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

BIULETYN

Nr 68 (1641), 11 maja 2018 © PISM

Estonia jako lider w zwiększaniu cyberbezpieczeństwa

Kinga Raś

Zaangażowanie Estonii we wzmocnienie cyberbezpieczeństwa jest wynikiem ataków hakerskich, jakich doświadczyła. Jednocześnie estońskie władze konsekwentnie podnoszą poziom cyfryzacji kraju oraz lobbują na rzecz efektywnego jednolitego rynku cyfrowego w UE. Dążenie Estonii do zwiększania cyberbezpieczeństwa stało się wręcz jej znakiem rozpoznawczym. Stosowanie przez nią kompleksowych i efektywnych rozwiązań sprawia, że może ona być dla Polski wzorcowym partnerem w cyfryzacji i zwalczaniu zagrożeń cybernetycznych.

W marcu br. estoński rząd skierował do parlamentu projekt ustawy o cyberbezpieczeństwie. Dokument określa zasady organizacji bezpieczeństwa sieci i systemów informatycznych w sektorze publicznym i prywatnym. Transponuje też do estońskiego prawa unijną dyrektywę 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych. Tak zwana dyrektywa NIS, której termin wdrożenia upłynął 10 maja br., wymaga m.in., by każde państwo UE wyznaczyło organ odpowiedzialny za cyberbezpieczeństwo i opracowało strategię przeciwdziałania zagrożeniom cybernetycznym. Regulacje mają ustandaryzować kryteria bezpieczeństwa w sieci oraz nakładają obowiązek informowania stosownych organów krajowych o incydentach cybernetycznych.

Modernizacja przepisów. W Estonii nowelizacja przepisów i wdrożenie wytycznych unijnych odzwierciedlają istniejącą praktykę. Większość regulacji obowiązywała bowiem już wcześniej na mocy ustaw: o stanie nadzwyczajnym oraz o łączności elektronicznej. Nowy dokument ma uporządkować kompetencje i obowiązki podmiotów odpowiedzialnych za bezpieczeństwo w sieci, w szczególności za zapobieganie zagrożeniom oraz zarządzanie ryzykiem i systemami informatycznymi. Dlatego wdrażanie odpowiednich zabezpieczeń obejmie przede wszystkim serwery pocztowe oraz systemy obiegu dokumentów. Dotychczas stosowano je w systemach spełniających formalnie kryteria bazy danych. Ustawa definiuje jednocześnie listę tzw. kluczowych dostawców usług. W porównaniu z wcześniejszymi przepisami nowe prawo obejmie także Estońską Fundację Internetową, zarządzającą domeną .ee, oraz dostawców usług cyfrowych, w tym sklepy internetowe, wyszukiwarki i usługi danych w chmurze.

Cyfryzacja po estońsku. Estonia jest pionierem cyfryzacji w Europie i oferuje swoim obywatelom ponadprzeciętne rozwiązania internetowe, także w administracji publicznej. Już w latach 90. opracowano system platformy cyfrowej X-Road, umożliwiającej integrację systemów informatycznych i bezpieczny przesył danych. Od 2001 r. w Estonii obowiązuje elektroniczny dowód osobisty, który posiada 86% obywateli. Identyfikacja osób w sieci umożliwiła wprowadzenie w 2005 r. powszechnego głosowania przez internet. W wyborach parlamentarnych i lokalnych w 2009 r. głosowało tak kilkanaście procent wyborców, a w każdych kolejnych – ponad 20%. Najbardziej popularną usługą państwowej e-administracji jest internetowe zeznanie podatkowe, z którego korzysta ponad 96% podatników.

O priorytetowym traktowaniu cyfryzacji przez rząd estoński świadczy także dofinansowywanie tego sektora w administracji publicznej. W czteroletniej perspektywie budżetowej w 2018 r. Estonia zwiększyła

do 52,7 mln euro środki na rozwój infrastruktury systemu e-usług z 18,6 mln euro w 2017 r., a od przyszłego roku planuje podwyżki pracowników branży IT w administracji publicznej o 20%.

Cyfryzacja sprzyja tworzeniu przyjaznego środowiska inwestycyjnego. W Estonii można m.in. założyć firmę w ok. 15 minut, co dla tzw. małego państwa stanowi istotny czynnik rozwoju gospodarczego. Dodatkowo w 2014 r. Estonia wdrożyła program e-Residency, czyli cyfrowy identyfikator, który, bez względu na miejsce zamieszkania, oferuje uproszczone rozpoczęcie i łatwe prowadzenie biznesu w ramach UE. Dotychczas wnioski o jego przyznanie złożyło ponad 37 tys. osób ze 156 państw, a celem zdecydowanej większości z nich było założenie firmy, w tym w sektorze IT.

Cyberbezpieczeństwo. Duża zależność Estonii od systemów informatycznych pociąga za sobą jej znaczną podatność na zagrożenia cybernetyczne. Mimo dotychczasowych ataków hakerskich państwo to nie zawróciło ze ścieżki postępującej informatyzacji, a wręcz nasila działania w tym zakresie, co przekłada się na coraz większe znaczenie cyberbezpieczeństwa. Estonia jako pierwsza na świecie przyjęła w 2008 r. strategię cyberbezpieczeństwa, która w 2014 r. została znowelizowana. Od ataku cybernetycznego ze strony Rosji w 2007 r. Estonia nie tylko traktuje tę sferę jako strategiczny wymiar bezpieczeństwa, ale też skutecznie zabiega o jego wzmocnienie na poziomie unijnym.

Według raportu RIA – organu odpowiedzialnego za cyberbezpieczeństwo – w 2016 r. Estonia odnotowała 2248 incydentów cybernetycznych (w Polsce według raportu ABW z 2015 r. liczba ta wyniosła 8914). Większość z nich była spowodowana przez złośliwe oprogramowanie (30%), tzw. botnety (22%), próby wyłudzeń informacji (13%) lub złośliwe oprogramowanie szyfrujące – tzw. *ransomware* (11%). Około 20–30% ataków cybernetycznych było wymierzonych w instytucje rządowe. W sektorze publicznym najbardziej narażona na zakłócenia okazała się ciągłość działania systemu informatycznego, wspierającego inne serwisy usługowe bądź stanowiącego jego zabezpieczenie. Sektor ten był też podatny na ataki w celu wyłudzenia informacji. Estońskie analizy wskazują też na rosnące ryzyko zagrożenia atakami cybernetycznymi na administrację lokalną. Brak wystarczającej ochrony sieci dotyczy też organizacji pozarządowych.

Estonia stara się kompleksowo zwiększać swoje cyberbezpieczeństwo, ponieważ atakowane były m.in. podmioty świadczące powszechne usługi społeczeństwu. Na przykład w 2016 r. zagrożony został wysoce zinformatyzowany estoński system opieki zdrowotnej. W jednym z największych szpitali w kraju oprogramowanie *ransomware* z zainfekowanych komputerów kilkakrotnie rozprzestrzeniło się na jego serwer. Ponadto w 2016 r. została zaatakowana sieć komputerowa Viru Keemia Grupp (VKG) – przedsiębiorstwa działającego w branży łupków bitumicznych. Monitoring sieci wykrył złośliwe oprogramowanie, co zidentyfikowano jako ukierunkowany atak. Kontrola serwera wskazała na działalność APT28 – grupy powiązanej z rosyjskim wywiadem.

Z estońskiej perspektywy cyberbezpieczeństwo przekłada się na sprawne funkcjonowanie jednolitego rynku cyfrowego. Estonia, jako jego zwolenniczka, mobilizowała państwa członkowskie UE do wspólnych działań na rzecz cyfryzacji m.in. podczas swojej prezydencji w Radzie UE. Obecnie lobbuje na rzecz wdrożenia kluczowych inicjatyw unijnych w tym zakresie. Dotyczą one m.in. ochrony danych osobowych w sieciach komórkowych i na platformach internetowych, przepisów o prawie autorskim, swobodnego przesyłu danych nieosobowych, a także opodatkowania usług internetowych. Estonia zacieśnia też współpracę międzypaństwową w zakresie wymiany danych: od lutego br. estońska platforma danych X-Road została połączona z fińską Suomi.fi. Premier Estonii Jüri Ratas opowiada się za rozszerzeniem współpracy estońsko-fińskiej na państwa bałtyckie i nordyckie.

Wnioski. W Estonii nowelizacja przepisów dotyczących cyberbezpieczeństwa polega przede wszystkim na uporządkowaniu dotychczasowych regulacji oraz ich adaptacji do zmieniających się uwarunkowań, nie zaś na wdrażaniu zupełnie nowych rozwiązań. Estonia stara się przy tej okazji doskonalić technologie reagowania na konkretne incydenty w cyberprzestrzeni. Służyć temu mają m.in. poprawa infrastruktury sieci, skoordynowane administrowanie systemami informatycznymi oraz wzmocnienie działu IT w administracji.

Wspierając działania na rzecz cyberbezpieczeństwa, estońskie władze opowiadają się za utworzeniem jednolitego rynku cyfrowego, dopatrując się w tym wymiernych zysków, szczególnie w perspektywie rozwoju e-gospodarki. Promują więc rozwiązania, które sprzyjają bezpieczeństwu w sieci oraz realnie działają na korzyść Estonii jako państwa atrakcyjnego dla inwestorów zagranicznych, w tym spoza UE.

Doświadczenie Estonii w tworzeniu e-administracji i ochronie systemów informatycznych sprawia, że jest ona dla Polski wzorcowym partnerem do współpracy. Aby skutecznie reagować na nowe zagrożenia, Polska mogłaby wykorzystać estońskie doświadczenie w zapewnieniu bezpiecznych e-usług dla administracji publicznej, w tym samorządowej. Dla Polski przydatne mogą okazać się estońskie praktyki w zakresie ochrony danych osobowych i wprowadzania systemu dowodów elektronicznych. W interesie Polski jest też działanie na rzecz zwiększenia cyberbezpieczeństwa na wschodniej flance NATO. Sprzyja temu współpraca regionalna, w tym przy wsparciu tzw. centrów kompetencji NATO w Tallinnie i Rydze.