aut. Jakub Wiech 23.03.2018

CYBERNETYCZNA WOJNA OJCZYŹNIANA: ROSYJSCY HACKERZY PLANUJĄ ATAK NA AMERYKAŃSKI SEKTOR ENERGETYCZNY

Hakerzy pod egidą rosyjskiego rządu dopuszczają się cyberataków na energetyczną infrastrukturę krytyczną Stanów Zjednoczonych – taki alert wysłała 15 marca amerykańska rządowa jednostka ds. walki z zagrożeniami informatycznymi US-CERT. Ostrzeżenie to jest efektem analiz Departamentu Bezpieczeństwa Wewnętrznego (DHS) i Federalnego Biura Śledczego (FBI). Doniesieniom administracji i służb wtórują media, które sugerują, że cyberataki na ukraińskie elektrownie z grudnia 2015 roku były rozgrzewką dla rosyjskich hakerów przed starciem z USA.

18 sierpnia 1941 roku około godziny 20:30, żołnierze NKWD **wysadzili tamę** na rzece Dniepr w Zaporożu, będącą elementem **Dnieprzańskiej Elektrowni Wodnej**. Rozkaz zniszczenia tej budowli wydał sam Józef Stalin. Wybuch wyrwał w tamie dziurę długości około 150 metrów, przez którą przedostała się woda, tworząc **gigantyczną falę uderzeniową**. Miało to uniemożliwić Niemcom przebycie Dniepru po prospekcie Lenina, który biegł na koronie zapory. Powstałe wskutek wybuchu **„dnieprzańskie tsunami”** miało też uderzyć w znajdujące się w strefie przybrzeżnej **niemieckie wojska**. Jednakże, wysadzenie tamy nie przyniosło nazistom znaczących strat (zginęło około 1500 żołnierzy). Okazało się jednak prawdziwą **hekatombą miejscowej ludności**. Fala tocząca się po Dnieprze **przyniosła śmierć 120 tysiącom osób**, zamieszkałych w przybrzeżnych miejscowościach. Choć o ofiarach tych nawet na Ukrainie mało kto pamięta, to właśnie tę historię przywołuje poczytny portal The Hill już na wstępie swego artykułu o **rosyjskim zagrożeniu cybernetycznym dla amerykańskiej infrastruktury energetycznej**. To wstęp do tekstu, który wskazuje na istnienie rosyjskiej tradycji atakowania sektora energii.

The Hill, amerykańskie medium opisujące kulisy waszyngtońskiej i międzynarodowej polityki, **zestawia bowiem wydarzenia sprzed prawie 80 lat z historią najnowszą**, a konkretnie z wypadkami, które miały miejsce 23 grudnia 2015 roku. Wtedy też, ta sama elektrownia wodna została **ponownie zaatakowana** przez rosyjskie siły. Tym razem jednak, był to atak **cybernetyczny**, dokonany za pośrednictwem maleware’u (złośliwego oprogramowania) zwanego Black Energy.

Atak na ukraińską sieć energetyczną z 2015 roku to **pierwsza w historii udana cybernetyczna akcja ofensywna przeciwko infrastrukturze energetycznej**. Hakerzy, którzy jej dokonali byli w stanie naruszyć systemy trzech dystrybutorów energii na Ukrainie i czasowo odłączyć przesył prądu do odbiorców.

Najbardziej ucierpieli klienci spółki Prikarpatiaoblenergo. Ze względu na **odcięcie 30 podstacji, około 230 tysięcy osób zostało bez energii**. Dystrybutor potrzebował nawet 6 godzin, by opanować sytuację. Cyberatak dotknął też odbiorców usług Czerniowiecoblenergo oraz Kijowoblenergo. Tam rozmiar strat był jednak znacznie mniejszy.

Jak poinformowały władze tych spółek, ataki były prowadzone z komputerów, które **znajdowały się na terytorium Federacji Rosyjskiej.**

Przykłady z Ukrainy został przywołane nie bez powodu. 15 marca amerykańska jednostka ds. walki z zagrożeniami informatycznymi US-CERT opublikowała **alert dotyczący rosyjskiego zagrożenia dla amerykańskiego systemu energetycznego**. Specjaliści pracujący dla rządu USA nie pozostawiają miejsca na domysły – **mówią wprost o niebezpieczeństwie i działaniach ofensywnych ze strony „podmiotów powiązanych z rosyjskim rządem”**. Według ekspertów, rosyjscy hackerzy mieli od marca 2016 roku penetrować m.in. sektor elektroenergetyki oraz sieci amerykańskich elektrowni jądrowych. Jest to zatem pierwszy w historii przypadek, gdy Stany Zjednoczone otwarcie oskarżyły Rosję o atak hackerski na ich infrastrukturę energetyczną.

„Departament Bezpieczeństwa Wewnętrznego oraz FBI uznają tę działalność za wielopoziomową kampanię naporową prowadzoną przez **podmioty związane z rosyjskim rządem**, które za swój cel biorą sieci małych przedsiębiorstw, gdzie instalują złośliwe oprogramowanie, przeprowadzają ataki phishingowe oraz uzyskują zdalny **dostęp do sieci sektora energetycznego**. Po uzyskaniu dostępu, te powiązane z rosyjskim rządem podmioty przeprowadzają rozpoznanie sieciowe i zbierają informacje dotyczące dostępu do Systemu Kontroli Przemysłowej (Industrial Control Systems, ICS)” – napisał w swoim ostrzeżeniu US-CERT.

Niezwykła kategoryczność oraz ton alertu przykuła uwagę mediów. Wspomniany już The Hill w tytule artykułu opisującego doniesienia US-CERT stwierdził, że Rosja „zrobiła już rozgrzewkę” przed „zmasowanym atakiem na sieć elektroenergetyczną USA”. O zagrożeniu pisały też inne czołowe redakcje: Politico, Bloomberg, Agencja Reutera. Z treści tych przebijał jeden, spójny komunikat: **Stany Zjednoczone wskazują Rosję jako zagrożenie ich bezpieczeństwa energetycznego.**

W jeszcze ostrzejszym tonie wypowiedział się **sekretarz energii USA, Rick Perry**. W swoim wystąpieniu przed senacką komisją służb zbrojnych powiedział on, że rosyjskie cyberataki na amerykańską energetykę to **„akt wojny”.**

O wojennych nastrojach za oceanem poświadczyć może styl, w jakim The Hill kończy swój artykuł o rosyjskich cyberatakach. Jak żywo przypomina on wydźwiękiem poezję tyrtejską. „Niech chuligani dowiedzą się, że **jest cena za zaatakowanie naszej infrastruktury** krytycznej i za kradzież naszej technologii. Amerykańska opinia publiczna musi wiedzieć, że nasz kraj odpowiedział w sposób znaczący. **Nie trzeba mówić o tym bezpośrednio. Wystarczy, że będziemy słyszeć, iż ktoś gdzieś płaci właśnie swoją cenę za zaatakowanie Stanów Zjednoczonych**”.

Czy zatem można przyjąć, że **cyberwojna amerykańsko-rosyjska wisi na włosku**? Niestety, symptomów, które wskazują na przygotowania do takiego konfliktu jest bardzo dużo. W sierpniu ubiegłego roku jeden z zakładów przedsiębiorstwa petrochemicznego **w Arabii Saudyjskiej padł ofiarą cyberataku**. Celem było dokonanie sabotażu i doprowadzenie do eksplozji. Nie udało się dotychczas zidentyfikować sprawców. Jak podaje portal CyberDefence24, musieli posiadać bardzo zaawansowane umiejętności i zasoby. Według osób prowadzących śledztwo, które chciały zachować anonimowość, w **operacje musiał być zaangażowany rząd innego państwa** (Rosja znalazła się w kręgu podejrzanych). Ich zdaniem jedynie błędny kod w komputerach atakujących zapobiegł eksplozji.

Co ważne, saudyjski zakład posiada **amerykańskie oprogramowanie**, które używane jest w ponad 18 tysiącach obiektów infrastruktury technicznej na całym świecie. James A. Lewis z waszyngtońskiego think-tanku Center for Strategic and International Studies powiedział w wywiadzie dla The New York Times, że atakujący mogą użyć tej samej techniki w Stanach Zjednoczonych co w Arabii Saudyjskiej przeciwko tym samym rozwiązaniom technologicznym. **Warto zaznaczyć, że USA to strategiczny partner biznesowy i militarny Arabii Saudyjskiej**.

Natomiast w lipcu 2017 roku, amerykańskie media doniosły, że celem cyberataku stała się **elektrownia jądrowa w Wolf Creek** w stanie Kansas. Hackerzy, którzy włamali się do jej systemów, mieli mapować strukturę sieci, by przygotowywać plany przyszłych uderzeń.

Czy biorąc pod uwagę powyższe okoliczności, można przewidywać **rychły wybuch cyberwojny**? Wydaje się, że społeczność międzynarodowa coraz bardziej oswaja się z perspektywą takiego konfliktu. Na anglojęzycznej Wikipedii można już znaleźć hasło *Cyberwarfare by Russia (ang. Cyberwojny prowadzone przez Rosję)*. Zawiera ono opisy ataków cybernetycznych i innych podobnych akcji, za które odpowiedzialne ma być państwo Władimira Putina. Na liście zaatakowanych krajów znajdują się m.in. Estonia, Francja, Gruzja, Niemcy i właśnie USA. Miejmy nadzieję, że zestawienie to **nie poszerzy się o hasło** „*amerykańsko-rosyjska wojna cybernetyczna*".