Cyberbezpieczeństwo

5 Wojskowy Szpital Kliniczny z Polikliniką SPZOZ w Krakowie zgodnie z decyzją Ministra Obrony Narodowej został ustanowiony operatorem usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560), w zakresie udzielania świadczeń opieki zdrowotnej.
Usługa kluczowa to udzielenie świadczenia opieki zdrowotnej przez podmiot leczniczy.

Za operatora usługi kluczowej uznaje się podmiot, jeżeli:

1) świadczy usługę kluczową,
2) świadczenie tej usługi zależy od systemów informacyjnych,
3) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

Operator usługi kluczowej ma podejmować odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez niego sieci i systemy informatyczne oraz odpowiednie środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia takich usług kluczowych, z myślą o zapewnieniu ciągłości tych usług.

W szpitalu wdrożono Politykę Bezpieczeństwa Informacji 5 Wojskowego Szpitala Klinicznego z Polikliniką SP ZOZ w Krakowie oraz System Zarządzania Bezpieczeństwem Informacji.

Na System Zarządzania Bezpieczeństwem Informacji (SZBI) składają się: polityka, procedury, instrukcje, wytyczne, związane zasoby i działania, wspólnie zarządzane przez Szpital dążący do ochrony jego aktywów informacyjnych.
SZBI jest systematycznym podejściem do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w Szpitalu w celu osiągnięcia celów biznesowych.

5 WSKzP SP ZOZ egzekwuje stosowanie wewnętrznych procedur i instrukcji. Każda osoba (żołnierz/pracownik/procesor) mająca dostęp do informacji zobowiązana, jest zgodnie z posiadanymi uprawnieniami do zapoznania się z Polityką Bezpieczeństwa Informacyjnego oraz złożenia stosownego oświadczenie, potwierdzającego znajomość jej treści oraz przestrzegania jej zapisów.

5 WSKzP SP ZOZ zobowiązany jest do szacowania ryzyka dla swoich usług kluczowych, zbierania informacji o zagrożeniach i podatnościach, stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego oraz zgłaszania incydentów poważnych do Centrum Nadzoru CSIRT MON.

Podstawę do identyfikacji ryzyka stanowią procesy i aktywa 5 WSKzP SP ZOZ, których realizacja ma bezpośredni wpływ na świadczenie usługi cyfrowej w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, a tym samym na określenie poziomu akceptowalności

ryzyka.

W 5 WSKzP SP ZOZ w celu powiązania i skoordynowania działań w zakresie bezpieczeństwa informacji, oraz skutecznego osiągania założonych celów, powołano:

1) Pełnomocnika Komendanta Szpitala ds. Systemu Zarządzania Bezpieczeństwem Informacji,
2) Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji, który zobowiązany jest do natychmiastowego podjęcia działań określonych w odpowiednich procedurach w przypadku naruszenia zasad bezpieczeństwa informacji.

Reakcja na niepożądane zdarzenia (incydenty) lub podatności:

1. Każdy pacjent, osoba odwiedzająca pacjentów, pracownik, współpracownik Szpitala:

1) w przypadku zauważenia:

a) próby przełamania zabezpieczeń, próby nieautoryzowanego wejścia na chroniony obszar;
b) powzięcia wątpliwości co do stanu technicznego urządzeń informatycznych, na których przetwarzane są dane osobowe;
c) innych budzących wątpliwości w zakresie przestrzegania bezpieczeństwa informacji, a mogących wpłynąć na świadczenie usług, proszony jest o zgłoszenia niezwłocznie zaobserwowanej sytuacji do Pełnomocnika Komendanta Szpitala ds. Systemu Zarządzania Bezpieczeństwem, tel. 126308022 w godzinach od 7:00 do 15:00 (tel. alarmowy 729316899) lub przesłanie jej opisu na adres e-mail: incydent@5wszk.com.pl

Wybór środka przekazu zgłoszenia powinien być adekwatny do zaistniałej sytuacji. Wyboru dokonuje zgłaszający.

2) w przypadku zauważenia próby pozyskania w sposób nielegalny danych o innej osobie, proszony jest o zgłoszenie zaobserwowanej sytuacji do Inspektora Ochrony Danych, tel. (12) 126308073, e-mail: incydent@5wszk.com.pl.

2. Każdy użytkownik (żołnierz/pracownik lub osoba z firmy zewnętrznej współpracującej ze Szpitalem) ma obowiązek zgłaszania zauważonych przez siebie incydentów oraz notować wszystkie szczegóły związane z incydentem.

Ponadto dostrzegający:

1) zdarzenie, incydent bezpieczeństwa informacji,
2) nieprawidłowe działanie systemów w aspekcie bezpieczeństwa informacji,
3) próby podszywania się pod pacjenta, nieautoryzowane próby podłączeń do infrastruktury Szpitala, fałszywe wiadomości mailowe wysyłane do personelu Szpitala,
4) inne zdarzenie mogące mieć wpływ na bezpieczeństwo informacji,

jest zobowiązany zaobserwowaną sytuację niezwłocznie zgłosić do Pełnomocnika Komendanta Szpitala ds. Systemu Zarządzania Bezpieczeństwem, tel. 126308022 w godzinach od 7:00 do 15:00 (tel. alarmowy 729316899) lub przesłać jej opis na adres e-mail: incydent@5wszk.com.pl.

Wybór środka przekazu zgłoszenia powinien być adekwatny do zaistniałej sytuacji. Wyboru dokonuje zgłaszający. Zabrania się użytkownikowi zgłaszającemu problem lub naruszenie bezpieczeństwa wykonywania jakichkolwiek działań „na własną rękę” rozwiązujących problem, za wyjątkiem działań niezbędnych dla zapewnienia bezpieczeństwa osobom i mieniu. Użytkownik w miarę możliwości powinien zabezpieczyć materiał dowodowy. Powyższe działania mają na celu zapobieganie

incydentom na wczesnym etapie ich rozwoju.

Za szybką reakcję na pojawiające się incydenty z góry dziękujemy.

Do jednych z wielu obowiązków nałożonych na Operatora Usługi Kluczowej, jest obowiązek opublikowania na stronie internetowej Szpitala podstawowych informacji związanych z zagrożeniami cyberbezpieczeństwa. Ma to na celu umożliwienie pacjentom oraz podmiotom współpracującym, zrozumienia zagrożeń cyberbezpieczeństwa i zastosowanych skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

Główne zagrożenie spowodowane przez ataki zewnętrzne i wewnętrzne:

1. Emisja ujawniająca, polega na ulotności informacji poprzez emisję elektromagnetyczną w systemach informatycznych.

2. Luki w zabezpieczeniach, np.:

1) łatwe do odgadnięcia hasła,
2) zapisywanie hasła oraz loginu w miejscach łatwo dostępnych,
3) nieaktualne oprogramowanie,
4) złe obchodzenie się z informacjami poufnymi,
5) słaba świadomość personelu,
6) brak ostrożności w obchodzeniu się oprogramowaniem z nieznanych źródeł,
7) nieodpowiedzialność producenta.

3. Maskarada inaczej podszycie (ang. Spoofing). Może mieć katastrofalne skutki, ponieważ omija związki zaufania stworzone na potrzeby autoryzowanego dostępu do systemu. Polega na takim sposobie okazywania informacji w sieci, aby pozostali użytkownicy myśleli, że jest on autoryzowanym użytkownikiem, choć
w rzeczywistości jest kimś innym.

4. Nieautoryzowany dostęp – polega na uzyskaniu dostępu do zasobów sieci oraz ich manipulacja przez nieautoryzowanego osobnika.

5. Odmowa świadczenia usługi, jest procesem uniemożliwiającym dostarczenie usług uprawnionym użytkownikom, z powodu chwilowej niedostępności obiektu w sieci lub zniszczenie systemu.

6. Podszywanie się, wprowadzanie w błąd – atak wykorzystujący błąd użytkownika, tak aby uważał, że ma do czynienia np. z właściwą osoba lub zasobem.

7. Tylne wejście, jest nieudokumentowanym wejściem do legalnych programów. Programiści celowo konstruują furtki-alternatywne wejścia w czasie testowania aplikacji. Po wejściu napastnik przejmuje kontrole nad aplikacją.

8. Wirusy komputerowe, programy kryjące aplikacje stworzone w celu wyrządzenia szkody w systemie informatycznym. Zalicza się do nich np.:

1) Bakteria (ang. Bacteria) – program, którego zadaniem jest wielokrotne uruchomienie swojego kodu w celu pochłonięcia całkowitych zasobów komputera (np. czasu procesora, pamięci operacyjnej, przestrzeni dyskowej) co prowadzi do upadku systemu.
2) Bomba czasowa (ang. Time Bomb) – złośliwa aplikacja, która uruchamia się tylko w określonym czasie (nie w czasie zainfekowania), np. ważna data, lub w momencie spełnienia określonych warunków.

3) Bot – program (w tej klasyfikacji szkodliwy) symulujący i wykonujący pewne czynności w zastępstwie człowieka. Jego funkcje mogą być wykorzystywane do rozprzestrzeniania szkodliwego oprogramowania.
4) Fileless malware – „Bezplikowe” szkodliwe oprogramowanie, jest odmianą oprogramowania związanego z komputerami, które można zidentyfikować jako artefakt w pamięci RAM. Najczęściej wykorzystywany w ataku z użyciem oprogramowania już zainstalowanego na stacji użytkownika np. z użyciem skryptów PowerShella.
5) Keylogger – to rodzaj oprogramowania szpiegującego, które w sposób niezauważalny dla użytkownika rejestruje naciśnięcia klawiszy, pozwalając atakującemu na przejęcie informacji lub danych wrażliwych.
6) Koń trojański – określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje implementuje, uruchamia niepożądane funkcje np. oprogramowanie szpiegujące, bomby logiczne, furtki – backdor pozwalające na przejecie kontroli nad systemem.
7) Robak – samoreplikujący się program komputerowy – szkodliwy, rozprzestrzeniający się w systemach teleinformatycznych poprzez wykorzystanie luk lub brak ostrożności i niewłaściwe zachowanie użytkownika. Najczęstszą formą dystrybucji jest email.
8) Rootkit – narzędzie wykorzystywane do ataków pozwalające na ukrycie niebezpiecznych plików i procesów przed operatorem – administratorem systemu. Pozwala atakującemu na utrzymanie i kontrole nad systemem bez wywołania alarmów. Rootkit może zostać przesłany do systemu za pośrednictwem „konia trojańskiego”.
9) Ransomware – typ szkodliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych a następnie żąda od zaatakowanego okupu za przywrócenie stanu pierwotnego.
10) Spyware – to rodzaj szkodliwego oprogramowania wykorzystywanego przez atakującego do pozyskania wrażliwych informacji pozwalających na dalszą eskalację ataku lub wykorzystanie ich w celach przestępczych np. oszustwa.
11) Wirus – program (szkodliwy) komputerowy posiadający zdolność powielania się, rozprzestrzeniający się w systemach poprzez plik – nosiciela. Wirus może wywoływać w systemie różne skutki w zależności od jego przeznaczenia.

9. Włamanie do sieci, jest jednym z głównych zagrożeń systemu. Mogą być od wewnątrz i od zewnątrz, Typowe włamania mają na celu uzyskanie dostępu do konta innego użytkownika,

10. Działania hakerskie,

1) przechytrzenie lub wykorzystanie niewiedzy osób zajmujących się bezpieczeństwem w danej firmie lub instytucji poprzez:

a) użycie odgadniętego lub wykradzionego hasła;
b) wtargnięcie do sieci poprzez dziurę w zaporze ogniowej;
c) wykorzystanie pozostawionych i niebezpiecznych usług np. FTP (ang. File Transfer Protocol) i inne,

2) wykorzystywanie wiedzy na temat błędów programowych:

a) doprowadzenie do przepełnienia bufora uruchamiając złośliwy kod;
b) użycie furtek programowych w oprogramowaniu bez poprawek;
c) łamanie oraz szukanie plików zawierających informacje na temat haseł systemowych,

3) podrzucenie ofierze złośliwego oprogramowania w postaci konia trojańskiego pod przykrywka nowej gry, aplikacji itp.,

4) wykorzystywanie różnych narzędzi hakerskich, drobne programy mogą wiele zdziałać w

niepoprawnie zabezpieczonej sieci.

5) Zagrożenia socjotechniczne. Wykorzystywanie są przez zaawansowanych napastników, którzy z wielką cierpliwością rozpracowują sposób ataku na sieć, czyhając na błąd administratora lub użytkownika. Wyróżnia się tu:

a) atak z podszywaniem się, wykorzystywanie fałszywego ubioru, identyfikatora służb porządkowych itp., w celu zdobycia informacji do dostępu;
b) atak „na ignoranta", nakłonienie lub podpuszczenie kogoś, aby wyjaśnił, potwierdził lub zaprzeczył pewne informacje;
c) atak z podpuszczeniem, wypowiadanie różnych kłamstw by zdobyć w odpowiedzi informacje;
d) atak nieustający, ciągłe nękanie ofiary poczuciem winy, onieśmielanie i inne negatywne oddziaływania w celu zdobycia informacji;
e) atak przez obserwację, rejestrowanie aktywności i działań ludzi w określonym czasie;
f) atak z przynętą, wykorzystanie atrakcyjności seksualnej w celu zdobycia informacji lub dostępu;
g) atak brutalny, atak z użyciem siły, zastraszenie, szantaż;
h) atak z help desc, podszycie się pod nowego użytkownika potrzebującego pomocy;
i) atak z fałszywą ankietą, obietnica wygrania wycieczki do egzotycznych krajów po udzieleniu odpowiedzi na kilka pytań dotyczących firmowej sieci komputerowej.

Podstawowe pojęcia:

1. Bezpieczeństwo – stan niezagrożenia, spokoju i pewności
2. Bezpieczeństwo informacyjne – jest podstawą szeroko rozumianego bezpieczeństwa. Obejmuje wszystkie formy wymiany, przechowywania i przetwarzania informacji. Rozpatrywane jest w aspektach; organizacyjnym, technicznym i prawnym.
3. Cyberatak – nieuprawnione, ofensywne działanie w cyberprzestrzeni, którego celem jest uzyskanie dostępu do systemu teleinformatycznego, sieci komputerowej lub stacji komputerowej, celem naruszenia poufności, dostępności, integralności lub autentyczności danych lub informacji.
4. Cyberbezpieczeństwo – proces, na który składają się czynności, których celem jest zapewnienie poufności, dostępności, integralności i autentyczności przetwarzanych danych i informacji oraz powiązanych z nimi usług.
5. Cyberprzestrzeń – rozumie się przez to przestrzeń w rozumieniu art. 2 ust. 1b ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP.
6. Cyberprzestępca – osoba wykorzystująca systemy komputerowe, sieć internetową do działalności przestępczej, głównie pozyskiwania środków finansowych. Jego celem oraz narzędziem do dokonania przestępstw mogą być ludzie lub systemy komputerowe.
7. Cyberterrorysta – osoba wykorzystująca aktu przemocy przy zastosowaniu środków komunikacji elektronicznej, wywołując zagrożenie, grożąc utratą życia lub zagrożeniem życia w celu osiągnięcia celów ideologicznych lub politycznych.
8. Haker – osoba o bardzo dużych praktycznych umiejętnościach informatycznych, z bardzo dobrą orientacją w systemach, sieciach, Internecie, a także systemach operacyjnych i językach programowania. Funkcjonują różne pod kategorie hakera, z których negatywnym jest „black haker" – działający w celu wyrządzenia szkody, dla zysku. Potocznie określenie używane w odniesieniu do wszystkich atakujących.
9. Haktywista – specjalista (haker), który wykorzystuje swoje umiejętności i techniki ataku z powodów politycznych lub szeroko pojętym interesie społecznym.
10. Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
11. Insider – osoba będąca użytkownikiem systemu teleinformatycznego, posiadająca uprawnienia oraz dostęp do systemów, która z różnych pobudek może dokonywać naruszeń bezpieczeństwa, wpływać na prawidłowe funkcjonowanie systemów powodując incydenty.

12. Podatność – słabość lub luka w systemie przetwarzania informacji.
13. Reagowanie na incydent – postępowanie będące odpowiedzią na zaistniały incydent.
14. Zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji.
15. Zdarzenie – każde zdarzenie, w którym próbuje się zmienić stan bezpieczeństwa systemu lub naruszyć politykę bezpieczeństwa.

Prawna ochrona bezpieczeństwa informacji
(przykłady przestępstw)
Rozdział XXXIII Kodeksu karnego – Przestępstwa przeciwko ochronie informacji
Art. 267.
§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
Rodzaj przestępstwa – tzw. hacking
§ 2.Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
§ 3.Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
Rodzaj przestępstwa – podsłuch komputerowy, sieciowy (sniffing-nieuprawnione przechwycenie (podsłuchanie)
§ 4.Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.
§ 5. Ściganie przestępstwa określonego w § 1 – 4 następuje na wniosek pokrzywdzonego.
Art. 268.
§ 1.Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
Rodzaj przestępstwa – naruszenie integralności komputerowego zapisu informacji
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.
Art. 268.
§ 1.Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
Rodzaj przestępstwa – naruszenie integralności komputerowego zapisu informacji
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.
Art. 269.
§ 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega

karze pozbawienia wolności od 6 miesięcy do lat 8.
Rodzaj przestępstwa – niszczenie danych informatycznych
§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.
Art. 269a.
Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych,
w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Rodzaj przestępstwa – sabotaż komputer
Art. 269b.
§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Rodzaj przestępstwa – tzw. narzędzia hakerskie
§ 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.
§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.
Art. 269c.
Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Ostatnia aktualizacja
18/11/2022
Data opublikowania
11/10/2022
Author
e-jankowska
Historia zmian
