IZBA POLMED

CYBERBEZPIECZEŃSTWO W SZPITALACH

BEZPIECZEŃSTWO CYFROWE JEST KLUCZOWE DLA OCHRONY DANYCH PACJENTÓW ORAZ ZAPEWNIENIA CIĄGŁOŚCI DZIAŁANIA SZPITALA. TEN PRZEWODNIK PRZEDSTAWIA PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA.

Dlaczego cyberbezpieczeństwo jest ważne?

Prawie wszystkie szpitale korzystają z rozwiązań cyfrowych – od systemów IT służących do prowadzenia dokumentacji medycznej po cyfrowe wyroby medyczne. Podmioty lecznicze są coraz bardziej narażone na ataki na ich infrastrukturę informatyczną – które mogą zaszkodzić nie tylko zasobom szpitala, ale i bezpieczeństwu pacjentów

Głównym celem cyberprzestępców jest sektor opieki zdrowotnej (3.)

Jakie regulacje prawne obowiązują szpitale w odniesieniu do cyberbezpieczeństwa?

Zgodnie z **Dyrektywą NIS 2**(1.), szpitale są zobowiązane do wdrożenia odpowiednich środków bezpieczeństwa, które minimalizują ryzyko cyberataków i chronią dane pacjentów. Również przepisy **RODO**(2.) nakładają obowiązek szczególnej ochrony danych osobowych pacjentów, a naruszenia mogą skutkować wysokimi karami finansowymi.

88% organizacji ochrony zdrowia doświadczyło średnio 40 ataków w zakresie cyberbezpieczeństwa w 2022 (4.)

Kto ma wpływ na cyberbezpieczeństwo?

Zapewnienie odpowiedniego cyberbezpieczeństwa to zadanie zarówno (i) organizacji – które muszą drożyć odpowiednie rozwiązania techniczne (oprogramowanie, infrastrukturę fizyczną) i organizacyjne (procedury, polityki, szkolenia) jak i (ii) pracowników – którzy muszą stosować obowiązujące w szpitalu rozwiązania i procedury.

Dane medyczne są 10-krotnie cenniejsze niż dane kart kredytowych (5.)

(1.) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (2.) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. (3.) IBM X-Force Threat Intelligence Report 2016. (4.) The Ponemon Institute, 2023 Ponemon Healthcare Cybersecurity Report. (5.) Reuters, 2014.

GŁÓWNE ZAGROŻENIA

Ataki ransomware

przestępcy szyfrują dane, żądając okupu za ich odblokowanie

Phishing

wyłudzenia danych przez fałszywe maile i strony internetowe

Kradzież danych

nielegalne pozyskanie danych pacjentów

Ataki na systemy IT

zakłócanie funkcjonowania urządzeń i systemów szpitalnych

Cyberbezpieczeństwo to odpowiedzialność nas wszystkich. Przestrzegając poniższych zasad, pomagamy chronić dane pacjentów oraz zapewnić bezpieczne środowisko pracy.

- Uważaj na podejrzane e-maile i linki → Nie podawaj danych logowania ani informacji poufnych bez weryfikacji nadawcy.
- Unikaj instalowania nieznanych programów → Regularnie aktualizuj oprogramowanie antywirusowe.
- Używaj skomplikowanych haseł zawierających litery, cyfry i znaki specjalne → Zmieniaj je regularnie.
- Włącz autoryzację dwuskładnikową tam, gdzie to możliwe, aby zwiększyć bezpieczeństwo logowania.
- Kontroluj dostęp i udostępniaj informacje tylko tym, którzy jej potrzebują, aby wykonywać swoje obowiązki.
- Przestrzegaj przepisów RODO oraz innych regulacji dotyczących ochrony danych osobowych.
- Stosuj szyfrowanie danych wrażliwych podczas przechowywania i przesyłania.

Brak wdrożenia odpowiednich rozwiązań technicznych i organizacyjnych zapewniających odpowiedni poziom cyberbezpieczeństwa może skutkować odpowiedzialnością karną i odszkodowawczą!