Analizy OSW

OŚRODEK STUDIÓW WSCHODNICH 2.03.2011 www.osw.waw.pl

RFN przyjmuje strategię bezpieczeństwa cybernetycznego

23 lutego rząd RFN przyjął strategię bezpieczeństwa cybernetycznego. Niemcy planują wzmożone przeciwdziałanie atakom cybernetycznym o podłożu kryminalnym, terrorystycznym i wywiadowczym. RFN niepokoi się wzrostem szpiegostwa przemysłowego dotykającego w coraz większym stopniu niemieckie firmy, zwiększaniem się liczby ataków cybernetycznych na sieci informatyczne administracji federalnej oraz pojawieniem się programów, które mogłyby zagrozić krytycznej infrastrukturze informatycznej w RFN (jak np. Stuxnet, który wpływał na działanie oprogramowania firmy Siemens kontrolującego linie produkcyjne, elektrownie i rurociągi w Iranie). Według ostatniego raportu kontrwywiadu za rok 2009 nt. zagrożeń bezpieczeństwa w RFN cyberataki na firmy i instytucje w Niemczech przeprowadzane są najczęściej z Chin i Rosji.

Strategia ma na celu wypracowanie zintegrowanego cywilnego podejścia do kwestii bezpieczeństwa cybernetycznego. Celem rządu jest poprawa: (1) bezpieczeństwa krytycznej infrastruktury informatycznej – m.in. w sektorze energetycznym, telekomunikacyjnym, transportowym czy gospodarki wodnej; (2) bezpieczeństwa systemów informatycznych wykorzystywanych przez obywateli RFN oraz przez małe i średnie przedsiębiorstwa; (3) bezpieczeństwa teleinformatycznego administracji federalnej i landowej. Planuje się dalsze rozwijanie istniejących programów (np. KRITIS w przypadku krytycznej infrastruktury informatycznej), zwiększenie oferty informacyjnej dla małych i średnich przedsiębiorstw czy stworzenie jednolitej i bezpiecznej infrastruktury sieciowej dla administracji federalnej. Ponadto rząd chce stworzyć Narodowe Centrum Bezpieczeństwa Cybernetycznego, które poprawiłoby współpracę wszystkich struktur rządowych zajmujących się tym problemem i służyłoby koordynacji programów zabezpieczających infrastrukturę informatyczną. Powstać ma również Narodowa Rada Bezpieczeństwa Cybernetycznego, która ma za zadanie strategiczne planowanie prewencyjne i w ramach której ma współpracować większość resortów oraz przedstawiciele niemieckiej gospodarki. Ponadto zapowiadane są działania na poziomie unijnym i międzynarodowym, m.in. dążenie do rozszerzenia mandatu Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), do wspierania przez NATO stosowania jednolitych standardów również w cywilnej krytycznej infrastrukturze informatycznej oraz do wypracowanie międzynarodowego kodeksu postępowania państw w cyberprzestrzeni. <jus>