Instytut Europy Środkowej

Komentarze IEŚ

Redakcja: Beata Surmacz (dyrektor IEŚ), Tomasz Stępniewski (z-ca dyrektora IEŚ), Agnieszka Zajdel (sekretarz redakcji), Aleksandra Kuczyńska-Zonik, Jakub Olchowski, Konrad Pawłowski, Agata Tatarenko

Nr 8 (8/2019) | 24.04.2019

ISSN 2657-6996

Aleksandra Kuczyńska-Zonik

Zagrożenia w cyberprzestrzeni – nowe wyzwania dla państw bałtyckich

W 2018 r. państwa bałtyckie zostały uznane za lidera wśród państw UE w walce z rosyjskim wpływem w cyberprzestrzeni według rankingu Kremlin Watch. Estonia, Litwa i Łotwa znalazły się także w czołówce państw najlepiej przygotowanych na zagrożenia informatyczne według raportu National Cyber Security Index 2018 (odpowiednio 3, 6 i 12 miejsce). Państwa bałtyckie są bardzo podatne na tego typu zagrożenia ze względu na ostrą krytykę Rosji, obecność mniejszości rosyjskojęzycznej i jej związki z organizacjami przestępczymi pochodzącymi z Rosji, słabość systemów informatycznych oraz nieświadomość samych użytkowników.

Rosja – największym zagrożeniem dla cyberprzestrzeni państw bałtyckich. W kwietniu i maju 2007 r. w związku z przeniesieniem pomnika tzw. Brązowego Żołnierza z centrum Tallina na miejscowy cmentarz wojskowy, które wzbudziło sprzeciw zarówno rosyjskojęzycznych mieszkańców Estonii, jak i Rosji, doszło do jednego z najpoważniejszych cyberataków przeciwko Estonii. Ataki typu DDoS – tzw. odmowa dostępu – polegające na wysyłaniu fałszywych prób skorzystania z usług i zajęciu wszystkich wolnych zasobów systemu komputerowego, dotknęły infrastrukturę informatyczną instytucji państwowych: strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji oraz szkół publicznych. Cyberataki osiągnęły apogeum 9 maja (rosyjski Dzień Zwycięstwa), gdy ich celem stał się też sektor prywatny, w tym dwa największe estońskie banki: Hansapank i SEB Ühispank oraz dziennik „Postimees". Działania były prowadzone przez wielu hakerów powiązanych z rosyjską organizacją „Nasi", zależną od Kremla. Z tego powodu w 2008 r. podjęto decyzję o utworzeniu w Tallinie Centrum Doskonalenia Obrony przed Cyberatakami NATO (NATO CCD COE), którego celem jest zarządzanie bezpieczeństwem w cyberprzestrzeni.

W ostatnich latach zanotowano wiele przykładów tego typu działalności przestępczej z udziałem rosyjskich służb wywiadowczych, zamieszanych m.in. w domniemany atak na Organizację ds. Zakazu Broni Chemicznej (która w tym czasie badała sprawę Siergieja Skripala i użycia broni chemicznej w Doumie w Syrii) i Światową Agencję Antydopingową. Najpoważniejsze ataki dotknęły sieci elektroenergetyczne (państwa bałtyckie są w dalszym ciągu częścią rosyjskiej sieci energetycznej, ale planują synchronizację z siecią UE) oraz system dystrybucji paliw. Hakerzy powiązani z organizacjami w Rosji pozostawali niezauważeni w systemach wewnętrznych przez wiele miesięcy. Testowali bałtyckie sieci elektroenergetyczne pod kątem słabości i poznawali sposób ich kontrolowania, aby móc je wyłączyć w dowolnym momencie. W 2015 r. systemy informatyczne łotewskiego Ministerstwa Spraw Wewnętrznych zostały zaatakowane przez oprogramowanie szpiegujące, prawdopodobnie pochodzenia rosyjskiego, po tym jak systemy zostały połączone w ramach jednego organu nadzorującego. W styczniu 2018 r. doszło do cyberataku na łotewski system informatyczny Urzędu Skarbowego (VID) i strony głównej Rady Ministrów oraz łotewskiej służby zdrowia, przeprowadzonego z kilku państw (systemów komputerowych), zarówno z UE, jak i spoza niej (w sumie ponad 20 państw). Hakerzy najczęściej stosowali metodę DDoS. Ataki nie spowodowały większych utrudnień (niekiedy tymczasowe zawieszenie systemu), w niektórych przypadkach były nawet niezauważalne dla przeciętnych użytkowników. Częstotliwość ataków cybernetycznych zwykle rosła, gdy Rosja przeprowadzała duże ćwiczenia wojskowe w pobliżu swoich granic z państwami bałtyckimi, np. w okresie rosyjsko-białoruskich manewrów Zapad 2017 (14-20 września). Cyberincydenty dotknęły również instytucje państwowe na Litwie, gdzie w związku z sesją Światowego Kongresu Tatarów Krymskich, na której omawiano kwestię masowych naruszeń praw człowieka na okupowanym przez Rosję Krymie (11 kwietnia 2016 r.), zablokowano witrynę parlamentu, częściowo uniemożliwiając transmisję dyskusji.

Ataki na infrastrukturę krytyczną, systemy informatyczne i social media. Ataki cybernetyczne na infrastrukturę krytyczną, systemy informatyczne instytucji państwowych, służby zdrowia i sektora finansowego motywowane

politycznie stanowią największe zagrożenie dla państw bałtyckich, chociaż liczba incydentów o niższym stopniu zagrożenia jest również alarmująca. W Estonii tylko w 2017 r. odnotowano 10 923 przypadki naruszeń cyberbezpieczeństwa – o jedną trzecią więcej niż w 2016 r. Tylko 122 incydenty miały bezpośredni wpływ na usługę niezbędną do funkcjonowania państwa i społeczeństwa, co oznacza spadek w ciągu ostatnich trzech lat. Atakowano także system informatyczny w estońskim sektorze opieki zdrowotnej – spośród 32 incydentów 10 miało bezpośredni wpływ na pracę szpitali i lekarzy. Nieco mniejszy wzrost przestępczości w cyberprzestrzeni zanotowano na Litwie – o 10-15% w stosunku do lat poprzednich. W 2017 r. było to 54 414 incydentów, które dotyczyły głównie sfery usług łączności elektronicznej i dostawców usług hostingowych na Litwie.

Coraz większym problemem staje się wykorzystywanie przez hakerów popularnych serwisów społecznościowych w celach politycznych i dezinformacyjnych. Według badań NATO StratCom COE w 2017 r. ok. 60% rosyjskojęzycznych kont na Twitterze zawierających posty o NATO i kwestiach wojskowych w państwach bałtyckich pochodziło ze zautomatyzowanych kont tzw. botów. W przypadku angielskojęzycznych kont – było to ok. 39%. Wyraźny wzrost tego rodzaju działalności zanotowano w czasie ćwiczeń Zapad 2017, kiedy to od sierpnia do października boty stworzyły 52% wszystkich wiadomości w języku angielskim. W 2018 r. usunięto kilkadziesiąt fałszywych kont na Facebooku powiązanych z rosyjskim Sputnikiem, częścią grupy informacyjnej Rossiya Segodnya (RT), rozsyłających w państwach bałtyckich propagandowe wiadomości o tematyce antynatowskiej i antyzachodniej. Hakerzy wykorzystali także popularną stronę społecznościową Draugiem.lv, na której w dniu wyborów parlamentarnych na Łotwie (6 października 2018 r.) pojawiły się prorosyjskie hasła, symbole i zdjęcia prezydenta Rosji. Dane użytkowników nie zostały jednak naruszone. Duża popularność portali społecznościowych, nieświadomość użytkowników oraz brak odpowiedniej reakcji właścicieli portali na naruszenia powodują, że social media są podatne na różnego rodzaju zagrożenia.

Porażki i sukcesy państw bałtyckich w walce z cyberzagrożeniami. Państwa bałtyckie znajdują się na politycznej linii frontu napięć między Zachodem a Rosją, stąd wielokrotnie były celem ataku ze strony zagranicznych podmiotów. A Ryga, jak wynika z raportu Marka Galeottiego opublikowanego przez European Council on Foreign Relations, obok Sztokholmu i Berlina, jest jednym z hubów rosyjskich organizacji przestępczych działających w różnych państwach Europy Zachodniej. Najpoważniejsze ataki były skierowane przeciwko infrastrukturze krytycznej oraz systemom instytucji państwowych, w tym sektorom zagranicznemu i obronnemu. Polegały one na włamywaniu się do systemu informatycznego, działaniu w nim w sposób niezauważony i uzyskaniu długoterminowych danych z systemu – np. regularnego dostępu do korespondencji e-mail i przetwarzanych dokumentów. Podatne na cyberzagrożenia są także social media ze względu na upolitycznione treści komunikatów i brak stosownej reakcji nadzorców popularnych serwisów społecznościowych oraz za sprawą nieświadomych użytkowników. Niektóre aplikacje, np. świadcząca usługi transportowe Yandex.Taxi, działająca w Wilnie, Rydze i Tallinie od 2018 r., wymagają dostępu do wielu poufnych danych, a zebrane informacje są przechowywane na serwerach kontrolowanych przez rosyjską firmę. Problemem jest również brak specjalistów ds. bezpieczeństwa IT.

Obecnie spośród państw bałtyckich to Estonia może pochwalić się największymi sukcesami w walce z cyberzagrożeniami. Estonia znalazła się pierwszej dziesiątce państw w rankingu Global Cybersecurity Index (GCI) 2017, a jej wkład w poprawę globalnego bezpieczeństwa cybernetycznego jest największy. Toomas Hendrik Ilves, były prezydent Estonii, jest aktywnym działaczem na rzecz cyberbezpieczeństwa, a Marina Kaljurand, była minister spraw zagranicznych Estonii, do marca br. pełniła funkcję przewodniczącej Globalnej Komisji ds. Stabilności Cyberprzestrzeni. Estonia przoduje również w najnowszych rozwiązaniach technologicznych (e-residency; i-voting). W działania na rzecz poprawy bezpieczeństwa w cyberprzestrzeni włączają się także Litwa i Łotwa. Między innymi w 2014 r. w Rydze utworzono Centrum Komunikacji Strategicznej NATO (NATO StratCom COE). W 2018 r. Litwa zaproponowała utworzenie tzw. „cyber Schengen" zone, na wzór obszaru swobodnego przepływu osób w UE, w celu lepszego zwalczania przestępczości cybernetycznej.