Cyberdefence 24

04.02.2017

CYBERWOJNA O BALTIC PIPE? ATAKI ROSYJSKICH SŁUŻB NA CZECHY, POLSKĘ I NORWEGIĘ [ANALIZA]

Instytucje w Czechach, Polsce i Norwegii padły ofiarą ataku cyfrowego, za którym stali rosyjscy hakerzy z grup APT 28 i APT 29 związani z GRU i FSB. Ich powodem są najprawdopodobniej wspólne polsko-norwerskie i polsko-czeskie strategiczne projekty gazowe zagrażające Gazpromowi.

Rosyjski cyberatak na Norwegię

Pod koniec tygodnia miał miejsce atak rosyjskich hakerów na norweskie: MSZ, MON, kontrwywiad (PST), Partię Pracy i inne ważne instytucje. Został on wymierzony w dziewięć kont poczty elektronicznej osób pracujących we wspomnianych instytucjach i jednego pracownika uniwersyteckiego.

Norwegowie oskarżyli o atak jednostkę hakerów APT 29 związaną z rosyjskim FSB. W ostatnim czasie była ona niezwykle aktywna włamując się do wielu instytucji państw zachodnich. Wśród najbardziej znanych incydentów warto wymienić tu atak cyfrowy przypuszczony na serwery amerykańskiej Komitetu Partii Demokratycznej.

Atak na Norwegię miał być wysoce zaawansowany, charakterystycznych dla wywiadów państw posiadających bardzo duże możliwości cybernetyczne. Użyto tzw. spear phishingu wysyłając wiadomości poczty elektronicznej ze skomplikowanym kodem. Norweski kontrwywiad nie ujawnił efektów ataku.

Premier Norwegii Erna Solberg w rozmowie z agencją prasową NTB powiedziała, że wrogie działania hakerskie uderzyły w „demokratyczne systemy zarządzania państwem”. Niemniej rzecznik MSZ Frode Andersen stwierdził, iż atak nie naruszył systemów komputerowych ministerstwa.

To nie pierwszy tego typu incydent w Norwegii. W ubiegłym roku Rosjanie próbowali wpłynąć na działalność Norweskiego Komitetu Noblowskiego, by zapobiec przyznaniu Pokojowej Nagrody Nobla ukraińskiemu prezydentowi Petro Poroszence.

Fot. domena publiczna / pixabay.com

Rosyjski cyberatak na Czechy

Tymczasem kilka dni przed cyberatakiem dokonanym na Norwegię minister spraw zagranicznych Lubomir Zaoralek poinformował o podobnych działaniach podjętych przez hakerów w stosunku do Republiki Czeskiej. Chodzi o konta mailowe czeskiego MSZ – w tym należące do ministra i wiceministrów. Zdaniem polityka autorem ataków były służby wywiadowcze obcego państwa.

Minister podkreślił, że hakerom nie udało się uzyskać dostępu do poufnych informacji. Włamali się jednak do systemu odpowiedzialnego za komunikację zewnętrzną. Ponadto udało im się dostać do skrzynki pocztowej ministra, która zawierała jednak tylko jawne informacje. Zaoralek oświadczył, że ataki hakerskie na MSZ obserwowano od początku roku. We wspomnianej sprawie trwa śledztwo oraz prowadzone są działania, by zapobiec podobnym atakom w przyszłości.

Minister wyjaśnił, że zdarzenie „było podobne do tych, których ofiarą padły instytucje amerykańskiej Partii Demokratycznej". Nie wskazał jednak sprawcy, choć sugestia, iż byli to Rosjanie wydaje się czytelna. Działania hakerów polityk określił jako bardzo zaawansowane i dlatego jego zdaniem musieli być oni powiązani z jakimś państwem o znacznych zdolnościach cybernetycznych.

W czeskiej agencja wywiadu trwa ocena rozmiar ataku. System MSZ uchodzi za jeden z najlepiej zabezpieczonych pośród wszystkich systemów administracji w kraju. Rzeczniczka prasowa Ministerstwa Spraw Zagranicznych dodała, że inne instytucje rządowe mogły również stać się celem ataków hakerskich. Nie można wykluczyć, że w ich przypadku złamano zabezpieczenia

Czeska strona śledcza Neovlivni.cz podaje, że hakerom udało się wykraść tysiące plików ze skrzynki pocztowej Ministra Spraw Zagranicznych i jego podsekretarzy, oraz iż jest to największy tego typu incydent w ostatnich latach. Informacje te nie zostały jednak potwierdzone.

To nie pierwszy atak rosyjskich hakerów na czeskie instytucje państwowe. W 2013 roku czeskim służbom udało się namierzyć sprawców ataku na Ministerstwo Obrony, ale rosyjski dostarczyciel usług

internetowych odmówił współpracy tak samo, jak służby państwowe Kremla. Rzeczniczka prasowa czeskiego MSZ powiedziała, że czeskie instytucje atakowane są praktycznie codziennie. Czechy są również celem agresywnych operacji informacyjnych prowadzonych przez Rosję.

Głośny był również atak na skrzynkę pocztową premiera Bogdana Sobotki w 2015 roku, kiedy to hakerom udało się wykraść wiele materiałów i umieścić na jednej ze stron internetowych.

Cyberataki na Czechy, Norwegię i Polskę są ze sobą związane

Atak na czeski MSZ świadczy o wyraźnym wzroście aktywności rosyjskich hakerów przeciwko państwom NATO. Warto w tym kontekście przypomnieć, że niedawno grupa Fancy Bear zaatakowała również polskie MSZ (nie odnosząc sukcesu). Zdaniem Vlado Bizika eksperta ds. cyberbezpieczeństwa z think-thanku European Values z siedzibą w Pradze, atak na czeski MSZ przypominał operacje przeciwko polskiemu odpowiednikowi. W obu przypadkach użyto trojana, którego jest bardzo ciężko wykryć. Co ciekawa także w przypadku Norwegii użyto zaawansowanego złośliwego oprogramowania. Jest to charakterystyczne dla służb wywiadowczych państw używając hakerów.

Rosyjskie intencje

Warto zauważyć, że Norwegię, Polskę i Czechy łączą projekty gazowe wchodzące w tym roku w decydującą fazę (np. studium wykonalności i procedura open season dla planowanego gazociągu Baltic Pipe), które mogą zagrozić dominacji rosyjskiego Gazpromu w regionie Europy Środkowej. Chodzi o kwestię budowy tzw. Korytarza Norweskiego, w skład którego wejdzie rurociąg pomiędzy Polską i Danią oraz łącznik z szelfem na Morzu Północnym. Dzięki tej infrastrukturze gaz z Norwegii dotrze do Polski.

Tymczasem kraje Grupy Wyszehradzkiej przy wsparciu Unii Europejskiej przygotowują sieć gazociągów, które je zintegrują. To tzw. Korytarz Północ-Południe, który będzie mógł rozprowadzać norweskie błękitne paliwo po Europie Środkowej.

Kluczowa w tym kontekście jest budowa polsko-czeskiego łącznika gazowego (chodzi o Stork II, którego los premierzy Polski i Czech omawiali niedawno w Wiśle). Czechy są krajem, który może być ciekawym rynkiem zbytu zarówno dla surowca z szelfu Morza Północnego jak i rosyjskiego napływającego do Europy Środkowej przez Nord Stream, a w przyszłości być może również Nord Stream 2. Kolejną ciekawą kwestią jest decyzja władz w Pradze odnośnie ewentualnego wsparcia Rosjan w zakresie budowy łącznika gazowego z Austrią (projekt Baci), która chciałaby integracji z Gazociągiem Północnym 2.

Wszystko to składa się na grę wywiadów, w której informacje są na wagę złota. Można je uzyskać nie tylko za pomocą klasycznych metod wywiadowczych, ale również dzięki skutecznym cyberatakom.

Warto nadmienić, że rosyjscy hakerzy wielokrotnie w przeszłości prowadzili kampanie szpiegowskie w sektorze energetycznym, który jest dla nich absolutnie kluczowy, ze względu na charakter ich gospodarki. Z rozległych działań szpiegowskich znana była np. grupa „Diuków" zidentyfikowana przez firmę F-Secure w 2015 roku. Sposoby jej działania opierały się także na wysyłaniu spreparowanych wiadomości poczty elektronicznej zawierających złośliwe dokumenty Word i PDF.

Inne cele Rosji

Oczywiście wątek energetyczny może być tylko jednym z elementów łączącym te trzy państwa. Czechy mogły stać się celem ze względu na aresztowanie rosyjskiego hakera Jewgienij Nikulina, które miało miejsce w Czechach. Obecnie czeka on na ekstradycję do Stanów Zjednoczonych (również Rosja zażądała jego ekstradycji). Oskarżono go o włamania na strony takich mediów społecznościowych, jak Formspring, LinkedIn and Dropbox.

W przypadku Norwegii zainteresowanie rosyjskie może wiązać się również ze zwiększoną aktywnością wojsk amerykańskich w tym kraju. Chodzi o dyslokację żołnierzy piechoty morskiej, którzy mają przejść przeszkolenie w warunkach arktycznych.

W przypadku Polski może chodzić o podobne kwestie oraz przyszłości relacji polsko-białoruskich, które nowy rząd próbuje na nowo ustabilizować.

Ostatnim powodem może być po prostu chęć przetestowania zabezpieczeń państw NATO przez rosyjskich hakerów. Prawdopodobieństwo tej tezy rośnie wraz z ostatnim atakiem wymierzonym na

sektor bankowy w Polsce, dysponujący najlepszymi zabezpieczeniami.

Operacje APT 28 i APT 29 powinny być lekcją dla politycznych decydentów, że Rosja coraz częściej będzie korzystała z cyberataków do realizowania swoich celów politycznych. Dlatego kwestia cyberbezpieczeństwa powinna być potraktowana z należytą powagą.

Andrzej Kozłowski, Piotr Maciążek