Zbigniew Świerczyński
Milstar

„Praktyczne szkolenia typu obrona-atak w cyberprzestrzeni i ich znaczenie w doskonaleniu poziomu ochrony danych”

Aktualnie posiadanie sprawnie działającego zespołu zajmującego się wykrywaniem i reagowaniem na incydenty bezpieczeństwa teleinformatycznego jest jednym z kluczowych elementów systemu ochrony danych. Tego typu zespoły są podstawą działania Security Operations Center (SOC), które w dużej mierze pomagają realizować wymagania techniczne ochrony danych osobowych opisane w RODO oraz koncepcje Krajowych Ram Polityki Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej na lata 2017-2022. W Krajowych Ramach podkreśla się znaczenie zarówno kompleksowych ćwiczeń symulujących ogólnokrajowy incydent, jak również ćwiczeń o mniejszym zasięgu, w tym sektorowych, w celu ciągłego doskonalenia personelu, narządzi i procedur.

Reakcja na incydenty bezpieczeństwa teleinformatycznego wymusza podejmowanie różnego typu działań technicznych i decyzji przy ograniczonej wiedzy i czasie. Wielowątkowość działań, konieczność przekazywania na bieżąco informacji pomiędzy członkami zespołu SOC i presja czasu, to czynniki które potrafią „sparaliżować” nawet najlepiej przygotowanego teoretycznie inżyniera. Z tego powodu coraz większym uznaniem cieszą się praktyczne ćwiczenia typu obrona-atak w cyberprzestrzeni, w których powierzona do obrony infrastruktura teleinformatyczna jest atakowana przez tzw. red team’y. Przy organizacji tego typu ćwiczeń kluczowe jest odpowiednie zasymulowanie „poligonu cybernetycznego”, metodyczne przygotowanie scenariuszy działań oraz kryteriów oceny poszczególnych ćwiczących, czy też całych zespołów. W trakcie prezentacji zostaną przedstawione zasady przygotowania i prowadzenia tego typu ćwiczeń.