kod szkolenia: BS.IT 00 MZ / PL DL 3,5 NFZ

Security Awareness dla szpitali i placówek medycznych – jak chronić dane pacjentów i zapewnić ciągłość działania w dobie cyberataków

Sektor ochrony zdrowia jest jednym z najczęściej atakowanych w Polsce i w całej UE – ponad 40% incydentów dotyczy szpitali i przychodni. Ataki ransomware czy wycieki danych pacjentów prowadzą nie tylko do strat finansowych, ale także do zagrożenia życia i zdrowia chorych. Szkolenie ma na celu zwiększenie świadomości personelu medycznego i administracyjnego, aby potrafili rozpoznać zagrożenia i odpowiednio na nie reagować.

Odbiorcy szkolenia

Szkolenie adresowane jest do:

- lekarzy, pielęgniarek, ratowników medycznych
- pracowników administracji i rejestracji
- dyrekcji oraz osób zarządzających placówkami zdrowia
- pracowników IT wspierających systemy medyczne

Korzyści

- Zrozumienie realnych konsekwencji cyberataków dla pacjentów i szpitala (opóźnienia w leczeniu, paraliż oddziałów, koszty)

- Umiejętność rozpoznawania prób phishingu, wyłudzeń i fałszywych logowań
- Wiedza jak reagować na incydenty (np. ransomware, awarie systemów EHR)
- Świadomość obowiązków wynikających z przepisów NIS2 i UKSC (od 2026)
- Poznanie dobrych praktyk w zakresie bezpieczeństwa danych medycznych i dostępu do systemów

Program szkolenia

1. Wprowadzenie – dlaczego sektor medyczny jest celem cyberataków (PL i światowe przykłady z ostatnich lat)
2. „Co naprawdę może pójść źle” – Ransomware w szpitalach – realne incydenty i ich konsekwencje
3. Wyciek danych pacjentów – jak wygląda kradzież i sprzedaż informacji medycznych
4. Higiena cyfrowa personelu – Phishingi / socjotechniki – przykłady z placówek ochrony zdrowia (maile, fałszywe loginy do portali medycznych, SMS-y)
5. Bezpieczeństwo konta – dlaczego hasło to za mało (MFA, klucze sprzętowe, passkeys)
5. AI i nowe zagrożenia w ochronie zdrowia – od błędnych rekomendacji do deep faków
6. Regulacje NIS2/UKSC – obowiązki szpitali, rola zarządu, kary i wsparcie finansowe
7. Jak reagować na incydent – od wykrycia po współpracę z CSIRT i dyrekcją
8. Dobre praktyki „bezpieczny dyżur”
9. Podsumowanie i pytania

Oczekiwane przygotowanie uczestnika

Nie jest wymagane doświadczenie techniczne – szkolenie jest dostosowane do personelu medycznego i administracyjnego. Podstawowa znajomość obsługi komputera i systemów rejestracyjnych jest wystarczająca.

Szkolenie obejmuje

Metoda szkolenia

- wykład

Czas trwania

1 dni / 3 godzin

Język

- Szkolenie: polski
- Materiały: polski