Zbigniew Świerczyński
Prezes Zarządu
MILSTAR sp. z o. o

„Rola Security Operations Center (SOC) w wypełnianiu wymagań RODO”

Aktualnie jednym z częściej poruszanych tematów z zakresu bezpieczeństwa informatycznego jest kwestia obowiązywania od maja 2018 roku nowego unijnego rozporządzenia dotyczącego ochrony danych osobowych (tzw. RODO lub GDPR). Wymagania nakładane przez to rozporządzenie na podmioty przetwarzające dane osobowe, oprócz należytej ochrony przed zagrożeniami dla bezpieczeństwa danych osobowych, w dużej mierze dotyczą zapewnienia odpowiedniej obsługi i rozliczalności incydentów bezpieczeństwa. Drugim nurtem w zakresie bezpieczeństwa informatycznego, który się wzmógł w ostatnim roku jest organizacja krajowego systemu cyberbezpieczeństwa. Zagadnienie opisano w Strategii Cyberbezpieczeństwa Polski na lata 2016-2020 opracowanej przez Ministerstwo Cyfryzacji. Jednym z istotniejszych założeń tej strategii jest tworzenie struktury wyspecjalizowanych zespołów, których zadaniem będzie szeroko rozumiane zarządzanie incydentami bezpieczeństwa. W zależności od szczebla działania zespoły te mają miały różne obowiązki i są nazywane Lokalnymi Zespołami Reagowania (LZR), Security Operations Center (SOC), lub Computer Security Incident Response Team (CSIRT). Te ostatnie mogą koordynować działania w ramach konkretnego sektora gospodarki lub na szczeblu ogólnokrajowym tak, jak to aktualnie robi NCCyber.

Oba nurty, RODO oraz tworzenie zespołów zarządzających incydentami bezpieczeństwa, korelują ze sobą, ponieważ posiadanie sprawnie działającego zespołu typu SOC/CSIRT w dużej mierze pomoże realizować zadania opisane w RODO. Celem prezentacji jest pokazanie w jakim stopniu posiadanie dobrze wyposażonego i zorganizowanego zespołu SOC/CSIRT pozwoli wypełnić wymagania wprowadzane przez to rozporządzenie.