**Badanie Fortinet: 54% szpitali w Polsce, które doświadczyły cyberataku, zostało zaatakowanych za pomocą phishingu**

W 31% placówek, które doświadczyły próby naruszenia bezpieczeństwa, doszło do włamań na konta personelu. Szpitale w większości przypadków posiadają takie rozwiązania ochronne jak firewalle czy antywirusy, zaś potrzebują więcej szkoleń i specjalistów.

**[Warszawa, 26.10.2022] Fortinet, światowy lider w dziedzinie szerokich, zintegrowanych i zautomatyzowanych rozwiązań ochronnych, ogłosił wyniki badania stanu bezpieczeństwa IT w polskich szpitalach. Ukazują one, jakie zmiany zaszły w szpitalnej infrastrukturze informatycznej w czasie pandemii COVID-19 oraz jakie są najpilniejsze potrzeby inwestycyjne i wyzwania w szpitalach w Polsce w zakresie cyberbezpieczeństwa.**

Badanie zostało zrealizowane na zlecenie Fortinet przez centrum badawczo-rozwojowe Biostat. Kluczowe płynące z niego wnioski, to:

* Zdecydowana większość szpitali wśród posiadanych rozwiązań ochronnych wskazuje na oprogramowanie antywirusowe (92%) oraz firewalle (91%).
* Wśród placówek, które odnotowały przypadki naruszenia bezpieczeństwa, najważniejszym zagrożeniem pozostawał phishing i inne ataki socjotechniczne (54%).
* Największe wyzwania związane z zapewnieniem ochrony środowisk IT w szpitalach dotyczą czynnika ludzkiego – respondenci wskazują na potrzebę szkoleń dla personelu oraz niedobór specjalistów.
* Prawie połowa badanych już teraz spodziewa się, że w 2023 roku będzie dysponowała większym budżetem na bezpieczeństwo IT. W ciągu minionych dwóch lat środki na ten cel w większości przypadków pozostawały na tym samym poziomie.

**Phishing i inne ataki socjotechniczne najczęstszym zagrożeniem dla szpitali**

Od początku pandemii, a więc od marca 2020 roku, do prób naruszenia bezpieczeństwa infrastruktury IT doszło w 13% badanych placówek ochrony zdrowia. Na szczęście wśród respondentów, którzy tego doświadczyli, w 77% przypadków problem został wykryty tego samego dnia, w którym doszło do incydentu. Cyberprzestępcy najczęściej atakowali szpitale za pomocą metod socjotechnicznych, w tym phishingu (54%), ataków typu DDoS (15%) oraz z użyciem oprogramowania szpiegującego (8%). W 31% placówek, które doświadczyły próby naruszenia bezpieczeństwa, doszło do włamań na konta personelu.

76% badanych wskazało, że dostrzega wyzwania związane z zachowaniem cyberbezpieczeństwa w swojej placówce. Wśród nich najwięcej dotyczyło czynnika ludzkiego. Najczęściej podkreślano niewystarczającą liczbę szkoleń (21%). Jednocześnie okazało się, że tylko w 16% placówek w ostatnich latach regularnie odbywały się działania edukacyjne dla personelu z zakresu cyberbezpieczeństwa, a okazjonalnie w 38%. W przypadku 1/3 badanych szpitali szkoleń nie było, lecz istnieją plany przeprowadzenia ich w przyszłości.

Ponadto, według wyników badania, w więcej niż co trzecim szpitalu (36%) brakuje specjalistów zajmujących się infrastrukturą IT. Jest to stan, który utrzymuje się w ciągu ostatnich dwóch lat. W analizowanym okresie jedynie w 23% placówek liczba specjalistów wzrosła.

Utrzymująca się popularność zagrożeń socjotechnicznych sprawia, że konieczne staje się przyjęcie proaktywnego podejścia do bezpieczeństwa, zwłaszcza że cyberprzestępcy stale zmieniają swoje taktyki, a ich działania coraz częściej są zautomatyzowane i bazują na sztucznej inteligencji. Jako że phishing najczęściej dystrybuowany jest za pomocą poczty elektronicznej, warto, aby placówki ochrony zdrowia posiadały odpowiednie narzędzia zabezpieczające oraz budowały kulturę cyberświadomości wśród swojego personelu, zapewniając mu odpowiednią liczbę i zakres szkoleń.

**Ocena stanu infrastruktury IT i jej bezpieczeństwa**

Respondenci zgłaszają problemy związane z dostępnością specjalistów i brakiem szkoleń, są natomiast zadowoleni z obecnego ogólnego stanu infrastruktury IT w szpitalach (76%) oraz stanu jej bezpieczeństwa (74%).

Najpopularniejsze rozwiązania ochronne, obecne w niemal każdej badanej placówce, to: oprogramowanie antywirusowe (92% wskazań), firewalle (91%) i VPN (Virtual Private Network – 89%) (89%). Powszechne są także rozwiązania zapewniające bezpieczeństwo urządzeniom końcowym (komputerom, smartfonom, laptopom) – wskazało na nie 78% ankietowanych. W porównaniu z wynikami badania Fortinet z 2014 roku[[1]](#footnote-1) znacząco wzrosła popularność stosowania systemów VPN (z 64%). Więcej użytkowników zabezpiecza również urządzenia końcowe (wzrost z 72%). Uwagę zwraca natomiast stosunkowo niska popularność podejścia Zero Trust Access (26%). Wśród rozwiązań ochronnych, które mają być wdrażane w przyszłości, respondenci wskazywali m.in. systemy wykrywania i zapobiegania włamaniom - IDS+IPS, a także systemy do ochrony urządzeń końcowych

Ankietowani specjaliści wskazali też najważniejsze potrzeby inwestycyjne w zakresie bezpieczeństwa IT. Na pierwszym miejscu znalazło się stworzenie środowiska i procedur gwarantujących ochronę przed utratą danych (25%), a w dalszej kolejności – oprogramowanie zabezpieczające urządzenia końcowe (18%) oraz rozwiązania chroniące infrastrukturę sieciową (16%).

Z uwagi na charakter danych, jakie przetwarzają jednostki ochrony zdrowia, bardzo istotne jest, aby dysponowały najnowocześniejszymi środkami ochronnymi, jak zapory sieciowe nowej generacji (NGFW), czy bazujące na sztucznej inteligencji oprogramowanie EDR/XDR do ochrony urządzeń końcowych. Rozwiązania te powinny być zunifikowane w ramach jednej platformy, która zapewni lepszy wgląd w stan bezpieczeństwa środowiska IT, pozwoli na jego dokładne monitorowanie i szybkie wykrywanie zagrożeń oraz odciąży pracowników odpowiedzialnych za bezpieczeństwo.

Równie ważne jest posiadanie polityki bezpieczeństwa, do której mieliby stosować się wszyscy pracownicy placówki oraz wdrażanie nowoczesnego podejścia do zachowania cyberbezpieczeństwa, jak Zero Trust Network Access, według którego wszystkie osoby, urządzenia i aplikacje łączące się z firmową siecią muszą być weryfikowane i uwierzytelniane. Zastosowanie tego modelu umożliwia odejście od konieczności używania tradycyjnych rozwiązań VPN w celu zabezpieczenia zasobów, do których potrzebny jest zdalny dostęp.

**Szpitale chcą inwestować więcej w bezpieczeństwo infrastruktury IT**

W czasie pandemii 67% placówek posiadało takie same środki na bezpieczeństwo IT jak wcześniej. Większym budżetem niż przed pandemią dysponuje niemal co trzeci badany podmiot (31%).

Można spodziewać się, że w przyszłym roku szpitale będą miały więcej pieniędzy na zapewnienie bezpieczeństwa infrastrukturze IT. Natomiast już teraz 46% zakłada, że ich budżet na te cele wzrośnie, a co trzeci jeszcze nie ma takiej wiedzy. Należy więc przypuszczać, że ostatecznie odsetek ten będzie wyższy. Wpływ na poprawę poziomu ochrony ma m.in. możliwość pozyskania dotacji z Narodowego Funduszu Zdrowia na zakup systemów cyberbezpieczeństwa. 93% respondentów deklaruje świadomość możliwości uzyskania takich środków, a 90% spośród nich – chęć skorzystania z tej formy wsparcia.

**Komentarz Jolanty Malak, dyrektor Fortinet w Polsce:**

*Jednostki ochrony zdrowia przechowują i przetwarzają ogromne ilości bardzo wrażliwych danych swoich pacjentów. Unikalność i niezastępowalność danych medycznych czyni je wyjątkowo ważnymi i wymaga bardzo skutecznych mechanizmów chroniących przed ich utratą lub wyciekiem. To bardzo ważne, że osoby odpowiedzialne za utrzymanie bezpieczeństwa IT w szpitalach mogą liczyć także na dodatkowy budżet pochodzący z dotacji od NFZ. Wyniki badania po raz kolejny pokazują też, jak istotne jest zapewnienie pracownikom odpowiedniej wiedzy na temat zagrożeń w sieci*. *Prawidłowo przeszkolony personel powinien nie tylko móc rozpoznać atak phishingowy i rozumieć, na czym polegają zagrożenia socjotechniczne, ale też wiedzieć, kogo poinformować w przypadku otrzymania podejrzanie wyglądającej wiadomości e-mail.*

**Metodologia badania:**

Badanie zostało przeprowadzone metodą CATI w lipcu 2022 roku przez centrum badawczo-rozwojowe Biostat na próbie 100 placówek medycznych w Polsce, w skład których wchodziły zarówno podmioty prywatne, jak i publiczne. 3/5 badanych stanowiły szpitale powiatowe lub miejskie, co czwarty respondent wypowiadał się w imieniu wojewódzkiego szpitala specjalistycznego (25%). W badaniu udział wziął również jeden respondent wypowiadający się w imieniu instytutu badawczo-rozwojowego. Ankietowanymi były osoby odpowiedzialne za szpitalną infrastrukturę IT.

**Informacja o firmie Fortinet**

Firma Fortinet (NASDAQ: FTNT), dzięki swojej misji zabezpieczania ludzi, urządzeń i danych, gdziekolwiek się znajdują, umożliwia stworzenie cyfrowego świata, któremu zawsze można ufać. Dlatego największe światowe przedsiębiorstwa, dostawcy usług i organizacje rządowe wybierają Fortinet, aby bezpiecznie przyspieszyć swoją cyfrową transformację. Platforma Fortinet Security Fabric zapewnia szeroką, zintegrowaną i zautomatyzowaną ochronę przed różnego rodzajami ataków. Zabezpiecza urządzenia, dane i aplikacje o znaczeniu krytycznym oraz połączenia od centrum danych, przez chmurę, po biuro domowe. Ponad 595 tys. klientów zaufało Fortinetowi w zakresie ochrony swoich firm, co sprawia, że firma zajmuje pierwsze miejsce na świecie pod względem liczby dostarczonych urządzeń zabezpieczających. Instytut szkoleniowy Fortinet NSE, działający w ramach programu firmy Training Advancement Agenda (TAA), zapewnia jeden z najobszerniejszych programów edukacyjnych w branży, dzięki czemu szkolenia z zakresu cyberbezpieczeństwa i nowe możliwości zawodowe są dostępne dla wszystkich zainteresowanych. Więcej informacji można znaleźć pod adresem <https://ww.fortinet.com>, na [blogu Fortinet](https://www.fortinet.com/blog?utm_source=pr&utm_campaign=blog) lub

w [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs).

1. Raport Fortinet o informatyzacji polskich placówek ochrony zdrowia, 2014 r. [↑](#footnote-ref-1)