

auditor



Cyberbezpieczeństwo w **branży medycznej**

Poznaj działania gwarantujące **zwiększenie poziomu cyberbezpieczeństwa**

1. OMÓWIENIE TRENDÓW I PROBLEMÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM

Cyberbezpieczeństwo nieustannie podlega ewolucji. Jego zmieniający się charakter, w połączeniu z wysokim ryzykiem i słabą ochroną sprawia, że jest obarczone dużą niepewnością. W założeniu powinno zapewniać ochronę użytkownikom i systemom komputerowym, ale coraz częściej specjaliści odpowiedzialni za cyberbezpieczeństwo są wystawiani na próbę.

Liczba ataków phishingowych w porównaniu z poprzednim rokiem wzrosła o 196%. W dodatku hakerzy stosują coraz bardziej skomplikowane metody działania, których skutki mogą wpłynąć na przestój procesów biznesowych. Organizacje tracą nie tylko zaufanie, ale też ogromne pieniądze. Dla przykładu: atak ransomware kosztuje polską firmę średnio 1,5 miliona złotych¹.



196%

o tyle wzrosła
liczba ataków



1,5 mln zł

tyle średnio kosztuje
atak ransomware



3,5 mln

około tylu specjalistów
od cyberbezpieczeństwa
brakuje obecnie na świecie



17,5 tys.

około tylu specjalistów
od cyberbezpieczeństwa
brakuje obecnie w Polsce

W obliczu zbliżającej się recesji podmioty poszukują sposobów na obniżenie kosztów. Niestety budżet na cyberbezpieczeństwo jest często jednym z pierwszych, które podlegają redukcji. Redukowane są więc także nakłady na zatrudnienie. Obecnie na świecie brakuje około 3,5 miliona specjalistów od cyberbezpieczeństwa, a w Polsce – 17,5 tysiąca.

Zgodnie z prognozami: w 2023 roku wzrośnie liczba ataków na infrastrukturę krytyczną. Oznacza to, że działania z zakresu cyberbezpieczeństwa powinny być traktowane priorytetowo zarówno na szczeblu państwowym, jak i organizacyjnym.

Ten rok prawdopodobnie przyniesie ataki na publiczne i prywatne placówki służby zdrowia, urzędy administracji oraz instytucje publiczne, które świadczą usługi służby zdrowia. Dojdzie nie tylko do chaosu i strat finansowych, ale też do bezpośrednich skutków dla społeczeństwa, w tym do zagrożenia zdrowia i życia ludzkiego.

¹ <https://blog.sagenso.com/cyberbezpieczenstwo-w-2023-roku-prognozy-i-trendy>, [dostęp: 18.01.2023].

dr Adam Józefiak, adiunkt na Politechnice Śląskiej,
administrator sieci komputerowych



www.linkedin.com/in/adamjosefiok



Po pierwsze należy spodziewać się znaczącego nasilenia ataków ze strony Rosji. Zdecydowany prym będzie wiodł trend związany z ransomware. Warto pamiętać, że rynek usług związanych z włamaniami do systemów informatycznych ciągle rośnie. W darknecie obecnie funkcjonują już „firmy” oferujące modele subskrypcyjne, płatne w bitcoinach, dzięki którym można zaprogramować ataki na konkretne systemy konkretnych przedsiębiorstw. Bez wątpienia rok 2023 będzie obfitował w tego typu ataki. Drugim wyzwaniem będzie znaczący niedobór kadry wyspecjalizowanych pracowników. Już na początku ubiegłego roku braki szacowano na ponad 25 tys. pracowników: obecnie trend niestety nie jest optymistyczny. Następnym aspektem będzie zdecydowany wzrost ataków na infrastrukturę IoT oraz wszelkie usługi chmurowe. Kolejna sprawa to dedykowane i wyspecjalizowane ataki, które nie będą już prowadzone w sposób chaotyczny, ale precyzyjny. Rosnące możliwości obliczeniowe komputerów pozwalają na dokonanie precyzyjnych oraz uciążliwych ataków. Ataki takie będą kierowane głównie na słabsze punkty infrastruktury. Czekają nas więc otwarta wojna o „cyber etaty”, szczególnie dotyczące doświadczonych pracowników, mających za sobą dziesiątki projektów i tysiące godzin przy konsoli.

2. ANALIZA OBECNEGO POZIOMU CYBERBEZPIECZEŃSTWA W BRANŻY MEDYCZNEJ

Szpitala i organizacje opieki zdrowotnej stanowią jeden z głównych celów cyberprzestępców. Organizacje opieki zdrowotnej mają do czynienia z dużą ilością danych osobowych, które są niezwykle cenne dla grup hakerskich. Niemalże wszystkie organizacje ochrony zdrowia są narażone na incydenty w zakresie cyberbezpieczeństwa. Pytanie nie brzmi więc, czy dana placówka zostanie zaatakowana, ale kiedy to się stanie.



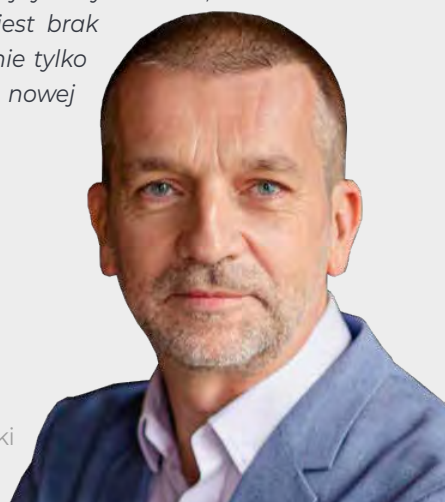
Statystyki nie kłamią: **89% organizacji** ochrony zdrowia odnotowało średnio **43 cyberataki rocznie**, co daje prawie jeden atak tygodniowo². Tylko od 2018 do 2021 roku nastąpił **84% wzrost** liczby naruszeń w branży opieka zdrowotna³, a prognozy mówią, że liczba ataków wciąż będzie wzrastać⁴.

64% organizacji ochrony zdrowia zgłasza, że **czuje się zagrożona**, ale **tylko 48%** z nich **posiada plan przeciwdziałania** temu zagrożeniu⁵. Co niepokojące, **41% organizacji** opieki zdrowotnej, **które nie doświadczyły** jeszcze ataku **uważa, że w przyszłości prawdopodobnie padną ofiarami cyberprzestępców**⁶.

3% szpitali wykazuje słaby, **63%** szpitali wykazuje średni, a tylko **20%** dobry lub bardzo dobry poziom cyberbezpieczeństwa. Prawdą jest niestety, że o poziomie cyberbezpieczeństwa w publicznych placówkach medycznych decyduje ten szpital, którego **poziom zabezpieczeń jest najniższy**.

Myszę, że największym wyzwaniem dla szpitali będzie nowelizacja ustawy krajowym systemie cyberbezpieczeństwa (KSC / ang. NIS2). Oznacza to, że system ochrony zdrowia będzie podlegać nowym regulacjom. Na samodzielne publiczne zakłady opieki zdrowotnej zostaną nałożone obowiązki związane z dyrektywą unijną oraz wspomnianą krajową ustawą, która powinna pojawić się już niebawem. Oprócz konieczności przeprowadzenia analizy ryzyka i wdrożenia procedur dojdzie tutaj niezbędność implementacji rozwiązań pozwalających na zwiększenie poziomu cyberbezpieczeństwa. Kolejnym wyzwaniem, z jakim mierzą się podmioty funkcjonujące w obszarze służby zdrowia, jest brak specjalistów do spraw cyberbezpieczeństwa (zresztą problem ten dotyczy nie tylko tej branży). Zwiększa to trudność implementacji zmian wynikających z nowej ustawy.

Przemysław Kucharzewski, Dyrektor Zarządzający,
producent rozwiązania z obszaru cyberbezpieczeństwa



www.linkedin.com/in/przemyslawkucharzewski

3. POTENCJALNE ZAGROŻENIA I RYZYKA DLA BRANŻY MEDYCZNEJ

Incydenty związane z cyberbezpieczeństwem mogą zagrozić podłączonym do sieci urządzeniom medycznym oraz systemom danych, niezbędnym do bezpiecznego i skutecznego świadczenia opieki zdrowotnej. Konsekwencje mogą obejmować zmianę terminów wizyt czy operacji, przekierowywanie pojazdów ratunkowych lub nawet zamknięcie jednostek opieki i całych organizacji. Brak odpowiednich zabezpieczeń może także prowadzić do narażenia pacjentów na poważne niebezpieczeństwo.

Sporą część incydentów można udaremnić lub zminimalizować ich skutki. Jednak wymaga to wdrożenia odpowiednich środków. Zarządzanie ryzykiem związanym z cyberbezpieczeństwem w środowisku opieki zdrowotnej jest jednak wyzwaniem.

Reakcja na cyberzagrożenia wymaga kompleksowego programu bezpieczeństwa, aby zapobiec atakom na krytyczne urządzenia i systemy. Problemem jest także znalezienie odpowiednich profesjonalistów i pracowników działu IT.

¹ <https://blog.sagenso.com/cyberbezpieczenstwo-w-2023-roku-prognozy-i-trendy/>, [dostęp: 18.01.2023].

² <https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/>, [dostęp: 18.01.2023].

³ <https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/>, [dostęp: 18.01.2023].

⁴ Healthcare Cybersecurity Report Q4 2021, Herjavec Group, 2021.

⁵ <https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/>, [dostęp: 18.01.2023].

⁶ <https://expertsights.com/insights/healthcare-cyber-attack-statistics/>, [dostęp: 18.01.2023].

4. CYBERBEZPIECZEŃSTWO KLUCZEM DO OCHRONY BRANŻY MEDYCZNEJ

Mając na uwadze tak duże ryzyko wpływające na ciągłość funkcjonowania placówek medycznych warto dążyć do jego minimalizacji. Odpowiednia reakcja może zapobiec wystąpieniu potencjalnych zagrożeń ze strony cyberprzestępców.

Na podstawie VI edycji „Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą” przygotowaliśmy zestaw wskazówek, dzięki którym poziom cyberbezpieczeństwa w Twoim szpitalu znacząco wzrośnie. Najczęściej wskazywane przez badane placówki potrzeby to odporność na cyberataki (68,9%), zwiększenie ochrony danych osobowych (65,9%) oraz poprawa stanu wiedzy o zagrożeniach informatycznych wśród pracowników/kierownictwa jednostki (59,4%).

Jakie działania w tym zakresie należy podjąć?

1. zwiększyć odporność infrastruktury IT na cyberataki	68,9%
2. zadbać o odpowiednią ochronę danych osobowych pacjentów i pracowników	65,9%
3. podnieść świadomość i stan wiedzy o zagrożeniach informatycznych wśród pracowników	59,4%
4. poprawić ciągłość działania systemów informatycznych	58,7%
5. uświadomić pracownikom i kadrze zarządzającej ryzyko związanego ze stosowaniem systemów	55,8%
6. zwiększyć ochronę poczty elektronicznej używanej w szpitalu	49,8%

Źródło: VI Edycja „Badanie stopnia informatyzacji podmiotów wykonujących działalność leczniczą 2022”.



Maciej Kaczyński, Założyciel i CEO BTC Sp. z o.o.,
Architekt Systemu



www.linkedin.com/in/maciej-kaczyński

Kluczem do zapewnienia bezpieczeństwa IT jest wdrożenie systemów do zarządzania infrastrukturą IT oraz elementów ochrony danych (systemy klasy DLP – Data Loss Prevention). O ile zakup i wdrożenie systemu do zarządzania infrastrukturą jest prosty i dość szybki w czasie, o tyle opracowanie i wdrożenie polityk bezpieczeństwa musi być przemyślane i właściwie zaplanowane. Zbyt rygorystyczne polityki bezpieczeństwa utrudnią działanie organizacji, zbyt lekkie doprowadzą do podatności i pozornej ochrony. Czas wdrożenia polityk DLP jest stosunkowo długi – może wynieść nawet do 10 miesięcy. Kluczowy jest też czynnik ludzki – bez właściwego, stabilnego zespołu IT – nie da się zapewnić skutecznego bezpieczeństwa. Mamy w Polsce wielu wybitnych specjalistów bezpieczeństwa IT, często pasjonatów, których warto zaangażować do tego typu projektów. I pamiętajmy, że nie ma skutecznych w 100% zabezpieczeń, nie ma systemów, które są idealne i bezbłędne. Ale gdy nie rozpoczniemy wdrożeń procesów zapewnienia bezpieczeństwa to na pewno nie będziemy bezpieczni. To jest akurat pewne.

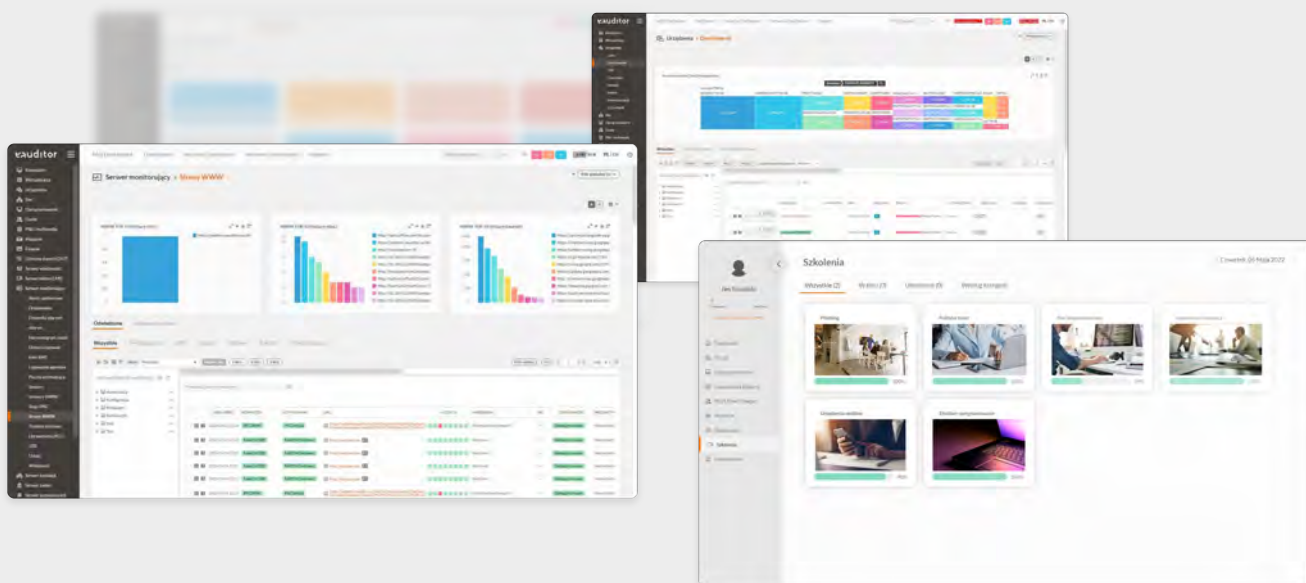
5. ROZWIĄZANIA WSPIERAJĄCE ZWIĘKSZENIE POZIOMU CYBERBEZPIECZEŃSTWA W BRANŻY MEDYCZNEJ

4 kluczowe działania, które zapewnią wzrost poziomu cyberbezpieczeństwa w branży medycznej:

- ✓ Wdrożenie zaawansowanych systemów informatycznych do zapewnienia bezpieczeństwa IT.
- ✓ Implementacja rozwiązań mających na celu szyfrowanie danych oraz nadzorowanie działań użytkowników na firmowych sprzętach w celu zabezpieczenia przed utratą danych.
- ✓ Edukowanie pracowników poprzez prowadzenie regularnych szkoleń i kampanii informacyjnych dążąc do zwiększenia świadomości zagrożeń cybernetycznych.
- ✓ Prowadzenie audytów bezpieczeństwa, aby zidentyfikować słabe punkty infrastruktury i potencjalne zagrożenia.

eauditor

System zapewniający ochronę danych medycznych na najwyższym poziomie



Analiza kluczowych wskaźników bezpieczeństwa IT (SOC)



Zdalne i masowe szyfrowanie dysków wewnętrznych i zewnętrznych (USB)



Rozbudowane polityki DLP do kompleksowej ochrony przed wyciekiem danych



Cykliczne procesy szkoleniowe z polityk bezpieczeństwa IT dla personelu medycznego








Masowe blokowanie podłączenia nieautoryzowanych nośników USB



Blokowanie dostępu do stron www (BTC Website Classification) i uruchamianych procesów (BTC Process Classification)

Odwiedź naszą stronę eauditor.eu

JAKIE OBSZARY WSPIERA SYSTEM EAUDITOR?

 Zarządzanie komputerami	 Użytkownicy	 Monitorowanie urządzeń	 Bezpieczeństwo	 Edukacja i komunikacja
Dashboard – informacja o infrastrukturze IT	Informacja o użytkownikach online	Godzina włączenia, wyłączenia, uśpienia	Zdalne szyfrowanie dysków (BitLocker)	Zdalne szkolenia pracowników
Zdalna instalacja / deinstalacja	Godzina zalogowania, wylogowania	Lokalizacja komputera po IP (komputer za NATem)	Szyfrowanie BitLocker USB	Definiowanie własnych materiałów szkoleniowych
Zdalny pulpit (RDP, RTC, VNC, UVNC)	Monitorowanie pracy (czas aktywności, nieaktywności)	Podłączane urządzenia zewnętrzne USB	Blokowanie nieautoryzowanych urządzeń zewnętrznych USB	Gotowe filmy instruktażowe w zakresie bezpieczeństwa
Zdalne zarządzanie Intel VPro / AMT	Monitorowanie uruchamianych aplikacji	Monitorowanie i zarządzanie usługami	Blokowanie procesów (HV)	Automatyczna komunikacja z użytkownikami
Zdalna konfiguracja	Monitorowanie uruchamianych procesów	Monitorowanie wydajności (RAM, HDD, CPU)	Blokowanie drukarek i wydruków (HV)	Wyświetlanie pilnych komunikatów u użytkowników (Alert)
Zdalny restart	Monitorowanie drukarek i wydruków	Monitorowanie dzienników zdarzeń	Blokowanie uruchamianych stron www	Wyświetlanie komunikatów u użytkowników
Zdalne wykonywanie skryptów CMD (kilkadziesiąt wbudowanych)	Monitorowanie stron www na podstawie zawartości (machine learning)	Monitorowanie procesów pracownika	Monitorowanie / blokowanie otwieranych dokumentów (HV)	
Zdalne wykonywanie skryptów powershell (kilkadziesiąt wbudowanych)	Monitorowanie poczty i załączników poczty wychodzącej		Blokowanie dostępu do nieautoryzowanych sieci WIFI (HV)	
Wsparcie techniczne	Zdalne szkolenia pracowników i monitorowanie postępu procesu szkoleniowego		Monitorowanie i blokowanie dostępu do magazynów danych chmurowych (HV)	

Podsumowanie

Statystyki są alarmujące: **liczba cyberataków na szpitale rośnie i będzie wzrastać**. Organizacje ochrony zdrowia pomiędzy 2020, a 2025 rokiem wydadzą na cyberbezpieczeństwo 125 mld USD⁷. Tych liczb nie można bagatelizować. Podczas gdy silna strategia i program prewencyjny nadal będą miały zasadnicze znaczenie, inwestowanie w odporność cybernetyczną nie jest już opcją, a prawdziwą koniecznością.

⁷ <https://expertinsights.com/insights/healthcare-cyber-attack-statistics/>, [dostęp: 18.01.2023].

Jak podkreślają specjaliści ds. cyberbezpieczeństwa – **zadaniem obrony przed atakami hakerskimi jest przede wszystkim monitorowanie i uświadamianie użytkowników na temat kolejnych wariantów znanych wcześniej zagrożeń.** Zbiorowa odporność systemu jest bowiem najlepszym sposobem na ochronę przed cyberprzestępcami.

Jedną z możliwości zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w placówkach medycznych jest zakup systemu IT. To skuteczny sposób zapobiegania cyberzagrożeniom w infrastrukturze IT, który zapewnia nie tylko wzrost bezpieczeństwa informatycznego, ale także wpływa na efektywność funkcjonowania organizacji.

Aktualnie **trwa nabór wniosków w ramach NFZ na wdrożenie systemów teleinformatycznych** oraz związanych z nimi usług. Działanie to ma na celu wsparcie cyberbezpieczeństwa w placówkach medycznych m.in. poprzez zakup oprogramowania IT spełniającego wymagania niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa IT.



Nabór wniosków na wdrożenie systemów teleinformatycznych w ramach NFZ

Termin na złożenie wniosku:

31 października 2023 roku

Kwota dofinansowania:


240 - 900 tys. zł

Chcesz dowiedzieć się więcej na temat działania systemu eAuditor? Wypełnij formularz i **umów się bezpłatną i niezobowiązującą prezentację.**

Kontakt

 Formularz

 info@btc.com.pl

 +48 91 48 17 204

