PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIULETYN

Nr 9 (1246), 22 stycznia 2015 © PISM

Ochrona infrastruktury krytycznej przed cyberatakami – pilne zadanie dla NATO i UE

Wojciech Lorenz

Atak hakerów na firmę Sony ukazał słabość zabezpieczeń sieci komputerowych, od których może być uzależnione funkcjonowanie infrastruktury krytycznej, zapewniającej stabilność państw, a nawet całych regionów. Aby w przyszłości uniknąć ataków o znacznie poważniejszych skutkach, rządy i firmy prywatne muszą podjąć skoordynowane działania w celu wprowadzenia jednolitych standardów cyberbezpieczeństwa. NATO i UE powinny też jak najszybciej opracować wspólne procedury umożliwiające efektywną współpracę narodowych zespołów reagowania na zagrożenia teleinformatyczne (CERT).

Pod koniec 2014 r. sieć komputerowa firmy Sony Pictures na kilka tygodni została sparaliżowana przez zmasowany atak hakerów, którzy domagali się wstrzymania premiery komedii o zamachu na przywódcę Korei Północnej Kim Dzong Una. Sprawcy ataku skradli ok. 100 terabajtów danych, m.in. poufnych dokumentów, prywatnych e-maili oraz nieopublikowanych scenariuszy i filmów. Zainfekowali także systemy wirusem, którego zadaniem było wymazanie danych z twardych dysków. Firma Sony przyznała, że nie była przygotowana na atak, który już został uznany za najpoważniejszy w historii USA. Incydent ten ukazał słabość zabezpieczeń przed cyberatakami nie tylko w Hollywood, ale także w innych firmach uzależnionych od sieci komputerowych. Należą do nich operatorzy infrastruktury krytycznej, m.in. elektrowni, sieci energetycznych, rafinerii, rurociągów, systemu finansowego, sieci teleinformatycznych czy transportowych, od których uzależnione jest sprawne funkcjonowanie państwa.

Rosnące zagrożenie dla infrastruktury krytycznej. Ponieważ infrastruktura krytyczna jest kluczowa dla bezpieczeństwa państwa i jego obywateli, stanowi niezwykle atrakcyjny cel ataków teleinformatycznych. Na czele listy możliwych celów znajdują się sieci elektroenergetyczne, których wyłączenie uruchomiłoby tzw. efekt kaskadowy, wywierając negatywny wpływ także na inne elementy infrastruktury (telekomunikacja, systemy bankowe etc.), które są uzależnione od zasilania. Ze względu na zasięg sieci konsekwencje takiego ataku mogłyby być odczuwalne nawet przez kilka państw. Ryzyko takiego scenariusza wzrasta wraz z rozwojem sieci elektroenergetycznych, tworzeniem tzw. inteligentnych sieci zapewniających komunikację między wszystkimi uczestnikami rynku energetycznego oraz powstawaniem połączeń regionalnych. Chociaż niektóre elementy infrastruktury, np. elektrownie atomowe, pozostaną odseparowane od zewnętrznych systemów teleinformatycznych i internetu (tzw. *air gaps*), również one mogą stać się celem ataku z użyciem zaawansowanej broni cybernetycznej, która może się dostać do systemu przez przenośne urządzenia USB. Możliwości takiej broni ukazały wirusy: Stuxnet, który w 2010 r. zdestabilizował działalność irańskich ośrodków wzbogacania uranu, i Shamoon, który dwa lata później wymazał dane z 30 tys. komputerów giganta naftowego Saudi Aramco.

O zwiększającym się zagrożeniu dla stabilności infrastruktury krytycznej może świadczyć m.in. szybki wzrost liczby ataków. W 2014 r. firma Deutsche Telekom, która w Europie i USA ma ok. 160 mln klientów, odnotowywała do miliona ataków w ciągu każdego dnia, trzy razy więcej niż rok wcześniej. Eksperci są zgodni, że za większość ataków na infrastrukturę odpowiadają słabo wyszkoleni hakerzy, którzy nie mają umiejętności i środków pozwalających na stworzenie zaawansowanych broni cybernetycznych. Stosując proste metody działania na dużą skalę,

najczęściej stanowią zagrożenie dla stabilności systemów teleinformatycznych, rzadziej natomiast są w stanie doprowadzić do ich trwałego uszkodzenia. Jednak nawet mniej doświadczeni hakerzy będą coraz częściej korzystać z rozwijającego się czarnego rynku usług i narzędzi cybernetycznych, na którym można zakupić informacje o lukach w oprogramowaniu komputerowym (tzw. *zero day vulnerabilities*), a następnie użyć ich do bardziej zaawansowanych ataków. Jednocześnie wraz z napięciami między Zachodem a Rosją, Iranem i Koreą Północną, a także pogłębiającym się kryzysem na Bliskim Wschodzie, należy liczyć się ze wzrostem prawdopodobieństwa ataków na infrastrukturę krytyczną przeprowadzanych lub wspieranych przez państwa. Ataki na Estonię (2007), Gruzję (2008) i Ukrainę (2014) wskazują, że zdolności cybernetyczne stały się jednym z wielu standardowych narzędzi, stosowanych w polityce międzynarodowej do wywierania presji i osiągania celów politycznych i/lub gospodarczych. Państwa mogą korzystać z pośrednictwa hakerów do prowadzenia szerokiego spektrum nieskomplikowanych ataków, licząc na to, że wyjątkowo trudno znaleźć winnych takich działań. Jednocześnie mogą pracować nad zaawansowanymi broniami cybernetycznymi, które wymagają zaangażowania wielu ekspertów i znaczących środków finansowych (koszt stworzenia wirusa Stuxnet szacowany jest na 10 mln USD), jednak będą po nie sięgać tylko w wyjątkowych sytuacjach, kiedy osiągnięcie pożądanego efektu będzie uzasadniało koszty i ryzyko wykrycia sprawcy.

Działania na poziomie państwowym. Odpowiedzialność za bezpieczeństwo infrastruktury krytycznej ponoszą państwa, które często nie wykorzystują wszystkich dostępnych metod działania w cyberprzestrzeni. Chociaż w ostatniej dekadzie większość członków UE i NATO przyjęła strategie cyberbezpieczeństwa, dokumenty te trzeba regularnie uaktualniać i uwzględniać w nich najlepsze doświadczenia innych państw. Jeden z najczęściej pojawiających się wniosków w sprawie przygotowywania strategii to przeprowadzenie szerokich konsultacji z sektorem prywatnym, który w wielu krajach jest głównym właścicielem i zarządcą infrastruktury krytycznej. Włączenie w prace nad strategią wszystkich środowisk, których będzie ona dotyczyła, zwiększa szanse na osiągnięcie zapisanych w niej celów. Strategie powinny być także wsparte mechanizmami regularnej oceny zagrożeń oraz uaktualnianymi definicjami infrastruktury krytycznej, w oparciu o możliwe do zweryfikowania kryteria.

Aby zwiększyć bezpieczeństwo infrastruktury krytycznej, trzeba także stworzyć efektywne partnerstwa publiczno-prywatne (PPP), których brakuje w wielu krajach UE i NATO. Takie zinstytucjonalizowane forum współpracy powinno prowadzić do regularnych spotkań między przedstawicielami rządu i administracji a sektorem prywatnym na różnych szczeblach w celu koordynowania działań i skutecznego reagowania na zmiany zachodzące w cyberprzestrzeni. Dzięki PPP większość państw UE i NATO powinna aktywniej promować ujednolicone, wysokie standardy w obszarze cyberbezpieczeństwa, zmniejszając koszty takich działań. Firmy, które dbają o bezpieczeństwo, mogą np. otrzymywać niższe stawki ubezpieczeń, ochronę przed pozwami sądowymi ze strony poszkodowanych w ataku czy certyfikaty potwierdzające wysoki poziom zabezpieczeń. Dzięki takim zachętom łatwiej byłoby też nakłaniać prywatne firmy do przeprowadzania niezależnych audytów zabezpieczeń sieci teleinformatycznych.

Eksperci są jednak zgodni, że najsłabszym elementem we wszystkich zabezpieczeniach są pracownicy firm, którzy nie przestrzegają podstawowych zasad bezpieczeństwa. Dlatego priorytetem dla rządów i firm prywatnych muszą być kampanie informacyjne i wspieranie cyberedukacji.

Potencjał współpracy UE i NATO. Dostrzegając rosnące znaczenie sieci teleinformatycznych dla stabilności państw, Unia Europejska i Sojusz Północnoatlantycki uznały cyberbezpieczeństwo za jeden ze swoich priorytetów. UE koncentruje się głównie na cywilnym wymiarze bezpieczeństwa, ale zaczęła wspierać także rozwój zdolności koniecznych do zabezpieczania jej działań w obszarze wojskowym w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO). Państwa członkowskie przyjęły strategię bezpieczeństwa cybernetycznego (2013), uzgodniły ramy polityki w zakresie cyberobrony (EU Cyber Defence Policy Framework, 2014) i pracują nad dyrektywą bezpieczeństwa teleinformatycznego, która ma zobowiązać państwa członkowskie do przestrzegania podstawowych standardów, w tym do wprowadzenia narodowych centrów reagowania – CERT.

Głównym zadaniem NATO w obszarze cyberbezpieczeństwa jest ochrona sieci wykorzystywanych przez dowództwa, jednostki i instytucje sojuszu. NATO oferuje także wsparcie państwom członkowskim w razie ataku cybernetycznego na elementy infrastruktury krytycznej. Na szczycie w Walii w 2014 r. państwa członkowskie przyjęły wzmocnioną politykę cyberobrony (Enhanced Cyber Defense Policy) i pracują nad doktryną odpowiedzi na ataki cybernetyczne z zastosowaniem gwarancji sojuszniczej solidarności zapisanych w art. 5 traktatu waszyngtońskiego. UE i NATO, mimo politycznych sporów utrudniających ich współpracę, koordynują swoje wysiłki, aby uniknąć powielania działań. Obie organizacje próbują rozwinąć pełne spektrum cywilnych i wojskowych mechanizmów oraz narzędzi ułatwiających zdolność do oceny zagrożeń (ćwiczenia i edukacja), wykrywanie incydentów (rozwój sensorów), wymianę informacji i skoordynowane usuwanie skutków ataków (poprzez narodowe ośrodki CERT), wykrywanie sprawców i pociąganie ich do odpowiedzialności (zbieranie dowodów i harmonizacja procedur prawnych) oraz pogłębianie współpracy z państwami partnerskimi.

Priorytety Polski. Polska powinna wprowadzić do agendy szczytu NATO w Warszawie w 2016 r. wzmocnienie ochrony infrastruktury krytycznej przed cyberatakami poprzez pogłębienie zdolności do współdziałania między NATO i UE na poziomie operacyjnym. Głównym narzędziem taktycznej współpracy powinny się stać cywilno-wojskowe zespoły reagowania CERT, działające w oparciu o jednolite procedury, które umożliwią członkom UE i NATO wymianę informacji oraz udzielanie sobie wzajemnego wsparcia. Gdyby wprowadzenie takich rozwiązań okazało się zbyt ambitne, Polska powinna promować pogłębioną współpracę na poziomie regionu Morza Bałtyckiego, w którym wraz z rozwojem nowych połączeń energetycznych rośnie ryzyko ataków na infrastrukturę krytyczną.