Cyberbezpieczeństwo

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - życie obowiązuje od dnia 28 sierpnia 2018 r. Celem ustawy jest stworzenie Krajowego Systemu Cyberbezpieczeństwa (KSC), który umożliwi sprawne działania na rzecz wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo RP.

Ustawa oraz towarzyszące jej rozporządzenia wykonawcze w pełni wdrożą do polskiego porządku prawnego tzw. dyrektywę NIS. Nowe regulacje tworzą prawne podstawy funkcjonowania krajowego systemu cyberbezpieczeństwa, ustalają zasady jego rozbudowy i zwiększenia poziomu zabezpieczeń systemów teleinformatycznych a także pozwalają ograniczyć potencjalne skutki incydentów oraz cyberzagrożeń, w tym straty finansowe.

Najważniejszym elementem krajowego systemu cyberbezpieczeństwa są tzw. Operatorzy Usług Kluczowych, czyli dostawcy ważnych usług zależnych od systemów informacyjnych (np. firmy energetyczne, przewoźnicy lotniczy i kolejowi, szpitale, podmioty istotne dla infrastruktury ICT itd.).

Podmioty te są zobowiązane m.in. 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 tzw. CSIRT-ów (tj. Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego).

W czerwcu 2019 r. Szpital, na mocy decyzji administracyjnej, został uznaniu za operatora usługi kluczowej.