Kamila Sacewicz

Niemiecka strategia ochrony cyberprzestrzeni[1]

Wprowadzenie

W dniu 23 lutego 2011 r. rząd RFN przyjął *Strategię Cyberbezpieczeństwa dla Niemiec*, która ma zapewnić stosowną ochronę sieci teleinformatycznych bez szkody dla ich funkcjonalności i rozwoju. Ujęte w strategii cele to: wzmocniona ochrona przed zamachami cybernetycznymi infrastruktury krytycznej (w Niemczech zalicza się do niej m.in. sektor teleinformatyczny i telekomunikacyjny), ochrona systemów teleinformatycznych, utworzenie Narodowego Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (NCAZ – *Nationales Cyber-Abwehrzentrum*)[2] oraz Narodowej Rady Cyberbezpieczeństwa (*Nationaler Cyber-Sicherheitsrat*)[3].

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. W konsekwencji opracowano niemiecką strategię, która ma na celu zapewnienie akceptowalnego poziomu bezpieczeństwa zasobów informacyjnych państwa.

Poniżej przedstawiono jej ważniejsze elementy.

Organy właściwe rzeczowo do realizacji *Strategii* i jej adresaci

Celem niemieckiego rządu pozostaje wniesienie znaczącego wkładu w bezpieczeństwo cyberprzestrzeni. W ten sposób pragnie przyczynić się do utrzymania i dalszego rozwoju dobrobytu gospodarczego i społecznego państwa.

Myśl przewodnia niemieckiej strategii ochrony cyberprzestrzeni zakłada, że o jej bezpieczeństwie stanowi suma wszystkich krajowych oraz międzynarodowych działań na rzecz dostępności infrastruktury teleinformatycznej, jak też jej nienaruszonej integralności, autentyczności oraz poufności zawartych w niej danych.

Z uwagi na powyższe adresatami strategii pozostają sektor publiczny oraz prywatny, a także społeczeństwo oraz partnerzy międzynarodowi.

Za realizację postanowień strategii na gruncie krajowym odpowiadać mają powołane na jej podstawie Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (NCAZ) oraz Narodowa Rada Cyberbezpieczeństwa.

---

[1] Artykuł opracowano na podstawie materiałów publikowanych przez MSW RFN (www.bmi.bund.de), m.in. *Strategii Cyberbezpieczeństwa dla Niemiec*, a także informacji poświęconych niemieckiej architekturze cyberbezpieczeństwa, materiałów prasowych, komunikatów oraz materiałów publikowanych przez Pełnomocnika Rządu Federalnego ds. Teleinformatyki (www.ciobund.de).

[2] NCAZ to platforma współpracy organów niemieckiej administracji właściwych w sprawach ochrony cyberprzestrzeni.

[3] Organ koordynujący współpracę pomiędzy organami administracji, a także na linii państwo–gospodarka.

Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (NCAZ)

W ramach realizacji postanowień niemieckiej strategii bezpieczeństwa cybernetycznego, w czerwcu 2011 r. oficjalną działalność rozpoczęło Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (NCAZ) stanowiące odpowiedź rządu na stale rosnące zagrożenia dla niemieckiej cyberprzestrzeni.

U podstaw decyzji o utworzeniu NCAZ leżały dane zebrane przez Federalny Urząd Bezpieczeństwa Teleinformatycznego. Zgodnie z opublikowanym przez urząd raportem wzrasta nie tylko liczba ataków cybernetycznych, ale także ich jakość, a tym samym poziom zagrożenia, jaki generują[4]. W 2009 r. miało miejsce 900 zamachów na komputery rządowe, w 2010 r. liczba incydentów wzrosła o kolejne 700[5], a przypadające z tego tytułu straty dla niemieckiej gospodarki w 2011 r. szacowane były na kilkanaście miliardów euro. Mając powyższe na uwadze, Ministerstwo Spraw Wewnętrznych RFN było zmuszone podjąć zdecydowane działania i w konsekwencji powołało do życia NCAZ, które ma pozostawać pierwszym ogniwem walki z zagrożeniami cybernetycznymi.

Podobnie jak utworzone w 2004 r. Wspólne Centrum Przeciwdziałania Terroryzmowi (GTAZ – *Gemeinsames Terrorismusabwehrzentrum*)[6], także i NCAZ stanowi platformę współpracy właściwych rzeczowo organów niemieckiej administracji. Niemcy nie zdecydowali się na instytucjonalizację prac Centrum ze względu na obowiązujący w RFN nakaz rozdziału (*Trennungsgebot*) służb specjalnych od służb policyjnych[7]. Decyzja ta umożliwia funkcjonowanie Centrum, jako że skupia ono:

- Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI – *Bundesamt für Sicherheit in der Informationstechnik*), który przewodzi pracom,
- Federalny Urząd Ochrony Konstytucji (*Bundesamt für Verfassungsschutz* – BfV),
- Federalny Urząd Ochrony Ludności i Reagowania Kryzysowego (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* – BBK),
- Federalny Urząd Kryminalny (*Bundeskriminalamt* – BKA),
- Federalną Służbę Wywiadu (*Bundesnachrichtendienst* – BND),
- Celny Urząd Kryminalny (*Zollkriminalamt* – ZKA),
- Policję Federalną (*Bundespolizei* – BPol),
- Bundeswehrę.

---

[4] BSI podaje, że co sekundę powstają dwa nowe szkodliwe oprogramowania, co minutę dochodzi do kradzieży dwóch tożsamości, każdego dnia odkrywa się 13 luk bezpieczeństwa w standardowym oprogramowaniu oraz 21 tys. zainfekowanych stron internetowych. W 2010 r. przy pomocy wirusa „stuxnet" udało się sabotować prace irańskich zakładów atomowych. Międzynarodowy Fundusz Walutowy przyznał, że w czerwcu 2011 r. padł ofiarą złożonych ataków na system, w którym przechowywane są dane dotyczące sytuacji finansowej zrzeszonych państw. W połowie 2011 r. zaatakowany został także amerykański koncern zbrojeniowy Lockheed Martin. Celem pozostawały dane dotyczące myśliwca wielozadaniowego F-35 Lightning II, jednak atak został udaremniony.

[5] Większość ataków na sieci rządowe Niemcy przypisują Chińczykom.

[6] Po 11 września 2001 r. BfV skoncentrował swoje wysiłki przede wszystkim na zwalczaniu terroryzmu i ekstremizmu o podłożu islamskim, czego efektem było utworzenie w Berlinie w grudniu 2004 r. analitycznego Wspólnego Centrum Przeciwdziałania Terroryzmowi. GTAZ nie jest samodzielną instytucją, daje natomiast szerokie możliwości współpracy pomiędzy skupionymi w swoich ramach 40 właściwymi rzeczowo organami.

[7] Po zakończeniu II wojny światowej alianci zobowiązali niemiecką administrację do ścisłego rozdziału organów bezpieczeństwa wykonujących czynności operacyjne od instytucji policyjnych uprawnionych do wykonywania czynności procesowych.

W razie potrzeby NCAZ otrzymuje także wsparcie od organów nadzoru elementów infrastruktury krytycznej[8].

Do najważniejszych zadań Centrum należą przeciwdziałanie zagrożeniom dla cyberprzestrzeni oraz ich zwalczanie, w tym wymiana informacji, analiza incydentów teleinformatycznych i ich ewaluacja, wypracowywanie mechanizmów skutecznej ochrony i prewencji oraz neutralizacja rezultatów ataków, a także ocena skuteczności realizacji postanowień strategii ochrony cyberprzestrzeni. Zrzeszone w Centrum organy dostarczają informacje zgodnie z właściwością rzeczową – BSI ocenia incydent pod względem technicznym, BfV bada, czy za atak odpowiada zagraniczna służba specjalna, a BBK ocenia skutki zamachów dla infrastruktury krytycznej. Pozostałe organy rozpoznają nowe metody i narzędzia ataku. W konsekwencji NCAZ potrafi w krótkim czasie przedstawić aktualną i kompleksową informację na temat zagrożeń dla cyberprzestrzeni. W ramach działań prewencyjnych NCAZ okresowo, a dodatkowo w razie potrzeby, przedstawia Narodowej Radzie Cyberbezpieczeństwa stosowne wytyczne, a w sytuacjach nadzwyczajnych raportuje bezpośrednio sztabowi kryzysowemu w MSW.

W praktyce w razie ataku cybernetycznego zrzeszeni w Centrum eksperci mają poddać analizie szkodliwe oprogramowanie, a następnie opracować raport sytuacyjny i udzielić organom administracji publicznej oraz zagrożonym przedsiębiorstwom prywatnym wytycznych co do dalszego postępowania, a także przedstawić niezbędne środki zaradcze.

Zgodnie z fikcyjnym scenariuszem przedstawionym dziennikarzom w przededniu otwarcia Centrum, jego zwykły cykl pracy może wyglądać następująco:

1. BSI uzyskuje informacje o luce bezpieczeństwa, której producent oprogramowania lub sprzętu nie potrafi skutecznie zabezpieczyć;
2. BSI przekazuje otrzymane informacje do NCAZ;
3. Równocześnie BfV dowiaduje się o podjętej „próbie sabotażu" polegającej na usiłowaniu zainstalowania szkodliwego oprogramowania w placówce zaliczanej do infrastruktury krytycznej przez jej pracownika;
4. BSI poddaje przedmiotowe oprogramowanie analizie technicznej;
5. BSI stwierdza, że wykorzystuje ono rozpoznaną lukę bezpieczeństwa;
6. Pracownicy NCAZ wspólnie formułują wniosek o zaistnieniu realnego zagrożenia dla infrastruktury krytycznej;
7. NCAZ ostrzega zagrożone jednostki organizacyjne prosząc jednocześnie o informacje zwrotne.

Powyższa procedura ma zapewnić kontrolę Centrum nad bezpieczeństwem niemieckiej cyberprzestrzeni.

---

[8] W Niemczech do infrastruktury krytycznej zaliczane są następujące sektory:
- transport i ruch powietrzny, kolejowy, drogowy, wodny;
- energia (elektryczność, elektrownie atomowe, olej mineralny, gaz);
- substancje szkodliwe (chemiczne, biologiczne, zbrojeniowe);
- teleinformatyka i telekomunikacja;
- finansowy i ubezpieczeniowy;
- zaopatrzenie (ratownictwo, zaopatrzenie w wodę, usuwanie odpadów);
- organa administracji i wymiaru sprawiedliwości (w tym policja, służby celne i wojsko);
- inne (media, znaczące instytuty naukowo-badawcze, dziedzictwo kulturowe).

Narodowa Rada Cyberbezpieczeństwa

W wyniku przyjętej przez Niemcy w lutym 2011 r. strategii bezpieczeństwa cybernetycznego utworzono Narodową Radę Cyberbezpieczeństwa. Pracom gremium przewodzi Pełnomocnik Rządu ds. Teleinformatycznych, a jego skład obejmuje:
– Urząd Kanclerski,
– Ministerstwo Spraw Zagranicznych,
– Ministerstwo Spraw Wewnętrznych,
– Ministerstwo Gospodarki i Technologii,
– Ministerstwo Sprawiedliwości,
– Ministerstwo Finansów,
– Ministerstwo Oświaty i Nauki,
– resort obrony,
– przedstawicieli krajów związkowych.

W razie potrzeby skład ten poszerzany jest o dalsze resorty, przedstawicieli biznesu i świata nauki.

Przedmiotowemu organowi powierzono koordynację współpracy w obrębie niemieckiego rządu, a także na styku państwa i gospodarki.

Priorytetowe kierunki działań

Strategia cyberbezpieczeństwa Niemiec, poza powołaniem opisanych wyżej NCAZ oraz Narodowej Rady Cyberbezpieczeństwa, wskazuje osiem dalszych celów strategicznych.

Kluczowa dla bezpieczeństwa cyberprzestrzeni RFN pozostaje ochrona teleinformatycznej infrastruktury krytycznej, która stanowi centralny element większości obiektów infrastruktury krytycznej państwa. W tym kontekście Niemcy planują kontynuację oraz rozbudowę planu wdrożeniowego KRITIS *(Kritische Infrastukturen* – Infrastruktury Krytycznej)[9]. Adresatami tego planu w większości pozostają prywatni operatorzy elementów infrastruktury krytycznej (zob. przypis nr 8). Rozszerzenie planu KRITIS o dalsze sektory i branże ma nastąpić na podstawie wyników badań prowadzonych przez Narodową Radę Cyberbezpieczeństwa.

Ochrony wymaga także infrastruktura teleinformatyczna użytkowana przez obywateli oraz przedsiębiorstwa małej i średniej wielkości. Dlatego też strategia przewiduje podjęcie szeregu inicjatyw edukacyjno-informacyjnych zmierzających do podniesienia świadomości zagrożeń oraz bezpiecznego użytkowania systemów teleinformatycznych, a także zakłada dokonanie przeglądu rozwiązań oferowanych przez operatorów teleinformatycznych. Ponadto zobowiązuje Federalne Ministerstwo Gospodarki i Technologii do utworzenia wspólnie z przedstawicielami przemysłu grupy zadaniowej „Bezpieczeństwo teleinformatyczne w gospodarce”[10].

Ważnym elementem strategii jest podniesienie poziomu zabezpieczeń systemów teleinformatycznych użytkowanych przez administrację publiczną. W tym celu w ramach innowacyjnego projektu *Sieci Federacji* zostanie utworzona jednolita

[9] KRITIS to plan realizacji założeń Narodowego Planu na Rzecz Ochrony Infrastuktury Teleinformatycznej (NPSI – *Nationaler Plan zum Schutz der Informationsinfrastrukturen*) w odniesieniu do elementów infrastruktury krytycznej.

[10] Grupa ta podjęła działalność z dniem 29 marca 2011 r.

i bezpieczna infrastruktura teleinformatyczna dla całości administracji publicznej, która połączy dwie obecnie użytkowane przez nią sieci. Kontynuowane będą też prace w ramach koncepcji *Federalne Zarządzanie Teleinformatyczne*, która poprzez skuteczne wykorzystanie rozwiązań teleinformatycznych zmierza do podniesienia jakości usług administracji, zagwarantowania jej niezakłóconego działania oraz podniesienia wydajności, a także wsparcia innowacyjności. Intensyfikacji ulec ma także współpraca operacyjna z krajami związkowymi, w szczególności w zakresie obsługiwanym przez Zespoły Reagowania na Incydenty Komputerowe (CERT – *Computer Emergency Response Team*). Nadzór nad rozwojem przedmiotowej kooperacji sprawować będzie Rada Planowania Teleinformatycznego – wiodące gremium na rzecz federalnej współpracy w zakresie teleinformatyki.

Zgodnie z założeniami strategii poprawie ma ulec skuteczność zwalczania przestępczości w cyberprzestrzeni. Cel ten ma zostać osiągnięty poprzez połączenie wysiłków organów ścigania, Federalnego Urzędu Bezpieczeństwa Teleinformatycznego (BSI) oraz świata gospodarki. Do bardziej efektywnego zwalczania cyberprzestępczości mają się też przyczynić inicjatywy na rzecz wsparcia słabo rozwiniętych krajów partnerskich. Niemcy będą także zabiegać o globalną harmonizację prawa karnego zgodnie z postanowieniami Rady Europy w sprawie przestępczości komputerowej. Zbadają też zasadność wprowadzenia podobnych rozwiązań na poziomie Organizacji Narodów Zjednoczonych.

Współpraca międzynarodowa na rzecz ujednolicenia systemów ochrony cyberprzestrzeni Europy i świata pozostaje kolejnym celem niemieckiej strategii. Niemcy wyrazili zamiar podjęcia wzmożonej aktywności na forach UE, ONZ, OBWE, Rady Europy, OECD i NATO na rzecz implementacji rozwiązań zgodnych z ich potrzebami, w tym na przykład na forum Unii Europejskiej zapowiedzieli poparcie wydłużenia oraz poszerzenia mandatu ENISA[11], a na forum Paktu Północnoatlantyckiego – działań na rzecz ujednolicenia standardów bezpieczeństwa dla elementów ochrony infrastruktury krytycznej. Niemcy będą też dążyć do ustanowienia instrumentu miękkiego prawa *Soft Law Codex for Norms of State Behaviour in Cyberspace* – kodeksu norm zachowań państw w cyberprzestrzeni. Podstawą kodeksu miałoby być wspólne dla wszystkich jego zwolenników postrzeganie cyberprzestrzeni jako podlegającej ochronie, a tym samym wymagającej środków ochrony i międzynarodowej współpracy, obejmującej m.in. pogłębienie współpracy krajowych Zespołów Reagowania na Incydenty Komputerowe (CERT).

Kolejnym celem strategii pozostaje długotrwałe zabezpieczenie niezawodnych systemów i komponentów teleinformatycznych. Z tego powodu Niemcy będą wspierać dalszy rozwój badań naukowych na rzecz innowacyjnych koncepcji bezpieczeństwa teleinformatycznego oraz ochrony infrastruktury krytycznej, także we współpracy ze swoimi partnerami zagranicznymi. Docelowo dla ochrony wrażliwych sektorów planują wykorzystywać jedynie takie komponenty, które będą odpowiadały wymogom uznanego na arenie międzynarodowej standardu certyfikacji.

W związku ze strategicznym znaczeniem bezpieczeństwa cybernetycznego dokument szczególne znaczenie przypisuje weryfikacji stanu zatrudnienia oraz racjonalnemu planowaniu zasobów ludzkich w odniesieniu do organów administracji wymagających bezpiecznej cyberprzestrzeni. Do pogłębionej współpracy międzyresortowej mają

[11] ENISA – Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (*European Network and Information Security Agency*).

przyczynić się ponadto wymiana personelu pomiędzy jednostkami administracji na większą niż dotychczas skalę oraz kierunkowe kursy szkoleniowe.

Ostatnim celem ujętym w strategii pozostaje zapewnienie instrumentarium umożliwiającego kompleksową ochronę cyberprzestrzeni. Przedmiotowy katalog narzędzi obejmuje monitorowanie zagrożeń, podejmowanie odpowiednich środków zaradczych oraz ewaluację uregulowań prawnych, a także ugruntowanie powyższych metod we współpracy z właściwymi rzeczowo jednostkami organizacyjnymi Federacji, krajów związkowych i gospodarki.

Podsumowanie

Analiza podstawowego dla ochrony niemieckiej cyberprzestrzeni dokumentu, tj. *Strategii Cyberbezpieczeństwa dla Niemiec* wyraźnie wskazuje, że Niemcy zabiegają o skuteczną ochronę cyberprzestrzeni. Strategia stanowi obowiązujący akt prawny, a na jej podstawie funkcjonują ciała właściwe rzeczowo w zakresie cyberbezpieczeństwa.

Nadrzędnym celem strategii pozostaje zapewnienie akceptowalnego poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa przy udziale sektorów publicznego i prywatnego, a także każdego obywatela i społeczności międzynarodowej.

Dokument wprowadza szereg rozwiązań, w tym:

- monitorowanie zagrożeń,
- wprowadzenie i ewentualną adaptację uregulowań prawnych,
- ustanowienie ciał koordynujących krajowe działania na rzecz ochrony cyberprzestrzeni,
- pogłębienie współpracy krajowej i międzynarodowej,
- rozwój zespołów reagowania na incydenty komputerowe CERT,
- unifikację systemów ochrony cyberprzestrzeni,
- współdziałanie z sektorem prywatnym,
- ustanowienie centrów kompetencyjnych dla sektorów publicznego oraz prywatnego,
- zapewnienie szczególnej ochrony krytycznej infrastrukturze teleinformatycznej,
- podjęcie działań proceduralno-organizacyjnych,
- wdrożenie inicjatyw edukacyjno-szkoleniowych,
- wsparcie projektów badawczo-rozwojowych,
- podniesienie skuteczności zwalczania przestępczości w cyberprzestrzeni.
- zaangażowanie Niemiec w kwestie dotyczące ochrony cyberprzestrzeni, w tym wprowadzenie kompleksowych mechanizmów współpracy właściwych rzeczowo organów krajowych oraz dążenie do rozwinięcia przyjętej strategii także o płaszczyznę międzynarodową wskazują, że Niemcy potrafią nie tylko skutecznie przeciwdziałać zagrożeniom dla szeroko pojętego bezpieczeństwa wewnętrznego, ale też poprzez wysiłki na rzecz zgodnej z interesem RFN globalnej unifikacji norm i standardów zabiegają o rolę lidera w kreowaniu cyberprzestrzeni.

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. W konsekwencji opracowano strategię, która ma na celu zapewnienie akceptowalnego poziomu bezpieczeństwa zasobów informacyjnych państwa.

Opracowanie prezentuje ważniejsze elementy strategii, charakteryzuje jej cele strategiczne, opisuje powołane do realizacji jej postanowień jednostki i definiuje adresatów strategii.

Abstract

The article describes the *Cyber Security Strategy for Germany* approved by the German government on 23rd February 2011.

Efficient functioning of administrative authorities and elements of critical infrastructure, unhampered economic growth and welfare of citizens require a reliable national IT-infrastructure and therefore necessitate effective protection against potential attacks. In consequence, a strategy aiming to ensure an acceptable level of IT security in Germany has been established.

The article presents major elements of the strategy, names its priorities, describes the units meant to execute its provisions and specifies its addressees.