miejsce na logo szpitala

CYBERMANUAL

PROSTE ZASADY BEZPIECZEŃSTWA CYFROWEGO W PODMIOCIE LECZNICZYM

Praktyczny przewodnik dla personelu medycznego i administracyjnego oraz wytyczne dla Zarządu.

OGÓLNOPOLSKIE STOWARZYSZENIE SZPITALI PRYWATNYCH

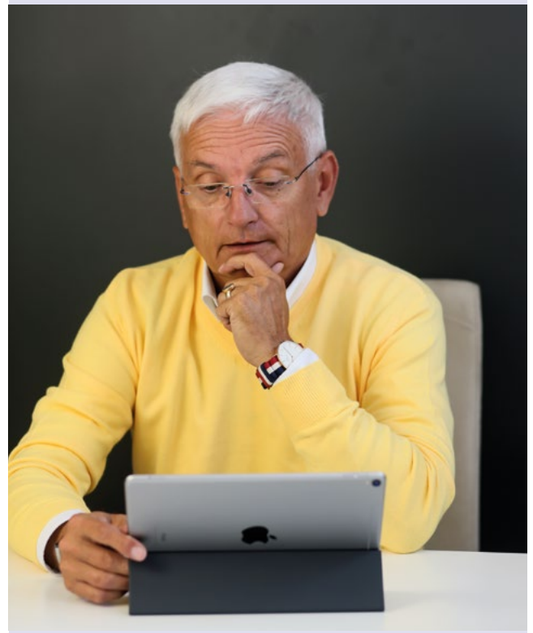
UNION EUROPÉENNE DE L'HOSPITALISATION PRIVÉE

UEHP 35 YEARS PRIVATE HOSPITALS SHAPING EUROPE'S HEALTH

SPIS TREŚCI

DLA PRACOWNIKÓW

DLA ZARZĄDU



Szanowni Czytelnicy,

Dlaczego cyberbezpieczeństwo to sprawa nas wszystkich?

W dobie cyfryzacji szpitala, komputer stał się takim samym narzędziem pracy jak stetoskop, ciśnieniomierz czy strzykawka. Większość informacji o zdrowiu naszych pacjentów – wyniki badań, historie chorób, dawkowanie leków – znajduje się w systemach informatycznych.
Musimy zrozumieć jedną kluczową rzecz: Cyberbezpieczeństwo w szpitalu to nie tylko ochrona danych, to przede wszystkim bezpieczeństwo pacjenta.
Gdy systemy komputerowe zostaną zablokowane przez hakerów:

- Lekarz nie może sprawdzić, czy pacjent nie jest uczulony na dany lek.
- Planowe operacje muszą zostać odwołane.
- SOR nie może sprawnie przyjmować chorych, bo nie działa rejestracja.
- Wyniki badań laboratoryjnych nie docierają na czas do oddziału.

Każdy z nas – niezależnie od tego, czy jest lekarzem, pielęgniarką, salową czy pracownikiem biurowym – jest strażnikiem tych danych. Ten poradnik pomoże Państwu zrozumieć, jak proste, codzienne nawyki mogą ochronić naszą placówkę przed paraliżem. wszystkich?

Andrzej Sokołowski
prezes Ogólnopolskiego
Stowarzyszenia Szpitali Prywatnych

Dla pracowników

ROZDZIAŁ 1:
Pułapki, czyli jak oszuści próbują nas podejść

Oszuści rzadko atakują „ściany” serwerów. Najczęściej próbują oszukać człowieka, licząc na pośpiech, zmęczenie lub rutynę.

1.1. Podszywanie się pod inne osoby (Phishing)

To najpopularniejsza metoda. Oszust wysyła e-mail lub SMS, który wygląda jak wiadomość z banku, z Ministerstwa Zdrowia, z NFZ-u, a nawet od dyrekcji szpitala lub działu informatyki.

Jak to wygląda? Dostają Państwo wiadomość z treścią: „Twoje hasło wygasa, kliknij tutaj, aby je zaktualizować” lub „W załączniku przesyłamy pilną fakturę do opłacenia”.

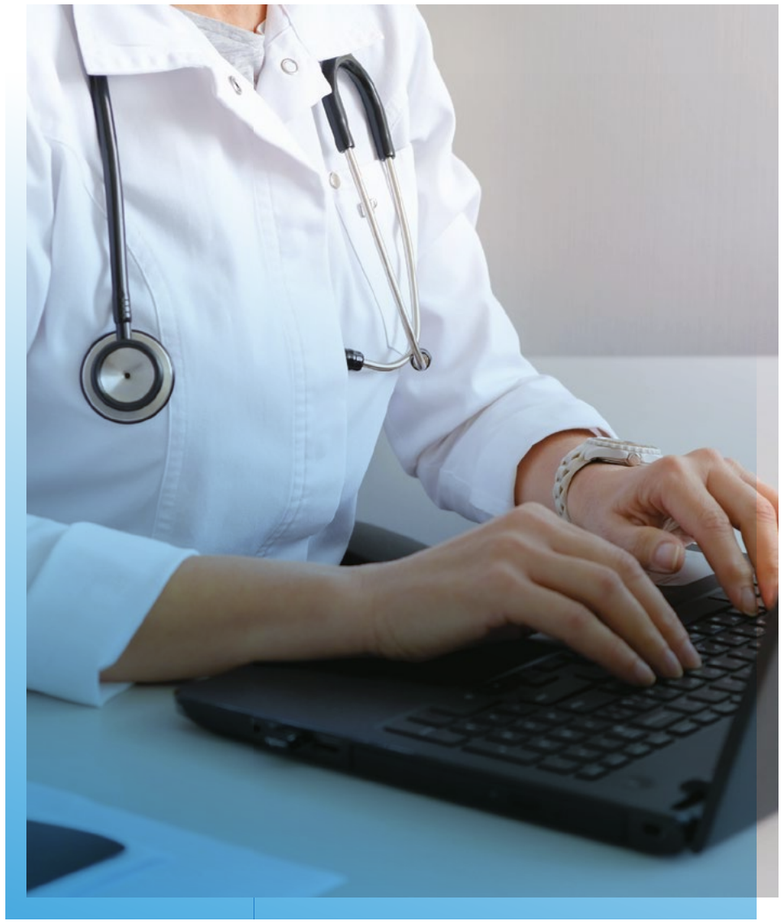
Na co zwrócić uwagę?

- **Presja czasu:** Wiadomość sugeruje, że musisz działać „natychmiast”, inaczej stanie się coś złego.
- **Błędy w nazwisku lub nazwie instytucji:** Często adres e-mail nadawcy różni się jedną literką od prawdziwego.
- **Podejrzane linki:** Nigdy nie klikaj w odnośniki w wiadomościach, których się nie spodziewałeś.

1.2. Cyfrowy haracz (Ransomware)

To wirus, który „zamyka” wszystkie pliki w komputerze na kłódkę. Na ekranie pojawia się komunikat, że jeśli szpital nie zapłaci okupu (często w milionach złotych), dane zostaną skasowane.

Taki wirus najczęściej dostaje się do systemu, gdy ktoś otworzy zarażony załącznik w e-mailu.



ROZDZIAŁ 2:
Złote zasady bezpiecznej pracy przy komputerze

Bezpieczeństwo zaczyna się od prostych czynności, które nie wymagają wiedzy technicznej, a jedynie uważności.

2.1. Hasło – Twój osobisty klucz

Hasło jest jak klucz do szafki z lekami narkotycznymi – nie zostawiamy go w zamku i nie oddajemy nikomu.

- Nie zapisuj haseł na kartkach: Przyklejanie haseł do monitora lub trzymanie ich pod klawiaturą to zaproszenie dla złodzieja.
- Nie udostępniaj swojego konta: Jeśli koleżanka prosi: „Zaloguj mnie na chwilę na swoim koncie, bo zapomniałam hasła”, grzecznie odmów. Wszystko, co zostanie zrobione na Twoim koncie, idzie na Twoje konto (również błędy medyczne!).
- Stwórz hasło, które łatwo zapamiętać, a trudno odgadnąć: Zamiast „haslo123”, użyj np. pierwszych liter słów Twojej ulubionej piosenki lub wiersza, dodając liczbę.

2.2. Zasada „Odchodzę – Blokuję”

To najważniejszy nawyk w szpitalu. Gdy nagle zostaniesz wezwany do pacjenta lub idziesz zrobić kawę:

- Zawsze blokuj ekran komputera. Nie musisz się wylogowywać. Wystarczy nacisnąć jednocześnie dwa klawisze: Znaczek Windows + litera L.
- Dlaczego to ważne? Pozostawiony komputer pozwala każdej postronnej osobie (np. odwiedzającym pacjentów) na wgląd w prywatne dane lub wprowadzenie zmian w systemie pod Twoim nazwiskiem.

2.3. Czyste biurko i bezpieczna drukarka

Ochrona danych to nie tylko komputer, to także papier.

- Nie zostawiaj wydruków: Jeśli drukujesz wyniki badań lub dane pacjenta, odbierz je z drukarki natychmiast. Dokumenty pozostawione na tacy w korytarzu są dostępne dla każdego.
- Niszczarka to Twój przyjaciel: Dokumenty zawierające dane osobowe, które nie są już potrzebne, muszą trafić do niszczarki, a nie do zwykłego kosza na śmieci.

ROZDZIAŁ 3:
Urządzenia prywatne i obce nośniki

Internet i nowoczesne gadżety niosą ze sobą ryzyko, o którym często zapominamy.

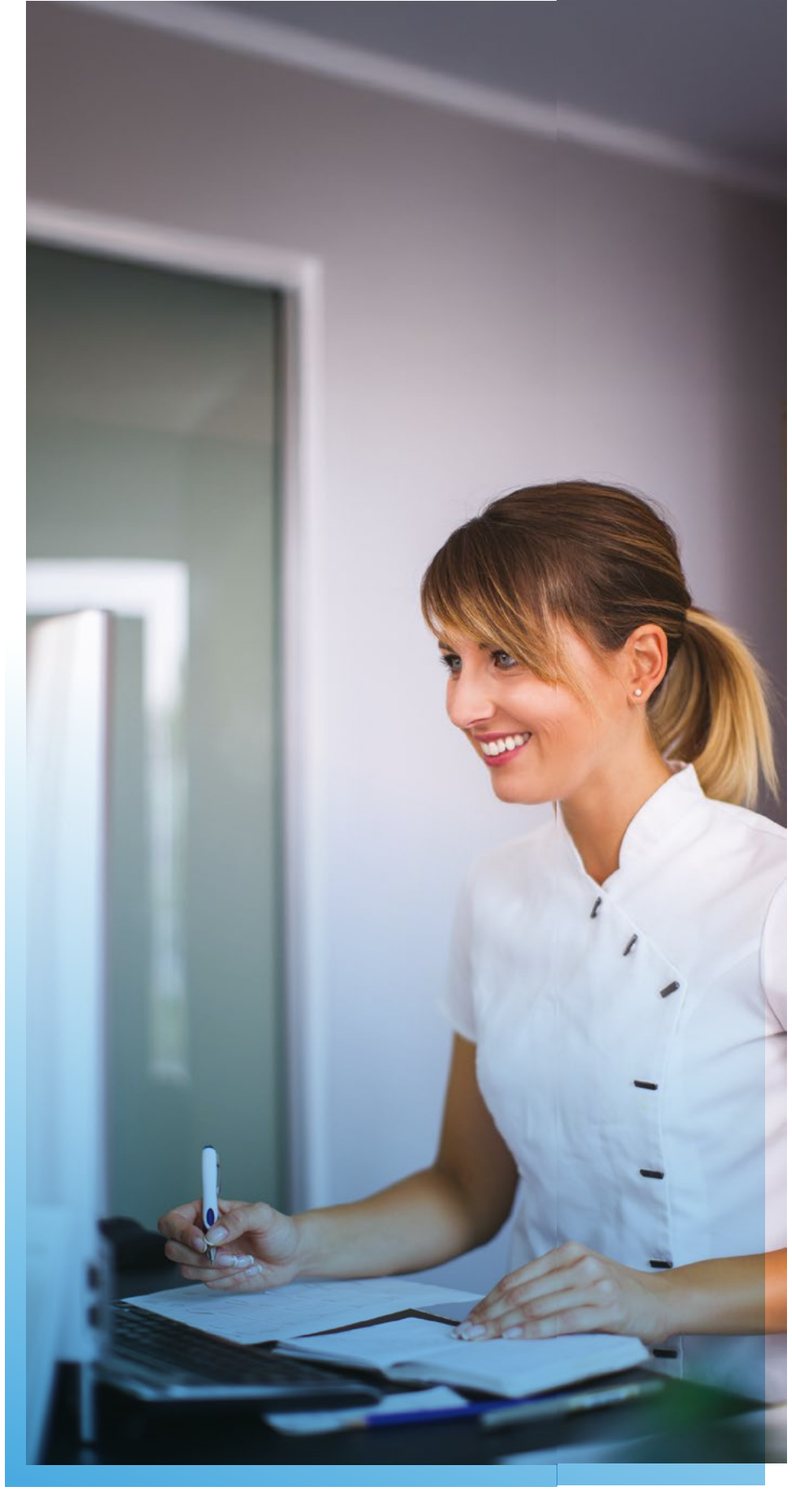
3.1. Pułapka „znalezionego pendrive'a"

Nigdy nie podłączaj do służbowego komputera pamięci USB (pendrive'ów), które znalazłeś na korytarzu lub które dostałeś jako gadżet na konferencji medycznej.

- To częsty sposób działania hakerów – podrzucają zainfekowane urządzenie, licząc na to, że ktoś z ciekawości sprawdzi, co jest w środku. Podłączenie takiego pendrive'a może zainfekować całą sieć szpitalną w kilka sekund.

3.2. Służbowe to służbowe, prywatne to prywatne

- Nie sprawdzaj prywatnej poczty na komputerze w pracy: Twoje prywatne konto e-mail może być mniej chronione niż system szpitalny. Otwierając tam załączniki, narażasz sieć szpitala.
- Nie instaluj własnych programów: Jeśli potrzebujesz kalkulatora medycznego lub słownika, poproś o to dział IT. Programy z niepewnych źródeł mogą „szpiegować" to, co wpisujesz na klawiaturze.



ROZDZIAŁ 4:
Co robić, gdy coś wzbudzi Twój niepokój?

Większość ludzi boi się przyznać do błędu w sieci. W naszym szpitalu chcemy to zmienić: **Zgłoszenie błędu to przejaw odpowiedzialności, a nie powód do wstydu.**

4.1. Objawy, które powinny Cię zaalarmować:

- Komputer nagle zaczął pracować bardzo wolno, „zacina się".
- Na pulpicie pojawiły się dziwne ikony lub okienka, których wcześniej nie było.
- Ktoś z Twoich kontaktów otrzymał od Ciebie e-mail, którego nie wysyłałeś.
- Strona internetowa, na którą zawsze wchodzisz, wygląda inaczej niż zwykle.

4.2. Procedura postępowania krok po kroku:

1. Zachowaj spokój.
2. Przerwij pracę na tym urządzeniu. Nie próbuj samodzielnie „naprawiać" systemu ani restartować komputera, jeśli nie polecił Ci tego informatyk.
3. Odłącz internet, jeśli potrafisz (np. wyciągnij kabel z tyłu obudowy).
4. Zadzwoń niezwłocznie do działu IT lub zgłoś to przełożonemu. Powiedz dokładnie, co się stało (np. „Kliknęłam w link w podejrzanym e-mailu").
5. Poinformuj współpracowników, aby nie otwierali podobnych wiadomości.

PODSUMOWANIE: Twoja osobista lista kontrolna (checklista)

Proszę, przeanalizuj te punkty przed każdym dyżurem. To zajmie tylko chwilę.

Hasło:
Czy moje hasło jest znane tylko mnie? Czy nie ma go zapisanego w widocznym miejscu?

Ekran:
Czy blokuję komputer za każdym razem, gdy wstaję od biurka (Windows + L)?

E-mail:
Czy sprawdzam, od kogo dostałem wiadomość, zanim otworzę załącznik?

Biurko:
Czy na moim stanowisku nie leżą luźne kartki z danymi pacjentów?

Kontakt:
Czy wiem, jaki jest numer telefonu do działu informatyki w razie awarii?

Państwa doświadczenie i wiedza medyczna są fundamentem naszego szpitala. Dodając do tego odrobinę czujności w świecie cyfrowym, tworzą Państwo najbezpieczniejsze środowisko dla naszych pacjentów.

Dziękujemy za Państwa codzienną uważność!

Gdyby jednak doszło do cyberataku, na kolejnej stronie przedstawiamy **Arkusz Pierwszej Pomocy Cybernetycznej**, przygotowany specjalnie dla personelu medycznego i niemedycznego. **Jest to gotowy dokument do wydrukowania i powieszenia w dyżurkach oraz punktach pielęgniarskich.**

ARKUSZ PIERWSZEJ POMOCY: CYBERATAK

Instrukcja dla personelu dyżurującego
(lekarze, pielęgniarki, administracja)

Hakerzy często wykorzystują nocne dyżury i presję czasu na SOR-ze.

Twoja szybka reakcja może uratować systemy szpitalne przed paraliżem.

1. Sygnały ostrzegawcze reaguj, gdy:

- Na ekranie pojawił się komunikat o zablokowaniu plików lub żądanie okupu.
- Komputer nagle zaczął pracować bardzo powolnie lub „sam klika”.
- Dostałeś podejrzany e-mail/SMS i kliknąłeś w link lub otworzyłeś załącznik.
- Otrzymujesz na telefon prośby o zatwierdzenie logowania (MFA), którego nie zlecałeś.

2. Algorytm postępowania (krok po kroku)

1. PRZERWIJ PRACĘ: Nie klikaj nic więcej, nie zamykaj okienek na siłę.
2. ODŁĄCZ SIECI: Jeśli potrafisz, wyciągnij kabel sieciowy z komputera lub wyłącz Wi-Fi. Nie wyłączaj samego komputera z prądu! (Informatycy muszą zabezpieczyć ślady w pamięci RAM).
3. ZADZWOŃ DO IT / SOC: Skontaktuj się z numerem alarmowym:
4. POINFORMUJ ZESPÓŁ: Ostrzeż kolegów na oddziale, by nie otwierali podobnych wiadomości.

PAMIĘTAJ:

Zgłoszenie incydentu „na wszelki wypadek” jest lepsze niż milczenie. Wczesna reakcja to mniejsze ryzyko dla Twoich pacjentów.

3. Czego absolutnie nie robić? (Zakazy)

- Nie naprawiaj sam: Nie instaluj programów antywirusowych „z internetu”.
- Nie czyść dowodów: Nie kasuj podejrzanych e-maili i nie „sprzątaj” pulpitu.
- Nie ulegaj presji: Jeśli ktoś dzwoni i prosi o hasło lub kod MFA „bo trwa awaria” – rozłącz się. To oszustwo.

4. Szybki raport dla informatyka

(Wypełnij i przekaż osobie z działu IT)

- Data i godzina zdarzenia:
- Numer/Nazwa komputera:
- Co się stało? (np. kliknięty link, dziwne okno):
- Czy podałeś hasło lub kod z telefonu? TAK / NIE

Numer alarmowy IT (24/7):

Osoba odpowiedzialna na oddziale:

Dla Zarządu

ROZDZIAŁ 5:
Obowiązki kadry zarządzającej w świetle Dyrektywy NIS2

Współczesne cyberbezpieczeństwo przestało być wyłącznie domeną dostawców usług IT czy pasywnym systemem ochrony serwerów. Wraz z wejściem w życie Dyrektywy NIS2, krąg podmiotów zobowiązanych do systemowego zarządzania cyberbezpieczeństwem został rozszerzony o sektor ochrony zdrowia, a odpowiedzialność za ten obszar została wprost przeniesiona na najwyższe szczeble zarządzania.

5.1. Skala zagrożeń: Dane i statystyki

Branża zdrowotna jest obecnie jednym z głównych celów cyberprzestępców. Jak wynika z badań prowadzonych przez Centrum e-Zdrowia, dynamika zagrożeń jest alarmująca:

- w 2023 roku w placówkach ochrony zdrowia odnotowano 405 różnych ataków.
- w 2024 roku liczba ta wzrosła ponad dwukrotnie, osiągając poziom 1028 incydentów.
- w 2025 roku liczba ataków w porównaniu z rokiem poprzednim wzrosła o 40%.

Szczególnym wyzwaniem jest gwałtowny wzrost liczby ataków typu ransomware, które skutkują paraliżem całej organizacji. W sektorze medycznym cyberbezpieczeństwo to nie tylko ochrona danych osobowych, ale przede wszystkim gwarancja bezpieczeństwa pacjentów, ciągłości świadczeń zdrowotnych oraz utrzymania zaufania społecznego.

5.2. Strategiczna rola Zarządu

Zgodnie z wymogami NIS2, organy zarządzające podmiotami leczniczymi pełnią kluczową rolę w systemie ochrony. Do ich bezpośrednich obowiązków należy:

- Zatwierdzanie środków zarządzania ryzykiem: Dyrekcja musi brać czynny udział w procesie wyboru i akceptacji strategii ochrony.
- Nadzór nad wdrażaniem: Zarząd jest odpowiedzialny za monitorowanie, czy przyjęte środki są skutecznie realizowane w codziennej pracy szpitala.
- Odpowiedzialność osobista: Nowe przepisy przewidują, że członkowie organów zarządzających mogą ponosić osobistą odpowiedzialność za naruszenia obowiązków w zakresie cyberbezpieczeństwa.

5.3. Synergia między IOD a Zespołem IT

Doświadczenie pokazuje, że cyberatak często obnaża luki prawne i techniczne jednocześnie. Skuteczne zarządzanie bezpieczeństwem wymaga ścisłej współpracy między Inspektorem Ochrony Danych (IOD) a zespołem IT. Aby zrealizować zalecenia NIS2, Dyrekcja powinna:

1. Wskazać wspólny obszar odpowiedzialności: Przykładowo, w drodze zarządzenia wewnętrznego, należy określić punkty styku kompetencji IOD i specjalistów ds. cyberbezpieczeństwa.
2. Ustalić obowiązek raportowy: Wprowadzenie cyklicznych spotkań oraz stałego mechanizmu raportowania do Zarządu pozwala na bieżąco korygować strategię ochrony.
3. Wyznaczyć wspólną procedurę incydentową: Dokument ten musi jasno określać obowiązek wzajemnego informowania się działów oraz wspólnego reagowania w celu zminimalizowania skutków ewentualnych naruszeń.

5.4. Planowanie, dokumentowanie i zasada rozliczalności

Wdrożenie standardów NIS2 to proces długofalowy, który wymaga zabezpieczenia odpowiednich zasobów. Cyberbezpieczeństwo musi zostać uwzględnione w:

- Planach finansowych: Jako niezbędna inwestycja w infrastrukturę i kompetencje personelu.
- Planach organizacyjnych: Poprzez włączenie procedur bezpieczeństwa w standardowe procesy zarządzania placówką.

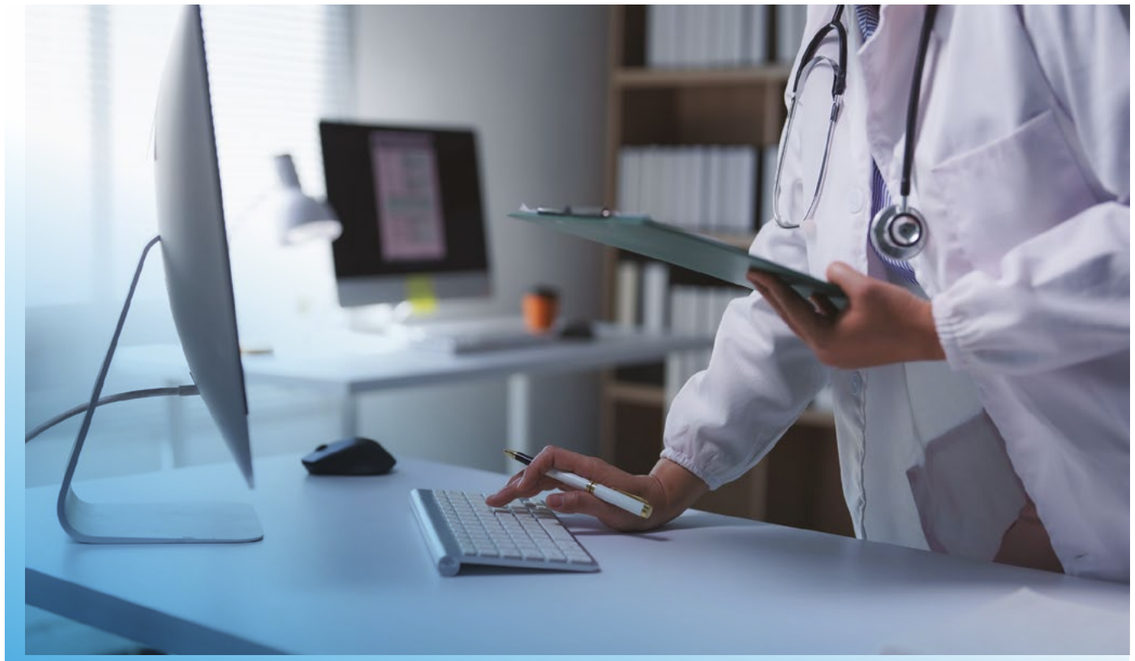
Kluczowym elementem jest dokumentowanie podejmowanych działań. Rzetelne zapisy decyzji zarządczych i podjętych kroków ochronnych mają ogromne znaczenie prawne – w przypadku wystąpienia incydentu pozwalają wykazać należytą staranność kadry zarządzającej.

Wnioski dla Zarządu:

Dyrektywa NIS2 jasno wskazuje, że cyberbezpieczeństwo w ochronie zdrowia stało się kwestią strategiczną, a nie wyłącznie techniczną.

Odporność systemów IT, rzetelne przygotowanie personelu oraz wysoka świadomość zarządcza będą w najbliższych latach kluczowe dla niezakłóconego funkcjonowania każdego podmiotu leczniczego.

ROZDZIAŁ 6: Ślad cyfrowy, sposób postępowania, zgłaszanie incydentów i współpraca z organami ścigania po ataku



W dobie powszechnej cyfryzacji każda aktywność w systemach medycznych pozostawia po sobie zapis binarnego „odcisku palca”. Zrozumienie natury tych dowodów oraz procedur ich zabezpieczania jest kluczowe dla ochrony prawnej podmiotu leczniczego oraz skuteczności działań Prokuratury, Policji (w tym Centralnego Biura Zwalczania Cyberprzestępczości) oraz zespołów reagowania takich jak CSIRT NASK.

6.1. Natura i lokalizacja śladu cyfrowego

Ślad cyfrowy to zapis binarny (ciąg zer i jedynek), będący fragmentem kodu generowanego przez sprzęt i oprogramowanie, dokumentujący każdą operację w systemie.

Fundamentem zabezpieczenia dowodów jest zbieranie tzw. logów (rejestrów zdarzeń) w systemach teleinformatycznych.

Kluczowe logi, które powinny być gromadzone:

- Logi wszelkich operacji uwierzytelniania oraz dostępów zdalnych.
- Logi ruchu sieciowego – brzegowego oraz w sieci LAN.
- Logi z systemów bezpieczeństwa.
- Logi z kluczowych serwerów.
- Logi z systemów dziedzinowych.
- Logi z systemu kopii zapasowych.

Wszystkie logi powinny trafiać do dedykowanego magazynu (np. tzw. log collector). Rekomendowane jest również zbieranie i monitorowanie logów z samego systemu gromadzącego te dane.

Gdzie szukać śladów w podmiocie leczniczym?

- Systemy medyczne: Zapisy aktywności w Elektronicznej Dokumentacji Medycznej (EDM) oraz systemach obrazowania (RTG, TK, MRI, PACS).
- Infrastruktura sieciowa: Logi serwerów, historia połączeń oraz zapisy w chmurze obliczeniowej.
- Komunikacja: Historia serwerów poczty elektronicznej oraz logowania użytkowników.

Należy pamiętać, że ślady cyfrowe bywają ulotne – dane w pamięci operacyjnej RAM mogą zostać bezpowrotnie utracone po wyłączeniu lub zrestartowaniu komputera.

6.2. Obowiązki prawne Zarządu (Art. 304 k.p.k.)

W przypadku stwierdzenia incydentu o charakterze przestępczym, na zarządzających spoczywają obowiązki wynikające z Kodeksu postępowania karnego:

- Art. 304. § 1. k.p.k.: Każdy, dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu, ma społeczny obowiązek zawiadomić o tym prokuratora lub Policję.
- Art. 304. § 2. k.p.k.: Instytucje państwowe i samorządowe są obowiązane niezwłocznie zawiadomić o przestępstwie oraz przedsięwziąć czynności zapobiegające zatarciu śladów do czasu przybycia organów ścigania.

W praktyce oznacza to prawny obowiązek zawiadomienia organów o podejrzeniu włamania, kradzieży danych czy niszczenia dokumentacji oraz aktywną ochronę cyfrowego „miejsca zdarzenia”.

6.3. Współpraca z CSIRT i zgłaszanie incydentu

Każdy incydent w ochronie zdrowia powinien zostać niezwłocznie zgłoszony do odpowiedniego zespołu reagowania (CSIRT). Docelowo (po pełnym wdrożeniu dyrektywy NIS2) zgłoszenia te będą kierowane do sektorowego zespołu CSIRT CeZ.

Kanały zgłoszeniowe:

1. Portal https://incydent.cert.pl/ lub system S46.
2. Sektorowy zespół CSIRT CeZ poprzez formularz: https://cez.gov.pl/pl/page/zglos-incydent lub e-mail: incydent@csirt.cez.gov.pl.

Ważne jest, aby zgłoszenia dokonać jak najszybciej, nawet jeśli nie posiadamy jeszcze kompletu danych – dodatkowe informacje można uzupełnić później, a szybka reakcja ogranicza skalę szkód.

6.4. Zasady „cyfrowej higieny” po wykryciu ataku

Aby ślad cyfrowy mógł posłużyć jako dowód, nie może zostać zmieniony przez niewłaściwe działania personelu. Jeśli jest to możliwe, zaleca się:

- Zakaz samodzielnej naprawy: Nie uruchamiaj programów antywirusowych ani narzędzi czyszczących na zainfekowanym urządzeniu – mogą one nadpisać logi lub bezpowrotnie uszkodzić pomocne pliki.
- Izolacja zamiast kasowania: Odłącz urządzenie od sieci (kabel/Wi-Fi), ale pozostaw je włączone (zachowanie pamięci RAM).
- Brak modyfikacji plików: Nie otwieraj, nie kopiuj i nie przenoś plików objętych atakiem. Prawidłowym działaniem jest wykonanie kopii binarnych.
- Dokumentacja zdarzenia: Niezwłocznie sporządź notatkę z czasem zauważenia anomalii i opisem komunikatów, gdyż szczegóły z czasem umykają.

6.5.Formularz zgłoszenia incydentu (Wzór dla personelu)

Pole formularza	Informacja (wypełnia pracownik)
Data i godzina zauważenia	/
Oddział / Komórka organizacyjna	
Stanowisko / Numer PC	
Używany system / aplikacja	HIS / PACS / Poczta / Inne:
Opis zdarzenia (co się stało?)	
Czy kliknięto w link/załącznik?	TAK / NIE / NIE WIEM
Czy podano hasło lub kod MFA?	TAK / NIE / NIE WIEM
Widoczne komunikaty (np. okup)	
Osoba zgłaszająca	

UWAGA

W przypadku wypełniania formularza przez dział IT, należy dołączyć techniczne parametry IoC (Indicators of Compromise), takie jak: nazwa hosta, IP, numer inwentarzowy urządzenia, podsieć oraz rodzaj zdarzenia. Są to dane, o które w dalszej kolejności może pytać zespół CSIRT.

Wnioski dla Zarządu:

Ślad cyfrowy jest „niemym świadkiem" przestępstwa. Rzetelne zabezpieczenie dowodów to najlepsza obrona przed zarzutem niedopełnienia obowiązków wynikających z art. 304 k.p.k. i dyrektywy NIS2. Dla zespołów CSIRT logi są jedynym źródłem precyzyjnej informacji pozwalającej na analizę wektora ataku i zawężenie grupy zainfekowanych urządzeń. W przypadku braku logów, jedynym bezpiecznym zaleceniem jest często reinstalacja wszystkich hostów w sieci, co drastycznie wydłuża czas paraliżu placówki i podnosi koszty przywrócenia ciągłości działania.

ROZDZIAŁ 7: Ubezpieczenie cybernetyczne – tarcza finansowa i operacyjna dla Zarządu

Jako zarządzający podmiotem leczniczym wiedzą Państwo, że ryzyka nie da się wyeliminować do zera – można nim jedynie zarządzać. W strategii „Nowoczesnego Szpitala 2026" ubezpieczenie cybernetyczne (Cyber Insurance) przestaje być tylko „polisą w szufladzie". Staje się operacyjnym mechanizmem reagowania kryzysowego, który wspiera szpital w najtrudniejszych pierwszych godzinach po ataku.

7.1. Więcej niż odszkodowanie: Gotowość operacyjna

Kluczowym błędem w postrzeganiu ubezpieczenia cyber jest traktowanie go wyłącznie jako instrumentu finansowego. W rzeczywistości nowoczesna polisa zapewnia dostęp do zespołów szybkiego reagowania (Incident Response). W momencie ataku zarządzający nie musi szukać na rynku informatyków śledczych czy wyspecjalizowanych prawników – ubezpieczyciel dostarcza ich w trybie 24/7.

7.2. Mechanizm reagowania krok po kroku

Zgodnie ze standardami bezpieczeństwa, proces obsługi incydentu w ramach ochrony ubezpieczeniowej dzieli się na pięć kluczowych etapów:

1. Wykrycie i zgłoszenie: Nawet jeśli skala ataku nie jest jeszcze znana, kluczowe jest niezwłoczne powiadomienie centrum pomocy (tzw. hotline 24/7). Incydentem może być zarówno blokada ransomware, jak i podejrzenie wycieku danych pacjentów czy paraliż systemów diagnostycznych.
2. Natychmiastowe wsparcie (Manager Incydentu): Ubezpieczyciel wyznacza osobę dedykowaną do koordynacji działań. Zarząd zyskuje partnera, który bierze na siebie ciężar zarządzania kryzysowego.
3. Wsparcie ekspertów: Szpital otrzymuje pomoc w trzech obszarach:
    - IT i Informatyka Śledcza: Zatrzymanie ataku, zabezpieczenie dowodów i analiza, jak doszło do włamania.
    - Wsparcie Prawne: Eksperci oceniają obowiązki notyfikacyjne wobec UODO oraz organów nadzorczych.
    - Komunikacja Kryzysowa: Specjaliści PR pomagają przygotować komunikaty dla pacjentów, mediów i personelu, chroniąc renomę placówki.
4. Opanowanie sytuacji i przywracanie ciągłości: Celem jest jak najszybszy powrót do udzielania świadczeń medycznych oraz ograniczenie skutków finansowych przestoju.
5. Obsługa roszczeń: Po opanowaniu kryzysu następuje formalne rozliczenie kosztów i ewentualnych roszczeń osób trzecich (np. pacjentów, których dane wyciekły).

7.3. Jakie ryzyka pokrywa ochrona?

Dla bezpieczeństwa placówki kluczowe jest, aby ochrona obejmowała najczęstsze zagrożenia w sektorze medycznym:

- Ataki Ransomware: Koszty odtwarzania danych i negocjacji.
- Wycieki danych (RODO): Koszty kar administracyjnych (jeśli prawo na to pozwala) oraz obrony prawnej.
- Oszustwa elektroniczne: Próby wyłudzenia środków finansowych szpitala.
- Błędy ludzkie: Nieumyślne naruszenie bezpieczeństwa przez pracownika (np. pozostawienie odblokowanego komputera).

Wnioski dla Zarządu:

Ubezpieczenie cybernetyczne to inwestycja w ciągłość działania. W dobie rosnącej liczby ataków na szpitale, posiadanie dostępu do wyspecjalizowanych ekspertów w ciągu kilkunastu minut od wykrycia problemu jest jedynym sposobem na uniknięcie długotrwałego paraliżu placówki i ogromnych strat wizerunkowych.

SUPLEMENT

Prawdopodobnie znasz funkcję podpowiadania tekstu w smartfonach. Wpisujesz słowo, a urządzenie sugeruje najbardziej prawdopodobny następny wyraz. Duże modele językowe (LLM) pozwalają chatbotom robić coś podobnego... ale na znacznie większą skalę".
- proste wyjaśnienie LLM w Computer History Museum w Mountain View w Dolinie Krzemowej, gdzie to wszystko się zaczęło

Lekarz i AI: Jak bezpiecznie korzystać z modeli LLM w codziennej pracy?

W gruncie rzeczy dla lekarza zrozumienie czym jest LLM[1] nie jest trudne. Wystarczy tylko na chwilę zatrzymać się i odciąć od infosfery przeładowanej click bait'ami i narracjami, które motywowane są różnymi interesami. Choć dzisiejsze modele oparte na transformerach trenowane są na miliardach i bilionach słów, to w gruncie rzeczy jest to metoda statystycznego odgadywania kolejnego najbardziej prawdopodobnego słowa na podstawie znanego kontekstu (wcześniej wprowadzonych słów).

Dzięki dużej sprawności i ogromnej mocy obliczeniowej, narzędzie statystyczne jakim jest LLM dość skutecznie sprawdza się w kilku obszarach pracy z tekstem. Są to:

- generowanie tekstu,
- redagowanie tekstu (parafrazowanie, podsumowanie, zmiana stylu, łączenie),
- streszczanie,
- tłumaczenie z jednego języka na inny lub tłumaczenie w obrębie tego samego języka (inaczej, prościej),
- wyszukiwanie informacji w tym w rozproszonych źródłach,
- przegląd literatury i analiza różnic,
- łączne zastosowanie kilku powyższych np. zamiana tekstu mówionego przez pacjenta na tekst pisany (speech2text), ustrukturyzowanie tekstu (struktura wywiadu z badania podmiotowego), wygenerowanie proponowanych zaleceń do akceptacji lekarza (np. zalecenia dietetyczne i z zakresu rehabilitacji).

W tych powodów współczesna medycyna sięga po Duże Modele Językowe (LLM), które rewolucjonizują pracę z tekstem i danymi. Należy podkreślać zawsze, że narzędzia te nie zastępują diagnozy, ale działają jako zaawansowani asystenci administracyjni lub badawczy.

Rozumiejąc, że LLM to tylko metoda statystycznego „losowania" słów łatwo dostrzec pierwsze niebezpieczeństwo nazywane halucynacją LLM. Niezależnie od okoliczności model zawsze „wylosuje" kombinację słów i ułoży ją w poprawną gramatycznie strukturę. Niestety podana przez model kombinacja może być zupełnie niepoprawna klinicznie.
W większości przypadków „losowanie" wypada poprawnie i model generuje przydatne wyniki.

Niestety internet podaje coraz więcej przykładów błędnych klinicznie rekomendacji ChataGPT i innych LLMów. Dla nabycia ostrożności zrozumienia zjawiska halucynacji LLMów warto śledzi plebiscyt Epic fAIls prowadzony przez Dyrektora Centrum Wiarygodnej SI prof. dr hab inż. Przemysława Biecek. W ostatnim Epic fAIls 2025 roku podano przykład zalecenia „dietetycznego" polegającego na zastąpieniu soli kuchennej inną toksyczną solą[2]. Podstawową i pierwszą zasadą bezpiecznego korzystania z modeli LLM określoną normą etyczną IEEE/ISO/IEC 24748-7000-2022[3] jest więc ODPOWIEDZIALNOŚĆ (ang. accountability) lekarza. Można bezpieczenie korzystać z narzędzi jakimi są LLMy, warto i to się po prostu dzieje - należy jednak stosować zasadę „ufam ale sprawdzam" każdorazowo oceniając wynik działania LLM tak, jak ocenia się wynik pracy asystenta lub stażysty (nawiasem mówiąc, czasem skłonnego do halucynacji). AI nie zastępuje diagnozy, może wspierać procesy administracyjne.

Po drugie modele językowe LLM najczęściej są dostępne w Internecie. Stąd powoływana norma stawia jasno drugie zalecenie jakim jest PRYWATNOŚĆ (ang. privacy). Do Internetu nigdy nie wpisujemy danych osobowych: imion, nazwisk, numerów PESEL oraz unikalnych opisów przypadków pozwalających na identyfikację pacjenta. Tego nie róbmy też w przypadku ChataGPT lub Gemini w przeglądarce internetowej lub telefonie.

Korzystając z LLM w ramach jednego z wyżej podanych 7 przypadków można bezpiecznie opisywać objawy używając ogólnych terminów: np. "pacjent, mężczyzna, 45 lat". Nawet w takim przypadku należy jednak pamiętać, że dane te "karmią model" – dane wpisane do publicznych modeli mogą służyć do ich dalszego uczenia. A zatem ten sam LLM zapytany przez kogoś innego może wylosować odpowiedź łącząc słowa i zdania, które wpisaliśmy. Z konstrukcji tej matematycznej maszyny wynika, że może ona połączyć informacje w sposób, którego nie zamierzaliśmy, identyfikując „pacjenta M, z zaawansowaną chorobą otyłościową oraz zmianami skórnymi i odbarwieniami w okolicy szyi" w małym mieście, zupełnie tak jak działają plotki - zgadując o kogo może chodzić. Umiejętność radzenia sobie z tego typu ryzykami lekarze doskonale opanowali. Po postu LLMy trzeba „odczarować" i traktować jak asystenta, współpracującego z wszystkimi w mieście. Czasem może coś „chlapnąć" niedyskretnie...

W przypadku pracy naukowej także nie należy wprowadzać do LLMów tego co odkrywcze i stanowi własność intelektualną. Choć warto „zatrudnić" LLM do wykonania przeglądu literatury i porównać wynik z własnym badaniem.

Najważniejsze zalecenia bezpiecznego korzystania z modeli LLM w codziennej pracy lekarza to ODPOWIEDZIALNOŚĆ i PRYWATNOŚĆ. Poniżej krótka lista kontrolna "Zanim klikniesz Wyślij":

- Czy usunąłem dane osobowe?
- Czy sprawdziłem wynik w innym źródle?
- Czy model posiada certyfikację medyczną (jeśli dotyczy)?
- Czy bez wykorzystania LLM postąpiłbym tak samo (zdiagnozował, zalecił, wnioskował)?

Na koniec warto zaznaczyć, dzisiaj łatwo można pogłębić wiedzę nt. bezpiecznego wykorzystania modeli LLM. Warto przy tym korzystać z zaufanych w środowisku klinicznym autorytetów unikając celebrytów wieszczących koniec świata lub powszechną „medycynę LLMów". Obie skrajności są fałszywe.

Dla zainteresowanych zaawansowanymi wskazówkami dotyczącymi bezpieczeństwa dużych modeli językowych dostępna jest publikacja projektu OWASP pt. „2025 Top 10 Risk & Mitigations for LLMs and Gen AI Apps"[4]. W codziennym życiu kierowanie się zwykłą dla lekarza odpowiedzialnością (należytą starannością) oraz poufnością (zapewnienie prywatności i ochrony danych) są najlepszymi praktykami bezpieczeństwa. Wystarczy wiedza, że - jak piszą autorzy ekspozycji w Computer History Museum w Dolinie Krzemowej - LLMy to narzędzie podpowiadania słów bazujące na zaawansowanej statystyce. Narzędzie choć bardzo użyteczne, jak każde narzędzie, ma ograniczenia.

Tomasz Jaworski,

IEEE CertifAIEd Authorized Assessor w zakresie Etyki AI,

Dyrektor ds. Cyberbezpieczeństwa w Sektorze Zdrowia

Palo Alto Networks

[1] przykładowe współczesne LLMy to Bielik (projekt SpeakLeash i Cyfronet AGH) oraz PLLuM (tworzony przez konsorcjum naukowe na zlecenie państwa). Globalni dostawcy udostępniają np. ChatGPT (OpenAI), Gemini (Google), Claude (Anthropic)

[2] https://tinyurl.com/33fufvar

[3] IEEE/ISO/IEC 24748-7000-2022 „IEEE/ISO/IEC International Standard - Systems and software engineering - Life cycle management - Part 7000: Standard model process for addressing ethical concerns during system design"

[4] https://genai.owasp.org/llm-top-10/

cyber360

"Cybersecurity under control, be smart, be prepared"

CyberDefender

Kompleksowa ochrona przed cyberzagrożeniami

Czym jest CyberDefender?

CyberDefender to zaawansowana usługa Managed Detection and Response (MDR), oferująca kompleksowe zabezpieczenia IT dla organizacji 24/7. W odróżnieniu od klasycznych rozwiązań SOC, MDR zapewnia nie tylko monitorowanie, ale również aktywne reagowanie na incydenty oraz proaktywną prewencję zagrożeń.

Jak działa CyberDefender?

- **Monitorowanie**
  stała analiza ruchu sieciowego i zachowań użytkowników
- **Analiza**
  wykrywanie anomalii, korelacja logów i analiza zagrożeń
- **Reakcja**
  automatyczna i manualna neutralizacja zagrożeń
- **Odbudowa**
  działania naprawcze i rekomendacje w zakresie zabezpieczeń

Dlaczego warto wybrać CyberDefender?

- **Natychmiastowa reakcja na incydenty**
  czas reakcji nawet 15 minut.
- **Zgodność z regulacjami**
  spełnia wymagania NIS2, DORA, RODO
- **Zaawansowane technologie**
  SIEM, SOAR, XDR, analiza Dark Web, phishing
- **Kompleksowe wsparcie**
  prewencja, monitorowanie, reagowanie, działania poincydentalne
- **Szybkie wdrożenie**
  podstawowe funkcjonalności już od 5 dni
- **Raportowanie w czasie rzeczywistym**
  monitoring zagrożeń i analiza podatności

Czy Twoja organizacja jest gotowa na cyberzagrożenia?

CyberDefender to więcej niż SOC – to kompleksowa strategia bezpieczeństwa!

office@cyber360.pl

ul. Władysława IV 43
81-395 Gdynia

cyber360.pl

BENEFIT SOLUTION | Broker ubezpieczeniowy

Jesteśmy brokerem ubezpieczeniowym wspierającym firmy w świadomym zarządzaniu ryzykiem. Jednym z naszych obszarów specjalizacji są ubezpieczenia cyber dla podmiotów prowadzących działalność leczniczą. Dobieramy ochronę tak, aby działała w praktyce, gdy liczy się czas, odpowiedzialność i bezpieczeństwo danych.
Zapewniamy wsparcie na każdym etapie – od negocjacji warunków po pomoc w likwidacji szkód.

Formularz oceny ryzyka	
Nazwa Spółki/ REGON/ Adres strony internetowej	
Skonsolidowane przychody za ostatni rok obrotowy	
Jaka jest maksymalna liczba osób, które musiałyby zostać powiadomione w przypadku naruszenia danych umożliwiających identyfikację osoby (PII)?	
Czy Posiadają Państwo wdrożone uwierzytelnianie wieloskładnikowe (MFA) dla wszystkich możliwości zdalnego dostępu do sieci, w tym do poczty elektronicznej?	
Które z poniższych zabezpieczeń obejmują kopie zapasowe systemów o znaczeniu krytycznym (można zaznaczyć więcej niż jedną odpowiedź): a) niezmienne kopie zapasowe lub kopie tylko do odczytu / WORM (jednokrotny zapis, wielokrotny odczyt), b) kopie całkowicie offline lub air-gapped, odłączone od reszty sieci, c)dostęp ograniczony przez odrębne konta uprzywilejowane, niepowiązane z Active Directory ani innymi domenami, d) dostęp ograniczony z użyciem uwierzytelniania wieloskładnikowego (MFA), e) żadne z powyższych.	
Które z poniższych technologii ochrony punktów końcowych są stosowane na wszystkich laptopach, komputerach stacjonarnych oraz serwerach (można zaznaczyć więcej niż jedną odpowiedź): a) zaawansowane oprogramowanie antywirusowe i antymalware z mechanizmami heurystycznymi, b) filtrowanie adresów URL lub stron internetowych, c) izolacja i ograniczanie aplikacji (application isolation and containment), d) scentralizowana platforma ochrony punktów końcowych, e) EDR, XDR, lub MDR, f) żadne z powyższych.	
Czy w ciągu ostatnich 3 lat doświadczyli Państwo jakiegokolwiek incydentu cybernetycznego (w tym awarii systemu, naruszenia danych, skarg, działań lub postępowań regulacyjnych związanych z bezpieczeństwem danych i/lub systemów) lub czy znane są Państwu jakiekolwiek okoliczności mogące skutkować roszczeniem z tytułu ubezpieczenia cybernetycznego?	

Na podstawie przesłanych danych z formularza otrzymają Państwo wstępną propozycję ochrony ubezpieczeniowej.
Zapraszamy do bezpośredniego kontaktu

www.b-solution.pl +48 575 355 095 a.subczynska@b-solution.pl

ADM Group

Skutecznie pozyskujemy granty i fundusze unijne dla sektora ochrony zdrowia, pomagając sfinansować inwestycje w zakresie:

- **cyberbezpieczeństwa,**
- cyfryzacji usług,
- modernizacji infrastruktury,

a także

- wdrażania nowoczesnych rozwiązań medycznych,
- realizacji programów profilaktycznych i rehabilitacyjnych.

www.admgroup.pl dotacje@admgroup.pl

CLICO

paloalto NETWORKS

WEBINARIUM

Przeglądarka jako nowa linia obrony szpitala

Praktyczne warsztaty Prisma Browser

21.04.2026, 10:00 – 11:30 | ONLINE

Codzienna praca personelu medycznego i administracyjnego coraz częściej odbywa się w przeglądarce — to właśnie tam realizowany jest dostęp do systemów, aplikacji i danych pacjentów.

Podczas praktycznych warsztatów pokażemy, jak **Prisma Browser** pozwala zabezpieczyć dokumentację medyczną i egzekwować wymagania bezpieczeństwa. **Bez zmian przyzwyczajeń klinicystów i personelu** przeglądarka zapewnia właściwe środki techniczne dla spełnienia wymagań regulatora.

Uczestnicy zobaczą w praktyce m.in. ochronę danych wrażliwych i naukowych (DLP), kontrolę dostępu użytkowników, ochronę plików, kontrolę schowka i zrzutów ekranu oraz wygodę wykorzystania przeglądarki jako elementu bezpieczeństwa w środowisku szpitalnym.

Warsztaty mają charakter **praktyczny** — krok po kroku przejdziemy przez konfigurację i testowanie kluczowych funkcjonalności.

Zarejestruj się i sprawdź, jak w praktyce zabezpieczyć pracę w przeglądarce.

PIERWSZY W EUROPIE STANDARD CYBERBEZPIECZEŃSTWA DLA MŚP

5 STREF DZIAŁANIA
48 KONTROLEK
GOTOWE ARTEFAKTY
CERTYFIKACJA
DODATKI SEKTOROWE

SPOŁECZNOŚĆ
ALERTY
EDUKACJA
DORADZTWO
USŁUGI PREMIUM

WWW.SHIELDNET.EU

STANDARD SPOŁECZNOŚĆ

Słownik skótów i pojęć

ORGANIZACJE, DYREKTYWY I FUNKCJE

CBZC: Centralne Biuro Zwalczania Cyberprzestępczości – jednostka Policji współpracująca przy ściganiu sprawców ataków.

CeZ: Centrum e-Zdrowia – jednostka podległa Ministerstwu Zdrowia, odpowiedzialna za utrzymanie i rozwój systemów centralnych oraz realizację strategicznych projektów e-zdrowia. W ramach bezpieczeństwa monitoruje skalę ataków w sektorze oraz prowadzi sektorowy zespół CSIRT CeZ, stanowiący główny punkt zgłaszania incydentów dla podmiotów leczniczych.

CSIRT: (z ang. Computer Security Incident Response Team) – zespół reagowania na incydenty bezpieczeństwa komputerowego (np. CSIRT NASK lub sektorowy CSIRT CeZ).

DORA: Unijne rozporządzenie dotyczące operacyjnej odporności cyfrowej sektora finansowego, wspomniane w kontekście zgodności usług ochronnych.

IOD: Inspektor Ochrony Danych – osoba odpowiedzialna w szpitalu za nadzór nad bezpieczeństwem danych osobowych.

NIS2: Unijna dyrektywa nakładająca na sektor ochrony zdrowia obowiązek systemowego zarządzania cyberbezpieczeństwem i wprowadzająca osobistą odpowiedzialność Zarządu.

RODO: Ogólne rozporządzenie o ochronie danych osobowych, regulujące m.in. kwestie wycieków danych pacjentów.

TECHNOLOGIE I SYSTEMY MEDYCZNE

EDM: Elektroniczna Dokumentacja Medyczna – cyfrowy zapis historii leczenia pacjenta.

HIS: (z ang. Hospital Information System) – kompleksowy system informatyczny do zarządzania pracą szpitala.

LLM: (z ang. Large Language Models) – Duże Modele Językowe (np. ChatGPT, Gemini), czyli narzędzia sztucznej inteligencji do pracy z tekstem oparte na statystyce.

MDR: (z ang. Managed Detection and Response) – zaawansowana usługa aktywnego monitorowania i reagowania na zagrożenia w trybie 24/7.

MFA: (z ang. Multi-Factor Authentication) – uwierzytelnianie wieloskładnikowe; dodatkowe potwierdzenie tożsamości, np. poprzez kod w telefonie.

PACS: System archiwizacji i przesyłania obrazów medycznych (np. z RTG czy rezonansu).

RAM: Pamięć operacyjna komputera; dane w niej zawarte są ulotne i znikają po wyłączeniu urządzenia, dlatego po ataku nie należy restartować sprzętu bez polecenia informatyka.

SOC: (z ang. Security Operations Center) – centrum operacji bezpieczeństwa zajmujące się monitorowaniem incydentów.

ZAGROŻENIA I INCYDENTY

Halucynacja LLM: Zjawisko, w którym model sztucznej inteligencji generuje treść poprawną gramatycznie, ale całkowicie błędną merytorycznie lub klinicznie.

IoC: (z ang. Indicators of Compromise) – wskaźniki naruszenia bezpieczeństwa, np. adresy IP czy nazwy hostów, o które pytają zespoły IT po ataku.

Logi: Rejestry zdarzeń; cyfrowe zapisy dokumentujące każdą operację wykonaną w systemie teleinformatycznym.

Phishing: Metoda oszustwa polegająca na podszywaniu się pod instytucje (np. bank, NFZ) w e-mailach lub SMS-ach w celu wyłudzenia haseł lub zainfekowania komputera.

Ransomware: Rodzaj złośliwego oprogramowania ("cyfrowy haracz"), które blokuje dostęp do plików i żąda okupu za ich odblokowanie.

Ślad cyfrowy: Zapis binarny będący fragmentem kodu generowanego przez sprzęt, dokumentujący aktywność użytkownika w systemie.