Kamila Sacewicz

Streszczenie

Artykuł przedstawia przyjętą w dniu 23 lutego 2011 r. przez rząd RFN *Strategię Cyberbezpieczeństwa dla Niemiec*.

Sprawne funkcjonowanie organów administracji, elementów infrastruktury krytycznej, niezakłócony rozwój gospodarki, a także dobrostan obywateli wymagają niezawodności infrastruktury teleinformatycznej państwa, a tym samym skutecznej ochrony przed wymierzonymi w nią potencjalnymi atakami. Opracowana strategia ma na celu zapewnienie akceptowalnego poziomu bezpieczeństwa zasobów informacyjnych państwa. Jej adresatami są sektor publiczny i prywatny, a także społeczeństwo oraz partnerzy międzynarodowi.

W publikacji przedstawiono jednostki powołane do realizacji postanowień strategii – Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni oraz Narodową Radę Cyberbezpieczeństwa. Pierwsza z nich stanowi platformę współpracy właściwych rzeczowo organów niemieckiej administracji i jest pierwszym ogniwem walki z zagrożeniami cybernetycznymi. Narodowej Radzie Cyberbezpieczeństwa powierzono zaś koordynację współpracy w obrębie niemieckiego rządu oraz na styku państwa i gospodarki.

Strategia cyberbezpieczeństwa Nemiec zawiera osiem celów strategicznych. Głównym z nich jest ochrona teleinformatycznej infrastruktury krytycznej. Ochrony wymaga także infrastruktura teleinformatyczna użytkowana przez obywateli i przedsiębiorstwa małej i średniej wielkości. Kolejnym istotnym elementem strategii jest podniesienie poziomu zabezpieczeń systemów teleinformatycznych użytkowanych przez administrację publiczną oraz zwiększenie skuteczności w zwalczaniu przestępczości w cyberprzestrzeni. Do celów niemieckiej strategii należą ponadto współpraca międzynarodowa na rzecz ujednolicenia systemów ochrony cyberprzestrzeni i świata oraz długotrwałe zabezpieczenie niezawodnych systemów teleinformatycznych. Kolejnym celem jest weryfikacja stanu zatrudnienia oraz racjonalne planowanie zasobów ludzkich w odniesieniu do organów administracji wymagających bezpiecznej cyberprzestrzeni, ostatnim celem strategii pozostaje natomiast zapewnienie instrumentarium umożliwiającego kompleksową ochronę cyberprzestrzeni.