WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

Dlaczego hakerzy kochają branżę medyczną i jak reagować na tę toksyczną miłość?

HOSPITAL 360 CONFERENCE 2025

Sylwia Raczyńska

SECURE MEDICA

WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

KIM JESTEŚMY?

Nasza misja: proaktywna ochrona polskiej służby zdrowia

- ➔ Symulujemy ataki hakerskie i przeprowadzamy testy odporności w **realnych warunkach**
- ➔ Wykrywamy luki bezpieczeństwa oraz tworzymy rekomendacje ich naprawy
- ➔ Przeprowadzamy szkolenia dla kadry zarządzającej szpitali
- ➔ Pomagamy wdrażać zabezpieczenia w dobie nowych regulacji (Dyrektywa NIS2)

SECURE MEDICA

WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

DLACZEGO HAKERZY KOCHAJĄ BRANŻĘ MEDYCZNĄ?

1 Jak bardzo podatna na ataki jest branża medyczna?

- Kto atakuje?
- Niska odporność cyfrowa
- Wartość danych medycznych

2 Case studies: ataki na polskie placówki

- Laboratoria ALAB
- Szpital MSWiA w Krakowie
- ICZMP w Łodzi

3 Jak reagować na cyberatak?

- Identyfikacja i izolacja
- Eliminacja i przywrócenie działania
- Wnioski, komunikacja i obowiązki prawne

4 Podsumowanie: Co robić? Jak żyć?

WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

1

Jak bardzo podatna na ataki jest branża medyczna?

- Kto atakuje?
- Niska odporność cyfrowa
- Wartość danych medycznych

KTO ATAKUJE?

Grupy cyberprzestępcze

Ransomware gangs – najczęściej odpowiedzialne (np. LockBit, ALPHV/BlackCat, Rhysida, Cl0p).

Motywacja: **pieniądze** – szyfrowanie systemów, żądanie okupu, publikacja danych pacjentów jako presja. Ofiary: od małych klinik po duże szpitale uniwersyteckie.

Grupy zajmujące się wyciekiem danych – sprzedają dane medyczne na darknecie (np. numery polis, dokumentacja pacjentów, recepty).

Dane medyczne są cenne, bo można je wykorzystać w **oszustwach ubezpieczeniowych** i **kradzieży tożsamości**.

Hacktywiści

Motywacja: **polityczna lub ideologiczna**.

Przykłady: ataki DDoS na systemy szpitalne w Europie w ramach protestów politycznych czy w czasie konfliktu Rosja–Ukraina. Cel: zakłócenie usług, wywołanie chaosu, presja medialna.

Aktorzy państwowi (APT – Advanced Persistent Threats)

Zdarzają się **szpiegowskie operacje sponsorowane przez państwa**.

Motywacje: kradzież badań medycznych i farmaceutycznych (np. szczepionki, biotechnologia), zdobycie danych pacjentów jako potencjalny zasób wywiadowczy.

ENISA wskazuje, że APT-y interesują się m.in. laboratoriami, firmami farmaceutycznymi i systemami e-zdrowia.

Insider Threat

Czasami zagrożenie pochodzi **od wewnątrz** – np. nieuczciwy pracownik wynoszący dane pacjentów.

Znacznie częściej jednak dochodzi do **nieumyślnych incydentów**: kliknięcie w phishing, nieuprawnione użycie prywatnych urządzeń, słabe hasła.

1

NISKA ODPORNOŚĆ CYFROWA

Przestarzała infrastruktura IT

Szpitale i kliniki często:

- używają **starego sprzętu i systemów** (np. Windows 7, XP w urządzeniach medycznych),
- nie mają zasobów na **ciągłe aktualizacje** czy dedykowane zespoły cyberbezpieczeństwa,
- posiadają **rozproszone systemy IT** (EHR, laboratoria, sprzęt IoMT).

Placówki muszą działać 24/7, co **utrudnia przerwy na modernizacje**.
Personel medyczny zwykle skupia się na pacjencie, a nie na cyberhigienie – co podnosi ryzyko phishingu czy słabych haseł.

Najprościej mówiąc: szpitale stały się **łatwym celem**, gdyż przechowują dane bezcenne dla przestępców, nie mają środków na solidną obronę, a jednocześnie nie mogą sobie pozwolić na przestój. To kombinacja, która czyni ochronę zdrowia jednym z najczęściej atakowanych sektorów publicznych w Europie.

Rozwój cyfrowej medycyny

Telemedycyna, IoMT (Internet of Medical Things), e-recepty, e-dokumentacja – cyfryzacja tworzy nowe punkty wejścia.

Urządzenia medyczne (np. pompy infuzyjne, tomografy) często mają **niskie zabezpieczenia**, ale są podłączone do sieci.

Integracja z systemami zewnętrznymi (ubezpieczyciele, laboratoria) zwiększa **podatność na ataki**.

Krytyczny charakter usług = presja na okup

Ochrona zdrowia to **usługa krytyczna** – każda godzina przestoju oznacza zagrożenie dla życia pacjentów.

Dla przestępców oznacza to **większe prawdopodobieństwo zapłaty okupu**, bo szpital nie może czekać tygodniami, aż systemy zostaną odbudowane.

Odwoływanie zabiegów, blokada laboratoriów, utrata dostępu do dokumentacji – prowadzi do **natychmiastowych konsekwencji klinicznych**.

WARTOŚĆ DANYCH MEDYCZNYCH

Dane zdrowotne są cenniejsze, niż dane finansowe

Pacjentów nie da się „zresetować” jak kart kredytowych. Rekord medyczny zawiera:

- dane osobowe (PESEL, adres, kontakt),
- informacje o stanie zdrowia, diagnozach, receptach,
- dane ubezpieczeniowe i finansowe.

Na czarnym rynku pełny rekord medyczny jest wyceniany **nawet 10x drożej** niż dane dotyczące karty płatniczej.

Możliwości wykorzystania:

- **oszustwa ubezpieczeniowe** (np. fikcyjne rozliczenia usług),
- **kradzież tożsamości**,
- **szantaż indywidualnych pacjentów** (np. ujawnienie wrażliwych diagnoz).

Presja regulacyjna i reputacyjna

Ujawnienie incydentu oznacza:

- konieczność zgłoszenia do regulatora (np. RODO, NIS2),
- potencjalne **kary finansowe**,
- utratę zaufania pacjentów.

Cyberprzestępcy uważają, że szpitale zapłacą, by uniknąć publicznego wycieku.

Znaczenie strategiczne (APT i szpiegostwo)

Dane i technologie medyczne mają znaczenie **geopolityczne i gospodarcze**.

Przykłady motywacji państwowych grup APT:

- **kradzież badań naukowych** (np. nad szczepionkami COVID-19, terapiami onkologicznymi),
- **dane populacyjne** – potencjalnie użyte w wywiadzie, modelowaniu zdrowia publicznego, a nawet w operacjach psychologicznych.

Branża medyczna staje się częścią **infrastruktury krytycznej** – jej destabilizacja osłabia państwo.

Ciekawostka: jeszcze kilkanaście lat temu cyberatak na szpital był nie do pomyślenia – nawet dla cyberprzestępców takie działanie było nieetyczne oraz było w branży potępiane.

WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

2

Case studies: ataki na polskie placówki

Laboratoria ALAB

Szpital MSWiA w Krakowie

ICZMP w Łodzi

Case studies: ataki na polskie placówki

ICZMP w Łodzi	**2022 – sparaliżowana infrastruktura IT szpitala**
Laboratoria ALAB	**2023 – wyciek ogromnej ilości danych wrażliwych w tym PESEL, adresy zamieszkania, imiona i nazwiska pacjentów**
Szpital MSWiA w Krakowie	**2025 – znacznie spowolnione działanie szpitala oraz chaos informacyjny**

Case studies: Instytut Centrum Zdrowia Matki Polki w Łodzi

Koniec października 2022 — INFILTRACJA

Uzyskanie **początkowego dostępu** do sieci szpitala przy użyciu skradzionych poświadczeń użytkownika.

Prawdopodobny wektor ataku: phishing, błędna konfiguracja systemów lub użycie słabych haseł administracyjnych bez MFA, które mogły zostać złamane metodami brute-force.

Koniec października 2022 — ROZPOZNANIE

Pracownicy zaczęli zauważać problemy z siecią (zgłoszone już przed 31.10.2022). W tym czasie atakujący cicho mapowali infrastrukturę, lokalizując krytyczne serwery i dane pacjentów, w tym systemy kopii zapasowych.

Eskalacja uprawnień: Przejęcie kontroli nad kontami administratorskimi i uzyskanie dostępu do kluczowych systemów.

Kradzież danych: przed zaszyfrowaniem atakujący prawdopodobnie skradli dane osobowe pacjentów oraz dokumentację medyczną.

Koniec października 2022 — DESTRUKCJA

Aktywowano ransomware **LockBit 3.0**, który **zaszyfrował pliki na maszynach wirtualnych i serwerze backupowym**, uniemożliwiając odzyskanie danych.

Skutki kliniczne: paraliż systemów, konieczność powrotu do dokumentacji papierowej, odwoływanie wizyt i badań, utrudnienia w wystawianiu recept, zagrożenie dla zdrowia pacjentów.

Skutki bezpieczeństwa danych: potencjalny wyciek danych pacjentów, zgłoszenie incydentu do UODO.

Początek listopada 2022 — REAKCJA

Personel IT zauważył spowolnienie działania systemu i problemy z dostępem do plików, a następnie całkowity paraliż sieci.

ICZMP prewencyjnie wyłączyło systemy IT, aby powstrzymać dalsze rozprzestrzenianie się infekcji.

Przywrócono ręczną dokumentację papierową. Szpital otrzymał wsparcie od Ministerstwa Zdrowia, Centrum e-Zdrowia oraz NASK.

Połowa listopada 2022 — ODZYSKIWANIE

Proces przywracania systemów z kopii zapasowych trwał wiele tygodni. Priorytetowo przywracano systemy kliniczne, podczas gdy pozostałe systemy zostały odtworzone później.

Koszty: Atak generował ogromne koszty związane z przestojem, odtworzeniem systemów, karami Urzędu Ochrony Danych Osobowych (UODO) oraz potencjalnymi odszkodowaniami.

Pełne przywrócenie systemów nastąpiło dopiero około połowy listopada 2022.

Case studies: Laboratoria ALAB

Październik 2023 — INFILTRACJA I ROZPOZNANIE

Napastnicy uzyskali nieautoryzowany dostęp do systemów ALAB, co umożliwiło pobranie danych medycznych i kontraktowych gromadzonych w latach 2017–2023.

Prawdopodobny wektor ataku: wykorzystanie luk w zabezpieczeniach systemów, przechwycenie poświadczeń użytkowników (np. phishing, słabe hasła lub brak MFA), a także potencjalne niewykryte podatności. Długotrwały dostęp pozwolił atakującym na ciche przeszukiwanie systemów i gromadzenie dużych zbiorów danych bez wykrycia przez administratorów.

17 listopada 2023 — PUBLIKACJA DANYCH

Grupa ransomware ***RA World*** **opublikowała próbkę wykradzionych danych** na swoim blogu, zawierającą wyniki ponad 50 000 badań medycznych oraz dane osobowe pacjentów.

Zakres danych: Ponad 110 000 plików z wynikami badań pacjentów.

Dane osobowe: Imię i nazwisko, PESEL, adres zamieszkania, daty badań, wyniki badań i identyfikatory testów.

19 listopada 2023 — WYKRYCIE ATAKU

Firma nie zauważyła wcześniejszego wycieku danych, mimo że pliki zostały umieszczone na blogu cyberprzestępców już 17 listopada.

ALAB zaobserwował ponowną próbę zmasowanego ataku na swoje serwery 19 listopada. Podjęto działania mające na celu zabezpieczenie systemów i zminimalizowanie skutków ataku.

21 listopada 2023 — REAKCJA

ALAB zgłosiło naruszenie danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (UODO).

Rozpoczęto postępowanie wyjaśniające oraz współpracę z Rzecznikiem Praw Pacjenta w celu ochrony interesów osób poszkodowanych

27 listopada 2023 — UPUBLICZNIENIE WYCIEKU

Po kilku dniach od zgłoszenia incydentu ALAB opublikował publiczne oświadczenie dotyczące wycieku danych.

Treść oświadczenia: Firma potwierdziła, że doszło do ataku ransomware, w wyniku którego wykradzione zostały dane pacjentów.

Reakcja: ALAB podjęło działania mające na celu zabezpieczenie danych oraz poinformowanie osób poszkodowanych.

Case studies: Szpital MSWiA w Krakowie

Przed 8 marca 2025 — INFILTRACJA I ROZPOZNANIE

Prawdopodobnie już w lutym 2025 napastnicy uzyskali dostęp do sieci szpitala.

Możliwe wektory ataku: phishing pracownika (otwarcie załącznika, kliknięcie linku), wkorzystanie podatności w serwerze poczty lub oprogramowaniu medycznym, użycie skradzionych danych uwierzytelniających.

Atakujący rozpoznali infrastrukturę i przygotowali oprogramowanie ransomware do rozprzestrzenienia się w całej sieci.

8 marca 2025 — EGZEKUCJA ATAKU

Lekarka dyżurna zauważyła problem – systemy informatyczne nie działały.

Informatyk po zalogowaniu zobaczył **klasyczny komunikat ransomware** – pliki zostały zaszyfrowane, a przestępcy żądali okupu.

Zablokowane zostały systemy elektronicznej dokumentacji medycznej (EDM), co w praktyce oznaczało brak dostępu do:

- historii leczenia,
- wyników badań,
- grafiku przyjęć pacjentów itp.

8 marca 2025 — PIERWSZE REAKCJE

Szpital wdrożył **procedury awaryjne** – natychmiastowe przejście na dokumentację papierową.

Zawiadomiono **policję, CERT Polska, Centrum e-Zdrowia, Ministerstwo Cyfryzacji i MSWiA**.

Wdrożono izolację zainfekowanych segmentów sieci, by ograniczyć dalsze rozprzestrzenianie się złośliwego oprogramowania.

9 marca 2025 — KOMUNIKATY PUBLICZNE

Minister cyfryzacji Krzysztof Gawkowski określił incydent jako **„groźny cyberatak”**, ale zapewnił, że życie i zdrowie pacjentów nie jest zagrożone a szpital działa w trybie awaryjnym.

Minister spraw wewnętrznych Tomasz Siemoniak poinformował o uruchomieniu **koordynacji służb** i intensywnym dochodzeniu.

Potwierdzono, że doszło do **naruszenia danych osobowych** – szpital musiał oficjalnie zgłosić incydent do UODO.

10 marca i kolejne tygodnie — STABILIZACJA

10 marca Dyrekcja szpitala ogłosiła, że placówka **funkcjonuje niemal normalnie**, ale oddział neurologii wstrzymał przyjęcia planowe, karetki przestały dowozić pacjentów w stanach ostrych oraz rejestracja elektroniczna przestała funkcjonować.

W kolejnych dniach marca trwało stopniowe przywracanie systemów z kopii zapasowych. Szpital przewidywał, że pełne przywrócenie cyfrowych usług zajmie **kilka tygodni**. Dochodzenie prowadziło **Centralne Biuro Zwalczania Cyberprzestępczości (CBZC)**, we współpracy z prokuraturą i zespołami CERT.

WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

3

Jak reagować na cyberatak?

- Identyfikacja i izolacja
- Eliminacja i przywrócenie działania
- Wnioski, komunikacja i obowiązki prawne

MÓJ SZPITAL PADŁ OFIARĄ CYBERATAKU! CO ROBIĆ?

1 IDENTIFICATION

- Detekcja i weryfikacja ataku
- Natychmiastowa eskalacja
- Wstępna ocena skali ataku
- Zabezpieczenie dowodów ataku

2 CONTAINMENT

- Odcięcie od sieci zewnetrznej
- Segmentacja sieci wewnętrznej
- Działanie w trybie awaryjnym

3 ERADICATION

- Identyfikacja przyczyn cyberataku
- Usunięcie złośliwego oprogramowania
- Usunięcie podatności
- Rotacja haseł

4 RECOVERY

- Przywrócenie z kopii zapasowych
- Weryfikacja i testowanie
- Stopniowe uruchamianie usług
- Wzmożone monitorowanie

5 LESSONS LEARNED

- Raport poincydentalny
- Analiza Post Mortem
- Wdrożenie działań naprawczych

6 COMMUNICATION

- CSIRT NASK
- UODO
- ORGANY ŚCIGANIA
- KOMUNIKACJA WEWNĘTRZNA I ZEWNĘTRZNA

Jak najszybsze potwierdzenie, że incydent ma miejsce i określenie jego wstępnego zakresu

IDENTIFICATION

1

- Detekcja i weryfikacja ataku
- Natychmiastowa eskalacja
- Wstępna ocena skali ataku
- Zabezpieczenie dowodów ataku

Potwierdzenie, że nietypowe zachowanie systemu to faktycznie atak (np. na podstawie alertów z systemów bezpieczeństwa, informacji od pracowników, pojawienia się notatki z żądaniem okupu).

Powołanie i aktywacja Sztabu Kryzysowego / Zespołu Reagowania na Incydenty (CSIRT). Kluczowe jest, aby każdy pracownik wiedział, komu i jak zgłosić podejrzenie ataku.

Szybka analiza mająca na celu odpowiedź na pytania:

- Które systemy są dotknięte? (np. system szpitalny HIS, system laboratoryjny LIS, poczta)
- Jakie oddziały lub lokalizacje są zagrożone?
- Jaki jest potencjalny wpływ na bezpieczeństwo pacjentów i ciągłość działania?

Forensics First: Przed podjęciem jakichkolwiek działań naprawczych, kluczowe jest zabezpieczenie nietrwałych dowodów (np. pamięć RAM serwerów, logi sieciowe). Należy wykonać obrazy dysków skompromitowanych maszyn, aby umożliwić późniejszą analizę bez zacierania śladów.

Powstrzymanie rozprzestrzeniania się ataku i odizolowanie napastnika od reszty infrastruktury

CONTAINMENT

2

- Odcięcie od sieci zewnetrznej
- Segmentacja sieci wewnętrznej
- Działanie w trybie awaryjnym

To pierwszy i najważniejszy punkt. Należy natychmiast odłączyć zainfekowaną część sieci (lub w razie wątpliwości całą placówkę) od internetu.

Jeśli to możliwe, należy odizolować zainfekowane komputery i serwery od reszty sieci lokalnej, aby zapobiec dalszemu rozprzestrzenianiu się np. ransomware.

Downtime Procedures: Uruchomienie wcześniej przygotowanych procedur funkcjonowania bez dostępu do kluczowych systemów IT.

- Priorytet: Utrzymanie ciągłości opieki nad pacjentami.
- Działania: Powrót do papierowej dokumentacji, ręczne procesy rejestracji, komunikacja telefoniczna i przez gońców.

Całkowite usunięcie przyczyny incydentu z sieci placówki

ERADICATION

3

- Identyfikacja przyczyn cyberataku
- Usunięcie złośliwego oprogramowania
- Usunięcie podatności
- Rotacja haseł

Root Cause Analysis: Na podstawie zebranych dowodów należy ustalić, jak atakujący dostał się do sieci (np. phishing, niezabezpieczona usługa RDP, niezałatana luka).

Wyeliminowanie wirusów, trojanów, malware i innych narzędzi użytych przez atakujących.

Załatanie luki bezpieczeństwa, która umożliwiła atak. Bez tego kroku przywrócenie systemów mija się z celem, bo atakujący może natychmiast wrócić.

Zmiana wszystkich haseł, które mogły zostać skompromitowane, zwłaszcza kont administracyjnych i usługowych.

Bezpieczne i kontrolowane przywrócenie normalnego funkcjonowania systemów

RECOVERY

4

Odtwarzanie systemów i danych z czystych, zaufanych kopii zapasowych wykonanych przed datą incydentu.

Przed podłączeniem do sieci produkcyjnej, przywrócone systemy muszą zostać dokładnie przeskanowane i przetestowane w izolowanym środowisku w poszukiwaniu śladów zagrożenia.

Przywracanie funkcjonalności etapami, zaczynając od systemów najbardziej krytycznych dla życia i zdrowia pacjentów (np. systemy na OIT, SOR).

Po przywróceniu systemów należy je intensywnie monitorować pod kątem wszelkich anomalii, aby upewnić się, że zagrożenie nie powróciło.

- Przywrócenie z kopii zapasowych
- Weryfikacja i testowanie
- Stopniowe uruchamianie usług
- Wzmożone monitorowanie

Wyciągnięcie wniosków z incydentu i wzmocnienie obrony, aby uniknąć podobnych sytuacji w przyszłości

LESSONS LEARNED

5

Raport poincydentalny

Analiza Post Mortem

Wdrożenie działań naprawczych

Raport Poincydentalny: Stworzenie szczegółowego raportu opisującego cały przebieg ataku, reakcję zespołu i skutki incydentu.

Spotkanie sztabu kryzysowego i kluczowych pracowników w celu omówienia, co zadziałało dobrze, a co należy poprawić w planie reagowania.

Aktualizacja procedur bezpieczeństwa, wdrożenie nowych narzędzi, przeprowadzenie dodatkowych szkoleń dla personelu.

Działania równoległe: komunikacja i obowiązki prawne

Zgłoszenia do Organów Regulacyjnych:

- CSIRT NASK: Zgłoszenie incydentu jako operator usługi kluczowej (zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa).
- Prezes Urzędu Ochrony Danych Osobowych (UODO): Zgłoszenie naruszenia ochrony danych osobowych w ciągu 72 godzin od jego stwierdzenia, jeśli istnieje ryzyko naruszenia praw lub wolności osób fizycznych.
- Organy Ścigania (Policja / Prokuratura): Złożenie zawiadomienia o podejrzeniu popełnienia przestępstwa.

Komunikacja Wewnętrzna:

Regularne i transparentne informowanie pracowników o statusie sytuacji, dalszych krokach i obowiązujących procedurach awaryjnych.

Komunikacja Zewnętrzna:

- Pacjenci: Zarządzanie informacją o utrudnieniach (np. odwołane wizyty, opóźnienia), zapewniając jednocześnie o bezpieczeństwie i ciągłości opieki w krytycznych obszarach.
- Media i Opinia Publiczna: Przygotowanie spójnych i rzeczowych komunikatów, aby uniknąć dezinformacji i paniki. W przypadku naruszenia danych o wysokim ryzyku, poinformowanie osób, których dane dotyczą, jest obowiązkiem prawnym (zgodnie z RODO).

6

COMMUNICATION

CSIRT NASK

UODO

ORGANY ŚCIGANIA

KOMUNIKACJA WEWNĘTRZNA I ZEWNĘTRZNA

WITH US, YOU CAN FEEL SAFE IN THE CYBERSPACE

4

Podsumowanie: Co robić? Jak żyć?

JAK DZIAŁA SECURE MEDICA?

1 Software Security

- Testy penetracyjne aplikacji internetowych
- Testy penetracyjne aplikacji lokalnych (fat client)
- Analiza kodu aplikacji
- Sprawdzenie istniejących podatności
- Przegląd konfiguracji systemów operacyjnych

2 Hardware Security

- Inwentaryzacja sprzętu IT
- Test przeciążeniowe infrastruktury (DDoS)
- Audyt dostępu do sprzętów komputerowych
- Testy penetracyjne infrastruktury
- Sprawdzenie istniejących podatności

3 Network Security

- Testy penetracyjne sieci lokalnej i zdalnego dostępu
- Przegląd konfiguracji Wi-Fi i VPN
- Sprawdzenie topologii sieci i segmentacji
- Audyt zabezpieczeń brzegowych (firewall, IDS/IPS)

4 Human Factor & Awareness

- AI-powered Vishing (test socjotechniczny)
- AI-generated Phishing (test socjotechniczny)
- AI-generated Fake Documentation (test socjotechniczny)
- AI-generated Impersonation (test socjotechniczny)
- Ankiety bezpieczeństwa i wywiady

5 Compliance & Governanc

- Ocena zgodności z NIS2 / KSC
- Przegląd polityk bezpieczeństwa IT
- Przegląd procedur bezpieczeństwa IT
- Przegląd procesów bezpieczeństwa IT

JAK DZIAŁA SECURE MEDICA?

Software Security

1

Aktywność	Opis	Efekt
Testy penetracyjne aplikacji webowych	Manualna i automatyczna weryfikacja aplikacji z perspektywy użytkownika zewnętrznego oraz wewnętrznego, w oparciu o dobre praktyki (OWASP Top 10).	1. **Wykrywamy błędy, zanim staną się problemem** – sprawdzamy aplikacje, aby wychwycić słabe punkty zanim zrobi to haker. 2. **Chronimy dane i działanie szpitala** – dobrze zabezpieczone systemy zmniejszają ryzyko wycieku danych, awarii lub sabotażu, który mógłby zaszkodzić reputacji szpitala. 3. **Oszczędzamy czas i pieniądze** – im wcześniej wykryjemy i naprawimy błąd, tym mniej to kosztuje. Dzięki temu unikamy drogich poprawek, przestojów i kryzysów.
Testy penetracyjne aplikacji lokalnych	Analiza logiki działania aplikacji, komunikacji z backendem oraz możliwości eskalacji uprawnień.	
Analiza kodu aplikacji	Przegląd kodu pod kątem typowych błędów bezpieczeństwa oraz podatności (np. brak walidacji danych, niewłaściwa obsługa sesji).	
Sprawdzenie wykrytych podatności	Retest luk w komponentach aplikacyjnych na podstawie wcześniej wykonywanych testów bezpieczeństwa.	
Przegląd konfiguracji systemów operacyjnych	Weryfikacja bezpieczeństwa środowiska uruchomieniowego aplikacji (m.in. uprawnienia, logging, hardening).	

JAK DZIAŁA SECURE MEDICA?

Hardware Security

2

Aktywność	Opis	Efekt
Inwentaryzacja sprzętu IT	Identyfikacja i skatalogowanie urządzeń wykorzystywanych w środowisku IT placówki medycznej. Pozwala to na lepsze zarządzanie ryzykiem IT oraz kontrolę nad cyklem życia urządzeń.	1. **Ochrona przed atakami na poziomie sprzętowym** – przeciwdziałanie zagrożeniom takim jak malware, backdoory sprzętowe wzmacnia odporność całego środowiska IT. 2. **Redukcja ryzyka sabotażu, kradzieży danych i trwałych kompromitacji** – ochrona komponentów sprzętowych minimalizuje ryzyko trwałego osadzenia złośliwego oprogramowania lub fizycznego sabotażu. 3. **Zabezpieczenie fizycznego i logicznego dostępu do urządzeń** – ogranicza możliwość manipulacji i nieautoryzowanego dostępu.
Testy przeciążeniowe infrastruktury (DDoS)	Symulacja ataków typu DDoS w celu sprawdzenia, jak infrastruktura reaguje na nagły wzrost ruchu sieciowego.	
Audyt dostępu do sprzętów komputerowych	Analiza sposobu zabezpieczenia fizycznego i logicznego dostępu do komputerów. Celem jest wykrycie luk, które mogłyby umożliwić nieautoryzowany dostęp.	
Testy penetracyjne infrastruktury	Przeprowadzanie kontrolowanych prób przełamania zabezpieczeń urządzeń w celu identyfikacji słabych punktów.	
Sprawdzenie istniejących podatności	Retest luk w komponentach infrastruktury na podstawie wcześniej wykonywanych testów bezpieczeństwa.	

JAK DZIAŁA SECURE MEDICA?

Network Security

3

Aktywność	Opis	Efekt
Testy penetracyjne sieci lokalnej i zdalnego dostępu	Weryfikacja odporności sieci LAN i połączeń zdalnych na ataki. Pozwala wykryć luki umożliwiające przejęcie dostępu do systemów.	1. **Wykrywamy zagrożenia, zanim zrobią to przestępcy** – testujemy, jak łatwo ktoś z zewnątrz mógłby dostać się do systemów i pokazujemy, gdzie są słabe punkty. 2. **Chronimy dostęp zdalny i sieci Wi-Fi** – Sprawdzamy, czy hasła, ustawienia i technologie używane w szpitalu są bezpieczne i aktualne. Dzięki temu nikt niepożądany nie połączy się zdalnie z siecią. 3. **Sprawdzamy, czy granice szpitala w Internecie są dobrze chronione** – analizujemy zapory i systemy wykrywające ataki, by upewnić się, że nie ma luk w miejscach, gdzie szpital łączy się ze światem.
Przegląd konfiguracji Wi-Fi i VPN	Ocena ustawień zabezpieczeń sieci bezprzewodowej i tuneli VPN. Umożliwia eliminację słabych haseł, nieaktualnych protokołów i błędów konfiguracyjnych.	
Sprawdzenie topologii sieci i segmentacji	Analiza podziału sieci na strefy i rozmieszczenia urządzeń. Celem jest ograniczenie rozprzestrzeniania się zagrożeń wewnątrz infrastruktury.	
Audyt zabezpieczeń brzegowych (firewall, IDS/IPS)	Kontrola konfiguracji zapór sieciowych i systemów wykrywania intruzów. Pozwala upewnić się, że krytyczne punkty styku z Internetem są właściwie chronione.	

JAK DZIAŁA SECURE MEDICA?

4 Human Factor & Awareness

Aktywność	Opis	Efekt
AI-powered Vishing (test socjotechniczny)	Symulacja ataków telefonicznych z użyciem AI, imitujących głos kadry zarządzającej. Testuje czujność personelu w sytuacjach nacisku i manipulacji głosowej.	1. **Lepsze przygotowanie na nowoczesne oszustwa z wykorzystaniem AI** – testy z użyciem sztucznej inteligencji uczą, jak nie dać się zmanipulować głosowi szefa czy sfałszowanemu dokumentowi. 2. **Zwiększona czujność pracowników** – pracownicy uczą się rozpoznawać próby oszustwa, dzięki czemu rzadziej dają się nabrać na fałszywe e-maile czy telefony. 3. **Ograniczenie ryzyka kosztownych błędów ludzkich** – świadomość zagrożeń pozwala uniknąć pomyłek, które mogłyby prowadzić do wycieku danych, przelewów do oszustów czy awarii systemów.
AI-generated Phishing (test socjotechniczny	Wysyłka realistycznych wiadomości phishingowych wygenerowanych przez AI. Umożliwia ocenę podatności na fałszywe e-maile i reakcje użytkowników.	
AI-generated Fake Documentation (test socjotechniczny)	Tworzenie fałszywych dokumentów (poleceń służbowych, faktur) przez AI. Testuje zdolność personelu do rozpoznania sfałszowanych treści.	
Impersonation (test socjotechniczny)	Symulacja podszywania się pod pracowników lub kontrahentów. Pomaga wykryć, czy pracownicy potrafią zweryfikować tożsamość nadawcy.	
Ankiety bezpieczeństwa i wywiady	Zbieranie danych o poziomie świadomości użytkowników w zakresie cyber-bezpieczeństwa.	

JAK DZIAŁA SECURE MEDICA?

Compliance & Governance

5

Aktywność	Opis	Efekt
Ocena zgodności z NIS2 / KSC	Weryfikacja, czy organizacja spełnia wymagania wynikające z dyrektywy NIS2 oraz ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). Działanie to pozwala zidentyfikować luki w zgodności, przygotować organizację do ewentualnych kontroli oraz uniknąć sankcji. Dodatkowo umożliwia dostosowanie struktur i praktyk bezpieczeństwa do wymagań nadchodzących regulacji.	1. **Przygotowanie organizacji do nadchodzących regulacji** – dzięki weryfikacji zgodności z NIS2 i KSC, szpital jest lepiej przygotowany na zbliżające się kontrole. 2. **Skuteczniejsze reagowanie na incydenty i zagrożenia** – ocena procedur pokazuje, czy zespół wie, co robić w sytuacji awaryjnej i czy działania są opisane jasno i praktycznie. 3. **Lepsza kontrola nad ryzykiem i dostępami w organizacji** – przegląd procesów pozwala dostrzec luki w zarządzaniu dostępem i reagowaniu na incydenty, co przekłada się na większą stabilność działania szpitala.
Przegląd polityk bezpieczeństwa IT	Analiza dokumentacji polityk w zakresie ochrony systemów i danych. Oceniamy ich zgodność z najlepszymi praktykami i obowiązującymi przepisami.	
Przegląd procedur bezpieczeństwa IT	Weryfikacja opisanych procedur bezpieczeństwa IT. Celem jest ocena ich skuteczności i praktycznego zastosowania.	
Przegląd procesów bezpieczeństwa IT	Ocena realizowanych procesów związanych z zarządzaniem ryzykiem, dostępem i incydentami. Pomaga wykryć luki organizacyjne i zwiększyć odporność operacyjną.	

STAY SAFE IN THE CYBERSPACE!

HOSPITAL 360 CONFERENCE 2025

https://secure-medica.eu/

SECURE MEDICA

sylwia.raczynska@secure-medica.eu

mikolaj.kawala@secure-medica.eu

piotr.nasilowski@secure-medica.eu