Cyberbezpieczeństwo

2023-04-21

Cyberbezpieczeństwo

Wojewódzki Szpital Specjalistyczny w Olstynie, jako operator usługi kluczowej, zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U z 2018 r, poz. 1560) wdrożył i eksploatuje system zarządzania bezpieczeństwem informacji.

Szpital analizuje ryzyka z zakresu bezpieczeństwa informacji, ochrony danych osobowych i cyberbezpieczeństwa.

Dla lokalizacji szpitala ustalono zasady ochrony pomieszczeń istotnych z punktu widzenia bezpieczeństwa procesu świadczenia usługi kluczowej. Ochronę fizyczną zapewniają w szczególności systemy kontroli dostępu (zamki mechaniczne i elektroniczne), system monitoringu wizyjnego, identyfikację pracowników oraz system przeciwpożarowy.

Ze względu na krytyczność systemów informacyjnych, urządzeń i narzędzi wspomagających proces utrzymania pacjenta przy życiu, Szpital został wyposażony w redundantne zabezpieczenia na wypadek zakłóceń lub utraty zasilania.

Szpital wdrożył system zarządzania bezpieczeństwem informacji i egzekwuje stosowanie wewnętrznych procedur i instrukcji. Każdy pracownik jest świadomy zapisów procedur systemowych oraz swoich obowiązków w tym zakresie. W odniesieniu do zagrożeń wynikających z braku przestrzegania zapisów w zakresie bezpiecznego przetwarzania informacji Szpital podejmuje działania uświadamiające zagrożenia, informując pracowników o wszelakich próbach ataków środowisk przestępczych na zasoby informacyjne Szpitala.

Szpital korzysta z usług zaufanych dostawców Internetu celem zmniejszenia prawdopodobieństwa błędów po stronie dostawcy, które mogłyby wpłynąć na ciągłość usług szpitala, utratę komunikacji lub bezpieczeństwa przesyłanych informacji.

Wojewódzki Szpital Specjalistyczny w Olsztynie, zobowiązany został ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa do zapewnienia użytkownikom usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych praktyk zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.
Dlatego poniżej przedstawiamy Państwu najważniejsze informacje dotyczące najczęściej występujących cyberzagrożeń oraz sposoby ochrony przed nimi.

Na co uważać?

Phishing

Przestępcy tworzą fałszywe strony Internetowe, żeby wyłudzić Twoje dane (loginy i hasła). Najczęściej wysyłają maile zawierające odnośniki do tych stron.

Jak się chronić?
Dokładnie weryfikuj adres witryny zanim się na niej zalogujesz. Nie wpisuj swojego loginu i hasła na podejrzanych stronach internetowych.

Malware/ ransomware

Często stosowane są ataki z użyciem szkodliwego oprogramowania (malware, ransomware itp.), hakerzy mogą wysyłać złośliwe oprogramowanie za pośrednictwem e-mail, dołączonego do e-mail załącznika.

Jak się chronić?
Nie otwieraj podejrzanych wiadomości oraz załączników, ponieważ w przypadku instalacji złośliwego oprogramowania na Twoim urządzeniu, hakerzy mogą przejąć dostęp np. do konta w Twoim banku.

Vishing

Przestępcy mogą do Ciebie zadzwonić i podawać się za pracownika Szpitala, instytucji np. SANEPID, Policji, Twojego przełożonego i prosić Cię o przekazanie Twojego loginu, hasła, nr PESEL, nr dowodu osobistego.
Podanie tych danych może skutkować kradzieżą Twojej tożsamości, umożliwieniem przestępcy

zalogowania się do Systemu.

Jak się chronić?
Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz.

Podstawowym elementem bezpieczeństwa w sieci Internet jest zastosowanie zasady ograniczonego zaufania i podwyższonej ostrożności.

Używaj oprogramowania antywirusowego i zapory sieciowej (firewall).

Korzystaj wyłącznie z legalnego oprogramowania.

Staraj się nie korzystać z sieci publicznych, jeżeli logujesz się do systemu.

Regularnie aktualizuj oprogramowanie oraz bazy danych wirusów.

Nie otwieraj podejrzanych e-maili oraz załączników. Zwracaj szczególną uwagę na załączniki posiadające kilka rozszerzeń plików jednocześnie np. faktura.pdf.zip, dokument.jar.doc.

Nie korzystaj ze stron, które nie mają ważnego certyfikatu (np. brak protokołu https) chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.

Nie zostawiaj swoich danych osobowych w niesprawdzonych serwisach i na stronach, zawsze czytaj dokładnie Regulaminy i Polityki, weryfikuj na co wyrażasz zgodę.

Nie wysyłaj e-mailem poufnych danych bez ich szyfrowania.

Pamiętaj, że Szpital, bank, czy urząd nie wysyła e-maili do swoich pacjentów/klientów/interesantów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji.

Regularnie aktualizuj system operacyjny na Twoim komputerze.

Aplikacje i programy pobieraj wyłącznie z oficjalnych źródeł.

Dodatkowe środki bezpieczeństwa

Blokuj ekran swojego urządzenia (np. hasło, PIN).

Włącz ustawienia blokady ekranu Twojego urządzenia.

Wpisując swoje hasło, pin, login zweryfikuj, czy nikt Cię nie nagrywa lub nie widzi tego, co wpisujesz.

Nie udostępniaj nikomu swojego loginu i hasła do systemu.

Unikaj stosowania haseł, które można łatwo z Tobą powiązać.

Hasło powinno mieć co najmniej 8 znaków w tym litery, cyfry i znaki specjalne.

Nie zapisuj haseł na kartkach, w notatniku

Stosuj różne hasła w różnych systemach.

Unikaj logowania do systemów z cudzych urządzeń.

Staraj się nie zapisywać haseł w pamięci przeglądarki.

Przed sprzedażą / oddaniem urządzenia innej osobie, usuń z niego wszystkie dane.

Jeżeli masz taką możliwość korzystaj z nakładek prywatyzujących na monitor (również w urządzeniu mobilnym) w miejscach publicznych.

Smartfony i tablety coraz częściej zastępują inne urządzenia osobiste. Pamiętaj, że podobnie jak domowe komputery, nasze urządzenia mobilne wymagają odpowiedniej ochrony.

Instaluj aktualizacje aplikacji i systemu operacyjnego w swoim urządzeniu mobilnym.

Pobieraj i instaluj aplikacje wyłącznie z oficjalnych sklepów z aplikacjami.

Nie uruchamiaj linków z wiadomości SMS lub e-mail, jeśli nie masz pewności, że pochodzą z bezpiecznego i zaufanego źródła.

Jeżeli nie korzystasz w danej chwili z Wi-Fi lub Bluetooth, wyłącz je.

Kontakt: cyberbezpieczenstwo@wss.olsztyn.pl

-  Polityka bezpieczeństwa WSS Olsztyn