DOBRE PRAKTYKI

cyberbezpieczeństwo w szpitalach

2024

OGÓLNOPOLSKIE STOWARZYSZENIE
SZPITALI PRYWATNYCH

Projekt graficzny i skład:
Joanna Piekarska-Norek

Redakcja: Maciej Wiśniewski

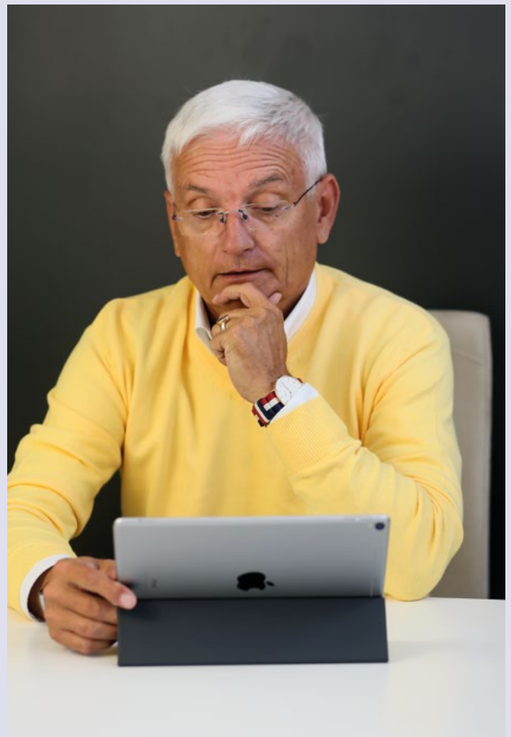
Wydawcy: OGÓLNOPOLSKIE STOWARZYSZENIE SZPITALI PRYWATNYCH

www.ossp.pl
www.szpitale.org

Druk:

ISBN: 978-83-946197-7-0

Gdynia 2024



Szanowni Państwo,

Przekazujemy do Państwa rąk kolejne opracowanie z serii „dobrych praktyk". Wracamy do tematu cyberbezpieczeństwa, gdyż od czasu poprzedniej publikacji niewiele się zmieniło a poziom zagrożenia wzrósł. Kolejny raz zwracamy uwagę na palący problem i brak rozwiązań. Wskazujemy potencjalne kierunki działań. Skutki zaniechań w zakresie cyberbezpieczeństwa w ochronie zdrowia mogą być katastrofalne dla pacjentów i szpitali zarówno publicznych jak i prywatnych.

Andrzej Sokołowski
Prezes Zarządu
Ogólnopolskiego Stowarzyszenia
Szpitali Prywatnych

SPIS TREŚCI

Tomasz Garbowski

NIS2, AI Act biurokratyczna przeszkoda czy realna wartość?

Wprowadzenie nowych, europejskich regulacji, takich jak NIS2 czy AI Act może dla niektórych brzmieć jak kolejna, biurokratyczna przeszkoda. Przepisy te jednak realnie zwiększą poziom bezpieczeństwa, odporności i jakości krytycznych, użytecznych publicznie usług. Dlatego dla pacjentów, a także całego sektora ochrony zdrowia są szansą oraz dobrą wiadomością.

Motywacja

NIS2 motywuje branżę ochrony zdrowia do wdrażania zaawansowanych, organizacyjnych i technicznych rozwiązań bezpieczeństwa zgodnych m. in. z międzynarodowymi standardami ISO 27000 w zakresie bezpieczeństwa informacji i ISO 22300 w zakresie odporności usług. To oznacza, że prywatne, medyczne informacje dotyczące milionów pacjentów będą lepiej chronione przed kradzieżą i wzrastającą liczbą cyberataków.

Zaufanie

Wdrażając wymagania bezpieczeństwa i systemy monitorowania oraz szybkiego reagowania na zagrożenia, pozwalające na proaktywne wykrywanie i neutralizowanie cyberataków minimalizuje się ryzyko, a tym samym zwiększa zaufanie do instytucji ochrony zdrowia, Państwa, czy wreszcie instytucji europejskich.

Odporność

Wymagania zwiększonej odporności operacyjnej zachęcają organizacje ochrony zdrowia do zaprojektowania oraz wdrożenia złożonych i niezawodnych systemów oraz planów ciągłości działania na wypadek szerokiego spektrum incydentów. Dzięki temu, niezależnie od sytuacji, pacjenci będą mieli zapewniony dostęp do krytycznych usług, bez uciążliwych zakłóceń, co jest szczególnie istotne w przypadkach poważnie zagrażających życiu oraz zdrowiu.

Dzięki sprawdzonym narzędziom do zarządzania ryzykiem i planowania awaryjnego, przestoje oraz zakłócenia usług medycznych będą systemowo minimalizowane. To oznacza, że opieka zdrowotna jest i będzie nieprzerwana, nawet w przypadku poważnych awarii czy ataków.

Zwiększona dojrzałość systemów odporności całej branży będzie miała długofalowy, pozytywny wpływ na zmniejszenie kosztów zakłóceń, a tym samym kosztów funkcjonowania podmiotów ochrony zdrowia, powiązanych w coraz bardziej złożone ekosystemy organizacyjne, biznesowe i technologiczne.

Innowacje

Europejskie i krajowe regulacje dotyczące odporności nie stoją w sprzeczności z wdrażaniem innowacyjnych rozwiązań technologicznych, wręcz przeciwnie. Długofalowo, przez zadbanie o właściwe zarządzanie ryzykiem, sprzyjają inwestycjom w bezpieczne i nowoczesne rozwiązania oparte o sztuczną inteligencja, robotyzację, hyperconectivity i telemedycynę. Dzięki nim pacjenci będą mogli liczyć na szybsze i bardziej precyzyjne usługi oraz spersonalizowaną, bardziej dostępną, a w pewnych sytuacjach bardziej ekonomiczną opiekę.

Lepsze zarządzanie danymi pacjentów, zaawansowane systemy do zarządzania dostępem sprzyjają bardziej zindywidualizowanej i skutecznej opiece, przy jednoczesnym zachowaniu prywatności oraz bezpieczeństwa w złożonym ekosystemie ochrony zdrowia.

Wiarygodność

Organizacje, które będą przestrzegać NIS2, czy AI Act będą mogły wiarygodnie komunikować, że dbają o najwyższe standardy bezpieczeństwa i ciągłość działania. To zwiększa zaufanie do nich oraz całej branży. Dzięki systemom zarządzania ryzykiem, organizacje mogą dostarczać wiarygodne dowody na to, że instytucja działa w sposób transparentny i odpowiedzialny. Dodatkowo, wymagania te motywują do proaktywnego podejścia do zagrożeń, w tym ich oceny i redukcji ich wpływu.

Proaktywna cyberodporność

Obok rozwiązań organizacyjnych, stosowanie sprawdzonych, nowoczesnych i adekwatnych rozwiązań oraz technologii cyberbezpieczeństwa stają się koniecznością oraz realną gwarancją dobrze wykonanej pracy przez liderów branży medycznej. Do takich rozwiązań należą m. in.:

- Standardy architektury i inżynierii bezpieczeństwa, takie jak: Zero Trust – model bezpieczeństwa oparty o zasadę „nigdy nie ufaj, zawsze weryfikuj", Security by Design – podejście do projektowania systemów IT, uwzględniające uwzględnienie zasad bezpieczeństwa na wszystkich etapach tworzenia i testowania oprogramowania, czy Security by Default – wprowadzające zasady konfiguracji systemów IT z domyślnymi ustawieniami bezpieczeństwa, minimalizującymi ryzyko związane z niewłaściwymi konfiguracjami;
- Systemy bezpieczeństwa sieci: technologie kontroli dostępu do sieci (NAC) oraz zarządzania bezpieczeństwem ruchu w sieciach, segmentacja sieci;
- Narzędzia do zarządzania i zabezpieczania urządzeń końcowych, w tym urządzeń mobilnych.
- Systemy ochrony, wykrywania oraz reakcji na zagrożenia na poziomie urządzeń końcowych użytkowników (EDR) oraz na poziomie sieci (NDR);
- Systemy kontroli dostępu oraz zarządzania tożsamością, w tym: systemy zarządzania tożsamością, uprawnieniami i dostępem użytkowników (IAM) oraz użytkowników uprzywilejowanych (PIM/PAM), technologie uwierzytelniania wieloskładnikowego (MFA);
- Systemy szyfrowania oraz bezpieczeństwa baz danych, zapobiegania wyciekowi danych (DLP), bezpieczeństwa aplikacji webowych (WAF);
- Systemy oraz procesy testowania bezpieczeństwa, w tym: Ethical Hacking – symulacje ataków w celu identyfikacji słabości w systemach IT, Testy Penetracyjne aplikacji oraz Red Teaming – zaawansowane testy, symulujące rzeczywiste ataki w pozwalające na ocenę skuteczności obrony organizacji, czy testy gotowości organizacji na obsługę incydentów (BAS);
- Zespoły (SOC) oraz systemy i technologie (SIEM, SOAR) odpowiedzialne za monitorowanie, wykrywanie i reagowanie na incydenty bezpieczeństwa w organizacji.

Leadership, działania przygotowawcze

Bez wątpienia, wdrożenie NIS2 będzie wymagało dużego zaangażowania całej firmy przy bezpośrednim wsparciu jej liderów. Punktem wyjścia do zdefiniowania i uruchomienia programu powinno być dobre zrozumienie wymagań dyrektywy NIS2 połączone z analizą zagrożeń dla sektora i organizacji, luk w jej aktualnym systemie zabezpieczeń i powiązanego z nimi ryzyka. Podejście takie pozwoli na podejmowanie właściwych decyzji dotyczących wyboru i wprowadzania adekwatnych zabezpieczeń i ich finansowania.

Budowa kultury bezpieczeństwa będącej fundamentem odpowiedzialności w organizacji, stosowanie najlepszych praktyk rynkowych, wykorzystanie ekspertów, wymiana wiedzy, czy testowanie odporności upewni nas, że dane pacjentów i usługi sektora ochrony zdrowia będą znacząco mniej narażone na wzrastające ryzyko.

Wdrożenie nowych regulacji NIS2, AI Act przyniesie szereg długofalowych korzyści dla pacjentów, całej branży ochrony zdrowia, ale i odporności w wymiarze krajowym oraz europejskim. Dane będą bezpieczniejsze, usługi medyczne bardziej niezawodne, a jakość opieki oraz krytycznych funkcji użyteczności publicznej fundamentalnie wyższa.

Zbigniew Kniżewski

O co chodzi z tymi „De-eR-ami"?

EDR, XDR, a może MDR? Jaką usługę wybrać i dlaczego?

Wstęp

Niedawne, szeroko nagłośnione cyberataki uświadomiły firmom i instytucjom, że wszyscy są narażeni i tak naprawdę nikt nie jest odporny na ataki. Jeśli przechowujesz i wykorzystujesz dane, które można uznać za cenne, a Twoja organizacja jest podłączona do Internetu, jesteś zagrożony. Problem ten dotyczy wielu branż, w tym sposób szczególny jednostek ochrony zdrowia.

Doniesienia te stawiają właścicieli i zarządzających w trudnej sytuacji, polegającej na przyswojeniu dużej ilości informacji na temat złożonego zagadnienia, jakim jest cyberbezpieczeństwo. Muszą nadrobić zaległości i znaleźć właściwy sposób ochrony. Co więcej, w miarę jak cyberprzestępcy wymyślają bardziej ukryte i wyrafinowane zagrożenia, **starsze środki bezpieczeństwa szybko stają się nieaktualne,** co zmusza organizacje wysokiego ryzyka takie jak m.in. jednostki ochrony zdrowia do **poszukiwania nowych rozwiązań.**

Wzrost pracy zdalnej wynikający z ograniczeń związanych z pandemią, szybki rozwój Internetu rzeczy oraz zwiększone wykorzystanie komunikacji i działań online zdecydowanie zwiększyły liczbę potencjalnie podatnych na ataki punktów końcowych, które mogą zaatakować cyberprzestępcy.

Zagrożone organizacje poszukujące kompleksowego rozwiązania stają w obliczu wysokich kosztów utworzenia wewnętrznego centrum operacyjnego ds. bezpieczeństwa SOC *(Security Operation Center)* oraz surowej rzeczywistości, w której brakuje specjalistów ds. cyberbezpieczeństwa.

Dlatego właściwym rozwiązaniem w zakresie cyberbezpieczeństwa dla organizacji z niewielkimi zespołami IT jest oparta o skuteczne oprogramowanie i wykwalifikowanych specjalistów usługa zarządzanego wykrywania i reagowania MDR *(Managed Detection and Response),* rozumiana jako rozwiązanie „pod klucz" z predefiniowanym pakietem zabezpieczeń, z całodobową pomocą zapewnianą przez doświadczonych specjalistów ds. cyberbezpieczeństwa w zewnętrznym centrum SOC. Usługi obejmują cztery punkty cyberbezpieczeństwa (wykrywanie, analiza, badanie i reakcja) wymagane do skutecznego zarządzania zagrożeniami.

Tego typu podejście rozwiązuje wiele problemów, z którymi borykają się organizacje poszukujące kompletnego pakietu cyberbezpieczeństwa lub aktualizujące istniejącą ochronę firmy.

Wiele organizacji już korzysta z MDR jako rozwiązania w zakresie cyberbezpieczeństwa. Jednak znalezienie odpowiedniego dostawcy i uzyskanie usług, które będą odpowiednie, może być większym wyzwaniem niż się spodziewano. Oferty dotyczące cyberbezpieczeństwa występują w wielu formach i często są różnie kategoryzowane przez różnych dostawców. Bez dokładnego sprawdzenia możesz otrzymać usługę zupełnie inną od oczekiwanej.

Ten krótki przewodnik o usłudze MDR ma pomóc Ci zrozumieć jej najważniejsze elementy składowe, porównać MDR z innymi rozwiązaniami i jak faktycznie wygląda korzystanie z MDR z punktu widzenia klienta.

MDR - czym jest ta usługa i jak działa?

Stosując definicję Gartnera, upraszczając ją nieco w celu lepszego zrozumienia przez szerokiego odbiorcę, usługi MDR zapewniają zdalnie świadczone funkcje nowoczesnego centrum operacji bezpieczeństwa MSOC *(Modern*

Security Operation Center), dostarczane „pod klucz" przy użyciu predefiniowanego stosu technologii w celu gromadzenia odpowiednich informacji, które są analizowane i kategoryzowane w sposób umożliwiający zbadanie ich przez ekspertów.

Aby zapewnić właściwą kompleksową ochroną MDR jest bardzo złożoną usługą. Wiele funkcji składowych można interpretować i realizować na wiele sposobów. Dlatego ważne jest, aby zrozumieć, w jaki sposób narzędzia i metody dostarczone przez dostawcę rozwiązania MDR realizują określone zadania polegające na wykrywaniu i eliminowaniu wyrafinowanych współczesnych zagrożeń. Decydując się na rozwiązanie MDR trzeba zwrócić uwagę na jego spójność i kompletność, w sensie zdolności do realizacji konkretnych zadań, takich jak:

- zarządzanie logami za pomocą SIEM *(Security Information and Event Management)*
- wykrywanie i reagowanie na punkty końcowe (komputery i serwery)
- sztuczna inteligencja do proaktywnej ochrony przed zagrożeniami
- analityka zachowań użytkowników przy pomocy UEBA *(User and Entity Behavior Analytics)*
- wykorzystanie automatyki SOAR *(Security Orchestration, Automation and Response),* aby skrócić czas reakcji
- monitorowanie sieci dla pełnej widoczności
- analiza przez ekspertów, którzy stanowią przedłużenie zespołu Klienta

Porównanie MDR z EDR i XDR

Osoby planujące inwestycje w cyberbezpieczeństwo dobrze zdają sobie sprawę, że MDR to nie jedyny akronim, który należy rozwikłać. Dostępnych jest wiele narzędzi i usług cyberbezpieczeństwa dla organizacji o różnym poziomie bezpieczeństwa i różnych potrzebach. Wśród nich najbardziej popularne są rozwiązania EDR i XDR.

Chciałbym zwrócić uwagę na zasadnicze różnice między nimi. Aby wybrać, które z nich będzie odpowiednie dla Twojej organizacji, warto poświęcić trochę czasu na porównanie tych trzech rozwiązań. Chociaż EDR, XDR i MDR mają wspólne cechy, takie jak zaawansowana analityka, ich zakresy i poziomy reakcji różnią się znacząco.

EDR koncentruje się na wykrywaniu i reagowaniu na zagrożenia na urządzeniach końcowych przy użyciu monitorowania i analizy w czasie rzeczywistym.

XDR rozszerza wykrywanie zagrożeń poprzez integrację danych z różnych źródeł, takich jak sieci i usługi w chmurze, w celu uzyskania ujednoliconego podejścia do bezpieczeństwa.

MDR oferuje dodatkowo zarządzane usługi bezpieczeństwa, w tym całodobowe monitorowanie i reagowanie na zagrożenia, korzystne dla organizacji o ograniczonych zasobach.

Wybór odpowiedniego rozwiązania cyberbezpieczeństwa zależy od konkretnych potrzeb organizacji w zakresie ochrony, monitorowania danych i możliwości reagowania. Poniżej bardziej szczegółowo omówię różnice między omawianymi narzędziami/usługami.

EDR *(Endpoint Detection and Response)*

EDR to rozwiązanie, które wykorzystuje analizę danych do identyfikowania potencjalnych zagrożeń dla punktów końcowych przed ich wystąpieniem, blokowania złośliwej aktywności i oferowania sugestii dotyczących środków zaradczych. Ten rodzaj ochrony stał się kluczowy wraz z rozwojem Przemysłu 4.0 oraz szerokim zastosowaniem urządzeń podłączonych zdalnie. Każde urządzenie połączone z siecią komputerową może stać się potencjalnym źródłem problemów. Te punkty końcowe są uważane za szczególnie podatne na zagrożenia, ponieważ często mają minimalne zabezpieczenia. Wykrywanie punktów końcowych umożliwia sprawdzenie aktywności i zidentyfikowanie podejrzanych zachowań. Co najważniejsze, zagrożenie można powstrzymać, zanim przedostanie się ono dalej do sieci. Rozwiązania EDR muszą zapewniać takie możliwości.

Chociaż te możliwości oferują znaczne korzyści w zakresie wykrywania i łagodzenia zagrożeń dla punktów końcowych, należy pamiętać, że **EDR jest rozwiązaniem zapewniającym jedynie bezpieczeństwo punktów końcowych.** Został zaprojektowany do współpracy z innymi narzędziami i profesjonalistami zajmującymi się bezpieczeństwem takimi jak SIEM czy SOAR.

XDR *(eXtended Detection and Response)*

Zrozumienie szczegółów rozszerzonej detekcji i reakcji XDR jest nieco trudniejsze, ponieważ znajduje się ono wciąż na wczesnym etapie rozwoju i może być różnie opisywane przez różnych dostawców. XDR wykorzystuje niektóre z tych samych technik co EDR, jednak **XDR wykracza poza EDR i obejmuje zarówno aktywność na punktach końcowych, jak i w sieci.**

Rozwiązania XDR gromadzą dane, aby pomóc identyfikować i izolować zagrożenia w sieciach, infrastrukturze chmurowej, komponentach SaaS *(Software as a Service),* punktach końcowych i innych komponentach sieci. Istnieją pewne wyidealizowane opisy XDR, które sugerują, że jest to wszechogarniająca ochrona. Jednak najdokładniej można scharakteryzować XDR jako kompleksową platformę zapewniającą te narzędzia.

XDR nie jest konkretnym narzędziem o określonych parametrach. Przypomina to bardziej zestaw różnorodnych narzędzi dostarczanych przez usługodawcę. **Podobnie jak EDR, XDR jest przeznaczony do instalacji i używania przez ekspertów ds. bezpieczeństwa w celu zapewnienia pełnej ochrony.**

MDR *(Managed Detection and Response)*

Po lepszym zaznajomieniu się ze składnikami zarządzanego wykrywania i reagowania można rozpoznać największą różnicę oferowaną przez to rozwiązanie. Chociaż zarówno EDR, jak i XDR są narzędziami używanymi przez profesjonalistów, **MDR to kompletny zestaw usług obejmujący interakcję ze specjalistami ds. cyberbezpieczeństwa.**

Narzędzia w rozwiązaniu MDR mogą obejmować:

- **EDR lub XDR**
- SIEM
- SOAR
- analizę ruchu sieciowego
- analizę zachowań użytkowników
- zarządzanie podatnościami
- wykrywanie włamań.

Oprócz narzędzi tworzących rozwiązanie MDR, **MDR zapewnia korzyści płynące ze zdalnego SOC świadczącego całodobowy dostęp do ekspertów ds. cyberbezpieczeństwa.**

Eksperci ci działają jako przedłużenie zespołu Klienta i zapewniają rutynową komunikację na temat bieżącego stanu cyberbezpieczeństwa, a także wsparcie, gdy pojawiają się alerty i aktywne zagrożenia.

Właśnie dlatego MDR jest najbardziej kompleksową usługą dostępną za pośrednictwem zewnętrznego dostawcy.

Porównanie dostawców MDR

MDR zapewniany przez uznanych specjalistów ds. cyberbezpieczeństwa zazwyczaj obejmuje niezbędne elementy, a także zaufany stos zabezpieczeń. Jednak różni dostawcy korzystają z różnych narzędzi i metod, aby osiągnąć podobne wyniki. Jeśli wybierzesz MDR dla swojego systemu cyberbezpieczeństwa, przed podjęciem ostatecznej decyzji najlepiej porównać renomowanych dostawców.

Istotne elementy, które różnią się w zależności od dostawcy MDR, obejmują styl komunikacji, oprogramowanie zabezpieczające, możliwości automatyzacji, zaangażowanie w reakcję na incydenty oraz usługi oferowane przez specjalistów ds.cyberbezpieczeństwa.

Co powinno zawierać Twoje Unikalne Rozwiązanie MDR?

Skuteczny MDR oferuje różnorodne zaawansowane narzędzia i usługi, które zapewniają Twojej firmie lub instytucji kompleksowe rozwiązanie bezpieczeństwa. Szukając dostawcy MDR, ważne jest, aby wziąć pod uwagę, w jaki sposób usługi tego dostawcy odpowiadają potrzebom Twojej organizacji. Usługi MDR powinny obejmować te możliwości.

Lista kontrolna dla elementów usługi MDR

1. Analiza zagrożeń
2. Ochrona 24 godzina na dobę, 7 dni w tygodniu, 365 dni w roku.
3. Dochodzenie w sprawie incydentu
4. Monitorowanie zagrożeń
5. Usługa zdalnego reagowania
6. Zaawansowana analityka
7. Wiedza i doświadczenie zespołu
8. Walidacja incydentu
9. Działania post incydentalne

Wyrafinowane ataki są często projektowane tak, aby były dyskretne, aby pomóc cyberprzestępcom osiągnąć swój cel, udając normalną aktywność sieciową. Narzędzia i funkcje MDR izolują te ataki do pojedynczego urządzenia lub obszaru działania, aby powstrzymać zagrożenia bez przełączania systemów biznesowych w tryb offline.

Wybór dostawcy MDR jest podobny do zapraszania nowego Partnera do swojej organizacji. Aby jak najlepiej dopasować usługę, ważne jest, aby upewnić się, że usługa dostawcy jest zgodna z przepływem pracy w Twojej

firmie i uwzględnia określone problemy związane z bezpieczeństwem.

Przed dokonaniem ostatecznego wyboru uzyskaj szczegółowe odpowiedzi na 10 najważniejszych pytań, które możesz zadać swojemu dostawcy MDR.

1. Czy znasz moją branżę?
2. Czy do współpracy z dostawcą będę potrzebować specjalistycznego oprogramowania?
3. Jaka jest główna forma kontaktu dostawcy z klientem?
4. Jak wygląda raportowanie?
5. Czy usługę MDR można dostosować?
6. Czy dostępna jest pomoc techniczna 24 godziny na dobę, 7 dni w tygodniu?
7. Jak sobie radzicie z proaktywnym wykrywaniem zagrożeń?
8. Czy zapewniona jest wszechstronna widoczność?
9. Czy rozwiązania używane w usłudze są zautomatyzowane i skalowalne?
10. Czy dostawca wspiera klienta w działaniach po incydencie?

Podsumowanie

Mam nadzieje, że ten krótki poradnik będzie pomocny w niezwykle istotnym i jednocześnie skomplikowanym procesie wyboru rozwiązania do zabezpieczenia organizacji przed cyberatakami. **W procesie tym kluczowa jest świadomość oczekiwań od dostawcy usługi, który będzie kluczowym Partnerem w zakresie bezpieczeństwa Waszej organizacji i danych Waszych pacjentów.**

Dlatego trzeba do tego wyboru się dobrze przygotować i dokonać go w sposób odpowiedzialny. Niezależnie od tego jak będzie się nazywać zamawiana usługa, jej zakres musi być jasno i precyzyjnie sformułowany, zwracając szczególną uwagę na dostępność i gotowość do wsparcia przez Partnera w wypadku stwierdzonego zagrożenia i po incydencie.

Takie podejście z zachowaniem należytej staranności zminimalizuje ryzyko utraty danych i przerwania ciągłości działania organizacji i wielowymiarowych strat z tym związanych.

Krzysztof Zgliński

Perspektywa ryzyk cybernetycznych w świetle ubezpieczeń dla szpitali

W zakresie ubezpieczeń niewątpliwie najważniejszym jest ubezpieczenie obowiązkowe odpowiedzialności cywilnej podmiotu prowadzącego działalność leczniczą. Jest to spełnienie wymogu Ustawy z dnia 15 kwietnia o działalności leczniczej, właściwego Rozporządzenia Ministra Finansów dla tego rodzaju działalności oraz instytucji nadzorujących.

Pozostałe ubezpieczenia są ubezpieczeniami dobrowolnymi. Czy są one nam zatem potrzebne – możemy przyjąć hipotezę, że nie. Nie musimy rozszerzać obowiązkowego ubezpieczenia odpowiedzialności cywilnej o nadwyżkę, ubezpieczać mienia w tym sprzętu medycznego, rozszerzać ochrony o ryzyka terrorystyczne, zawierać dodatkowej polisy w zakresie D&O i tym bardziej polisy w zakresie ryzyk cybernetycznych czy innych.

Przyjmując jednak hipotezę, że tak - to każde z wyżej wymienionych ryzyk ubezpieczeniowych w zakresach swojej ochrony, uwzględniając wyłączenia, daje realną możliwość przeniesienia ryzyka finansowego na ryzyka ubezpieczeniowe.

W kontekście ryzyk cybernetycznych występuje szereg argumentów, dla których powinniśmy dzisiaj rozmawiać niejako o obowiązku ubezpieczenia szpitala w tym zakresie.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa realizująca rozporządzenie tzw. unijnej dyrektywy NIS2 (NIS2 weszła w życie w drugiej połowie 2022 r.) była odpowiedzią na silny rozwój cyfryzacji i rosnące zagrożenia w tym obszarze. Przepisy zaostrzyły niektóre wymagania i kary dla przedsiębiorców oraz podmiotów kluczowych, w tym placówek ochrony zdrowia. Tak na przykład w przypadku podmiotów kluczowych przewiduje się kary w wysokości do 10 mln EUR lub 2% łącznego światowego obrotu w poprzednim roku. Dodatkowo przepisy wprowadziły obowiązki dla operatorów usług kluczowych (w skrócie OUK) z sektora ochrony zdrowia. Co warto odnotować, dotyczą one tych podmiotów, które posiadają Szpitalny Oddział Ratunkowy lub też należą do Systemu Podstawowego Szpitalnego Zabezpieczenia Świadczeń Opieki Zdrowotnej, co może dotyczy 130 szpitali. Oczywiście wcześniej przytoczone przepisy są powiązane z Ustawą z dnia 10 maja o ochronie danych osobowych.

Czy w związku z nieprawidłowościami podmiotu leczniczego w zakresie obsługi, przechowywania czy przetwarzania danych osobowych, kary administracyjne nakładane na taki podmiot leczniczy mogą zostać objęte zakresem ochrony ubezpieczenia od ryzyk cybernetycznych – co do zasady tak. Brzmienie definicji klauzuli „Kary Administracyjne" jednego z wiodących ubezpieczycieli: *„Kary Administracyjne oznaczają kary pieniężne nałożone przez organy administracji lub organy regulacyjne, w tym administrację federalną, stanową, lokalną oraz organy państw obcych działające w zakresie swoich kompetencji, na podstawie aktów administracyjnych wydanych w ramach Postępowań Regulacyjnych. Kary Administracyjne nie obejmują kar pieniężnych niemogących być przedmiotem ubezpieczenia w świetle przepisów prawa właściwego dla Umowy Ubezpieczenia lub prawa, na podstawie którego kara jest nakładana, kar nałożonych przepisami karnymi oraz zwrotu nienależnych korzyści, a także odszkodowań, których wysokość została zwiększona dla celów represyjnych".*

Czy ubezpieczyciel zawrze ze mną jako podmiotem leczniczym umowę ubezpieczenia i w ramach kompleksowego zakresu ochrony ubezpieczenia ryzyk cybernetycznych włączy w/w klauzulę Kar Administracyjnych? Ten temat rozwinę w dalszej części artykułu.

Z bardzo dużym zainteresowaniem zapoznałem się z wynikami anonimowej i dobrowolnej ankiety dotyczącej cyberbezpieczeństwa przeprowadzonej przez Ogólnopolskie Stowarzyszenie Szpitali Prywatnych oraz firmę Koma Nord wśród członków stowarzyszeń – „Dobre praktyki – cyberbezpieczeństwo w szpitalach". Publikacja OSSP ze stycznia 2023 r. (34 ankietowanych).

Pierwsza odpowiedź ubezpieczyciela, po analizie wyżej opisanych odpowiedzi z ankiety, dotycząca tego czy będzie on chciał złożyć ofertę i będzie zainteresowany zawarciem umowy ubezpieczenia ryzyk cybernetycznych nasuwa się sama – nie będzie chciał.

Ubezpieczyciele są zainteresowani ubezpieczeniem ryzyk przyszłych, niepewnych oraz takich na które ubezpieczony nie miał wpływu lub doprowadził do minimalizacji powstania zdarzenia ubezpieczeniowego.

W przypadku powyższych odpowiedzi i podejścia związanego z tym, że minimum 65% szpitali czuje średnie, małe lub bardzo małe zagrożenie różnymi rodzajami zagrożeń cybernetycznych trudno podjąć inną decyzję niż negatywną dotyczącą zawarcia umowy ubezpieczenia.

Pytanie	Ilość w %	Odpowiedź	Ilość w %	Odpowiedź
Czy podmiot doświadczył kiedykolwiek jednej z niżej wymienionych typów ataków?	**36%**	Szpitali doświadczyło ataków DDoS, Ransomware, ataków socjotechnicznych (24% największa ilość w tej kategorii) czy kradzieży danych z systemów szpitala	**65%**	Nie dotyczy
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii kradzieży danych z systemów szpitalnych	**76%**	Szpitali odpowiedziało, że czuje średnie, małe lub bardzo małe zagrożenie związane z kradzieżą danych	**6%**	Brak poczucia zagrożenia
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii atak socjotechniczny (wyłudzenie danych) na personel szpitala	**65%**	Szpitali odpowiedziało, że czuje średnie, małe lub bardzo małe zagrożenie związane z atakami socjotechnicznymi	**6%**	Brak poczucia zagrożenia
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii atak Ransomware na szpitalne systemy informatyczne	**69%**	Szpitali odpowiedziało, że czuje średnie, małe lub bardzo małe zagrożenie związane z atakiem ransomware	**6%**	Brak poczucia zagrożenia
Proszę określić poczucie zagrożenia związane z cyberbezpieczeństwem w kategorii atak DDoS na serwery szpitalne:	**74%**	Szpitali odpowiedziało, że czuje średnie, małe lub bardzo małe zagrożenie związane z atakiem DDoS	**12%**	Brak poczucia zagrożenia
Proszę o ogólną ocenę świadomości w zakresie cyberbezpieczeństwa personelu zatrudnionego w podmiocie leczniczym	**65%**	Szpitali oceniło swoją świadomość w zakresie cyberbezpieczeństwa na poziomie średnim, małym lub bardzo małym personelu medycznego	**9%**	Brak świadomości

Jak przekładają się powyższe odpowiedzi na statystyki dotyczące różnych rodzajów zagrożeń cybernetycznych? Poniżej przedstawiam listę najczęstszych ataków hakerskich na szpitale w Polsce i na świecie:

1. **Ataki typu ransomware:** W tym typie ataku hakerzy szyfrują dane szpitala i żądają okupu za ich odszyfrowanie. Odmowa zapłaty okupu (lub brak możliwości odtworzenia kopii zapasowych) może uniemożliwić szpitalowi dostęp do krytycznych danych i usług, co może zagrażać życiu pacjentów. Przykłady ataków ransomware na szpitale w Polsce to:
   - **Szpital Wojewódzki w Bydgoszczy (2022):** Hakerzy zaatakowali systemy IT szpitala i żądali okupu w wysokości 4 mln zł. Atak ten spowodował znaczne opóźnienia w leczeniu pacjentów i odwołanie niektórych operacji,
   - **Szpital Powiatowy w Wadowicach (2023):** Hakerzy zaatakowali systemy IT szpitala i żądali okupu w wysokości 500 tys. zł. Atak ten spowodował awarię systemu informatycznego szpitala, co utrudniło dostęp do danych pacjentów i opóźniło przyjęcia pacjentów,
   - **ALAB Laboratoria (2023):** Hakerzy wykorzystali oprogramowanie ransomware do zaszyfrowania części baz danych ALAB oraz plików zawierających wyniki badań. Celem atakujących było wyłudzenie okupu od firmy w zamian za odszyfrowanie danych. Wyciek danych dotyczył **ponad 50 tysięcy pacjentów** i obejmował m.in. ich imiona i nazwiska, adresy, numery PESEL, wyniki badań laboratoryjnych i dane medyczne,

Dla przypomnienia wyników przeprowadzonej ankiety – 69% szpitali odpowiedziało, że czuje średnie, małe lub bardzo małe ryzyko związane z atakiem Ransomware na systemy informatyczne szpitala!!!

2. **Ataki phishingowe:** W tym typie ataku hakerzy wysyłają e-maile lub wiadomości SMS do pracowników szpitala udając wiarygodne osoby lub instytucje, np. administratorów IT lub Ministerstwo Zdrowia. Celem tych ataków jest nakłonienie pracowników do ujawnienia poufnych informacji, takich jak hasła lub dane logowania, które hakerzy mogą następnie wykorzystać do włamania się do systemów IT szpitala.
3. **Ataki typu „man in the middle":** W tym typie ataku hakerzy przechwytują komunikację między dwoma systemami, np. między komputerem pracownika szpitala a systemem bankowym szpitala. Hakerzy mogą następnie podszywać się pod jedną ze stron i modyfikować dane przesyłane między systemami, np. kradnąc dane kart płatniczych szpitala lub przekierowując płatności na konto hakera.
4. **Ataki na łańcuch dostaw:** W tym typie ataku hakerzy atakują dostawców usług IT dla szpitali, np. firmy produkujące oprogramowanie lub świadczące usługi hostingowe. Celem tych ataków jest zainstalowanie złośliwego oprogramowania na systemach dostawcy, które może następnie zostać wykorzystane do włamania się do systemów IT szpitala.
5. **Ataki typu DDoS (Distributed Denial-of-Service):** W tym typie ataku hakerzy zalewają serwery szpitala ruchem sieciowym z wielu zainfekowanych komputerów. Celem tego ataku jest uniemożliwienie dostępu do usług szpitala, np. strony internetowej lub systemu rezerwacji wizyt.
6. **Inne:** ataki na słabe punkty w oprogramowaniu lub sprzęcie szpitala, ataki socjotechniczne polegające na manipulowaniu pracownikami szpitala lub ataki fizyczne polegające na włamaniu się do budynku szpitala i kradzieży danych.

Przykłady ataków hakerskich w Polsce można mnożyć:

- atak hakerski na klinikę „Budzik" przy warszawskim Centrum Zdrowia Dziecka. Pod koniec 2019 roku cyberprzestępcy zaatakowali system informatyczny, który został zablokowany. Sparaliżowało to pracę placówki, m.in. niemożliwe było sporządzenie obligatoryjnego raportu dla NFZ, co groziło utratą miesięcznych funduszy (przestarzała infrastruktura informatyczna, która opierała się na rozwiązaniach z 2012 roku),
- Instytut Centrum Zdrowia Matki Polki w Łodzi (2022) padł ofiarą hakerskiego cyberataku, podczas którego doszło do naruszenia danych osobowych. Po ataku szpital zdecydował się na zbudowanie nowej sieci, co trwało kilka tygodniu i było odczuwalne przez pacjentów, m.in. przesuwane były zaplanowane hospitalizacje,
- Wiele innych.

Według informacji Agencji Bezpieczeństwa Cybernetycznego i Infrastruktury (csirt) **w listopadzie 2022 roku doszło do ok. 10-20 ataków dziennie, natomiast w lutym 2023 roku było to już 40-60 (26% to były szpitale).** W kwietniu media obiegła informacja, że „Polska jest bombardowana przez hakerów" i doliczono się ponad 500 ataków hakerskich dziennie na polskie firmy strategiczne (marzec 2023 - eksperci cyberbezpieczeństwa zwrócili uwagę na wzmożone działania grupy hakerskiej Killnet, która za cel wzięła sobie ataki na placówki opieki medycznej. Ta prorosyjska grupa specjalizuje się w atakach DDoS, które doprowadzają do braku dostępu do systemów).

Zespół reagowania w NASK tylko w 2022 roku zarejestrował 43 incydenty bezpieczeństwa w sektorze ochrony zdrowia, co daje trzykrotny wzrost cyberataków w porównaniu do 2021 roku.

Wykorzystując komentarz nr 29/2022 Ośrodka Badań Azji, Centrum Badań nad Bezpieczeństwem Pana Konrada Rumińskiego – analityka ds. Japonii w Ośrodku Badań Azji należy dodatkowo zwrócić uwagę na zbieżności wielu ataków i wykorzystywanych technik oraz rodzajów ataków w różnych krajach. W komentarzu poruszona jest zbieżność ataków w Japonii do tych, które miały miejsce w Polsce (ransomware). Czy tego chcemy czy nie jesteśmy częścią globalnej infrastruktury IT z jej dobrymi i złymi stronami.

Druga odpowiedź ubezpieczycieli dotycząca zainteresowania zawarciem polisy ubezpieczenia ryzyk cybernetycznych, w świetle statystyk potwierdzających ataki hakerskie na szpitale w Polsce, z rok rocznymi kilkukrotnymi wzrostami, w zestawieniu do niskiej świadomości zagrożeń jest niestety również negatywna.

Z perspektywy ubezpieczycieli mając taką ilość danych z Polski oraz globalnie z innych krajów potwierdzających zdarzenia czy incydenty cybernetyczne trudno oczekiwać zainteresowanie czy chęć ubezpieczenia podmiotów z tak niskim poziomem zabezpieczeń oraz świadomości istnienia ryzyka. Dodatkowo bardzo istotnym elementem jest fakt, że dane z elektronicznej dokumentacji medycznej są bardzo cenne dla cyberprzestępców, osiągają od 10 do 100 razy większą wartość niż informacje o kartach kredytowych na czarnym rynku (przegląd Journal of Medical Systems z kwietnia 2020 r.). W związku z tym różne państwa czy grupy hakerskie tym bardziej będą zainteresowane atakami hakerskimi na szpitale. Analizując przekrojowe dane z rynku medycznego Stanów Zjednoczonych 94% szpitali doświadczyło w ostatnich 3 latach co najmniej jednego ataku hakerskiego. Zgodnie z trendami ilościowymi liczba ataków w najbliższych 2-3 latach prawdopodobnie potroi się. Statystyki w tym zakresie są niestety bardzo niekorzystne.

Odrębnym wątkiem wymagającym analizy i komentarza są budżety i inwestycje przeznaczane na poprawę bezpieczeństwa cybernetycznego w szpitalach.

Budżety szpitali i inwestycje w cyberbezpieczeństwo.

Koszt infrastruktury IT zabezpieczającej szpital przed atakami hakerskimi jest trudny do precyzyjnego określenia, ponieważ zależy od wielu czynników, takich jak:

- **Wielkość i złożoność szpitala:** Szpitale o większej liczbie łóżek i oddziałów, a także te, które posiadają bardziej rozbudowaną infrastrukturę IT, będą potrzebować droższej infrastruktury zabezpieczającej.
- **Rodzaj danych przechowywanych w szpitalu:** Szpitale, które gromadzą i przetwarzają wrażliwe dane medyczne, takie jak dane osobowe i historia choroby pacjentów, będą potrzebować bardziej rygorystycznych zabezpieczeń, co może zwiększyć koszty. W tym punkcie należy dodatkowo zaznaczyć, że pacjentami mogą być osoby publiczne, sławne, gdzie dodatkowo w grę będzie wchodziło wyższe ryzyko reputacyjne.
- **Poziom pożądanego bezpieczeństwa:** Szpitale mogą zdecydować się na wdrożenie różnych poziomów bezpieczeństwa, od podstawowych zabezpieczeń po zaawansowane rozwiązania chroniące przed wysublimowanymi atakami. Im wyższy poziom bezpieczeństwa, tym wyższe koszty.
- Wybór konkretnych rozwiązań: Na rynku dostępnych jest wiele różnych rozwiązań bezpieczeństwa IT, od oprogramowania antywirusowego i zapór sieciowych po systemy wykrywania włamań i szyfrowanie danych. Koszt tych rozwiązań może się znacząco różnić w zależności od producenta, funkcjonalności i skali wdrożenia.
- **Koszty personelu IT:** Szpitale będą potrzebować wykwalifikowanego personelu IT do wdrożenia, konfiguracji i zarządzania infrastrukturą bezpieczeństwa. Koszty te obejmują wynagrodzenia pracowników, szkolenia i certyfikacje.
- **Inne koszty pośrednie.**

Ogólnie rzecz biorąc, koszt infrastruktury IT zabezpieczającej szpital przed atakami hakerskimi może wahać się od kilkudziesięciu tysięcy złotych do kilku milionów złotych.

Odnosząc się po raz kolejny do wyników anonimowej ankiety dotyczącej cyberbezpieczeństwa za publikacją „Dobre praktyki – cyberbezpieczeństwo w szpitalach" – na pytanie:

Jaki wkład własny podmiot jest gotowy przeznaczyć na wzmocnienie cyberbezpieczeństwa przy założeniu dofinansowania 50%:

- Aż 71% szpitali odpowiedziało, że 100 000 PLN lub mniej (aż 48% jest gotowe przeznaczyć tylko 50 000 PLN),
- Tylko 23% szpitali odpowiedziało, że 400 000 PLN lub więcej (13% jest gotowe przeznaczyć 800 000 PLN - bardzo pozytywny sygnał).

Zgodnie z „HIPAA journal" w latach 2020 – 2025 w Stanach Zjednoczonych branża opieki zdrowotnej wyda ponad 125 000 000 000 USD (miliardów) na produkty i usługi w zakresie cyberbezpieczeństwa. W związku z brakiem przełożenia wskazanej wartości na ilość podmiotów reprezentujących branżę opieki zdrowotnej nie możemy przeliczyć wydatków per podmiot.

Trzecia odpowiedź ubezpieczycieli dotycząca zainteresowania zawarciem polisy ubezpieczenia ryzyk cybernetycznych, w świetle niskich nakładów inwestycyjnych, będzie prawdopodobnie negatywna. Dotyczy to szczególnie tych szpitali, które są niedoinwestowane w zakresie infrastruktury IT oraz procedur cybernetycznych.

Skala ubezpieczeń cybernetycznych w Polsce.

Dokładny procent szpitali w Polsce, posiadających ubezpieczenia cybernetyczne, jest trudny do ustalenia. Dostępne dane pochodzą z różnych źródeł i mogą się różnić metodologią badań.

- **Według Rzeczpospolitej:** W artykule z 2023 roku Rzeczpospolita podaje, że około 20% szpitali w Polsce posiada ubezpieczenia cybernetyczne,
- **Według szacunków jednego z globalnych ubezpieczycieli tylko 10-15%** szpitali posiadało tego typu ubezpieczenia,
- **Według ekspertów ds. cyberbezpieczeństwa:** eksperci szacują, że odsetek ten kształtuje się w granicach 10-15%.

Należy zaznaczyć, że te dane mogą być niedokładne i nie odzwierciedlać rzeczywistego stanu rzeczy. Różnice w metodologii badań i brak centralnego rejestru utrudniają precyzyjne oszacowanie.

Podsumowując: Dokładny odsetek szpitali prywatnych w Polsce posiadających ubezpieczenia cybernetyczne jest trudny do ustalenia, ale szacuje się, że jest to **około 10-20%**. Istnieje wiele powodów, dla których tak niski odsetek szpitali posiada tego typu ubezpieczenia, ale wraz ze wzrostem świadomości ryzyka cybernetycznego i dostępności bardziej konkurencyjnych ofert, można oczekiwać, że ta liczba będzie wzrastać.

Biorąc pod uwagę doświadczenia brokerów ubezpieczeniowych we współpracy z podmiotami leczniczymi szacujemy, że ilość szpitali posiadających aktywną polisę z ochroną w zakresie cyber jest zdecydowanie bliższa 10%.

Czwarty obszar, który jest szczegółowo analizowany przez ubezpieczycieli to skala biznesu i apetyt na ryzyko ubezpieczeniowe. Przy założeniu, że tylko około 10% szpitali posiada aktywną polisę ubezpieczeniową w zakresie cyber oferty składane szpitalom są bardzo selektywne.

Jako doświadczony broker ubezpieczeniowy z jedną ze specjalizacji w ubezpieczeniach odpowiedzialności cywilnej zawodowej dla sektora IT oraz ryzyk cybernetycznych podjęliśmy się zebrania kluczowych przyczyn słabych zabezpieczeń szpitali przed atakami cybernetycznymi oraz bardzo małej ilości szpitali posiadających aktywną ochronę ubezpieczeniową.

Zdefiniowane kluczowe przyczyny:

1. **Niedostateczne finansowanie:** Szpitale często borykają się z problemami finansowymi, co może prowadzić do ograniczenia środków przeznaczonych na cyberbezpieczeństwo. Inwestycje w infrastrukturę IT, szkolenia personelu i nowoczesne rozwiązania zabezpieczające mogą być postrzegane jako niepotrzebny wydatek.
2. **Brak świadomości ryzyka:** Niektórzy pracownicy szpitali, w tym personel medyczny i administracyjny, mogą nie zdawać sobie sprawy z ogromu zagrożeń cybernetycznych i ich potencjalnych konsekwencji. Brak odpowiedniej edukacji i szkoleń może prowadzić do zaniedbań w zakresie bezpieczeństwa.
3. **Złożona infrastruktura IT:** Szpitale posiadają rozbudowaną infrastrukturę IT, obejmującą wiele różnych systemów i urządzeń. Utrzymanie bezpieczeństwa w tak złożonym środowisku może być trudne i wymagające znacznych nakładów.
4. **Brak wykwalifikowanego personelu IT:** Znalezienie i utrzymanie wykwalifikowanych specjalistów ds. cyberbezpieczeństwa może być dla szpitali wyzwaniem. Brak odpowiedniej kadry może utrudniać wdrażanie i utrzymywanie skutecznych zabezpieczeń.
5. **Nieaktualne oprogramowanie i systemy:** Szpitale mogą korzystać z przestarzałego oprogramowania i systemów, które nie są odpowiednio zabezpieczone przed nowymi zagrożeniami cybernetycznymi. Brak regularnych aktualizacji i łatek może zwiększać podatność na ataki.
6. **Niewystarczające procedury bezpieczeństwa:** W niektórych szpitalach mogą brakować odpowiednich procedur bezpieczeństwa dotyczących korzystania z komputerów, przechowywania danych i reagowania na incydenty cybernetyczne.

Kluczowe przyczyny pokrywają się z najczęściej spotykanymi argumentami towarzystw ubezpieczeniowych przy odmowach złożenia oferty ubezpieczenia cyber dla szpitali:

1. Stare oprogramowanie zainstalowane w szpitalnych komputerach – według ankiety z publikacji OSSP Dobre praktyki – cyberbezpieczeństwo w szpitalach 45% szpitali posiada 101 i więcej komputerów w tym 24% posiada ponad 200 (spotykane oprogramowanie MS 7 i 8),
2. Brak regularnych aktualizacji oprogramowania,
3. Brak nadzoru administracyjnego i kontroli rodzajów oprogramowania przetrzymywanych lub wgrywanych do komputerów, wgrywanie nielegalnego lub nieautoryzowanego oprogramowania,
4. Brak lub niewystarczająca ilość zabezpieczeń typu firewall, autoryzowanych dostępów do danych wrażliwych (wspomaganie MFA), autoryzowanych dostępów zdalnych
5. Brak lub niewystarczająca jakość szyfrowania danych,
6. Brak lub niewystarczająca ilość szkoleń dla personelu, procedur chroniących przed zdarzeniami cybernetycznymi czy procedur będących planem działań po zdarzeniu/ataku cybernetycznym,
7. Jakość kopii zapasowych/back up'ów lub procedur i aktywnych działań doprowadzających do odzyskiwania kopii zapasowych (ćwiczenia z odzyskaniem minimum raz na rok),
8. Brak regularnych analizy wpływu na biznes w cyberbezpieczeństwie (BIA) oraz wprowadzania pełnoprawnych planów ciągłości zarządzania.

Jak szpitale mogą zabezpieczyć swoją infrastrukturę IT i zabezpieczyć swój biznes w kontekście konsekwencji związanych z ryzykami cybernetycznymi włączając ubezpieczenie?

Aby poprawić poziom bezpieczeństwa cybernetycznego w szpitalach, konieczne są następujące działania:

- **Zwiększenie inwestycji w cyberbezpieczeństwo:** Szpitale muszą zwiększyć wydatki na infrastrukturę IT, szkolenia personelu i nowoczesne rozwiązania zabezpieczające,
- **Podnoszenie świadomości ryzyka:** Należy przeprowadzać regularne szkolenia dla pracowników szpitala w zakresie cyberbezpieczeństwa, aby uświadamiać im zagrożenia i uczyć ich właściwych zachowań,
- **Wzmocnienie procedur bezpieczeństwa:** Należy opracować i wdrożyć kompleksowe procedury bezpieczeństwa dotyczące korzystania z komputerów, przechowywania danych i reagowania na incydenty cybernetyczne,
- **Regularne aktualizacje oprogramowania i systemów:** Należy regularnie aktualizować oprogramowanie i systemy do najnowszych wersji, aby zapewnić im odpowiednią ochronę przed nowymi zagrożeniami,
- **Współpraca z ekspertami:** Szpitale powinny współpracować z ekspertami ds. cyberbezpieczeństwa w celu oceny ryzyka, wdrożenia odpowiednich zabezpieczeń i reagowania na incydenty cybernetyczne,
- **Inne, które zostaną zdiagnozowane w wyniku audytów czy zaleceń pokontrolnych.**

Świadomie na pierwszym miejscu zostały wymienione aspekty dotyczące inwestycji w cyberbezpieczeństwo.

Oto kilka przykładów kosztów poszczególnych elementów infrastruktury IT:

- **Firewall:** Od kilku tysięcy złotych do kilkudziesięciu tysięcy złotych rocznie
- **System wykrywania włamań (IDS):** Od kilku tysięcy złotych do kilkudziesięciu tysięcy złotych rocznie
- **Oprogramowanie antywirusowe:** Od kilkudziesięciu złotych do kilkuset złotych na urządzenie rocznie
- **Usługi ITaaS:** Od kilkudziesięciu tysięcy złotych do kilku milionów złotych rocznie

Biorąc pod uwagę zarówno bezpośrednie, jak i pośrednie koszty cyberataków, inwestycja w infrastrukturę IT zabezpieczającą szpital przed atakami hakerskimi jest opłacalna w dłuższej perspektywie.

Odwołując się ponownie do przywołanych wcześniej wyników anonimowej ankiety wśród szpitali z ostatniej publikacji Dobrych praktyk należy dostrzec bardzo pozytywne działania zmierzające do poprawy bezpieczeństwa.

Na pytanie czy podmiot korzystał w 2022 roku z programu NFZ w zakresie wsparcia inwestycji w zakresie cyberbezpieczeństwa blisko połowa (47%) ankietowanych odpowiedziała pozytywnie. Oznacza to, że szpitale są świadome zagrożeń cybernetycznych i z zaangażowaniem sięgają po dostępne dofinansowanie.

Równie pozytywne odpowiedzi dotyczą przeznaczenia środków uzyskanych ze wsparcia – najwięcej zainwestowano w systemy do tworzenia kopii zapasowych, później urządzenia i oprogramowanie zabezpieczające sieć (firewall) oraz serwery i macierze dyskowe.

Jeszcze bardziej korzystne odpowiedzi, szczególnie w kontekście świadomości zagrożeń cybernetycznych, dotyczyły pytania: W jakich obszarach konieczna jest poprawa istniejących lub zastosowanie nowych zabezpieczeń? Odpowiedzi skupiały się na:

- Skany podatności, które pozwalają identyfikować zagrożenia we własnym środowisku IT
- Technologie, które ułatwiają precyzyjne monitorowanie bezpieczeństwa infrastruktury IT
- Systemy tworzenia kopii danych
- Urządzenia i oprogramowanie oraz wsparcie eksperckie dotyczące cyberbezpieczeństwa
- Urządzenia i oprogramowanie zabezpieczające sieć (firewall)
- Systemy kontroli dostępu administracyjnego i zarządzania uprawnieniami
- Serwery i macierze dyskowe

Analizując powyższe odpowiedzi z ankiety zwracam uwagę w jak wielkim stopniu zostały dostrzeżone konieczne poprawy w świetle zastrzeżeń ubezpieczycieli do składania ofert (str. 6).

Odnosząc się do pierwszych akapitów artykułu i odpowiedzi na pytania z tej samej ankiety (pytania/odpowiedzi w tabeli) trudno nie odnieść wrażenia, że wchodzimy na zupełnie inny poziom świadomości zagrożeń cybernetycznych. Nie wiem na ile można postawić hipotezę, że odpowiedzi zostały udzielone przez grupę stanowiącą nieco ponad 20% ankietowanych, którzy na zagrożenia odpowiadali, że są duże lub bardzo duże.

Pierwszy krok to audyt specjalistów w zakresie cyberbezpieczeństwa zakończony raportem poaudytowym z wnioskami i zaleceniami. W tym samym kroku warto aktywnie rozpocząć współpracę z brokerem ubezpieczeniowym, z którym zostaną omówione wymagania ubezpieczycieli oraz zostanie udzielone wsparcie przy uzupełnianiu niezbędnych wniosków.

Pytania ubezpieczycieli we wnioskach ubezpieczeniowych przede wszystkim dotyczą:

- **Danych dotyczących wnioskodawcy** (dane rejestrowe, przychody z podziałem na kraje, ilość pracowników etc.),
- **Rodzaj prowadzonej działalności** oraz, jeśli występują, podział na kraje (objęte/nie objęte sankcjami),
- **Prywatność danych** (ilość rekordów oraz rodzaj danych i inne),
- **Bezpieczeństwo danych i informacji** (dedykowani pracownicy, polityki prywatności, szkolenia, procedury, testy i inne),
- **Rodzaje i systemy informatyczne** (krytyczność systemów zachowanie ciągłości, autoryzacje oraz zdalne dostępy i inne),
- **Uwierzytelniania wieloskładnikowego** (w przypadku zdalnego dostępu do sieci i do poczty e-mail),
- **Procedur dotyczących wykonywania, przechowywania i testowania kopii zapasowych,**
- **Ochrona punktów końcowych,**
- **Szkolenia pracowników,**
- **Działalność multimedialna** (jeśli dotyczy),
- **Historia szkodowa,**
- **Oświadczenia.**

Oczywiście w każdej sytuacji, kiedy szpital nie może zostać zdefiniowany jako „best-in-class" ubezpieczyciel zachowuje prawo zadania dodatkowych pytań doprecyzowujących.

Drugi krok to kalkulacja oferty przez ubezpieczyciela i rekomendacja optymalnego zakresu ochrony wynikającego z wcześniej przeprowadzonej analizy potrzeb klienta.

Na tym etapie krytycznie ważnym jest wzajemna komunikacja i dokładne omówienie w jakich zakresach ochrony i w jakich sytuacjach zadziała ubezpieczenie oraz jakie czynności należy wykonać, żeby otrzymać odszkodowanie i należne wsparcie.

Rynek ubezpieczeń cybernetycznych na świecie i w Polsce rozwija się dynamicznie. Dzisiejsze oferty ubezpieczeniowe obejmują nie tylko zdefiniowane zakresy ochrony, ale szerokie wsparcie przy wystąpieniu zdarzenia cybernetycznego (np. assistance rozszerzony o zewnętrzne wsparcie IT). W zasadzie wsparcie w przypadku zdarzenia cybernetycznego jest oferowane przez prawie wszystkich ubezpieczycieli w Polsce.

Główne zakresy ochrony ubezpieczeń cybernetycznych dotyczą przede wszystkim*:

- Ubezpieczenie szkód własnych obejmujące m.in.:
  - Reakcja na Zdarzenie
  - Zakłócenie Działalności
  - Przywrócenie Systemu i Danych
  - Wymuszenie Komputerowe
- Ubezpieczenie OC:
  - OC z tytułu naruszeń prywatności i bezpieczeństwa sieci
  - OC z tytułu naruszeń związanych z działalnością medialną (jeśli włączona do zakresu)

- Rozszerzenia zakresu ubezpieczenia:
  - Awaryjna Reakcja na Zdarzenie
  - Koszty Ulepszenia
  - Przestępstwo Komputerowe
  - Wydatki związane z Wypłatą Nagrody
  - Oszustwo Telekomunikacyjne
- Podlimity dla zdarzeń:
  - Fundusz Rekompensaty Konsumenckiej
  - Szkoda Kartowa
  - Kary Administracyjne
  - Ransomware
  - Wykorzystanie Luki w Starym Programie
- Rozszerzenia ochrony na wypadek Incydentów Rozległych

Bezpłatne usługi dodatkowe udzielane w ramach zawartej Polisy:

- **Vulnerability Outreach Programme** – Zarejestruj się, aby regularnie otrzymywać alerty o krytycznych błędach i lukach w zabezpieczeniach, dostosowanych do rodzaju używanego oprogramowania. Komunikaty te zawierają praktyczne porady umożliwiające skuteczne ograniczenie ogólnej ekspozycji na ryzyko, aby nie dopuścić do wykorzystania poufnych informacji. Aplikacja dostarczona przez Chubb
- **Cyber Alert App od Chubb** – Za pośrednictwem aplikacji możesz w wygodny sposób zgłaszać wszelkie nagłe zdarzenia oraz incydenty techniczne, a także w pełni korzystać z usług wsparcia 24/7. Za pomocą zaledwie kilku kliknięć możesz nawiązać kontakt z dedykowanym Ekspertem Chubb, który specjalizuje się w reagowaniu na nagłe incydenty związane z zarządzaniem cyberbezpieczeństwem, w wygodny sposób przesłać nam wymaganą dokumentację związaną z ustaleniem przyczyn zdarzenia, czy zawiadomić o nim swojego pośrednika ubezpieczeniowego – a to nie wszystkie możliwości, które umożliwia nasza aplikacja. Pobierz ją już teraz w App Store lub Google Play Store.
- **Password Management Solution** – Aplikacja ułatwia zarządzanie bezpieczeństwem przechowywania licznych haseł i pozwala ograniczyć ryzyko wynikające z ich niewłaściwego zabezpieczenia lub zaniedbań pracowników, co zwiększa ryzyko infiltracji firmowej sieci przez cyberprzestępców. Usługa dostępna jest w języku angielskim, holenderskim, francuskim, niemieckim, włoskim, japońskim, koreańskim, portugalskim, uproszczonym chińskim, hiszpańskim i szwedzkim. Aplikacja dostarczona przez Dashlane
- **External Vulnerability Monitoring** – Bez ponoszenia dodatkowych kosztów za pośrednictwem dedykowanej platformy, możesz samodzielnie monitorować stopień bezpieczeństwa przetwarzanych danych oraz potencjalnych zagrożeń związanych z cyberatakami. Platforma wskazuje zarówno silne elementy stosowanych zabezpieczeń, jak i potencjalne błędy i luki, zapewniając pełny wgląd w bezpieczeństwo infrastruktury sieci Twojej organizacji. Usługa ta jest dostępna za pośrednictwem platformy internetowej BitSight Core, która nie wymaga instalacji sprzętu ani oprogramowania. Aplikacja dostarczona przez BitSight

Rozwiązania dostarczane przez Partnerów Biznesowych CHUBB są dostępne dla Klientów posiadających ważną polisę Ubezpieczenia Cyber, która uprawnia do skorzystania z dodatkowej zniżki.

- **Phishing Awareness Assessments** – Przeprowadź badanie wśród swoich pracowników, aby sprawdzić, czy odpowiednio reagują na próby ataków phishingowych w oparciu o najnowsze aktywne typy zagrożeń. A następnie wykorzystaj uzyskane dane celem wdrożenia odpowiednich środków mających na celu podniesienie poziomu cyberbezpieczeństwa Twojej organizacji. Usługa dostępna w 36 językach. Usługa dostępna za pośrednictwem Cofense
- **Falcon Prevent Ransomware Defence** – Uzyskaj dostęp do oprogramowania antywirusowego nowej generacji od CrowdStrike. Ochrona infrastruktury sieci komputerowej zapewniana przez całodobowe wykrywanie i blokowanie wielu zagrożeń typu ransomware lub taktyk stosowanych przez przeciwników. Rozwiązanie CrowdStrike zapewnia możliwości wykrywania złośliwego oprogramowania wykraczające poza tradycyjne programy antywirusowe. Usługa dostępna za pośrednictwem CrowdStrike

**Powyższe zakresy oraz wsparcie zostały opisane na przykładzie standardowych zakresów ochrony opisanych w ofercie/polisie CHUBB Polska.*

Trzeci krok to zawarcie polisy ubezpieczeniowej

Z doświadczeń brokerów ubezpieczeniowych wynika, że szpitale, które zawarły polisy ubezpieczeniowe w 100% odnawiają programy ubezpieczeniowe na kolejne lata.

Czwarty krok to regularna praca w zakresie poprawy i doskonalenia zabezpieczeń cybernetycznych.

Cyberbezpieczeństwo powinno być priorytetem dla wszystkich szpitali. Wdrażając odpowiednie rozwiązania i zwiększając świadomość ryzyka, szpitale mogą chronić dane pacjentów, zapewnić ciągłość działania i budować zaufanie pacjentów.

Potwierdzeniem nałożenia priorytetów na kwestie związane z cyberbezpieczeństwem są z roku na rok zwiększające się ataki hakerskie oraz ich skutki przekładające się na bardzo duże straty finansowe wynikające z konsekwencji takich działań.

Wsparcie i rola brokera ubezpieczeniowego we współpracy ze szpitalami przy ubezpieczeniach cybernetycznych

Kluczowym w rozpoczęciu prac związanych z potencjalnym zawarciem programu ubezpieczenia cyber jest świadomość zarządzających szpitalem w zakresie świadomości ryzyk cybernetycznych.

W oparciu o aktualny stan wiedzy, szkolenia personelu, dotychczasowe działania wdrażające właściwe poziomy zabezpieczeń, szczególnie po stronie oprogramowania, idealnie, gdyby zostały oparte o audyt zewnętrznej, profesjonalnej firmy zajmującej się cyberbezpieczeństwem. W wyniku audytu zarządzający będą mogli poznać obiektywny stan rzeczy i podjąć decyzje związane z realizacją zaleceń pokontrolnych lub zareagować na wyniki audytu.

Jak broker może pomóc szpitalowi w zawarciu programu ubezpieczenia cybernetycznego?

Broker ubezpieczeniowy jest zaufanym partnerem i doradcą szpitala w zakresie ubezpieczeń.

1. **Pierwszym krokiem jest szeroko pojęta analiza potrzeb szpitala.** W tym zakresie krytycznie ważnym jest szczegółowa analiza aktualnego stanu zabezpieczeń cybernetycznych. Równie ważnym krokiem jest dostęp do dotychczasowych prac i wdrożeń dotyczących zabezpieczeń, dostep do wiedzy i wniosków z audytów i wyników wniosków i zaleceń poaudytowych, procedur i szkoleń personelu jak również oczekiwanych zakresów i sum ubezpieczenia,

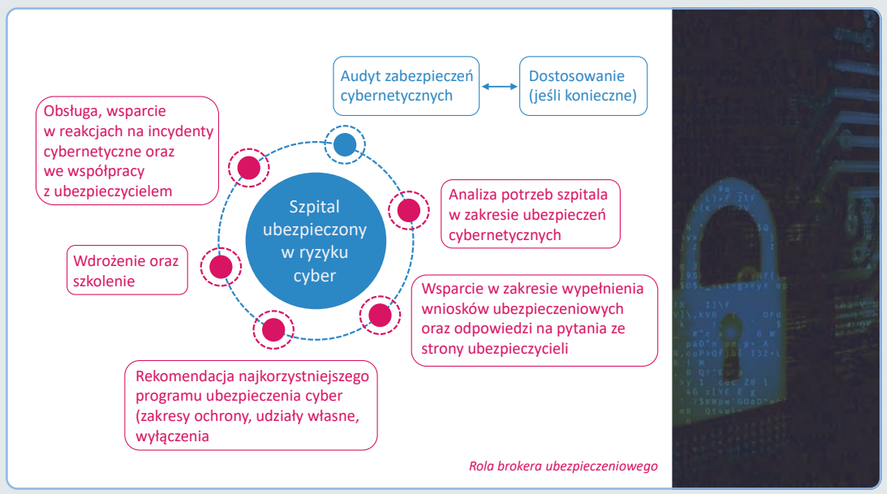
2. **Drugim krokiem jest pełne wsparcie szpitala w przygotowaniu i uzupełnieniu wniosków ubezpieczeniowych oraz prowadzeniu korespondencji z ubezpieczycielami.** Z doświadczeń brokerów etap dosłania do ubezpieczycieli wymaganych wniosków, odpowiedzi na pytania oraz danych i informacji jest stosunkowo pracochłonny i wymaga zaangażowania pracowników odpowiedzialnych w szpitalu za IT oraz cyberbezpieczeństwo (również we współpracy z zewnętrznymi dostawcami). Jest to krok konieczny do rozpoczęcia potencjalnej kalkulacji oferty przez ubezpieczyciela,

3. **Trzecim krokiem jest rekomendacja najkorzystniejszego programu ubezpieczenia ryzyk cybernetycznych** (często wariantowa). W wyniku negocjacji najkorzystniejszej oferty broker przygotowuje porównanie ofert, zakresów ochrony wraz z definicjami, sum ubezpieczenia oraz sublimitów dla poszczególnych zakresów oraz wyraźnie wskazuje ograniczenia lub wyłączenia. Odnośnie do ograniczeń oraz wyłączeń kluczowym jest rozumienie od czego i w jakich zakresach oraz limitach program ubezpieczenia cyber chroni szpital. Odrębnym elementem wymagającym omówienia są udziały własne. Ten etap należy potraktować jako priorytet w min. dwóch obszarach:
   - **Właściwego rozumienia zakresów ochrony i wyłączeń,**
   - **Wykorzystania złożonej oferty/ofert do niejako uzyskania drugiej niezależnej opinii na temat zabezpieczeń cybernetycznych w szpitalu. Składane oferty z ich zakresami ochrony oraz udziałami własnymi lub brak złożonych ofert wskazują bezpośrednio na ocenę ryzyka przez ubezpieczyciela,**

4. **Czwartym krokiem jest optymalne wdrożenie programu ubezpieczeń cybernetycznych poszerzone o szkolenie dla personelu medycznego.** Ten etap jest niejako przeniesieniem wiedzy z zakresu programu ubezpieczeniowego do personelu medycznego, który powinien znać główne zakresy ochrony oraz pozyskać wiedzę jak zareagować na incydent cybernetyczny, żeby została uruchomiona ochrona ubezpieczeniowa,

5. **Piątym etapem jest bieżąca współpraca i wsparcie brokera w codziennym funkcjonowaniu szpitala.** Brokerzy ubezpieczeniowi specjalizujący się w ryzykach ubezpieczeń cybernetycznych uczestniczą w wielu szkoleniach, uczestniczą w konferencjach i sympozjach pogłębiając swoją wiedzę. W ramach regularnych spotkań z zarządzającymi szpitalem Strony są w stanie dzielić się wiedzą i wykorzystywać najlepsze praktyki. Oczywiście nie do przecenienia jest wsparcie brokera na etapie incydentu cybernetycznego – profesjonalni brokerzy posiadają dedykowane osoby wspierające szpitale w likwidacji szkód oraz kontaktach z ubezpieczycielami.

6. **Ostatnim, szóstym etapem, jest rozpoczęcie prac odnowieniowych powtarzających powyżej opisane kroki.** Warto przy okazji tego etapu dodać, że odnawianie programów ubezpieczeniowych w zakresie ryzyka cyber dla szpital, osiąga wznawialność blisko 100%.



Rola brokera ubezpieczeniowego

Katarzyna Fortak Karasińska, Marta Woś

Cyberataki w szpitalach przyczyną wielu problemów prawnych

Rosnąca wartość danych medycznych gromadzonych przez podmioty lecznicze powoduje, że lawinowo wzrasta liczba ataków hackerskich. Skutki cyberataku na placówkę medyczną mogą być bardzo poważne. Oprócz tego, że mogą znacznie utrudnić, a nawet uniemożliwić realizowanie w placówce działalności leczniczej, skutkują również wieloma konsekwencjami prawnymi, a w efekcie również finansowanymi.

Wyciek danych wrażliwych

Cyberataki najczęściej mają postać wycieku danych wrażliwych zawartych w dokumentacji medycznej pacjentów z systemów danych podmiotu leczniczego, które są później rozpowszechniane przez cyberprzestępców niezgodnie z prawem i wolą administratora tych danych. Sytuacja, gdzie jedna z największych sieci laboratoriów diagnostycznych, której dane wrażliwe prawie 200 tys. pacjentów zostały upublicznione, pokazuje jak poważne mogą być skutki wycieku danych.

Blokada systemów IT

Przykładem cyberataku jest blokada systemów IT, która jest niezwykle dotkliwa dla podmiotu medycznego, który jej doświadczy. Blokada hackerska w irlandzkim systemie ochrony zdrowia naraziła na śmierć lub utratę zdrowia tysiące pacjentów. Pełne przywrócenie usług zajęło aż cztery miesiące. Wskutek ataku ucierpiało ponad 80 proc. infrastruktury IT, co wiązało się z wyłączeniem systemów komputerowych i utratą kluczowych informacji o pacjentach oraz danych diagnostycznych w 5-milionowej Irlandii. Pracownicy placówek medycznych zmuszeni byli przez okres przywrócenia pracy systemu do dokumentacji papierowej, nie działała poczta elektroniczna. Dane z testów laboratoryjnych musiały być pisane odręcznie i wprowadzane ręcznie – co prowadziło do większego ryzyka błędów. Innym głośnym przykładem wyłączenia systemów jest cyberatak na jeden z największych szpitali w Hiszpanii, który skutecznie odciął personel medyczny od systemu komputerowego. W wyniku ataku przełożono 150 operacji, odwołano 3000 konsultacji i 400 badań diagnostycznych.

Zhackowanie sprzętu medycznego

Kolejny przykład ataku cyberprzestępców w placówkach medycznych to zablokowanie przez hakerów podłączonego do komputera narzędzia w trakcie operacji albo wyłączenie urządzeń stale monitorujących stan zdrowia pacjentów, które wydaje się być szczególnie groźne dla pacjentów oddziałów intensywnej terapii lub intensywnej opieki medycznej. Takie ataki występują rzadziej, ale są najbardziej niebezpieczne dla życia i zdrowia pacjentów zhakowanego podmiotu.

Ataki hackerskie a naruszenie przepisów prawa

Ponieważ cyberataki często powodują niezgodne z prawem udostępnienie danych wrażliwych oraz blokują działalność szpitali, najczęściej dochodzi do naruszenia przepisów o ochronie danych osobowych, prawa w zakresie zgodności działania szpitala z przepisami o dzia-

łalności leczniczej, a także przepisami mającymi na celu ochronę praw pacjenta czy przepisami określającymi współpracę z NFZ. Naruszenia w tych zakresach mogą być podstawą wielu roszczeń skierowanych do placówki – zarówno roszczeń samych pacjentów lub ich rodzin, jak i roszczeń Prezesa Urzędu Ochrony Danych Osobowych z tytułu wystąpienia incydentu w zakresie ochrony danych osobowych pacjentów czy Narodowego Funduszu Zdrowia z tytułu nieprawidłowej realizacji umowy o udzielanie świadczeń opieki zdrowotnej.

Skutki naruszenia RODO

Naruszenie RODO może polegać na wycieku danych, nieprawidłowym przetwarzaniu danych osobowych, czy braku lub niestosowaniu się do dokumentacji dotyczącej ochrony danych osobowych w ramach instytucji.

Wobec faktu, że placówka medyczna w ramach swojej działalności przetwarza dane osobowe, musi przestrzegać odpowiednich zasad i wymogów ich dotyczących, w tym zapewnić odpowiednie bezpieczeństwo przetwarzanych danych. W przypadku gdy dojdzie do incydentu bezpieczeństwa np. wycieku danych, Dyrektor szpitala powinien:

1. **ocenić, czy doszło do naruszenia danych osobowych,** a jeśli takie naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych – **zgłosić w odpowiednim terminie takie naruszenie do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych,**
2. **poinformować osoby fizyczne, na które to naruszenie wywiera wpływ,** w niektórych przypadkach,
3. **zarejestrować każde naruszenie ochrony danych w wewnętrznej dokumentacji podmiotu leczniczego.**

Jeśli wystąpią nieprawidłowości, Prezes Urzędu Ochrony Danych Osobowych może wszcząć postępowanie wyjaśniające w celu ustalenia czy doszło do naruszenia przepisów o ochronie danych osobowych, a jeśli uzna, że tak – za takie naruszenie może zostać nałożona administracyjna kara pieniężna. Postępowanie może zostać również wszczęte z własnej inicjatywy Urzędu lub na wniosek osoby, która złożyła skargę, jeśli naruszenie jej bezpośrednio dotyczyło.

Maksymalna wysokość kary, która grozi szpitalowi to 20.000.000,00 EUR (w przypadku przedsiębiorstwa – maksymalnie 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa). Wysokość kary zależy od wielu czynników tj. stopnia i wagi naruszenia przepisów, kategorii i rodzaju danych osobowych, których dotyczyło naruszenie czy kształtu współpracy z organem nadzorczym w trakcie trwania postępowania wyjaśniającego.

Co istotne, kara pieniężna za zaistniałe naruszenie ochrony danych może zostać nałożona nawet wtedy, gdy nieprawidłowości zostaną usunięte przed zakończeniem postępowania przed Urzędem. Jeśli z okoliczności danej sprawy wyniknie, że nałożenie kary nie jest konieczne, organ nadzorczy może poprzestać na środkach niepieniężnych, zmierzających do usunięcia naruszenia i przywrócenia stanu zgodnego z prawem.

Dodatkowo, przepisy RODO dopuszczają również możliwość dochodzenia roszczeń z tytułu odpowiedzialności cywilnej przez osoby poszkodowane. Przepisy nie precyzują maksymalnych kwot takiego odszkodowania, niemniej na jego wysokość będzie miała wpływ ocena danego stanu faktycznego, a także stopień m.in. współpracy z organem nadzorczym i podjęte przez podmiot działania naprawcze.

Atak hackerski w kontekście naruszenia praw pacjenta

Cyberatak na podmiot leczniczy może naruszać szereg praw pacjentów zhackowanej placówki. W wyniku blokady systemu IT szpitala, może dojść do naruszenia:

- prawa pacjenta do dostępu do dokumentacji medycznej i informacji o stanie zdrowia pacjenta, w przypadku braku dostępu do dokumentacji medycznej,
- prawa pacjenta do wyrażenia zgody na zabieg medyczny – w przypadku odbierania od pacjenta pisemnej zgody z wykorzystaniem urządzeń mobilnych np. tabletu z rysikiem, na którym pacjent składa podpis, usunięcie dokumentacji medycznej wskutek ataku hackerskiego, może doprowadzić do sytuacji, w której podmiot leczniczy nie będzie w stanie udowodnić, że odebrał od pacjenta pisemną zgodę na przeprowadzone leczenie;
- prawa pacjenta do świadczeń zdrowotnych, w sytuacji braku możliwości wykonania zabiegu lub badania czy nawet przyjęcia pacjenta lub wystawienia skierowania lub zwolnienia lekarskiego, nawet w formie papierowej, przy braku dostępu do systemu placówki; Zachodzi zatem konieczność odwołania wizyt lekarskich i przesunięcia w czasie udzielenia pomocy medycznej, co może implikować dodatkowe roszczenia pacjentów z tytułu nieudzielenia lub odroczenia w czasie pomocy medycznej.
- prawa pacjenta do przejrzystej, obiektywnej, opartej na kryteriach medycznych, procedury ustalającej kolejność dostępu do świadczeń zdrowotnych, w sytuacji ograniczonych możliwości ich udzielenia, w przypadku braku dostępu do systemu rejestracji pacjentów,
- prawa pacjenta do udostępniania i przechowywania dokumentacji medycznej – w przypadku wycieku danych przy braku właściwego zabezpieczenia tej dokumentacji.

Naruszenie praw pacjenta może skutkować między innymi przyznaniem pacjentowi przez sąd odpowiedniej sumy tytułem zadośćuczynienia pieniężnego za doznaną krzywdę na podstawie art. 448 Kodeksu cywilnego, z wyjątkiem naruszenia prawa pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia. Pomimo wyłączenia możliwości dochodzenia zadośćuczynienia w sytuacji zawinionego naruszenia praw pacjenta do dostępu do dokumentacji medycznej nie oznacza to, że prawa te w ogóle nie korzystają z ochrony na zasadach ogólnych. W szczególności mogą znaleźć zastosowanie zasady dotyczące odpowiedzialności odszkodowawczej.

Zgodnie ze stanowiskiem NSA wyrażonym na gruncie wyroku z dnia 10 kwietnia 2018 r., II OSK 69/18, wykonanie obowiązku prowadzenia, przechowywania i udostępniania dokumentacji medycznej wymaga podjęcia działań zapewniających ochronę dokumentacji medycznej, przy czym przy jego wykonaniu podmiot leczniczy musi dołożyć szczególną staranność. Zaniechanie tego obowiązku stanowi praktykę naruszającą zbiorowe prawa pacjenta, chyba że utrata dokumentacji medycznej następuje w wyniku zdarzeń, które rozsądnie przewidująca jednostka nie mogła przewidzieć.

W razie uzasadnionych podejrzeń dopuszczenia się naruszenia zbiorowych praw pacjentów, Rzecznik Praw Pacjenta wszczyna postępowanie w przedmiocie uznania występowania w podmiocie praktyki naruszającej zbiorowe prawa pacjenta. Jeśli Rzecznik uzna, że w rzeczywistości doszło do wystąpienia praktyki naruszającej zbiorowe prawa pacjenta, wówczas nakazuje on jej zaniechanie, bądź wskazuje działania niezbędne do usunięcia skutków naruszeń zbiorowych praw pacjentów i wyznacza terminy podjęcia tych działań. Jeśli podmiot udzielający świadczeń zdrowotnych nie dostosuje się do nałożonego obowiązku, Rzecznik nakłada na ten podmiot karę pieniężną do kwoty 500.000 zł.

Wpływ ataku hackerskiego na kontrakty z Funduszem

Cyberatak stwarza też poważne utrudnienia w wykonaniu umowy z Funduszem w następujących obszarach:

- realizacja świadczeń opieki zdrowotnej – przy zhackowaniu systemu placówki lub aparatury medycznej wykonującej zabiegi lub badania diagnostyczne często nie jest możliwe wykonywanie świadczeń zdrowotnych pacjentom, zgodnie z umową z NFZ, przepisami prawa oraz zarządzeniami Prezesa NFZ.
- raportowanie danych do systemów ochrony zdrowia – naruszenie obowiązku przekazywania zdarzeń medycznych do P1 może skutkować nałożeniem przez NFZ kary umownej, a w dalszej przyszłości nawet pozbawieniem możliwości rozliczenia świadczeń z Funduszem;
- rejestracja pacjentów – brak dostępu do systemu rejestracji pacjentów oznacza naruszenie obowiązku placówki medycznej do prowadzenia systemu kolejowego pacjentów, o którym mowa w ustawie o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, szczególnie wobec systematycznego wprowadzania przez Fundusz centralnej e-rejestracji pacjentów,
- obsługa pacjentów – w przypadku cyberataku wszystkie czynności od przyjęcia pacjenta do placówki medycznej, które są wykonywane zdalnie musiałyby odbywać się w formie tradycyjnej, papierowej.
- prowadzenie i wykorzystanie elektronicznej dokumentacji medycznej, która jest niezbędna do udzielania świadczeń ratujących zdrowie i życie pacjentów. Skoro nie jest możliwe wykorzystanie elektronicznej dokumentacji medycznej to wszystkie dokumenty, w tym recepty, czy skierowania są wypisywane w formie papierowej, co niewątpliwie powoduje dalsze utrudnienia w obsłudze pacjenta.
- działanie systemów administracyjnych – w wyniku cyberataku może dojść do zablokowania m.in. systemu sprawozdawczego, który umożliwia raportowanie wykonanych świadczeń do Narodowego Funduszu Zdrowia. Brak możliwości raportowania świadczeń skutkuje brakiem płatności Funduszu za zrealizowane przez podmiot leczniczy świadczenia zdrowotne. Ponadto, świadczeniodawca nie będzie mógł złożyć oferty w postępowaniu konkursowym, wobec wymogu jej złożenia w dwóch również w formie elektronicznej. Co więcej, może dojść również do blokady systemu księgowego placówki medycznej. Z tym z kolei wiąże się wstrzymanie dostaw wyrobów medycznych oraz leków, a także wstrzymanie płatności na rzecz kontrahentów szpitala.

Nieprawidłowości w wykonywaniu kontraktów z NFZ mogą w konsekwencji spowodować nałożeniem przez Fundusz kar umownych opisanych w § 30 załącznika nr 1 do Rozporządzenia Ministra Zdrowia z dnia 8 września 2015 r. w sprawie ogólnych warunków umów o udzielanie świadczeń opieki zdrowotnej. Kary umowne, nałożone przez Fundusz nie mogą przekroczyć 4% kwoty zobowiązania wynikającego z umowy dla okresu rozliczeniowego, którego dotyczyły naruszenia.

Czasem zdarza się, że atak hackerski jest na tyle poważny, że podmiot leczniczy nie może przez to kontynuować działalności leczniczej. W takim wypadku należy pamiętać o obowiązku zgłoszenia do Funduszu przerwy w udzielaniu świadczeń. Jej niezgłoszenie może bowiem skutkować wypowiedzeniem przez Fundusz umowy ze świadczeniodawcą, bez zachowania okresu wypowiedzenia. Dodatkowo, o czasowym całkowitym albo częściowym zaprzestaniu działalności należy zawiadomić wojewodę, w terminie 3 dni roboczych od dnia zaistnienia okoliczności powodujących zaprzestanie działalności, pod rygorem nałożenia na kierownika podmiotu leczniczego kary pieniężnej.

Podsumowanie

Cyberataki wywołują wiele negatywnych konsekwencji dla podmiotu leczniczego oraz jego pacjentów. Brak możliwości korzystania z systemu informatycznego szpitala może skutkować:

- indywidualnymi roszczeniami pacjenta z tytułu naruszenia jego praw;
- roszczeniami pacjentów do sądu cywilnego z tytułu poniesionej szkody na skutek nieudzielenia świadczenia zdrowotnego w terminie;
- skargami indywidualnymi pacjenta do Rzecznika Praw Pacjenta;
- uznaniem przez Rzecznika Praw Pacjenta, iż doszło do naruszenia zbiorowych praw pacjentów (kary pieniężne do 50 000zł);
- karami finansowymi nałożonymi przez NFZ z tytułu nieprawidłowej realizacji umowy o udzielanie świadczeń zdrowotnych;
- odpowiedzialnością karną, zawodową oraz cywilną właścicieli szpitala jak personelu medycznego.

Maciej Wiśniewski

Podsumowanie

Dlaczego szpitale prywatne muszą inwestować w cyberbezpieczeństwo?

W niniejszym opracowaniu podjęliśmy próbę kompleksowego przedstawienia zagadnień związanych z możliwościami ochrony szpitali i innych podmiotów leczniczych przed skutkami cyberataków.

Mobilizująco w tym zakresie działa wchodząca wkrótce w życie dyrektywa NIS2, która niekoniecznie musi być postrzegana jako zło konieczne. Może warto spojrzeć na nowe regulacje unijne w sposób pozytywny i dostrzec, że stwarzają szansę na uporządkowanie organizacji i motywują do podjęcia systemowych działań mających na celu odpowiednie zabezpieczenie zarówno naszego interesu, jak i danych naszych pacjentów? Pomijając groźbę bardzo wysokich kar z tytułu zaniedbań prowadzących do utraty danych, konsekwencje zaniechań w tym obszarze mogą być wręcz katastrofalne.

Mamy naturalną skłonność do życzeniowego myślenia, że „jakoś to będzie"... Tymczasem ryzyko jest całkiem realne. W ostatnich latach odnotowujemy z roku na rok trzykrotny wzrost liczby cyberataków na placówki ochrony zdrowia w Polsce. Tymczasem zaledwie kilkanaście procent szpitali posiada ubezpieczenie od ryzyk cybernetycznych.

Można zaryzykować stwierdzenie , że odzwierciedla to odsetek szpitali dobrze zabezpieczonych, gdyż towarzystwa ubezpieczeniowe oferujące cyber-polisy nie chcą ubezpieczać placówek, które nie wykazały należytej staranności w tym zakresie.

Zatem czy jesteśmy bezbronni i skazani na przegraną?

Otóż nie. Kluczem jest wykazanie należytej staranności i dobranie odpowiednich środków technicznych i organizacyjnych adekwatnych do możliwości i potrzeb naszej organizacji. Cyberbezpieczeństwo nie może być kolejną „małpą wrzuconą na kark" szpitalnego informatyka. Trzeba zapewnić mu odpowiednie wsparcie ze strony działającego w trybie 24/7 specjalistycznego centrum wspomagającego „profilaktykę, diagnostykę, jak też leczenie" w przypadku gdy dojdzie do cyberataku. Wyboru kluczowego partnera w dziedzinie cyberbezpieczeństwa, jak też zakresu koniecznego wsparcia trzeba dokonać w sposób świadomy i odpowiedzialny.

Takie odpowiedzialne podejście wiąże się co prawda z konkretnymi wydatkami, które zapewne przekroczą wysokość wsparcia z NFZ, które szpitale mogą uzyskać na ten cel, niemniej jednak trzeba podjąć ten wysiłek finansowy i organizacyjny w interesie własnym i naszych pacjentów. Po „ciemnej stronie mocy" mamy bezwzględnych przestępców, którzy nie oszczędzają na środkach technicznych i bezwzględnie wykorzystują możliwości sztucznej inteligencji by poprawić skuteczność ataków.

Spójrzmy na NIS2 jak na szansę by uporządkować nasze organizacje. Musimy systematycznie monitorować ryzyka, zbudować świadomość, w pierwszej kolejności kadry zarządzającej, a następnie krzewić wiedzę na temat zagrożeń wśród pracowników i systematycznie sprawdzać ich reakcje na sytuacje potencjalnie niebezpieczne.

Nasze organizacje muszą „przesiąknąć" cyberbezpieczeństwem. Takie cyberbezpieczne szpitale będą postrzegane jako wiarygodne z punktu widzenia towarzystw ubezpieczeniowych, ale również z punktu widzenia pacjentów, co będzie stanowić istotny element przewagi konkurencyjnej.

Przy takim pozytywnym, proaktywnym podejściu naruszenie przepisów prawa w zakresie RODO i praw pacjenta w konsekwencji ataku hackerskiego nie będzie nam już poważnie zagrażać.