagować. «

Plansza wyświetlana na komputerze po ataku ransomware WannaCry w 2017 roku. System zostaje zablokowany, a hakerzy żądają okupu za jego odblokowanie. WannaCry zainfekował w ciągu jednego dnia ponad 230 000 systemów komputerowych w 150 krajach, powodując straty finansowe sięgające 4 mld USD

Dobrze przygotowany onboarding ma jeszcze jedną zaletę: pracownik szybko wdroży się w nowe obowiązki – celem zatrudnienia nowej osoby nie jest przeciągająca się nauka systemu, ale obsługa pacjenta i opieka nad nim. Pracownik powinien od pierwszego dnia wiedzieć, do kogo zwrócić się z pomocą i gdzie znaleźć wskazówki, gdy nie wie, gdzie kliknąć albo wprowadzić dane.

Często popełnianym błędem jest przeładowanie informacjami i intensywne szkolenia od pierwszego dnia pracy. Przedstaw nowej osobie plan w przejrzystej strukturze np. 7–30–90, opisując, czego osoba nauczy się podczas pierwszych 7, 30 i 90 dni pracy. Taka uporządkowana mapa drogowa działa uspokajająco na osoby mające problem z technologiami. Zadbaj o atmosferę szczerości – jeśli pracownik potrzebuje więcej czasu na naukę, stwórz takie możliwości. Pomysłem jest przyporządkowanie do pomocy wieloletniego pracownika, który na początku też miał problemy z systemem.

Pracę domową musi też odrobić dział IT tak konfigurując system, aby praca z nim była maksymalnie prosta i bezpieczna.

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 newralgiczne 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.

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

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

technologię: „Komputer powinien działać zawsze dobrze, a za bezpieczeństwo odpowiadają informatycy, dlatego nie muszę 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, jak 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 hakera, 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 wzmacnianie 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 o np. 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. Dbałość 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.

Phishing najczęstszą przyczyną kradzieży danych. Jak się bronić?

Każdego dnia wysyłanych jest ok. 3,4 miliarda wiadomości phishingowych. Część z nich trafia do skrzynki spamowej, część kasujemy od razu, bo nauczyliśmy się je rozpoznawać. Mimo to phishing jest ulubioną i skuteczną formą ataków cybernetycznych, także w medycynie. Na co zwracać uwagę?

Na maile o spadku od bogatego wujka zza granicy mało kto już się nabiera lub są odsiewane automatycznie przez skrzynki mailowe zanim je zdążymy przeczytać. Podobnie jest z informacjami o niedostarczonej przesyłce przez kuriera, które często już na pierwszy rzut oka wyglądają podejrzanie.

I choć wydaje nam się, że nie damy się nabrać, fakty są inne: według raportu *Proofpoint 2022 State of the Phish*, w ubiegłym roku 83% organizacji padło ofiarą ataku phishingowego. 25% wszystkich naruszeń danych wiąże się z phishingiem. Wystarczy nieuważne kliknięcie na link albo otwarcie PDF-a w zainfekowanej wiadomości, a na komputerze instalowane jest złośliwe oprogramowanie będące dla hakerów bramą do danych. Statystyki nie pozostawiają złudzeń: phishing jest nadal jednym z największych zagrożeń dla cyberbezpieczeństwa. I to mimo tego, że stosowany jest od lat i zdążyliśmy się już z nim oswoić.

Nie tylko my jesteśmy czujniejsi a systemy IT szczelniejsze. Także hakerzy doskonalą wiadomości phisingowe. Te najlepsze już nie zawierają rażących błędów językowych, literówek albo dziwnych, kolorowych czcionek. Mogą do złudzenia przypominać identyfikację graficzną banku lub firmy kurierskiej.

Oto kilka najważniejszych zasad pomagających skutecznie odróżnić wiadomość phishingową od autentycznego maila:

- Wiadomość informuje, że **należy natychmiast coś zrobić**, w przeciwnym razie grozi ci coś, np. utrata danych, zablokowanie konta, grzywna itd. Takich wiadomości nigdy nie wysyłają ani banki, ani urzędy. Groźby finansowe mają skłonić do szybkiego, emocjonalnego działania i wyłączenia racjonalnego myślenia (im dłużej myślimy o sprawie, tym bardziej wydaje nam się podejrzana);
- Wiadomość sugeruje, że trzeba **wprowadzić poufne dane**, takie jak numer konta bankowego, kod PIN do bankowości internetowej lub numer karty kredytowej albo zalogować się w serwisie, aby zweryfikować tożsamość. Dlatego niezależnie od phishingu, logować się należy zawsze na

stronach, które mamy zapisane albo które możemy wyszukać w wyszukiwarce. Linki w mailach mogą prowadzić do zdublowanych, fałszywych stron;

- Wiadomości phishingowe zawierają często **linki albo załączniki, których się nie spodziewamy**;
- Nadal zdarza się, że tekst wiadomości jest **źle napisany, a grafika niepodobna do poprzednio wysyłanych maili**;
- Tekst zawiera **różne czcionki albo nieprawidłowe znaki specjalne** (np. polskie);
- Wiadomość zawiera **bezosobowy wstęp**, jak „drogi kliencie" lub „proszę pana/proszę pani";
- Wiadomość **nie zawiera danych kontaktowych**;
- E-mail lub SMS zostały wysłane z adresu/e-mail, który **nie znajduje się na liście kontaktów**.

Tak jak zmieniają się metody hakerów, trzeba aktualizować swoje umiejętności w zakresie cyberbezpieczeństwa. Przykładowo, kilka lat temu dużo mówiło się o tym, że zaufane strony muszą zaczynać się od „https://"? Takie oznaczenie gwarantuje bezpieczne połączenie z godną zaufania witryną, czyli posiada certyfikat SSL. Niestety, coraz więcej oszustów phishingowych także stara się o certyfikat, aby zwiększyć skuteczność ataku.

Warto wyrobić sobie kilka nawyków, które pozwolą zwiększyć poziom bezpieczeństwa cybernetycznego. Po pierwsze, zasada sprawdzania linków w wiadomościach e-mail i sieciach społecznościowych przed ich kliknięciem. Ale z dużą czujnością, bo fałszywe witryny mogą mieć bardzo podobne adresy, różnić się jedynie kilkoma znakami. Każdy może kupić adres domeny, nawet jeśli jest podobny do dużej instytucji.

Po drugie, wiadomości z urzędów albo z banku można zweryfikować dzwoniąc do tych instytucji. Innym sposobem jest skopiowanie treści podejrzanego maila w Google, aby sprawdzić, czy nie ma ostrzeżeń przed tego typu wiadomościami. Po trzecie, bądź wyczulony na otwieranie załączników z nieznanych adresów e-mail. Mogą to być informacje

o fakturze, wezwanie do zapłaty, ważna wiadomość z banku itd. Jeśli już koniecznie chcesz się zalogować dla świętego spokoju, otwórz stronę bezpośrednio w przeglądarce, tak jak to robisz zwyczajowo, a nie klikając na odnośnik. Po czwarte, sprawdzaj, kto jest nadawcą wiadomości, a dla pewności wyszukaj w Google, czy adres e-mail naprawdę należy do instytucji, za którą się podaje.

Co zrobić, gdy otrzymasz wiadomość phishingową?

- Nigdy nie klikaj żadnych linków ani załączników w podejrzanych wiadomościach e-mail. Jeśli otrzymasz podejrzaną wiadomość, ale nie masz pewności, czy jest prawdziwa czy fałszywa, zweryfikuj ją: logując się na oryginalnej stronie z przeglądarki, dzwoniąc do instytucji, wpisując kilka pierwszych zdań z maila do Google;
- Zgłoś wiadomość do instytucji, pod którą się podszywa;
- Kliknij w skrzynce mailowej opcję „oznacz/zgłoś jako SPAM", dzięki której filtry doskonalą swoje umiejętności wykrywania oszustw;
- Usuń wiadomość (także z kosza).

I na koniec, eksperci zalecają przeglądanie skrzynki SPAM, bo nadal trafiają tam także prawdziwe maile, na które czekamy, a które algorytmy – z różnych przyczyn – zakwalifikowały jako fałszywe. Takie codziennie otwieranie SPAMu wyrabia nawyk czujności.

Phishing jest nadal skuteczny, bo wystarczy jedno omyłkowe kliknięcie, aby haker przejął kontrolę nad komputerem, uzyskał dostęp do danych albo wkradł się na konto bankowe. Phishing może być też wysyłany SMS-em albo przez popularne komunikatory internetowe, wówczas najczęściej hakerzy celują w przejęcie danych logowania do konta bankowego.

OCHRONA PRZED CYBERATAKAMI

Jak być bezpiecznym online

Stosuj silne hasła
Do każdego serwisu internetowego używaj innego hasła składającego się z małych i dużych liter, cyfr oraz znaków specjalnych.

Twórz kopie zapasowe danych
Przechowuj ją w innej lokalizacji, np. na dysku zewnętrznym albo w chmurze.

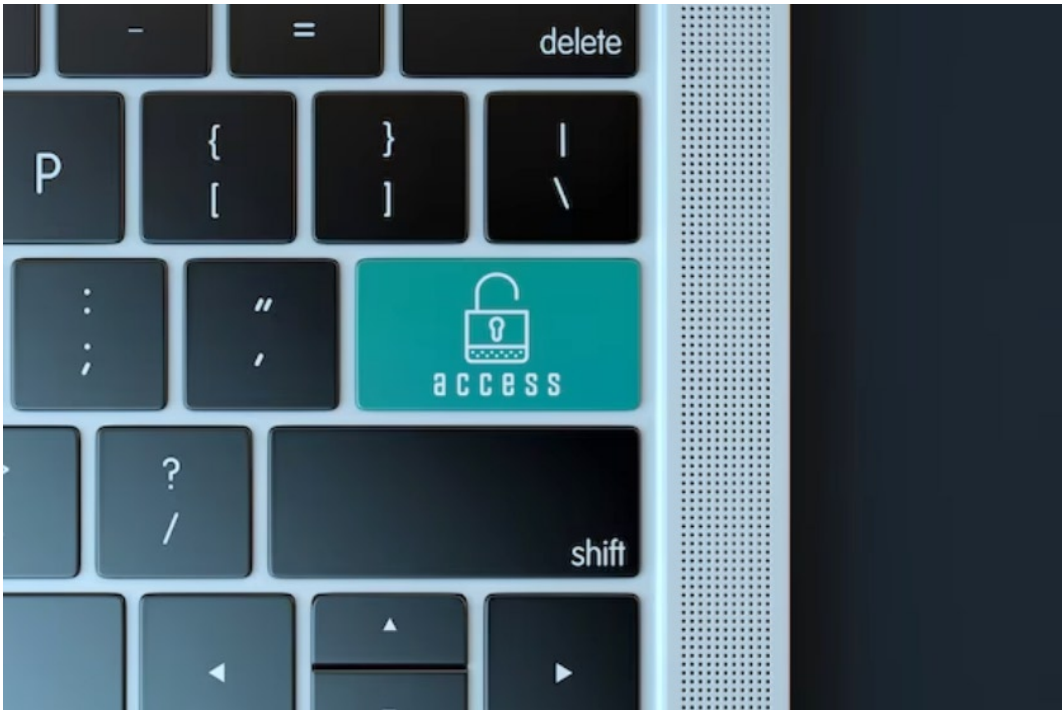
Uważaj na phishing
Nie klikaj w podejrzane maile oraz załączniki. Sprawdzaj zawsze, kto jest nadawcą e-maili. Status przesyłek weryfikuj tylko na zaufanej stronie www.

Korzystaj z chmury danych
To wbrew pozorom bezpieczniejsze rozwiązanie niż dysk lokalny.

Sprawdź ustawienia prywatności
Kto ma dostęp do Twojego komputera? Kto widzi Twoje posty w mediach społecznościowych? Czy masz silne hasło do komputera?

Chroń urządzenia programem antywirusowym
Systematycznie aktualizuj system antywirusowy oraz system operacyjny. Tam gdzie to możliwe, stosuj uwierzytelnianie dwuskładnikowe.

Stosuj systemy ochrony sieciowej
Zapory ogniowe są częścią systemów operacyjnych i dobrych programów antywirusowych. Stosuj min. 16-znakowe hasła do internetu domowego.



Insider threats, czyli jak chronić dane przed zagrożeniami wewnętrznymi

Zagrożeniem dla bezpieczeństwa danych medycznych nie są tylko hakerzy. Mogą nim być też pracownicy, którzy świadomie lub nieświadomi doprowadzają do wycieku danych. Podpowiadamy, jak zapobiegać tzw. insider threats.

Co to jest „insider threat”?

Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) definiuje zagrożenie wewnętrzne jako sytuację, gdy osoba z wewnątrz organizacji wykorzystuje swój autoryzowany dostęp, celowo lub nieumyślnie, aby wyrządzić szkodę w zasobach informacyjnych.

Najczęściej występującymi formami jest szpiegostwo, sabotaż, kradzież i cyberatak. Ale insder threats nie muszą być zamierzone i często wynikają z niewiedzy i błędów. To może być pomyłka w adresie e-mail i przypadkowe wysłanie dokumentacji medycznej do nieuprawnionej osoby, nieumyślne kliknięcie linka lub otwarcie załącznika w wiadomości phishingowej, niewłaściwa utylizacja dokumentów.

Czy placówki ochrony zdrowia są zagrożone?

Tak jak każda inna organizacja, także szpitale i przychodnie są narażone na wewnętrzne ataki. W ochronie zdrowia mogą one przybierać subtelne formy jak manipulacja danymi pacjenta w celu ukrycia błędu medycznego albo danymi rozliczeniowymi, aby uzyskać większą kwotę refundacji. Często wynikają z niewiedzy (wysyłanie dokumentacji pacjenta np.

Szczegóły o stanie zdrowia polityków i celebrytów są ulubionym tematem prasy bulwarowej. Źródłem danych są insiderzy, którzy sprzedają je albo ujawniają nieświadomie osobom nieuprawnionym (np. dziennikarze). Tego typu doniesienia mogą skończyć się sprawą w sądzie o naruszenie prywatności, cierpi też wizerunek placówki

mailem lub klikanie na niezweryfikowane linki w wiadomościach e-mail).

Jeszcze innym szkodliwym działaniem jest użycie danych pacjenta do celów innych niż leczenie oraz przekazanie ich nieuprawnionej osobie. Klasycznym przykładem jest sytuacja, gdy znana lub popularna osoba przebywa w szpitalu i do mediów przedostają się informacje o jej stanie zdrowia, a nawet zdjęcia. Są one przekazywane przez tzw. insidera, czyli człowieka z wewnątrz organizacji.

W ochronie zdrowia zdecydowanie rzadziej dochodzi – ze względu na charakter gromadzonych danych – do kradzieży danych strategicznych i biznesowych w celach konkurencyjnych albo działania o charakterze szpiegowskim.

Rodzaje zagrożeń wewnętrznych

Pod względem czynnika intencyjności, amerykańska CISA wyodrębnia 5 typów zagrożeń wewnętrznych:

- **Z zaniedbania.** Pracownik naraża organizację na zagrożenie przez nieostrożność. Mimo znajomości zasad bezpieczeństwa IT, dana osoba je ignoruje, stwarzając ryzyko dla organizacji. Przykładem jest przekazanie innemu pracownikowi hasła dostępu do systemu IT, zapisywanie danych z kartoteki pacjenta na nośniku USB, ignorowanie komunikatów o konieczności zainstalowania nowych aktualizacji i poprawek zabezpieczeń;
- **Przypadkowe.** Osoba mająca dostęp do informacji poufnych omyłkowo powoduje niezamierzone ryzyko dla organizacji. Najczęstszym przykładem jest nieumyślne kliknięcie hiperłącza lub otwarcie załącznika w wiadomości phishingowej zawierającej złośliwe oprogramowanie;
- **Intencjonalne.** Zagrożenia celowe to działania podejmowane w celu zaszkodzenia organizacji dla osobistych korzyści lub działania z takich pobudek jak zemsta czy zazdrość. Na przykład, pracownik, który czuje się traktowany w nieodpowiedni sposób (brak awansu albo premii) lub zostaje zwolniony dopuszcza się kradzieży zastrzeżonych danych.

Choć nie można ich wykluczyć, w placówkach zdrowia rzadkością są dwa pozostałe typy zagrożeń, czyli **zagrożenia w zmowie** (jeden lub więcej insiderów współpracuje z zewnętrznym podmiotem) oraz **zagrożenia ze strony osób trzecich** (nie będących pracownikami organizacji, ale którym przyznano dostęp do np. sieci i systemów IT, jak przykładowo firmy serwisujące sprzęt).

Ile zaufania, a ile kontroli, aby chronić skutecznie dane?

Zagrożenia wewnętrzne są nieuniknionym skutkiem ubocznym tego, że organizacja ufa swoim pracownikom, udzielając im dostępu do danych niezbędnych do wykonywania pracy. Dlatego są o wiele trudniejsze do wykrycia i monitorowania niż ataki hakerów z zewnątrz, wymagające przełamania barier cyberbezpieczeństwa.

Podstawą minimalizacji insider threats jest opracowanie odpowiedniego programu profilaktycznego, podobnie jak organizacja powinna dysponować strategią ochrony danych przed hakerami. Od razu warto zaznaczyć, że celem nie jest stworzenie kultury kontroli i braku zaufania – takie podejście nie zmniejszy zagrożeń, a jedynie doprowadzi do erozji zaufania, toksycznej kultury organizacyjnej i w efekcie – pogorszenia morale pracowników i jakości obsługi pacjenta.

Strategia tłumienia zagrożeń wewnętrznych powinna uwzględniać takie elementy jak:

- **Kontrola dostępu do danych.** Polega ona na określeniu ról pracowników i na ich podstawie przypisaniu w systemach IT uprawnień do wglądu do danych. Obowiązującą jest zasada minimalnych uprawnień – na początek odblokowywany jest dostęp do tych funkcji i informacji, które są niezbędne do wykonywania zadań, a potem się je rozszerza w miarę potrzeb;
- **Monitorowanie użytkowników.** W systemach IT są to np. dzienniki logowania dostępne z pozycji administratora. O takiej kontroli higieny informatycznej powinni być poinformowani pracownicy. Należy także analizować

nietypowe zachowania, jak pobieranie dużej ilości danych, podejrzanie częste logowania itd.;

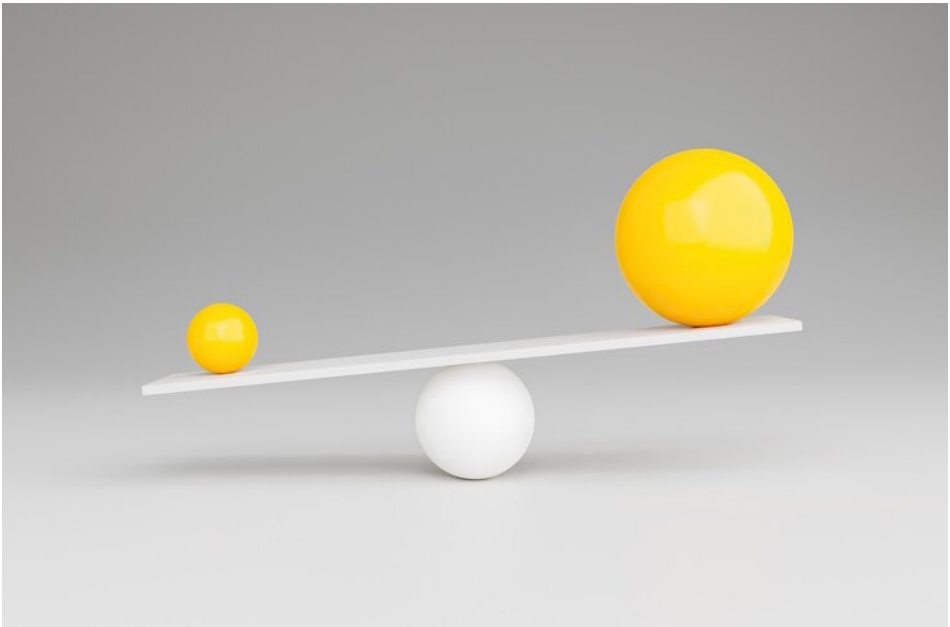
- **Systematyczne sprawdzanie jakości wprowadzanych danych** przez administratorów systemu IT, co jest elementem psychologicznym skłaniającym do zachowania higieny zapisu danych;
- **Blokowanie potencjalnie niebezpiecznych zachowań**, jak przykładowo portów USB (można to zrobić z poziomu administratora sprzętu);
- **Szkolenie pracowników.** Podnoszenie kompetencji cyfrowych i aktualizacja wiedzy z zakresu cyberbezpieczeństwa. System szkoleń powinien uwzględniać zagrożenia zewnętrzne i wewnętrzne;
- **Opracowanie planów reagowania na incydenty.** Scenariusze dochodzenia do źródła wewnętrznych wycieków danych, plan usuwania skutków oraz komunikacji kryzysowej;
- **Stworzenie białej i czarnej listy.** Określenie, co można robić na danym stanowisku pracy (np. tylko używanie systemu gabinetowego bez dostępu do internetu);
- **Podnoszenie kwalifikacji** osób odpowiedzialnych za monitorowanie i zapobieganie zagrożeniom wewnętrznym. W większości przypadków będzie to dział IT;
- **Przygotowanie procedur onboardingu i offboardingu.** Nowi pracownicy muszą znać zasady bezpiecznego przetwarzania danych i dostępu do zasobów informatycznych. Gdy pracownicy zmieniają miejsce pracy, należy na czas odbierać im dostęp do danych;
- **Wprowadzenie systemu zgłaszania nieprawidłowości**, przykładowo za pomocą anonimowych ankiet;
- **Uruchomienie uwierzytelniania dwuskładnikowego** dla krytycznych systemów, jak poczta e-mail, intranet, VPN itd.;
- **Przeprowadzanie wewnętrznych i zewnętrznych audytów zarządzania informacją.** Pozwalają one testować wdrożone procedury i zabezpieczenia danych;

– **Dokumentowanie wykrytych nieprawidłowości** dla celów dowodowych w przypadku naruszenia prawa oraz dla organów kontrolnych, jak np. Urząd Ochrony Danych Osobowych.

Najbardziej skrajne formy, jak badania psychologiczne, audyt życiorysu, kamery i wywiady środowiskowe stosowane są jedynie w organizacjach o strategicznym znaczeniu dla państwa narażonych na np. ryzyko szpiegostwa. Dlatego nie są stosowane w ochronie zdrowia..

Ufaj, ale sprawdzaj

Każda organizacja ochrony zdrowia musi bazować na wysokim zaufaniu do pracowników. Inaczej trudno sobie wyobrazić stworzenie pozytywnej i motywującej kultury pracy. Ale zaufanie nie wyklucza elementów kontroli, które nie są wymierzone przeciwko pracownikom, ale tworzone w trosce o dobro pacjentów, ochronę ich danych i prywatności. Tak jak w przypadku ochrony przed cyberprzestępcami, minimalizacja ryzyka ataków wewnętrznych wymaga stosowania wielowarstwowego systemu: nawet jeśli jedna warstwa zawiedzie, kolejna może zadziałać. ●



Wdrażając politykę zapobiegania zagrożeniom wewnętrznym, trzeba zachować równowagę pomiędzy zaufaniem do pracowników a kontrolą

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 phisingowych, 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 przez 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.

Zabezpieczenia techniczne w walce z hakerami

Zdaniem Jarosława Olejnika, dyrektora Biura Bezpieczeństwa Informacji i Ciągłości Działania w Centrali NFZ, menedżerowie szpitali powinni inwestować w technologie ułatwiające monitorowanie bezpieczeństwa infrastruktury IT, identyfikowanie zagrożeń w środowisku IT oraz wykrywanie cyberzagrożeń.

Wśród nich są takie rozwiązania informatyczne jak:

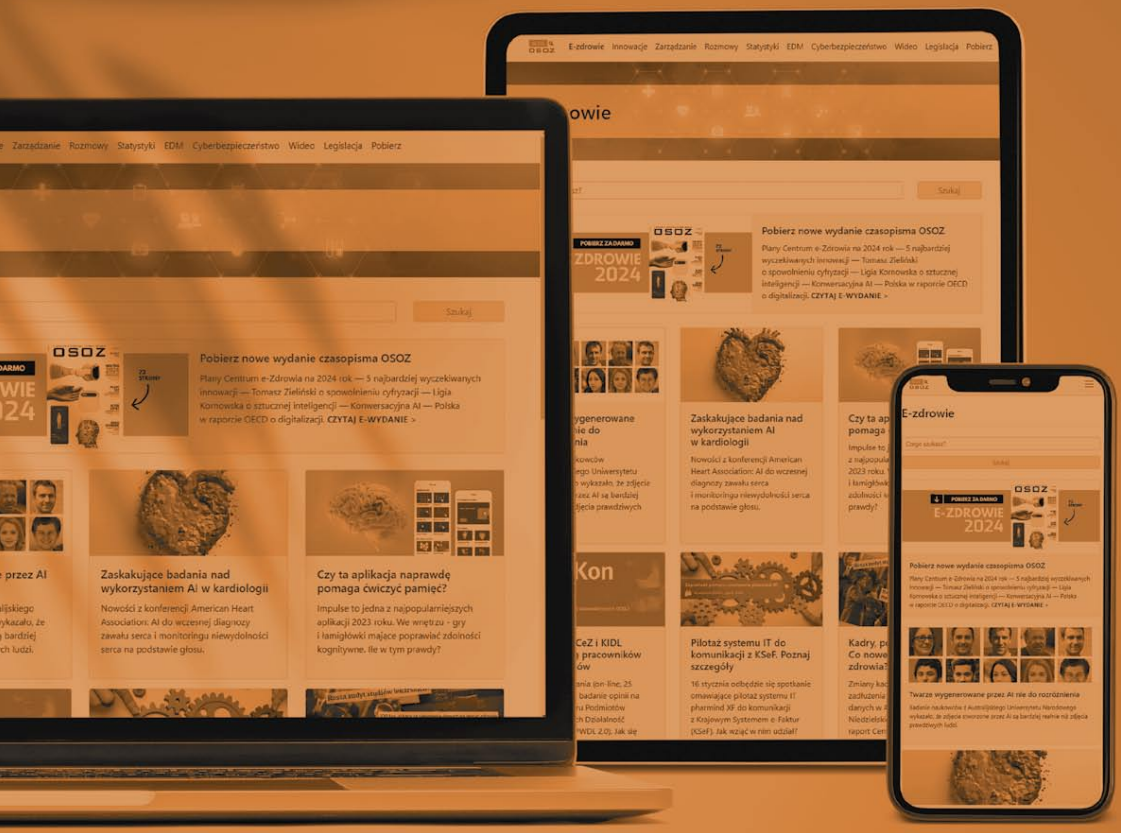
- **SIEM** (Security Information and Event Management) – systemy zbierające oraz analizujące informacje o incydentach, błędach i podatnościach w czasie rzeczywistym;
- **EDR** (Endpoint Detection and Response) – narzędzia służące wykrywaniu i reagowaniu na podejrzane aktywności w infrastrukturze IT;
- **IPS/IDS** (Intrusion Prevention System/Intrusion Detection System) – technologia bezpieczeństwa sieciowego, która stale monitoruje ruch sieciowy pod kątem podejrzanej aktywności i podejmuje kroki w celu zapobiegania zagrożeniom.

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 i najpewniejszą 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 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.

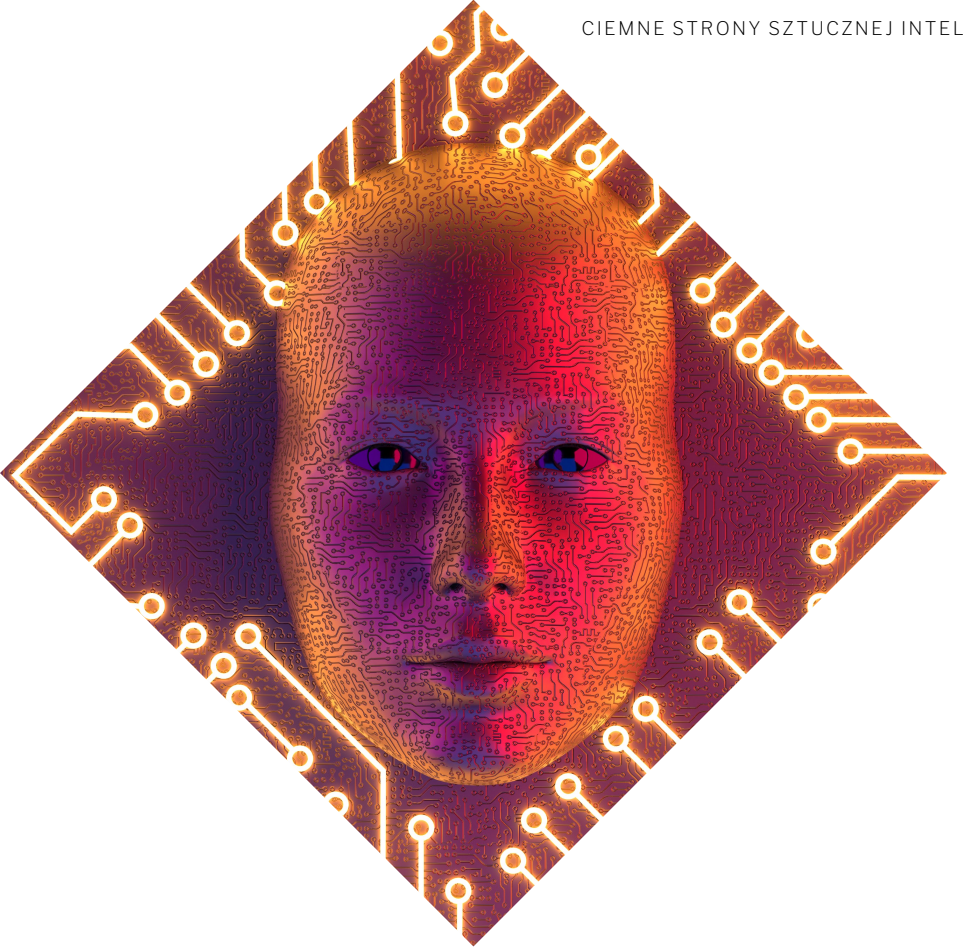


Nowy blog o e-zdrowiu

Praktyczne porady
Informacje z rynku zdrowia
Inspirujące wywiady

BLOG
OSOZ
blog.osoz.pl

ZESKANUJ KOD,
aby przejść do bloga



Raport: AI i dezinformacja na liście największych zagrożeń dla świata

Najnowszy raport Globalnych Ryzyk ostrzega przed skutkami niekontrolowanego rozwoju sztucznej inteligencji oraz manipulacją treściami z pomocą AI.

» Świat jest nękany przez triadę niebezpiecznych kryzysów: klimatyczny, zbrojny i gospodarczy. Do tego dochodzi teraz AI. «

Publikowany podczas Światowego Forum Ekonomicznego w Davos *Global Risk Report*, bierze pod lupę największe zagrożenia dla ludzkości w perspektywie 2- i 10-letniej. Od lat na czołowych miejscach są skutki zmian klimatycznych w postaci ekstremalnych zjawisk pogodowych, zanikającej bioróżnorodności, zapaści ekosystemu środowiska czy deficytu zasobów naturalnych.

Niebezpieczeństwa technologiczne

19. edycja raportu dużo miejsca poświęca zmianom technologicznym i ich wpływowi na społeczeństwo, w tym mediom społecznościowym i AI. Technologia znacznie ułatwia nasze życie i prowadzi do postępów w medycynie, ale ma też drugą, destruktywną stronę: Internet stał się miejscem swobodnego rozpowszechniania szkodliwych dla zdrowia i niebezpiecznych dla demokracji teorii spiskowych, koncentracja narzędzi sztucznej inteligencji jak ChatGPT w rękach kilku światowych koncernów może potencjalnie doprowadzić do uzależnienia od ich technologii, a generatywna AI wykorzystywana przez cyberprzestępców do generowania fake newsów zagraża bezpieczeństwu danych i prywatności.

Znajdujemy się w erze nowego wyścigu mocarstw – już nie zbrojeń, ale AI. Ten doprowadzi do nowego porządku geopolitycznego i gospodarczego, a głównymi graczami stają się Chiny i USA, które w imię rozwoju nowych technologii i wynikającego z niego wzrostu gospodarczego są gotowe – w przeciwieństwie do Europy – poświęcić takie wartości jak prywatność danych.

Dezinformacja to nie tylko dziwne teorie spiskowe. Niektóre fake newsy mogą nawet zagrażać życiu i zdrowiu (poprzez wprowadzanie w błąd opinii publicznej np. w kwestii szczepień), wpływać na wybory polityczne, zniekształcać kursy giełdowe. Powodują też pogłębiającą się nieufność wobec informacji, mediów i rządów jako źródeł wiedzy. Są odpowiedzialne za polaryzację poglądów i radykalizację. W ten sposób powstaje błędne koło, które może wywołać niepokoje społeczne.

Łatwe w użyciu interfejsy modeli sztucznej inteligencji (AI), których zastosowanie nie wymaga już trudnych do zdobycia umiejętności, spowodują eksplozję sfałszowanych informacji i tak zwanych „syntetycznych" treści: od zmanipulowanych nagrań wideo (tzw. deep fake) po fałszywe strony internetowe. Państwa na całym świecie dopiero rozpoczynają prace nad uregulowaniem AI. Dołączają do nich także kraje, które dotychczas bardzo liberalnie podchodziły do AI. Na przykład obowiązujące w Chinach wymogi dotyczące oznaczania znakiem wodnym treści generowanych przez sztuczną inteligencję mają pomóc w identyfikacji fałszywych informacji. Prezydent USA Joe Biden wydał rozporządzenie wykonawcze w sprawie AI, Europa wdraża w życie swój EU AI Act.

Jest jednak mało prawdopodobne, aby tempo rozwoju i skuteczność regulacji dorównały tempu ewolucji technologicznej.

Kategorie ryzyka

Ekonomiczne | Środowiskowe | Geopolityczne | Społeczne | Technologiczne

2 lata

1. **Dezinformacja i fake newsy**
2. Ekstremalne zjawiska pogodowe
3. Polaryzacja społeczna
4. **Cyber-zagrożenia**
5. Konflikt zbrojny
6. Brak perspektyw społecznych
7. Inflacja
8. Przymusowa migracja
9. Kryzys ekonomiczny
10. Zanieczyszczenie powietrza

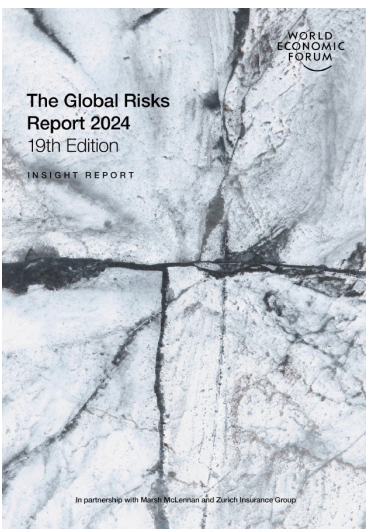
10 lat

1. Ekstremalne zjawiska pogodowe
2. Krytyczne zmiany na Ziemi
3. Zanikająca bioróżnorodność i zapaść ekosystemów
4. Deficyt zasobów naturalnych
5. **Dezinformacja i fake newsy**
6. **Skutki uboczne sztucznej inteligencji**
7. Przymusowa migracja
8. **Cyber-zagrożenia**
9. Polaryzacja społeczna
10. Zanieczyszczenie powietrza

Sztuczna inteligencja wpłynie na rynek pracy, doprowadzając do zaniku niektórych zawodów i rozwoju nowych, wymagających jednak zaawansowanych umiejętności inżynierii danych. Samodoskonalące się modele generatywnej sztucznej inteligencji mają coraz większą moc, wywołując zmiany w strukturach społeczno-ekonomicznych. Nie wiadomo jeszcze, kiedy będą na tyle potężne, że będzie można mówić o sztucznej ogólnej inteligencji (AGI, od ang. Artificial General Intelligence) będącej w stanie przejąć każde zadanie wykonywane obecnie przez człowieka. Wśród zagrożeń AGI wymienia się wyrafinowane możliwości tworzenia treści deep fake, utratę pracy przez niektóre grupy zawodowe, cyberataki, dyskryminację wynikającą z danych szkoleniowych, wykorzystanie AI do działań wojennych (tzw. broń autonomiczna).

Klasyczna AI nie stwarzała do tej pory takiego zagrożenia, bo jej możliwości były mocno ograniczone i wymagała dużego zaangażowania człowieka. To może się jednak szybko zmienić wraz z tym, jak modele takie jak GPT-4 chłoną miliardy danych z całego świata.

Raport wzywa do radykalnych działań mających na celu zminimalizowanie ryzyk technologicznych, w tym do większej regulacji AI i wprowadzenia narzędzie wykrywania i usuwania z internetu tzw. deep fake'ów.



Raport Globalnych Ryzyk 2024 ma ostrzegać przed zagrożeniami dla ludzkości i skłaniać rządy na całym świecie do podejmowania działań, aby im zapobiec

Nowe zagrożenia cybernetyczne oparte na sztucznej inteligencji

Sztuczna inteligencja pisze teksty, tworzy grafiki, diagnozuje pacjentów. Ma też ciemną stronę: z jej pomocą cyberprzestępcy są tak skuteczni, jak nigdy dotąd. Co trzeba wiedzieć o nowych metodach kradzieży danych z pomocą AI?

Choć algorytmy AI są od dawna wykorzystywane do łamania zabezpieczeń systemów IT, hakerzy od kilku miesięcy mają do dyspozycji nową broń: generatywną sztuczną inteligencję. Dla placówek medycznych już teraz mających zaległości w bezpieczeństwie cybernetycznym to bardzo zła wiadomość.

Liczba ataków hakerów na podmioty ochrony zdrowia rośnie systematycznie od kilku lat. Szpitale znajdują się w potrzasku: nie mają środków na inwestycje w cyberbezpieczeństwo, coraz trudniej im znaleźć ekspertów IT, którzy zgodziliby się na pracę za mniejsze pieniądze niż w innych branżach, a do tego o dużo większej odpowiedzialności (stawką jest często życie i zdrowie pacjentów). To oznacza, że obecnie stosowane systemy ochrony danych są zupełnie nieprzygotowane na AI w rękach hakerów.

Wirus napędzany AI zmienia się jak kameleon

Generatywna sztuczna inteligencja, jak ChatGPT, z powodzeniem pomaga hakerom indywidualizować i automatyzować ataki. Może generować miliony maili w różnych językach, dopasowanych do profilu kulturowego regionu świata. Stosowana jest do przygotowywania przekonujących wiadomości e-mail, personalizowanych do stylu osoby lub organizacji, pod którą podszywa się haker.

Coraz powszechniejszą formą ataku jest przykładowo zamieszczanie na YouTube lub w mediach społecznościowych filmów o popularnej tematyce, generowanych przez AI, odsyłających na zainfekowaną stronę www. Jednak największym zagrożeniem są nowej generacji ataki phishingowe. Systemy AI potrafią dzisiaj podrobić nie do poznania głos na podstawie kilkusekundowej próbki i płynnie prowadzić rozmowę telefoniczną. W ten sposób hakerzy są w stanie sfabrykować telefon z NFZ z prośbą o weryfikację danych albo od dyrektora placówki.

Oto cztery grupy cyberataków realizowanych z wykorzystaniem AI:

APT (Advanced Persistent Threat). Wyrafinowany, długotrwały i wielostopniowy cyberatak nakierowany na konkretną organizację lub osobę. Haker wkrada się do sieci, pozostając przez długi czas w ukryciu w celu kradzieży poufnych danych. W tym przypadku system sztucznej inteligencji jest stosowany do maskowania obecności cyberprzestępcy. Systemy AI

o dużej mocy mogą szybciej i skuteczniej niż ludzie atakować zasoby informatyczne oraz łamać hasła.

Phishing. Hakerzy stosują systemy AI do przetwarzania języka naturalnego, tworząc doskonale spersonalizowane wiadomości e-mail mające na celu nakłonienie osób do ujawnienia poufnych informacji. To może być też e-mail informujący o konieczności wyjaśnienia sprawy przez telefon – gdy ofiara zadzwoni pod wskazany numer, rozmowę prowadzi system AI.

Ataki typu deepfake. W tym przypadku sztuczna inteligencja jest wykorzystywana do generowania syntetycznych filmów lub nagrań audio. Dzięki tej technologii hakerzy mogą podszyć się pod zaufane osoby, jak administratorów sieci albo osoby z zarządu. Od czasu pojawienia się systemów generatywnej AI, przygotowanie ataków deepfake stało się dziecinnie proste.

Złośliwe oprogramowanie. Najsłabszym ogniwem klasycznych wirusów jest to, że gdy zostaną zidentyfikowane przez ekspertów cyberbezpieczeństwa, szybka aktualizacja programów antywirusowych pozwala skutecznie ograniczyć ich siłę rażenia. Taki program działa podobnie na każdym z milionów komputerów, który infekuje. Jednak wirusy wyposażone w elementy AI uczą się kamuflować i dostosowują sposób działania do określonej sytuacji, komputera, zachowań użytkownika.

Każdy może być hakerem

Jednak największym zagrożeniem bezpieczeństwa może być inny trend: dzięki sztucznej inteligencji każda osoba, która ma złe intencje, może z łatwością wygenerować i spersonalizować złośliwe oprogramowanie, w kilka sekund wygenerować wideo typu deep fake korzystając darmowych programów.

Minęły czasy, kiedy haker był wyjątkowo uzdolnionym informatykiem potrafiącym włamać się do najlepiej zabezpieczonych systemów. Wirusa może dzisiaj wygenerować

W lutym 2024 roku Open AI – twórca Chat-GPT – przedstawił nowy model AI, który pozwala tworzyć realistyczne filmy (na razie 60-sekundowe) na podstawie opisów. Zaskakują jakością, wiernym odwzorowaniem obrazu, dokładnością detali i kreatywnością AI

Kliknij na grafikę, aby zobaczyć, co potrafi Sora

laik, który uzyska dostęp do Darknetu (ukryta część internetu zawierająca nielegalne zasoby) albo dołączy do grupy hakerów w pozbawionym kontroli komunikatorze Telegram. Nowa generacja hakerów nie ma skrupułów. Nieważne czy atakowany system należy do banku czy szpitala – liczy się szybki zysk.

Do tego jeszcze dochodzi nowa sytuacja geopolityczna. W tle wojny w Ukrainie toczy się wojna w sieci. Liczba ataków rosyjskich lub prorosyjskich grup hakerów – takich jak Killnet czy Crop – na ochronę zdrowia wzrosła kilkukrotnie od lutego 2022, kiedy rozpoczęła się rosyjska inwazja.

AI zagraża i chroni

Z pomocą AI hakerzy doskonalą swoje metody działania. Ale sztuczna inteligencja pozwala jednocześnie lepiej chronić zasoby danych przed atakami.

Programiści korzystają z niej do wykrywania potencjalnych luk bezpieczeństwa. Algorytmy sprawiają, że filtry spamowe są w stanie zidentyfikować najbardziej wyrafinowane ataki phishingowe. Specjaliści bezpieczeństwa i eksperci IT w organizacjach sięgają do systemów cyberbezpieczeństwa opartych na AI, które przeczesują zasoby sieciowe i informatyczne w celu wykrycia słabych punktów bezpieczeństwa, przewidywania ataków oraz identyfikacji prób ataków. Potrafią w trybie ciągłym inwentaryzować i testować szczelność systemu informacyjnego i doskonalić metody obrony.

Możliwości zastosowania AI do wzmocnienia zabezpieczeń nie powinny jednak usypiać czujności. Nawet giganci nowych technologii, jak OpenAI – twórca ChatGPT – padają ofiarą ataków cyberprzestępców i to pomimo dużych inwestycji w systemy bezpieczeństwa cybernetycznego.

Dla podmiotów ochrony zdrowia oznacza to konieczność szybkiej aktualizacji procedur bezpieczeństwa danych. Konieczna staje się intensyfikacja szkoleń dla pracowników, aby wszyscy wiedzieli, jak bronić się przed atakami hakerów korzystających z AI – zwłaszcza typu phishing, które nadal stanowią największe zagrożenie cybernetyczne.

Fake newsy tworzone przez AI zalewają internet. Infodemia jest śmiertelnie niebezpieczna

Wypowiedzi fikcyjnych ekspertów, zmanipulowane zdjęcia i sfałszowane prace naukowe służą do rozpowszechniania nieprawdziwych informacji o lekach, szczepieniach oraz terapiach. Dzięki sztucznej inteligencji ich odróżnienie od faktów staje się coraz trudniejsze.

Grafika: Midjourney

Kłamstwo podparte dowodami

Barack Obama jako chirurg, Emmanuel Macron i Ursula von der Leyen jako lekarze oraz Theresa May jako pielęgniarka – sztuczna inteligencja jest w stanie wygenerować trudne od odróżnienia od prawdziwych fotografie. To może być też Bill Gates na spotkaniu z prezydentem Chin i USA w tajnym laboratorium, aby uzasadnić globalną teorię spiskową dotyczącą pandemii COVID-19. Albo filmy wideo pokazujące autorytety medyczne rzekomo polecające niesprawdzone naukowo terapie, a nawet zdjęcia polityków w rolach personelu medycznego, jak w naszym przykładzie.

Choć wyglądają realnie, łatwo się domyślić, że są sfałszowane – większość z nas wie, że to przecież były Prezydent USA, Przewodnicząca Komisji Europejskiej, Prezydent Francji i była Premier Wielkiej Brytanii. Problem pojawia się wówczas, gdy trudno zweryfikować prawdziwość informacji albo nie mamy na to czasu w natłoku informacji. Przykład: Ursula von der Leyen jest rzeczywiście z wykształcenia lekarzem.

Każdy może wpaść w echo chamber

Fake newsy przybierają czasami subtelniejszą formę np. pytań, na które nauka nie ma odpowiedzi, niemożliwych do spełnienia oczekiwań wobec medycyny, danych dobieranych pod z góry ustaloną tezę.

Podważanie dowodów naukowych nie jest niczym nowym. Przykładowo, w latach 50-tych przemysł tytoniowy robił wszystko, aby zdyskredytować badania dotyczące związku raka płuc z paleniem papierosów. Dzisiaj, dzięki internetowi i sztucznej inteligencji, bez ograniczeń można rozpowszechniać fałszywe lub wprowadzające w błąd informacje. W ich pułapkę może wpaść każdy, zwłaszcza w mediach społecznościowych. Jedno nieświadome polubienie informacji, zdjęcia lub filmu z fake newsem na Facebooku, Instagramie, Tik Toku albo YouTubie powoduje, że algorytmy AI zaczną wyświetlać podobne posty, odfiltrowując te krytyczne. Wówczas

użytkownik wpada w tzw. echo chamber (komorę echa), gdzie jego opinia jest manipulowana emocjonalnymi przekazami.

Błędne decyzje medyczne, malejące zaufanie

Infodemia zbiera śmiertelne żniwo, gdy osoba chora odmawia leczenia sięgając po „cudowne środki", albo nie chce się zaszczepić, czego doświadczyliśmy podczas pandemii COVID-19. Dokładna skala zgonów spowodowanych fake newsami nie jest znana, bo zjawisko trudno zbadać. Kanadyjskie badanie sugeruje, że fałszywe informacje o szczepieniach przeciwko COVID-19 doprowadziły do odmowy lub opóźnienia szczepień u 2,35 mln Kanadyjczyków, czego efektem było 2800 możliwych do uniknięcia zgonów i koszty ok. 300 mln USD tytułem dodatkowych hospitalizacji.

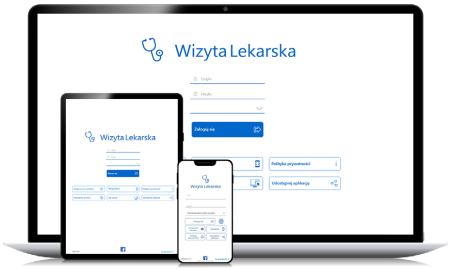
Problem narasta także w Polsce. Według informacji Narodowego Instytutu Zdrowia Publicznego – Państwowego Zakładu Higieny, w ostatnich 5 latach liczba uchyleń od obowiązkowych szczepień niemal się podwoiła – z 40,3 tys. w 2018 roku do 72,7 tys. w 2022 roku. Na przestrzeni 10 lat, wzrost jest dziesięciokrotny.

Nawet jeśli fake newsy nie powodują bezpośredniego zagrożenia dla życia lub zdrowia, mają niszczący wpływ na medycynę: spada zaufanie do lekarzy i nauki, podważane są kompetencje pracowników medycznych, pacjenci nie stosują się do zaleceń, maleje autorytet instytucji publicznych. Lekarze alarmują, że podczas wizyt muszą prostować przeczytane przez pacjentów w internecie informacje, a nawet spotykają się z bezpośrednią agresją. Pokonanie infodemii nie będzie łatwe. Eksperci apelują m.in. aby już od najmłodszych lat uczyć, jak rozróżniać fake newsy od faktów naukowych.

KAMSOFT

Pracuj mobilnie!

Wizyta domowa?
Potrzebna pilnie e-Recepta?
- sięgnij po Wizytę Lekarską.



Wizyta Lekarska to idealne rozwiązanie dla lekarzy, którzy cenią sobie łatwe w obsłudze, intuicyjne aplikacje z wieloma możliwościami.

Zarządzanie czasem przeznaczonym na wizyty.
Zaplanowane wizyty w aplikacji widoczne są w kalendarzu Google na Twoim urządzeniu mobilnym.

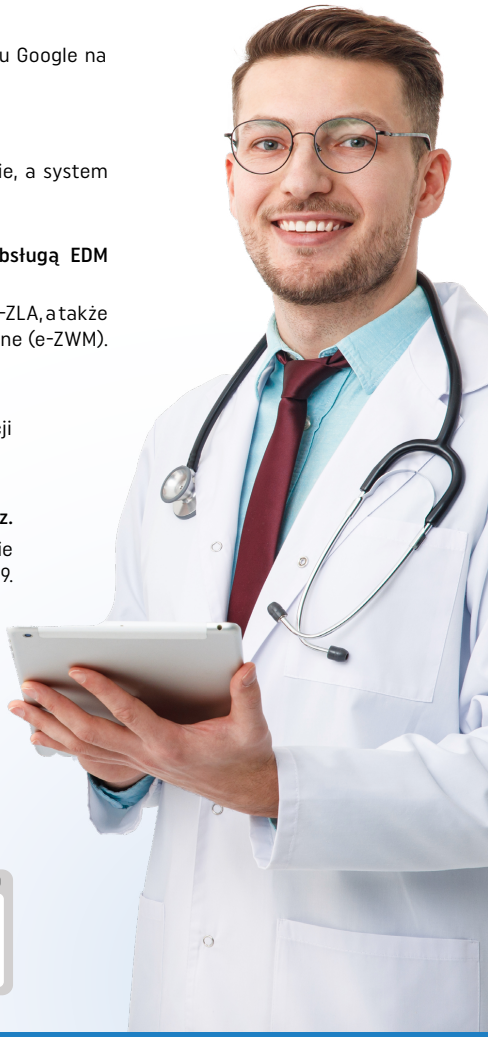
Wygodne i szybkie wystawianie e-Recept.
Wbudowany katalog leków KS-BLOZ ułatwia wyszukiwanie, a system podpowiedzi skraca czas wystawiania e-Recepty.

Wgląd w historię medyczną pacjenta wraz z pełną obsługą EDM niezależnie od miejsca i czasu.
Za pomocą aplikacji wystawisz e-Receptę, e-Skierowanie, e-ZLA, a także elektroniczne zlecenie na zaopatrzenie w wyroby medyczne (e-ZWM).

Oszczędność czasu.
Możliwość kopiowania, weryfikacji i edycji dokumentacji pacjenta z poprzedniej wizyty.

Dostęp do aktualnej bazy wiedzy kiedy tylko potrzebujesz.
Potrzebną wiedzę masz pod ręką, dzięki wbudowanej bazie wiedzy o lekach KS-BLOZ oraz rozpoznań ICD-10 i procedur ICD-9.

Współpraca z systemami gabinetowymi KAMSOFT.
Aplikacja Wizyta Lekarska zintegrowana jest z systemami medycznymi KS-SOMED, KS-PPS oraz SERUM.



Już teraz możesz zapoznać się z aplikacją Wizyta Lekarska - pobierz bezpłatną wersję demonstracyjną

Wizyta Lekarska
KAMSOFT S.A.

Pobierz z witryny Microsoft | POBIERZ Z Google Play | Pobierz w App Store

WERSJA DEMO

medycyna@kamsoft.pl
www.kamsoft.pl

Kim jest i dlaczego placówki medyczne potrzebują CMIO?

Dyrektor ds. Informacji Medycznej (Chief Medical Information Officer, CMIO) lub inaczej Dyrektor ds. Informatyki Medycznej pełni rolę pomostu pomiędzy obszarem medycyny i IT. Dlaczego warto stworzyć takie stanowisko w podmiocie leczniczym?

Lekarz i pasjonat e-zdrowia w jednym

CMIO to najczęściej lekarz, który posiada zainteresowania związane z nowymi technologiami w ochronie. Taka osoba nie musi mieć specjalnego wykształcenia, ale powinna orientować się w tematach związanych z e-zdrowiem.

W większości organizacji, CMIO nadal pełni rolę lekarza, kontynuując pracę z pacjentami. W zakresie dodatkowych kompetencji znajduje się zarządzanie i monitorowanie procesów digitalizacji, we współpracy z dyrektorem placówki i działem IT.

W klasycznym podejściu, to dział informatyki był dotąd odpowiedzialny za całość IT w organizacji ochrony zdrowia. Taki model utrwalił się w latach 90-tych – wiedzę o systemach IT posiadali tylko i wyłącznie informatycy, temat e-zdrowia był jeszcze mało znany, a informatyzacja ograniczała się do wdrażania prostych systemów do rozliczeń z płatnikami.

Jednak wraz z postępującą digitalizacją sektora zdrowia, takie podejście przestało się sprawdzać. O ile dział IT posiada kompetencje techniczne, zadaniem CMIO jest strategiczne wdrażanie systemów IT, obserwowanie trendów cyfryzacji i zagwarantowanie, że digitalizacja wychodzi naprzeciw bieżącym i przyszłym potrzebom podmiotu leczniczego związanym przykładowo z celami jakościowymi. Inaczej mówiąc – CMIO jest architektem cyfryzacji, podczas gdy dział IT dba o to, aby każdy element architektury IT został dobrze przygotowany i wdrożony.

CMIO dyryguje procesem cyfryzacji

Zadaniem CMIO jest dopilnowanie, aby placówka dojrzewała cyfrowo, a wdrażane rozwiązania IT tworzyły jeden, harmonijnie funkcjonujący ekosystem wymiany informacji. Infrastruktura IT decyduje o przepływach pracy oraz zasobach danych, które mogą być wykorzystane w systemach inteligencji biznesowej oraz przyszłych rozwiązaniach stosujących sztuczną inteligencję.

Do głównych kompetencji CMIO należy:

- strategiczny rozwój dojrzałości cyfrowej;
- nadzorowanie integracji architektury IT i danych;

» CMIO jest strategiem digitalizacji podmiotu leczniczego. «

- bieżąca analiza wykorzystania technologii, takich jak elektroniczna dokumentacja medyczna (EDM), w celu określenia ich wpływu na opiekę nad pacjentem;
- ustalanie standardów w zakresie stosowania wewnętrznej terminologii medycznej;
- szkolenie lekarzy w zakresie korzystania z oprogramowania; badanie, w jaki sposób oprogramowanie jest wykorzystywane;
- współdecydowanie o tym, jakie narzędzia cyfrowe są wdrażane;
- współpraca z kierownictwem wyższego szczebla w celu monitorowania przepływów informacji i aktualizacji zasobów IT;
- monitorowanie jakości wprowadzanych danych oraz wąskich gardeł w procesach administracyjno-klinicznych związanych z systemami IT lub ich brakiem;
- konsultowanie z kierownictwem zaburzeń wynikających z wdrożonych rozwiązań IT;
- wczesne diagnozowanie potencjalnych braków związanych z ochroną danych;
- poprawa jakości procesów klinicznych dzięki wprowadzaniu odpowiednich rozwiązań e-zdrowia;
- konsultowanie potrzeb w zakresie szkoleń personelu;
- monitorowanie słabych ogniw architektury IT, które mogą zwiększać niebezpieczeństwo wycieku danych.

Każda placówka ma inne wyzwania i zadania dla CMIO

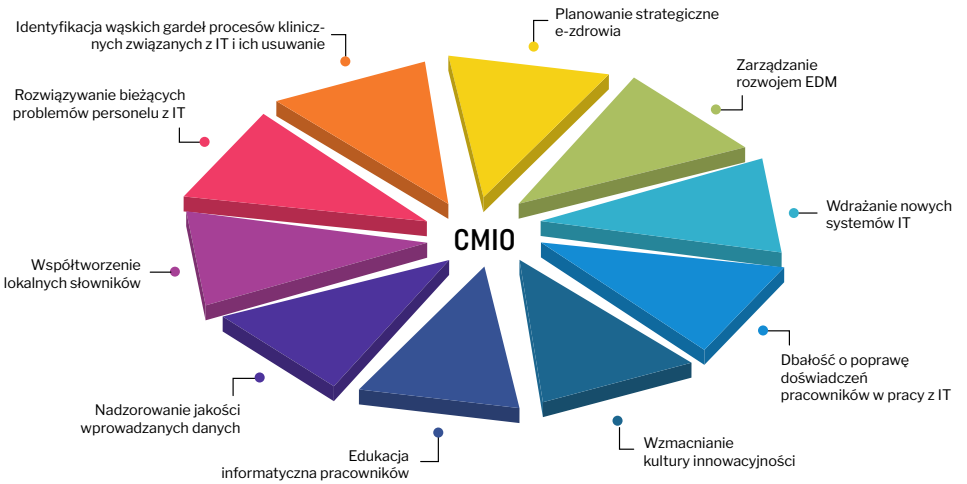
Stanowisko CMIO powinno podlegać bezpośrednio dyrektorowi placówki, bo ma wpływ na strategiczny rozwój placówki i inwestycje w IT. Kluczowym elementem jest tutaj zaufanie personelu do CMIO. Dlatego powinna być to osoba, która cieszy się dużym autorytetem w zakresie zarówno wiedzy klinicznej jak i technologicznej, empatyczna, rozumiejąca wyzwania personelu medycznego w obsłudze oprogramowania.

» Alternatywnie można utworzyć stanowisko Dyrektora ds. Cyfryzacji (CDO – Chief Digital Officer). CDO koordynuje zadania związane z transformacją cyfrową podmiotu. «

Rola Dyrektora ds. Informacji Medycznej nie jest sztywna i różni się w zależności od placówki. W dużych szpitalach może też obejmować np. współprojektowanie narzędzi typu business intelligence, wspierających proces podejmowania decyzji klinicznych. Z kolei w mniejszych przychodniach, głównym celem będzie harmonizacja rozwiązań IT z procedurami pracy, wsparcie personelu w problemach związanych z oprogramowaniem albo tworzenie innowacyjnej kultury pracy. CMIO jest jednocześnie rzecznikiem placówki w kwestiach związanych z informatyzacją. Aby być na bieżąco z trendami informatyzacji, powinien brać udział w konferencjach e-zdrowia.

Rola CMIO dla cyberbezpieczeństwa

Ochrona danych medycznych nie jest zadaniem CMIO, ale może on pełnić ważną rolę dodatkowego ogniwa systemu bezpieczeństwa, włączając element cyberbezpieczeństwa do strategii e-zdrowia. Będąc najbliżej personelu medycznego, orientuje się w problemach związanych z obsługą zasobów IT, jest w stanie wcześnie identyfikować potencjalne słabe punkty, współdecyduje o organizacji szkoleń z cyberbezpieczeństwa, orientuje się w nowych zagrożeń ze strony hakerów. Może też na bieżąco doradzać swoim współpracownikom, jak bezpiecznie przetwarzać dane medyczne i być wyczulonym na potencjalne ataki hakerów.



Dane w chmurze: bezpieczniej, wygodniej, perspektywicznie

Baza danych w chmurze zapewnia wyższy poziom cyberbezpieczeństwa, elastyczność rozbudowy zasobów pamięci, outsourcing trudno dostępnych usług IT. Chmura staje się koniecznością w ochronie zdrowia m.in. ze względu na szybki postęp digitalizacji i AI.

Bazy lokalne bez przyszłości, ale nadal popularne

Według ostatniego badania Centrum e-Zdrowia opublikowanego w grudniu 2023 roku, 59,3% placówek posiada repozytorium EDM (miejsce składowania dokumentów elektronicznych wraz z metadanymi na potrzeby ich wyszukiwania), z czego u 40,4% znajduje się ono w podmiocie (serwery), a 15,4% korzysta z umów powierzenia, czyli chmury. Dla porównania – w USA ok. 45% szpitali i systemów zdrowia korzysta z chmury, a do 2026 roku odsetek ten wzrośnie do ok. 70%.

Mimo wielu korzyści, przejście na chmurę rozbija się w polskiej ochronie zdrowia o koszty. Wiele placówek zrealizowało w ostatnich latach duże inwestycje IT sięgając do programów dofinansowania i często w ramach rozliczenia muszą utrzymać zaadaptowane rozwiązanie przez kilka lat, czego wymaga podmiot współfinansujący projekt. Zakupione serwery dobrze się sprawdzają i pokrywają bieżące potrzeby.

Równie silną barierą jest logistyka – przejście na chmurę to duże wyzwanie wymagające silnego zaplecza IT. A na te mogą sobie pozwolić tylko największe podmioty. Wokół chmury narosło też wiele mitów m.in. dotyczących wysokich cen. Choć porównanie bieżących kosztów może sugerować, że przechowywanie danych w chmurze jest droższe niż zakup lokalnego serwera, w perspektywie długookresowej to chmura jest korzystniejszym rozwiązaniem. Nie ma też wbrew obawom przeciwskazań do gromadzenia elektronicznej dokumentacji medycznej w chmurze, jeśli tylko dane nie są przekazywane poza Europejski Obszar Gospodarczy (EOG). Oferowane przez polskich dostawców IT rozwiązania chmurowe są zgodne z przepisami krajowymi i RODO i można na nich polegać.

Chmura zyskuje też w związku z rosnącym ryzykiem ataków cybernetycznych. Przechowywanie kopii bezpieczeństwa w chmurze nieraz okazało się ratunkiem dla placówki zaatakowanej przez hakerów, którzy zablokowali dostęp do danych na lokalnym serwerze.

Korzyść 1.
Uproszczenie infrastruktury IT i zarządzania ekosystemem danych

Podobnie jak w przypadku każdego outsourcingu, gromadzenie danych w chmurze oznacza przesunięcie na dostawcę rozwiązania wszystkich prac administracyjno-logistycznych. Nie trzeba budować własnej serwerowni, odpada koszt zakupu i utrzymania dysków oraz aktualizacji zasobów sprzętowych. A to czynności, które mogą być bardzo obciążające dla działu IT ze względu na konieczność konserwacji lokalnych zasobów.

Korzyść 2.
Szybki start, pełna elastyczność

Choć chmura sprawdza się we wszystkich podmiotach, to indywidualne praktyki lekarskie nieposiadające wsparcia IT, szczególnie docenią jej zalety. Wybierając oprogramowanie w modelu SaaS, czyli system IT jako usługę, podmiot medyczny w pełni ceduje administrowanie systemem na dostawcę. Nie trzeba ani budować sieci, ani zawracać sobie głowy instalacją systemu na komputerach. Dostęp do bazy dostępny jest z każdego urządzenia w ramach systemu, stąd dane pacjenta są zawsze tam, gdzie są potrzebne.

Korzyść 3.
Skalowalność i dojrzewanie cyfrowe

Wdrażanie elektronicznej dokumentacji medycznej, digitalizacja archiwizacji obrazów medycznych, uruchamianie nowych usług dla pacjentów, narzędzia AI – każdy nowy element ekosystemu cyfrowego powoduje skokowy wzrost zapotrzebowania na zasoby pamięci. Zamiast kupować nowe serwery, wystarczy skontaktować się z dostawcą usług chmurowych i zamówić dodatkową przestrzeń dyskową. Chmura nie nakłada też żadnych ograniczeń dalszego rozwoju, zwłaszcza że wszystkie nowe urządzenia medyczne są z reguły przystosowane do bezpiecznej integracji. Ekosystem cyfrowy staje się łatwo skalowalny, a placówka z łatwością może dokładać kolejne elementy infrastruktury IT.

Korzyść 4.
Bezpieczna wymiana EDM i analiza danych

Chmura wspiera działalność naukową dużych ośrodków medycznych. Łatwość analizy dużych, anonimowych zbiorów danych powoduje, że podmiot medyczny może poszerzyć skalę prowadzonych badań. W ten sposób pojawiają się nowe możliwości nawiązywania krajowej i międzynarodowej współpracy w ramach projektów badawczych. Chmura zyska jeszcze większe znaczenie wraz z uruchomieniem Europejskiej Przestrzeni Danych Medycznych (European Health Data Space, EHDS), nowego projektu Komisji Europejskiej, który ma ruszyć w 2025 roku.

Korzyść 5.
Bezpieczeństwo nawet w rozwiązaniu hybrydowym

Przechowywanie wykonywanej w czasie rzeczywistym kopii zapasowej danych poza siecią placówki jest kluczowe z punktu widzenia bezpieczeństwa cybernetycznego. Nawet jeśli hakerom uda się złamać inne zabezpieczenia, aktualna kopia bazy pozwoli szybko przywrócić procesy bez utraty strategicznych z punktu widzenia bezpieczeństwa pacjenta i procesów administracyjnych danych.

Korzyść 6.
Przygotowanie na wdrożenia usług generatywnej AI

» Najwięksi dostawcy usług chmurowych z USA jako AWS i Google oferują podmiotom medycznym pierwsze usługi oparte na generatywnej sztucznej inteligencji. «

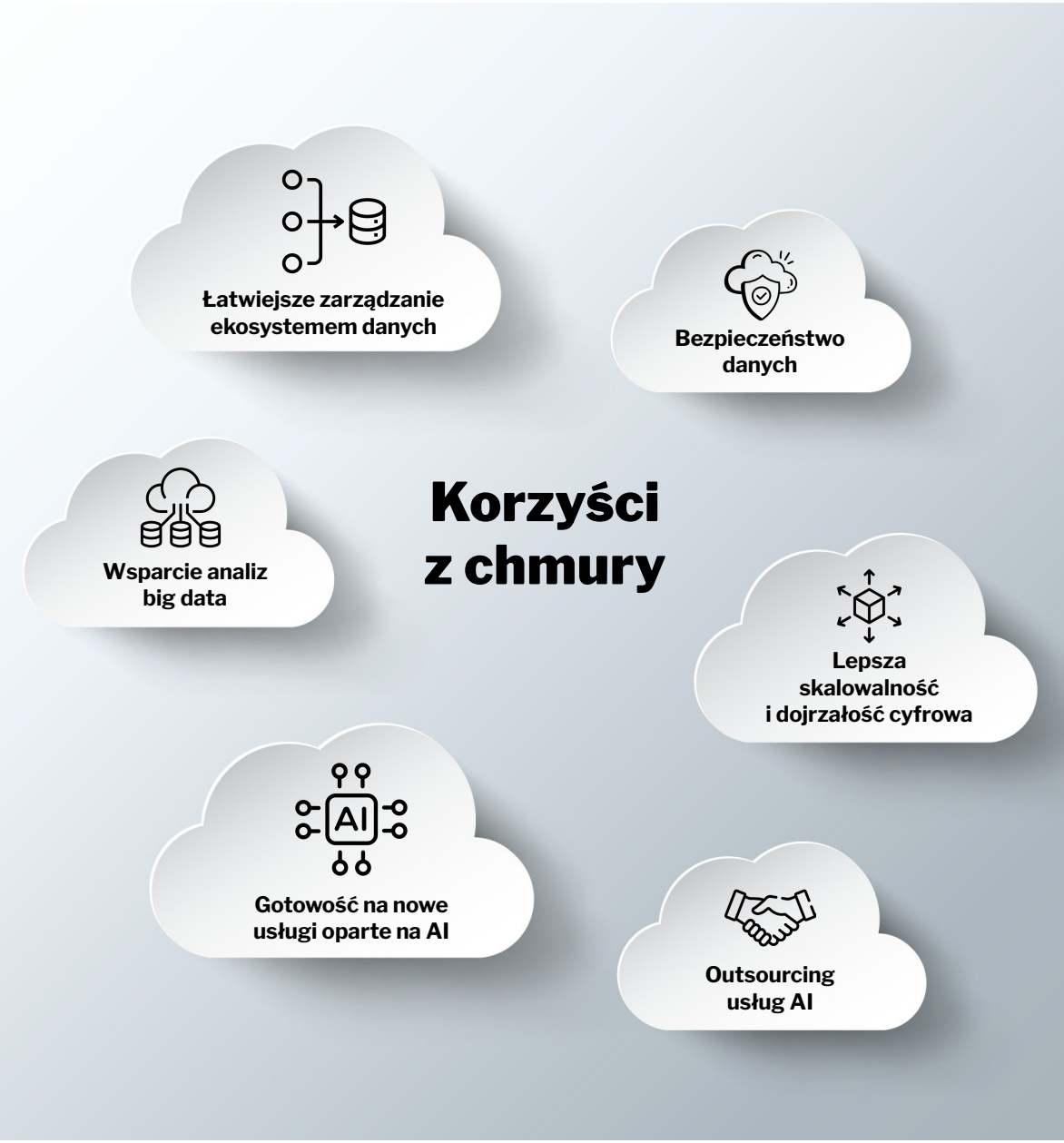
Chmura to coś więcej niż nowoczesny sposób przechowywania danych. To nowy rodzaj strategicznego podejścia do opieki zdrowotnej. Dzięki niej placówka może rozwijać koncepcje opieki koordynowanej, uruchamiać kreatywnie usługi cyfrowe dla pacjenta, rozwijać nowe lub integrować istniejące modele opieki bazujące na swobodnym dostępie do danych. Placówki korzystające z usług chmurowych zyskają szybciej dostęp do nowych usług opartych na generatywnej sztucznej inteligencji. Przykładowo, w sierpniu 2023 roku, amerykańskie placówki ochrony zdrowia podłączone do Google Cloud Healthcare jako pierwsze mogły testować nowy model AI przeznaczony do celów medycznych – Med-PaLM2. W październiku 2023, także Google uruchomił na swoje platformie

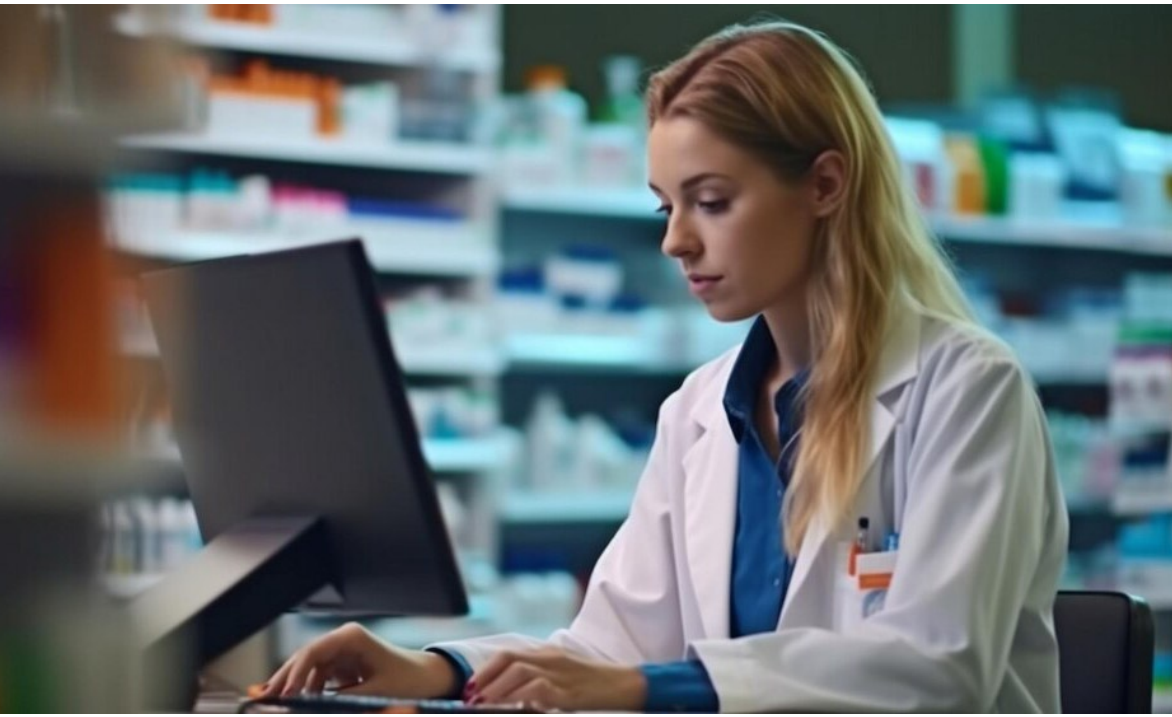
nowe narzędzia AI oparte na dużych modelach językowych (LLM), ułatwiające lekarzom wyszukiwanie informacji w różnych źródłach. Podobne rozwiązania wprowadza AWS Amazon Web Services, który jest liderem usług chmurowych w USA z udziałem 33% rynku.

Korzyść 7. Outsourcing trudno dostępnych usług IT

Placówki medyczne mają coraz większe trudności ze znalezieniem specjalistów IT. Wykwalifikowani pracownicy są wchłaniani przez inne branże, które mogą zaoferować o wiele lepsze stawki wynagrodzenia niż sektor zdrowia. Te niedobory pracowników w branży IT będą się w najbliższych latach zaostrzać. Gdy ciągłość zatrudnienia jest zagrożona, niektóre kompetencje IT warto scedować na dostawcę IT.

Rozwiązania chmurowe stają się standardem w każdej dziedzinie życia i ochrona zdrowia nie jest wyjątkiem. Chmura danych umożliwia swobodne wdrażanie nowych usług, takich jak AI, aplikacje mobilne, portale dla pacjentów, urządzenia IoT (internetu rzeczy) oraz prowadzenie analiz big data. Szybki postęp w dziedzinie sztucznej inteligencji tylko przyspieszy dewaluację lokalnych serwerów.


Łatwiejsze zarządzanie ekosystemem danych
Bezpieczeństwo danych
Wsparcie analiz big data
Korzyści z chmury
Lepsza skalowalność i dojrzałość cyfrowa
AI
Gotowość na nowe usługi oparte na AI
Outsourcing usług AI



Chmura w aptekach. Automatyczna ochrona przed utratą danych

Baza danych i zawarte w niej dane są krwiobiegiem placówki farmaceutycznej. Dzięki niej możliwa jest sprzedaż, rozliczenia, zarządzanie stanami magazynowymi. Dlatego na wypadek awarii sprzętu, dobrze mieć w gotowości aktualną kopię zapasową.

RepoCloud i CopyCloud zwiększają bezpieczeństwo danych

Baza danych jest strategicznym zasobem apteki – jej uszkodzenie lub zablokowanie zawsze ma poważne konsekwencje: od paraliżu sprzedaży do zaburzenia bieżącej działalności. Najgroźniejsze dla baz są cyberataki, złośliwe oprogramowanie blokujące dostęp do komputerów, ale również uszkodzenia na skutek zdarzeń losowych (zalanie, pożar, kradzież) albo awarii sprzętu. Nie zawsze można im zapobiec, ale można się zabezpieczyć przed ich skutkami, posiadając bezpieczną kopię zapasową tworzoną automatycznie w chmurze danych.

Mając na uwadze, jak ważną rolę odgrywają apteki w systemie ochrony zdrowia, firma KAMSOFT S.A. oferuje dwie dedykowane usługi chmurowe: CopyCloud i RepoCloud. Ich zadaniem jest zapewnienie ciągłości działania apteki w przypadku ewentualnego cyberataku lub zdarzenia losowego, w wyniku którego dane zostaną utracone lub uszkodzone. Sposób zapisu danych w chmurze jest zgodny z ustawą o ochronie danych osobowych RODO, a właściciel placówki nie musi się martwić o dane wrażliwe, bo wszystkie dokumenty w chmurze są odpowiednio zabezpieczone – zaszyfrowane specjalnym kluczem szyfrującym, do którego dostęp ma tylko apteka.

Jak działa przechowywanie w chmurze danych z apteki?

CopyCloud – kopia baz danych w chmurze – to usługa, która zabezpiecza dane przed ewentualną utratą lub uszkodzeniem. Jak to działa? Co godzinę tworzona jest kopia danych zgromadzonych w systemie aptecznym (KS-AOW). Oznacza to, że dane w zaszyfrowanej postaci są automatycznie wysyłane do chmury. Co ważne, klucz dostępowy posiada tylko apteka, dzięki czemu w przypadku ewentualnej awarii lub cyberataku apteka może szybko odzyskać utracone dane.

RepoCloud – repozytorium dokumentów elektronicznych w chmurze – zabezpiecza dokumenty realizacji recepty (DRR) i e-Recepty zgromadzone w bazie danych systemu

KS-AOW. Pobrane z Systemu Informacji Medycznej (SIM) e-Recepty oraz wytworzone DRR na bieżąco są wysyłane do chmury w zaszyfrowanej postaci. Dzięki temu lokalna baza danych systemu aptecznego posiada mniejszą objętość, bo przechowywane są dokumenty tylko z trzech ostatnich miesięcy. Ma to swoje praktyczne uzasadnienie: przeciążony sprzęt pracuje wolniej, co nieraz prowadzi do awarii i negatywnie wpływa na wydajność pracy. Co ważne, każdy przekazany do chmury dokument farmaceuta może w każdej chwili wyświetlić w systemie aptecznym. RepoCloud w przyszłości będzie także repozytorium dla informacji przekazanych z SIM o stanie realizacji recepty, dokumentacji z przeglądów lekowych oraz szczepień realizowanych w aptekach.

Apteki, które korzystają równocześnie z dwóch usług CopyCloud i RepoCloud mogą praktycznie bez ponoszenia straty odzyskać dane ze sprzedaży, zakupów i stanów magazynowych. Więcej informacji o rozwiązaniach chmurowych dla aptek można uzyskać pod adresem: apteka@kamsoft.pl.

OTWARTY SYSTEM OCHRONY ZDROWIA

OSOZ

Wydawca:
KAMSOFT 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

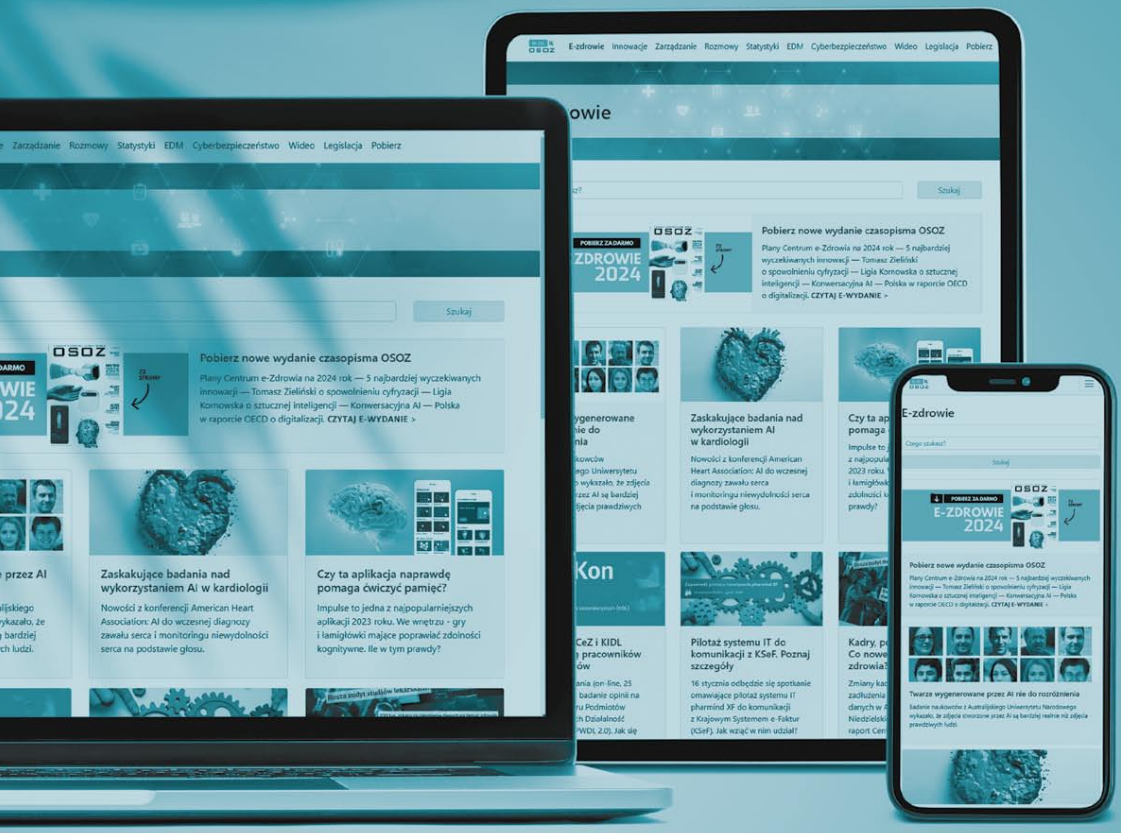
Zespół redakcyjny:
Zygmunt Kamiński,
Agnieszka Golec.

Współpracownicy:
Jakub Betka,
Michał Chodorek,
Monika Grabska,
Jeremi Olechnowicz.

Skład i łamanie: Piotr Chamera

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

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



Nowy blog o e-zdrowiu

Praktyczne porady
Informacje z rynku zdrowia
Inspirujące wywiady

BLOG
OSOZ
blog.osoz.pl

ZESKANUJ KOD,
aby przejść do bloga