PREZYDENT ILVES DLA CYBERDEFENCE24: ROSYJSKI ATAK NA ESTONIĘ BYŁ SAMOBÓJCZĄ BRAMKĄ

"Rosyjskie ataki z 2007 roku nazwałbym strzeleniem sobie samobójczej bramki." (...) "Wojsko powoli zmienia kurs i cyberbezpieczeństwo także dla nich staje się coraz ważniejsze.". O cyberbezpieczeństwie Estonii, roli NATO i bezpieczeństwie ochrony infrastruktury krytycznej mówi w wywiadzie dla Cyberdefence24.pl były prezydent Estonii Thomas Hendrik Ilves i jego doradczyni ds. bezpieczeństwa Merle Maigre**.**

Andrzej Kozłowski: Estonia jest postrzegana jako państwo frontowe konfrontacji NATO z Rosją. Czy ta sytuacja ma również miejsce w świecie wirtualnym?

Thomas Hendrik Ilves: Musimy rozróżnić przestrzeń fizyczną od wirtualnej, w której nie ma czegoś takiego jak granice czy państwa frontowe. Spójrzmy na ostatni atak na Komitet Partii Demokratycznej, który prawdopodobnie został przeprowadzony z terytorium Rosji. Odległość między Stany Zjednoczonymi a Rosją jest olbrzymia, ale w cyberprzestrzeni nie ma czegoś takiego jak obszar i nie ma również tradycyjnie rozumianego dystansu. Jeśli chodzi o świat fizyczny i tradycyjną walkę kinetyczną, może to być prawdą, ponieważ graniczymy z Rosją. W odniesieniu do cyberprzestrzeni, Estonia była pierwszym państwem, który stał się celem politycznie ukierunkowanego cyberataku, na poziomie mogącym wpłynąć na funkcjonowanie państwa. Obecnie tego typu ataki są coraz powszechniejsze, większe i groźniejsze.

Estonia była pierwszą ofiarą. Oczywiście w tamtym okresie byliśmy przytłoczeni atakiem. Nie miał on jednak na celu penetracji naszych systemów i sieci, tylko utrudnienie dostępu do systemów i stron internetowych, czyli był to atak DDoS – Distributed Denial of Service, który w tamtym czasie 10 lat temu był wystarczająco silny, żeby wpłynąć na Estonię. Dzisiaj atak na takim poziomie nie byłby w stanie nam zagrozić. Obecnie jednak obserwujemy o wiele większe ataki typy DDoS, czego doświadczyliśmy pod koniec października. Ich ofiarą padła firma DYN zajmująca się konwertowaniem adresów IP w adresy DNS, których używają ludzie. Był to niewątpliwe bardzo efektywny atak dzięki wykorzystaniu rzeczy podłączonych do internetu w ramach tzw. IoT. Wcześniej taka sytuacja nie miała miejsca, a z pewnością nie na taką skalę.

Problemem jest, że takich urządzeń podłączonych do internetu są miliony. To nie jest złośliwe oprogramowanie, które ludzie ściągają przez przypadek na własne komputery. Jeśli odwiedzisz stronę porno, to będzie to główny sposób na zainfekowanie twojego komputera i stanie się częścią botnetu. Obecnie o wiele prościej jest zainfekować urządzenia IoT, które mają hasła zabezpieczające takie jak np. 12345 czy 00000. To jest głupie, ale takich przypadków jest bardzo dużo. Wszystkie te urządzenia IoT z bardzo słabymi zabezpieczeniami mogą stać się celem hakerów i zostać użyte do przeprowadzenia ataków DDoS.

A.K.: Wspomniał Pan, że w 2007 roku Estonia ucierpiała z powodu masowego ataku DDoS i chciałbym zapytać, co Estonia zrobiła w ostatnich latach, żeby przygotować się na podobne incydenty?

T.H.I.: Przede wszystkim zwiększyliśmy naszą odporność na ataki oraz skróciliśmy czas przywracania pracy systemów. Dodatkowo wdrożyliśmy takie narzędzia jak lustrzane strony internetowe, które stanowią replikę oryginalnych stron internetowych. Podczas zmasowanego ataku DDoS na Gruzję w 2008 roku, udzieliliśmy temu państwu lustrzanych stron. Głównym zagrożeniem, moim zdaniem, nie jest jednak DDoS, ale tzw. integralność danych (ang. *data integrity*). Wszyscy ludzie są oburzeni na agencje wywiadowcze po tym, jak Edward Snowden ujawnił ich szpiegowską działalność w internecie. Jeżeli ktoś może odczytać, jaka jest moja grupa krwi z chmur czy zapisów na twardym dysku, nie przeszkadza mi to. Jednak sytuacja, w której ktoś ją zmienia, manipuluje kartą pacjenta, może sprowadzić poważne kłopoty. To jest oczywiście tylko teoretyczny przykład, nie mam wiedzy, czy taki incydent miał miejsce w rzeczywistości. W ten sposób możesz zasugerować wszystko np. w bankach.

Integralność danych jest częścią tzw. trójkąta CIA (skrót nie pochodzi od Central Intelligence Agency – przyp. red.), ale oznacza: poufność (*Confidentiality*), integralność (*Integrity*) i dostępność (*Accessibility*). DDoS jest atakiem na dostępność. Poufność jest kwestią prywatności i ochrony danych – czego przykładem jest ostatnia kradzież maili Hillary Clinton. Ostatni element trójkąta, czyli integralność. Moim zdaniem ataki wymierzone właśnie w ten obszar będą najgroźniejsze, ponieważ mogą doprowadzić do powstania zniszczeń fizycznych. Przykładem tego był Stuxnet. Złośliwy robak komputerowy, który powodował, że wirówki do wzbogacania uranu, zamiast zwalniać, przyspieszały i się psuły. Komputery i pełna automatyka doprowadziły do powstania takiej sytuacji i to jest klasyczny atak na integralność IoT.

Merle Maigre: Należy wymienić dwie inne rzeczy, oprócz tego, co powiedział prezydent. Dla nas atak z 2007 roku był dzwonkiem ostrzegawczym i w rezultacie znacznie usprawniliśmy swoje sieci i systemy jeszcze podczas trwania ataków. Zintensyfikowaliśmy również współpracę między różnymi agencjami, skoncentrowaliśmy swoje zadania i usługi związane z cyberbezpieczeństwem w odniesieniu do państwa, infrastruktury krytycznej oraz utworzyliśmy konkretne miejsce odpowiedzialne za monitorowanie całej sytuacji. Obecnie wszyscy to robią, ale w 2007 roku nie był to powszechny proceder. Po drugie, mamy ochotniczą gwardię narodową do walki konwencjonalnej, która nazywa się Estońską Ligą Obrony i tam również jest komponent cyber.

A.K.: Panie Prezydencie czy może Pan przybliżyć, czym jest Estońska Liga Obrony?

T.H.I.: Tradycyjna Home Guard, w skład której najczęściej wchodziła ludność z terenów wiejskich jak np. farmerzy, którzy chcą bronić swojej ziemi w przypadku pojawienia się kłopotów. Mamy w Estonii dużo maniaków komputerów, którzy normalnie pracują jako administratorzy systemów, programują, zajmują się grami komputerowymi czy bezpieczeństwem banków. Takich osób potrzebuje również administracja państwowa. Niestety ludzie z branży IT zarabiają ogromne pieniądze, co uniemożliwia ich zatrudnienie przez administrację państwową. Nawet NSA ma podobne problemy. Żadna pensja oferowana w sektorze publicznym w Estonii nie może się równać się z tym, co ci ludzie zarabiają w sektorze prywatnym czy co mogą zarobić. Ludzie czują jednak obowiązek patriotyczny i poczucie dumy ze swojego kraju ze względu na IT, dlaczego w takim razie mają go nie wspomóc? To był powód, dla którego stworzyliśmy ochotniczą jednostkę skoncentrowaną na aspektach cyberobrony.

A.K. W Estonii służba wojskowa jest obowiązkowa. Czy w jej ramach prowadzone są szkolenia oddziałów odpowiedzialnych za cyberbezpieczeństwo?

T.H.I.: Nie za bardzo. Nieliczne osoby, które mają odpowiednie umiejętności komputerowe, są zaangażowane w takie projekty. Mogą one odgrywać specjalną rolę podczas ćwiczeń wojskowych. Mój syn odbył swoją obowiązkową służbę wojskową, obecnie jest rezerwistą i przebywa w Brukseli. Podczas ćwiczeń rezerwy jedno z nich dotyczyło właśnie kwestii IT. Najczęściej jednak służba, jaką odbywają, dostarcza tylko podstawowych umiejętności.

M.M.: Obowiązkowa służba wojskowa skupia się raczej na ciężkich ćwiczeniach fizycznych. Musisz nauczyć się podstaw walki i przetrwania. Pierwszy miesiąc jest dla każdego taki sam i polega na intensywnym treningu w lesie. Ktoś, kto specjalizuje się w IT i nie jest wystarczająco sprawny, żeby przejść ten intensywny trening, powinien udać się do Estońskiej Ligi Cyberobrony, gdzie ma więcej możliwości wykorzystania swoich umiejętności i nie musi spędzać czasu na ćwiczeniach terenowych.

A.K.: Czy uważa Pan, że Rosja może również zaatakować infrastrukturę krytyczną w państwach NATO, podobnie jak zrobiła to na Ukrainie i czy w Estonii prowadzone są specjalne przygotowania na wypadek takiego scenariusza?

T.H.I.: Jesteśmy bardzo dobrzy w monitorowaniu infrastruktury krytycznej. Problemem w wielu państwach jest odpowiedzialność sektorowa. Jedna z gałęzi władzy, np. ministerstwo, bierze odpowiedzialność za ochronę granic, policja jest odpowiedzialna za coś innego, a za system elektryczny jeszcze inny podmiot. Problemem jest też brak dialogu pomiędzy tymi stronami. Obecnie mamy zintegrowany system monitorujący wodę, elektryczność, granice. To jest jedna rzecz. W tym wypadu pomaga nam to, że jesteśmy małym krajem, zdecydowanie łatwiej nam się jest zabezpieczyć. Nie martwię się zbytnio Estonią, ponieważ nasze systemy rządowe oparte są na PKA (Publiczny klucz autoryzacji). Inni tak nie mają i dlatego pojawia się u nich poważny problem. Najgorszym przypadkiem, o którym wiem, była kradzież danych wszystkich pracowników federalnych w Stanach Zjednoczonych. Wszelkie informacje na ich temat znajdowały się w jednej bazie danych i jak się okazuje, była ona niewłaściwe zabezpieczona. Incydent ten jest znany pod nazwą: atak na OPM i miał miejsce w 2015 roku. To jest straszne, ktoś teraz zna wszystkie dane pracowników federalnych, w tym profile psychologiczne osób. Jest to prawdziwy skarb dla każdego wywiadu. Jeżeli masz szyfrowanie na wysokim poziomie, system monitorowania sieci 24/7, PKA to bazy danych są zdecydowanie lepiej zabezpieczone niż w innych miejscach.

A.K.: Estonia posiada wiele innowacyjnych rozwiązań cyberbezpieczeństwa. W jaki sposób wspiera system globalnego cyberbezpieczeństwa?

T.H.I.: Jako prezydent promowałem rozwiązania PKA wszędzie. Moim zdaniem problemem jest, że architektura bezpieczeństwa współczesnego internetu została stworzona na początku lat 80. dla czegoś, co nazywało się bitnetem. Łączył on prawie 3 tys. placówek akademickich na terenie całego kraju i było to przed erą protokołu HTTP, ale był już stosowany protokół TCP/IP. Jedyne, co należało wiedzieć, to adres poczty elektronicznej i hasło. Obecnie mamy miliardy osób podłączonych do internetu i ten system nie działa już tak, jak powinien. Dokładnie rzecz biorąc to on działa, ale nie jest wystarczająco silny, żeby chronić wszystkie skrzynki pocztowe czy bazy danych. Jeśli mamy opierać się na hasłach, nawet jeżeli są długie i skomplikowane – nie zagwarantują one bezpieczeństwa. Dlatego potrzeba systemów PKA, autoryzacji dwuskładnikowej. Są to absolutnie minimalne standardy bezpieczeństwa. Powstaje następujący problem: kraje mówią, że nie będą miały narodowych dowodów osobistych. Ale w ten sposób narażają się na ryzyko.

M.M.: Jeśli chodzi o wkład Estonii w system globalnego bezpieczeństwa, to wymieniałbym NATO i Centrum Doskonalenia Obrony przed Atakami Cybernetycznymi zlokalizowane w Tallinnie. Jest to również jeden z pozytywnych skutków ataków z 2007 roku.

T.H.I.: Od 2004 roku, czyli od naszej akcesji do NATO, mówiłem naszym sojusznikom, że musimy zająć

się cyberbezpieczeństwem. Rosyjskie ataki z 2007 roku nazwałbym strzeleniem sobie samobójczej bramki. W 2007 roku członkowie NATO byli świadkami cyberataku na Estonię, przed którym ostrzegaliśmy od 2004 roku. Dopiero wtedy udało się utworzyć Centrum Doskonalenia Obrony przed Atakami Cybernetycznym. Kolejne 9 lat trwał proces uznania cyberprzestrzeni za kolejny obszar prowadzenia działań zbrojnych. Stało się to dopiero na szczycie w Warszawie w 2016 roku.

A.K.: W jednym z artykułów napisał Pan, że naszym problemem w NATO jest wojskowo-wywiadowcze myślenie o kwestiach zagrożeń z cyberprzestrzeni.

T.H.I: Problemem jest, że wywiady państw członkowskich nie dzielą się informacjami. Interoperacyjność oznacza, że możesz wziąć francuski pocisk i umieścić go w niemieckim karabinie/dziale czy brytyjską rakietę i podwiesić pod amerykański samolot. Państwa wciąż nie dzielą się informacjami, jeśli chodzi o cyberbezpieczeństwo. MI6, CIA czy BND nie rozmawiają ze sobą zbyt chętnie i nie przekazują sobie pozyskanych informacji. Wynika to z pewnego specyficznego sposobu myślenia. Stanowi to problem, ponieważ jedna z tych stron identyfikuje nowy rodzaj zagrożenia, ale nie dzieli się tą informacją z pozostałymi. Ten program znaleziony w hiszpańskich sieciach, może zaraz znaleźć się w sieciach estońskich.

M.M.: Sposób myślenia w wywiadzie od czasów wydarzeń na Ukrainie powoli się zmienia i wzrasta potrzeba wymiany informacji, co się obecnie dzieje. Proces ten zachodzi jednak bardzo powoli.

A.K.: Wracając do NATO: jaką rolę ta tradycyjna organizacja polityczno-wojskowa powinna odgrywać w cyberprzestrzeni?

M.M.: NATO musi uwzględnić cyberbezpieczeństwo jako naturalny element ćwiczeń. Odnotowujemy tutaj spory postęp.

T.H.I.: Corocznie, w kwietniu organizujemy największe ćwiczenia z zakresu cyberbezpieczeństwa na świecie. Jest to wydarzenie wymagające dużego wysiłku. Biorą w nich udział drużyny z różnych państw, które wzajemnie ze sobą rywalizują. Ćwiczenia odbywają się w czasie rzeczywistym. Jedna strona stara się zniszczyć serwery drugiej czy też sieci energetyczne, a dokładnie rzecz biorąc systemy komputerowe odpowiedzialne za nie.

Upłynęło trochę czasu, zanim państwa zrozumiały znaczenie cyberbezpieczeństwa. Wojsko powoli zmienia kurs i cyberbezpieczeństwo także dla nich staje się coraz ważniejsze. NATO jest organizacją odpowiedzialną za działanie na obszarze transatlantyckim. W cyberprzestrzeni nie możemy wyodrębnić obszarów geograficznych. Możemy tak samo zaatakować Stany Zjednoczone jak Estonię i nie ma znaczenia, czy jest się blisko czy daleko od Rosji. Moim zdaniem potrzebujemy organizacji skupiającej demokracje liberalne z całego świata. Australia nie jest częścią NATO i nie może dołączyć do Sojuszu, ponieważ położona jest na południowo-wschodnim Pacyfiku. Z drugiej jednak strony Australia, Nowa Zelandia, Japonia to demokratyczne państwa, które mogą zostać zaatakowane takimi samymi cyberatakami jak Estonia, Polska czy Stany Zjednoczone.

Musimy mieć szerszą od obecnej perspektywę, kogo mamy bronić w cyberprzestrzeni. NATO jest oczywiście pierwszą organizacją, do której się zwracamy i to jest bardzo dobre. Ale musimy myśleć szerzej. Kryteria, żeby dołączyć do NATO: rządy oparte na poszanowaniu prawa, demokracja liberalna z wolnymi wyborami. Są jednak państwa poza obszarem transatlantyckim, które wyznają nasze wartości, np. Australia, Nowa Zelandia czy Japonia. Co więcej, państwa te są również podatne na cyberataki i to, co stało się w Niemczech czy Stanach Zjednoczonych może powtórzyć się w tych państwach, w których ktoś będzie starał się zmanipulować wyniki wyborów.

M.M.: Musimy chronić nie tylko systemy i sieci wojskowe, ale również obiekty cywilne takie jak np.

systemy bankowe.

T.H.I.: Cyberataki mogą sparaliżować infrastrukturę cywilną i wojskową danego państwa lub przedsiębiorstwa. Widzieliśmy to pod koniec października podczas ataku na DYN. Nie trzeba nikogo zastrzelić.

A.K.: Jak wygląda estońsko-polska współpraca w obszarze cyberbezpieczeństwa?

T.H.I.: Pracujemy blisko, wymieniając informacje, i nasza współpraca z Polską jest jedną z najlepszych. Układa się ona bardzo dobrze niezależnie od rządu sprawującego władzę w państwie.

M.M.: Polityka zagraniczna, bezpieczeństwa w tym cyberbezpieczeństwo. We wszystkich tych obszarach współpraca wygląda bardzo dobrze.

Czytaj też: Pierwsza ofiara Brexitu? Może być nią Estonia