Podstawowe zagrożenia cyberbezpieczeństwa i zasady ochrony w ochronie zdrowia dla Pacjenta

Przewodnik po bezpiecznym korzystaniu z cyfrowych usług medycznych

⚠ ZAGROŻENIE

Dlaczego ochrona zdrowia jest celem cyberataków?

Wartość danych medycznych

Na czarnym rynku dane medyczne są cenniejsze niż informacje z kart kredytowych - mogą być wykorzystane do kradzieży tożsamości i wyłudzania świadczeń

Przestarzałe systemy

Rosnąca cyfryzacja przy jednoczesnym stosowaniu starych systemów informatycznych tworzy luki w zabezpieczeniach

Zagrożenie dla życia

Każda przerwa w działaniu systemów medycznych może bezpośrednio zagrażać zdrowiu i życiu pacjentów

Najczęstsze zagrożenia w sektorze ochrony zdrowia

Phishing

Fałszywe wiadomości e-mail lub SMS podszywające się pod placówki medyczne, mające na celu wyłudzenie danych logowania, PESEL-u czy informacji o ubezpieczeniu

Ransomware

Złośliwe oprogramowanie blokujące dostęp do systemów szpitalnych i żądające okupu za odblokowanie - może sparaliżować całą placówkę

Luki w oprogramowaniu

Brak regularnych aktualizacji systemów medycznych tworzy otwarte furtki dla cyberprzestępców

Ataki na urządzenia IoT

Urządzenia medyczne podłączone do sieci (pompy insulinowe, monitory) mogą stać się punktem wejścia dla hakerów

Cyberatak może zatrzymać leczenie

Realne zagrożenie dla życia pacjentów w momencie ataku na systemy medyczne

⚠ SKUTKI ATAKÓW

Realne skutki cyberataków dla pacjentów

Zagrożenie życia i zdrowia

Opóźnienia w diagnozach, odwołane zabiegi operacyjne, brak dostępu do historii choroby w sytuacjach ratujących życie

Utrata prywatności

Ujawnienie najbardziej wrażliwych informacji: historia chorób psychicznych, uzależnień, stosowane leki, wyniki badań genetycznych

Kradzież tożsamości

Ryzyko wyłudzenia świadczeń medycznych na Twoje dane, fałszywych recept na silne leki, oszustw ubezpieczeniowych

Kryzys zaufania

Utrata wiary w bezpieczeństwo placówek medycznych i obawa przed korzystaniem z e-usług zdrowotnych

Jak chronić swoje dane medyczne?

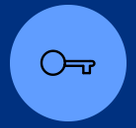
Zasady dla Pacjenta

Oficjalne kanały

Korzystaj wyłącznie z oficjalnych platform, takich jak Internetowe Konto Pacjenta (pacjent.gov.pl). Nigdy nie loguj się przez linki z e-maili

Unikaj podejrzanych linków

Nigdy nie klikaj w linki z nieznanych SMS-ów, e-maili czy wiadomości dotyczących zdrowia, recept lub wyników badań



Bezpieczne logowanie

Loguj się na IKP tylko przez zaufane metody: Profil Zaufany, bankowość elektroniczną lub e-dowód osobisty

Silne hasła

Ustaw unikalne, złożone hasła (min. 12 znaków) i aktywuj uwierzytelnianie dwuskładnikowe wszędzie, gdzie to możliwe

Bezpieczne korzystanie z Internetowego Konta Pacjenta

Czym jest IKP?

Internetowe Konto Pacjenta to bezpieczna platforma rządowa umożliwiająca dostęp do Twoich danych medycznych, e-recept i e-skierowań

pacjent.gov.pl

01

Szyfrowanie danych

IKP chroni dane podczas przesyłania i przechowywania za pomocą zaawansowanego szyfrowania

02

Automatyczne wylogowanie

System wylogowuje Cię po okresie bezczynności, chroniąc przed dostępem osób nieuprawnionych

03

Oficjalne powiadomienia

Prawdziwe powiadomienia o e-receptach przychodzą wyłącznie z adresów gov.pl - inne to phishing

04

Ochrona PIN-u

Nigdy nie udostępniaj PIN-u ani kodów dostępu innym osobom, nawet członkom rodziny

24/7 OCHRONA

Rola Centrum e-Zdrowia i Zespołu CSIRT CeZ

Zespół CSIRT CeZ to specjalistyczna jednostka odpowiedzialna za cyberbezpieczeństwo w polskiej ochronie zdrowia

Kompleksowa ochrona

- Całodobowy monitoring zagrożeń i natychmiastowa reakcja na incydenty bezpieczeństwa
- Regularne szkolenia personelu medycznego i audyty bezpieczeństwa w placówkach
- Wsparcie techniczne dla pacjentów i instytucji w zakresie ochrony danych
- Koordynacja działań prewencyjnych i reagowanie na ataki w skali krajowej

Kontakt: **info@csirt.cez.gov.pl**

Co zrobić w przypadku podejrzenia ataku lub wycieku danych?

Natychmiastowe zgłoszenie

Skontaktuj się z placówką medyczną lub CSIRT CeZ (info@csirt.cez.gov.pl). Każda minuta ma znaczenie w powstrzymaniu skutków ataku

Zmiana haseł

Niezwłocznie zmień hasła do IKP, poczty e-mail i wszystkich powiązanych usług. Użyj silnych, unikalnych haseł

Monitoring aktywności

Regularnie sprawdzaj swoją historię medyczną, wystawione recepty i skierowania na IKP w poszukiwaniu podejrzanych wpisów

Czujność

Zachowaj szczególną ostrożność wobec nieoczekiwanych telefonów, SMS-ów i e-maili dotyczących Twojego zdrowia

Podsumowanie i apel do Pacjentów

Twoja odpowiedzialność

Dane medyczne to Twoja prywatność i bezpieczeństwo - chronisz nie tylko siebie, ale też cały system ochrony zdrowia

Edukacja i świadomość

Świadome korzystanie z cyfrowych usług zdrowotnych to pierwszy krok do skutecznej ochrony przed zagrożeniami

Zasady bezpieczeństwa

Stosuj podstawowe zasady: silne hasła, oficjalne kanały, ostrożność wobec linków i regularne monitorowanie konta

Wspólne działanie

Razem - pacjenci, personel medyczny i instytucje - możemy skutecznie przeciwdziałać cyberzagrożeniom w ochronie zdrowia