OGÓLNOPOLSKIE STOWARZYSZENIE
SZPITALI PRYWATNYCH

81-350 Gdynia
Plac Kaszubski 1
www.ossp.pl

Stanowisko Ogólnopolskiego Stowarzyszenia Szpitali Prywatnych dotyczące konieczności ochrony przed cyber-zagrożeniami i dostosowania w tym zakresie do regulacji prawnych wynikających z dyrektywy NIS2 dla sektora kluczowego Ochrona Zdrowia.

Szpitale w Polsce, stają w obliczu coraz poważniejszych wyzwań w zakresie informatycznym, z których największe dotyczą cyberbezpieczeństwa. Wraz z postępującą cyfryzacją systemów opieki zdrowotnej, wzrasta liczba zagrożeń, którym muszą sprostać placówki medyczne.

W tym gronie, w roli szczególnej znajdują się też szpitale prywatne, będące częścią rynku szpitalnictwa w Polsce, a równocześnie awangardą nowoczesnej diagnostyki i leczenia metodami o niskiej inwazyjności. Ich struktura i nowoczesność - choć dobrze dopasowane do potrzeb rynku zdrowotnego - wymagają istotnego i dopasowanego wsparcia w rozwoju, aby sprostać wyzwaniom stojącym przed sektorem.

OSSP z zadowoleniem przyjęła dotychczasowe działania organów centralnych w zakresie poprawy cyberbezpieczeństwa i deklaruje współudział oraz dalsze wsparcie tego typu działań.

W związku z koniecznością poniesienia kolejnych nakładów na zapewnienie tak rozumianego bezpieczeństwa cybernetycznego przez bardzo dużą grupę interesariuszy, należy niezwłocznie podjąć działania w celu zbudowania modeli finansowania rozwiązań techniczno-organizacyjnych niezbędnych do właściwej implementacji wymogów Dyrektywy NIS2.

Poniżej przedstawiamy kilka kluczowych wyzwań, które dotyczą szpitali w Polsce, uwzględniając również wpływ dyrektywy NIS2.

1. Ataki ransomware

Szpitale są szczególnie narażone na ataki typu ransomware, gdzie cyberprzestępcy blokują dostęp do systemów informatycznych lub danych pacjentów, a następnie żądają okupu za ich odblokowanie. Incydenty tego typu mogą sparaliżować działalność szpitala, opóźniając leczenie pacjentów, a w skrajnych przypadkach prowadzić do zagrożenia życia.

Rekomendujemy stworzenie przez CeZ platformy wymiany informacji na temat tego typu zagrożeń i wypracowanie scenariuszy postępowania w przypadku ataku.

2. Zarządzanie starzejącymi się systemami IT

Wiele szpitali w Polsce korzysta z przestarzałych systemów informatycznych, które są bardziej podatne na cyberataki. Problemem jest brak regularnych aktualizacji oprogramowania, a także brak wsparcia technicznego dla starszych systemów, co zwiększa ryzyko wycieków danych i ataków hakerskich.

Dostawcy systemów informatycznych muszą otrzymać z CeZ jasne wytyczne, do których muszą się dostosować, zarówno w zakresie cyberbezpieczeństwa, jak i interoperacyjności, zgodnie z Ustawą o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta.Rekomendujemy udostępnienie podmiotom

leczniczym nadzorowanych przez CeZ aplikacji zweryfikowanych pod kątem cyberbezpieczeństwa, z jednolitym poziomem systemu zabezpieczeń, udostępnionych np. w domenie otwartej.

3. Niedostateczna edukacja personelu

Wiele incydentów cyberbezpieczeństwa wynika z ludzkich błędów. Brak regularnych szkoleń dla personelu medycznego z zakresu bezpiecznego korzystania z systemów IT, phishingu oraz zarządzania hasłami prowadzi do podatności na ataki. Szpitale muszą inwestować w podnoszenie świadomości pracowników na temat zagrożeń cybernetycznych.

Rekomendujemy wprowadzenie sterowanego centralnie systemu cyklicznych szkoleń i weryfikacji kompetencji personelu placówek medycznych w zakresie cyberbezpieczeństwa.

4. Niedostateczne zasoby personelu w obszarze IT i cybersecurity

Można postawić tezę, że w przypadku większości podmiotów leczniczych występuję niedostatek zasobów w zakresie IT. Regułom jest wskazywanie osób z zespołów IT jako odpowiedzialnych za obszar cyberbezpieczeństwa. Niedostatek zasobów wynika m.in. z bardzo dużej konkurencyjności specjalistów IT na rynku pracy. Podmioty lecznicze przegrywają tę konkurencję o specjalistów z podmiotami które są w stanie zapewnić korzystniejsze warunki finansowe zatrudnienia. Niedostatek zasobów przekłada się bardzo mocno na możliwości reagowania i działania pracowników IT w zakresie cyberbezpieczeństwa. Obszar ten wymaga ciągłej uważności, najlepiej w modelu 24/7/365.

Rekomendujemy rozwój programów informatyki medycznej na kierunkach technicznych na poziomie szkół średnich i wyższych.

5. Braki w infrastrukturze cyberbezpieczeństwa

Wiele szpitali boryka się z brakiem środków na rozwój zaawansowanych narzędzi zabezpieczających. Brakuje inwestycji w nowoczesne technologie, takie jak systemy detekcji włamań, segmentacja sieci czy regularne audyty bezpieczeństwa, co naraża je na większe ryzyko ataków.

Wszyscy interesariusze systemu ochrony zdrowia powinni mieć równe prawa w dostępie do środków przeznaczanych na wsparcie w zakresie cyberbezpieczeństwa.

6. Zarządzanie dużymi ilościami danych pacjentów

Związane z cyfryzacją i rosnącą liczbą danych o pacjentach (m.in. elektroniczne historie chorób, wyniki badań) stwarza wyzwania związane z ich ochroną. Wyciek danych medycznych może mieć katastrofalne skutki zarówno dla pacjentów, jak i dla placówek medycznych, prowadząc do odpowiedzialności prawnej oraz utraty zaufania publicznego. Incydent z Alab Laboratoria powinien uświadomić jak krytyczne jest przeciwdziałanie utracie danych.

Wspieramy inicjatywę powstania Ogólnopolskiej Sieci Medycznej, mając nadzieję, że podmioty lecznicze będą mogły z niej korzystać na równych prawach. Widzimy konieczność stworzenie centralnego systemu repozytoriów danych medycznych.

7. Wpływ dyrektywy NIS2

Dyrektywa NIS2, która weszła w życie w Unii Europejskiej, w tym w Polsce, nakłada nowe wymagania na instytucje uznawane za krytyczne, w tym na placówki medyczne. Kluczowe aspekty NIS2 dotyczące szpitali:

Należy określić liczbę podmiotów kwalifikujących się jako kluczowe i ważne zgodnie z Dyrektywą oraz podmiotów funkcjonujących w łańcuchach dostaw.

Każdy podmiot powinien dokonać oceny wpływu dyrektywy NIS2 na możliwości prowadzenia działalności zgodnie z Dyrektywą.

W zależności od tej oceny powinien przyjąć program inwestycyjny uwzględniający nadrzędność dyrektywy w kontekście strategii cyberbezpieczeństwa.

Dla podmiotów zrzeszonych w OSSP Zarząd stowarzyszenia deklaruje pomoc w dokonaniu takiej oceny.

8. Obowiązek zgłaszania incydentów: Szpitale muszą zgłaszać wszelkie poważne incydenty cyberbezpieczeństwa do odpowiednich organów krajowych. Wymusza to większą przejrzystość i pozwala na szybsze reagowanie na zagrożenia.

Instytucją właściwą do zgłaszania incydentów jest sektorowy CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) prowadzony przez Centrum e-Zdrowia (CeZ). Celowe są wspólne z CeZ w zakresie działania ukierunkowane na wzrost świadomości w zakresie cyberbezpieczeństwa w sektorze prywatnym.

9. Podwyższone standardy zabezpieczeń: Dyrektywa NIS2 wprowadza wyższe standardy w zakresie zabezpieczeń IT, co oznacza, że szpitale muszą wdrożyć bardziej zaawansowane systemy ochrony. W szczególności chodzi o systemy zarządzania ryzykiem, kontrole dostępu oraz monitorowanie sieci w czasie rzeczywistym. Konieczne jest opisanie zasad korzystania z tego oprogramowania (obowiązki producenta i prawa szpitala po zakupie oprogramowania.

OSSP rekomenduje wprowadzenie karty dobrych praktyk przy zakupie, wdrożeniu i aktualizacjach oprogramowania dla systemów medycznych.

10. Kary za niewłaściwe zabezpieczenia: Nie wdrożenie odpowiednich środków zabezpieczeń może skutkować nałożeniem kar finansowych na placówki medyczne. Zmusza to szpitale do większych inwestycji w obszarze cyberbezpieczeństwa. Kwestią kluczową wydaje się uczenie systemu, a nie karanie jego użytkowników. Należy z rozwagą podejść do problemu i przyjąć okres dostosowawczy z jasno zdefiniowanymi kryteriami.

Rekomendujemy rozważne szafowanie karami oraz zrównanie pod tym względem podmiotów publicznych i prywatnych.

11. Rozbudowa struktur zarządzania kryzysowego: Zgodnie z wymogami NIS2, szpitale powinny mieć plany awaryjne na wypadek cyberataków, w tym procedury szybkiego odzyskiwania systemów i danych po incydentach. To zmusza do posiadania odpowiednich systemów kopii zapasowych oraz testowania procesów reagowania na ataki.

Niezależnie od odpowiednich zabezpieczeń infrastrukturalnych i systemów zarządzania backupami, należy udzielić odpowiedniego wsparcia informatykom szpitalnym, którzy z reguły nie mają wystarczająco czasu i właściwych kompetencji w zakresie cyberbezpieczeństwa. Celowe jest korzystanie z specjalistycznych usług zewnętrznych w zakresie monitorowania zagrożeń i reakcji na incydenty, których zakup powinien być finansowany w ramach dotacji NFZ lub z innych źródeł. Dotychczasowe dotacje NFZ wykluczały możliwość finansowania tego typu usług.

Podsumowanie

Wyzwania informatyczne, w tym dotyczące cyberbezpieczeństwa, w polskich szpitalach są złożone i obejmują zarówno techniczne aspekty, jak i zarządzanie zasobami ludzkimi. Wprowadzenie dyrektywy NIS2 dodatkowo zaostrza wymagania w tym zakresie, co może być dla niektórych placówek trudnym wyzwaniem, ale jednocześnie daje szansę na zwiększenie poziomu ochrony i odporności na cyber-zagrożenia. Placówki ochrony zdrowia dysponują ograniczonymi zasobami finansowymi, które mogą przeznaczyć na rozwiązania w zakresie informatyzacji. Dotychczasowe programy wsparcia finansowane poprzez NFZ dobrze skupiały się na zapewnieniu możliwości odtworzenia się po cyber-incydencie (systemy backupu danych) czy też dostarczaniu oprogramowania zabezpieczającego stacje komputerowe i należy wykorzystać ich doświadczenia w kolejnych działaniach cyfryzacyjnych. W obecnej sytuacji należy przyjąć jednak zdecydowanie szersze spektrum działania.

Ogólnopolskie Stowarzyszenie Szpitali Prywatnych (OSSP) jako reprezentant grupy istotnych interesariuszy systemu ochrony zdrowia w Polsce stoi na stanowisku, że o kwestiach dotyczących informatyzacji sektora należy rozmawiać w sposób partnerski ze wszystkimi partnerami. OSSP deklaruje aktywny udział w pracach zespołów koncepcyjnych i wdrożeniowych prowadzących prace implementacyjne dla rozwiązań cyfryzacyjnych.

Równocześnie OSSP deklaruje prowadzenie własnych działań dotyczących rozwiązywanie problemów cyberbezpieczeństwa i zaprasza do współpracy inne organizacje i podmioty, którym leży na sercu dobro pacjentów polskiego systemu ochrony zdrowia.

Za Zarząd OSSP
Andrzej Sokołowski
Prezes OSSP