Krakowskie Studia Małopolskie
2017, nr 22

Karol Piękoś

ATAKI CYBERNETYCZNE NA SYSTEMY BANKOWE ORAZ INFRASTRUKTURĘ KRYTYCZNĄ – ANALIZA WYBRANYCH PRZYPADKÓW

Pojęcie infrastruktury krytycznej jest stosunkowo nowe, jednak ochrona tego kluczowego obszaru jest prowadzona od czasów starożytnych. Wówczas nie wyodrębniano infrastruktury krytycznej organizacyjnie oraz nie definiowano czym jest. Pomimo to prowadzono już określone działania na rzecz zabezpieczenia niektórych obiektów w państwie, ponieważ zdawano sobie sprawę z ich kluczowego znaczenia dla funkcjonowania organizacji państwowej. W starożytnym Egipcie ważną rolę dla działania państwa odgrywały spichlerze oraz system irygacyjny. W przypadku Fenicjan taką rolę pełniły porty morskie oraz urządzania potrzebne do budowy okrętów, za pomocą których kontrolowano morskie szlaki wodne[1].

Infrastrukturą krytyczną nazywamy rzeczywiste oraz cybernetyczne systemy, które są niezbędne do minimalnego funkcjonowania gospodarki i państwa. Nie każdy obiekt o charakterze strategicznym należy do infrastruktury krytycznej. Przynależność danego obiektu do tego systemu jest ściśle określona przez kryteria wskazane w niejawnym załączniku Narodowego Programu Infrastruktury Krytycznej[2].

Zgodnie z ustawą o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. infrastruktura krytyczna obejmuje następujące systemy:

a) zaopatrzenia w energię, surowce energetyczne, paliwa;
b) łączności;
c) sieci teleinformatycznych;

[1] K. Stec, *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, „Bezpieczeństwo Narodowe" 2011, nr 19, s. 181.

[2] *Infrastruktura krytyczna*, http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 9.12.2017].

d) finansowe;
e) zaopatrzenia w żywność;
f) zaopatrzenia w wodę;
g) ochrony zdrowia;
h) transportowe;
i) ratownicze;
j) zapewniające ciągłość działania administracji publicznej;
k) produkcji składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[3].

Szczególne znaczenie infrastruktury krytycznej dla właściwego funkcjonowania państwa powoduje, że jest ona poddana szczególnej ochronie. Ścisłe zdefiniowanie czym jest infrastruktura krytyczna wymusiło na organach państwowych wskazanie podmiotów właściwych do zarządzania infrastrukturą krytyczną oraz jej ochrony. Nie było by to możliwe bez stworzenia podstaw prawnych, które są fundamentem dla funkcjonowania systemu ochrony kluczowych dla państwa obszarów. Bardzo ważną rolę dla ochrony infrastruktury krytycznej pełni współpraca publiczno-prywatna[4]. Dzięki współdziałaniu możliwe jest poprawienie warunków bezpieczeństwa oraz stworzenie przejrzystych zasad i procedur. Jest to istotne, ponieważ wiele obiektów infrastruktury krytycznej obecnie należy do podmiotów prywatnych.

Współpraca sektora prywatnego i państwowego polega na:
- wymianie informacji;
- stworzeniu kanałów informacji dla sygnałów alarmowych, nadawanych ze służb państwowych;
- zapewnieniu bezpieczeństwa danym, które są tajemnicą handlową, pochodzącym od operatorów[5].

Minister cyfryzacji Anna Streżyńska w listopadzie 2016 r. na antenie Radia Z stwierdziła, że w Polsce mają miejsce ataki na infrastrukturę krytyczną oraz instytucje finansowe z poza Polski[6]. Nie jest wiadome z jakich kierunków

---

[3] Dz.U. 2017, poz. 209, 1566.

[4] J. Trubalska, *Wybrane aspekty ochrony infrastruktury krytycznej w Polsce*, „Zeszyty Naukowe WSEI. Seria Administracja" 2015, nr 1, s. 116.

[5] Infrastruktura krytyczna – współpraca z biznesem, http://rcb.gov.pl/infrastruktura-krytyczna-wspolpraca-z-sektorem-prywatnym/ [dostęp: 9.12.2017].

[6] [b.a], *Polska na celowniku hakerów. Streżyńska: ,,Na instytucje finansowe oraz infra-*

pochodziły prowadzone działania mające na celu zakłócenie funkcjonowania kluczowych dla bezpieczeństwa państwa obiektów ani jaki wpływ na działanie infrastruktury krytycznej miały te ataki.

Na świecie tego typu ataki często okazują się skuteczne oraz szkodliwe w skutkach. Przykładem jest atak hakerów na elektrownię znajdującą się w Zaporożu. Nagła awaria elektrowni miała miejsce 23 grudnia 2016 r. Z powodu zatrzymania jej pracy bez dostępu do energii elektrycznej pozostało około 700 tys. gospodarstw domowych. Ukraińskie władze o atak oskarżyły Rosję[7]. Eksperci firmy antywirusowej ESET poinformowali, że przerwa w dostawie prądu prawdopodobnie była spowodowana działaniem zagrożeń BlackEnergy oraz KillDisk, które atakujący zainstalowali na komputerach pracowników jednego z lokalnych dostawców energii[8].

Kolejny poważny atak hakerski na Ukrainie miał miejsce w czerwcu 2017 r. Działania hakerów zostały wymierzone w system bankowy i telekomunikacyjny, najważniejsze lotniska w kraju, rządowe sieci komputerowe, elektrownie, ciepłownie oraz metro w Kijowie. W ataku został wykorzystany wirus Petya, który potrafi szyfrować komputery. Za odblokowanie twórcy szkodliwego oprogramowania żądali od ofiary 300 dolarów okupu w kryptowalucie bitcoin. Według Antona Heraszczenko, ówczesnego doradcy szefa MSW i deputowanego do ukraińskiego parlamentu, za atak odpowiedzialna jest Rosja.

Pierwszą instytucją, która informowała o ataku był Narodowy Bank Ukrainy. Wówczas sygnalizowano że istnieją problemy z realizowaniem płatności i obsługą klientów. Działania hakerów doprowadziły do wstrzymania operacji finansowych jednego z największych banków Ukrainy, Oszczadbanku. Problemy z płatnościami były sygnalizowane przez kijowskie metro. Hakerzy zaatakowali w tym samym czasie również sektor energetyczny oraz porty lotnicze w Boryspolu pod Kijowem i portu lotniczego Kijów. Działania hakerów nie doprowadziły jednak do wstrzymania lotów.

---

strukturę krytyczną przypuszczane są ataki spoza naszego kraju", https://wpolityce.pl/polityka/314490-polska-na-celowniku-hakerow-strezynska-na-instytucje-finansowe-oraz-infrastrukture-krytyczna-przypuszczane-sa-ataki-spoza-naszego-kraju?strona=2 [dostęp: 9.12.2017].

[7] [b.a], *„Milowy krok" w działalności hakerów. Wyłączyli wielką elektrownię*, https://www.tvn24.pl/wiadomosci-ze-swiata,2/awaria-elektrowni-na-ukrainie-i-700-tys-domow-bez-pradu,608526.html [dostęp: 19.12.2017].

[8] [b.a], *Cyberatak wstrzymał dostawy prądu na Ukrainie*, eset.pl, https://www.eset.pl/O_nas/Centrum_prasowe/Aktualnosci,news_id,11207 [dostęp: 9.12.2017].

Z powodu ataku problemy pojawiły się również w nieczynnej elektrowni, która znajduje się w Czarnobylu. Rozprzestrzeniający się wirus spowodował, że zainfekowano sieć komputerową znajdującego się tam obecnie zakładu przechowującego zużyte paliwo jądrowe. Działania hakerów doprowadziły również do awarii strony internetowej elektrowni.

W tym samym czasie ofiarami ataku stały się również instytucje na całym świecie, głównie w Rosji oraz USA. W przypadku Rosji doszło do zainfekowania systemu Banku Centralnego tego kraju oraz kilku przedsiębiorstw. W USA zaatakowano koncern farmaceutyczny Merck[9].

Wykorzystane do ataku oprogramowanie miało na celu niszczenie danych lub usuwanie informacji o przeprowadzanych operacjach. Skutki takiego działania są trudne do oceny. Wstrzymanie funkcjonowania systemów informatycznych oraz proces odzyskiwania danych szacuje się na miliardy dolarów. Finansowe straty ataku są istotne, ale w dłuższej perspektywie bardziej szkodliwe mogą okazać się skutki o charakterze politycznym i biznesowym. Państwo, które jest narażone na różnego rodzaju ataki przeprowadzane z wykorzystaniem systemów informatycznych może wiele stracić, np. wysokotechnologiczne wsparcie nie zostanie przekazane Ukrainie w przyszłości, zaś inwestorzy ograniczą środki przeznaczone na inwestycje. Zmasowane ataki mogą również w znaczącym stopniu przyczyniać się do destabilizacji politycznej określonego państwa. Natychmiastowa ocena skutków takich ataków jest zatem niemożliwa[10].

Do ataków hakerskich na elektrownie doszło również w Korei Południowej. W 2014 r. systemy komputerowe operatora elektrowni jądrowych w tym kraju zostały złamane. W grudniu 2014 r. władze Korei Południowej poinformowały, że posiadają możliwości pozwalające na zablokowanie prób infiltracji, prowadzonych przez cyberprzestępców. Śledczy z tego kraju ustalili, że adres IP komputera, za pomocą którego w sieci nastąpiła publikacja wykradzionych dokumentów pochodzi z Korei Południowej. Zatrzymany twierdził jednak, że nie ma nic wspólnego z atakiem[11].

---

[9] [b.a], *Fala zmasowanego ataku hakerskiego rozlewa się na kolejne kraje. Wirus może być trudny do pokonania*, https://www.polskieradio.pl/42/273/Artykul/1782264,Fala-zmasowanego-ataku-hakerskiego-rozlewa-sie-na-kolejne-kraje-Wirus-moze-byc-trudny-do-pokonania [dostęp: 9.12.2017].

[10] M. Tomaszkiewicz, *Czołgi nie wjechały, ale cyberatak będzie kosztował Ukrainę więcej niż nalot dywanowy*, http://www.newsweek.pl/swiat/cyberatak-na-ukrainie-skutki-wieksze-niz-po-nalocie-dywanowym,artykuly,412567,1.html [dostęp: 9.12.2017].

[11] [b.a], *Korea Płd.: atak hakerski na elektrownię jądrową. Wykradziono informacje bez*

Firma Korea Hydro and Nuclear Power, która jest operatorem zaatakowanej elektrowni jądrowej przyznała, że nie ma zagrożenia dla instalacji jądrowych, w tym 23 reaktorów. Do ataków przyznał się jeden z użytkowników portalu społecznościowego Twitter, który domagał się wyłączenia trzech generatorów starszej generacji. Twierdził on, że jest przywódcą grupy posiadającej swoją siedzibę na Hawajach, która sprzeciwia się energetyce jądrowej. Użytkownik uważający się za lidera tej organizacji groził, że w przypadku niespełnienia postawionego przez niego ultimatum opublikuje kolejne informacje dotyczące elektrowni. Prokuratura z Seulu prowadziła wówczas śledztwo, które dotyczyło wycieku danych dotyczących zaatakowanej elektrowni. Wśród udostępnionych plików pojawiły się plany reaktorów jądrowych oraz koszty zużycia energii elektrycznej i narażenia na promieniowanie[12].

Kolejny poważny atak hakerski miał miejsce w Korei Południowej w 2016 r. O zdarzeniu poinformował Lee Cheol-hee, członek rządzącej Partii Demokratycznej, rok po incydencie. Atakujący zdołali się włamać do centrum danych obrony. Hakerom udało się wykraść plany operacyjne 5015. Dotyczyły one działań na wypadek wojny Korei Południowej i USA z Koreą Północną. Według dostępnych informacji wykradziono 235 gigabajtów danych, z czego 80% nie zostało wówczas zidentyfikowane. Zdaniem Ministerstwa Obrony Korei Południowej, władze Korei Północnej zdobyły informacje na temat południowokoreańskich elektrowni oraz rozmieszczenia wojsk[13].

Współcześnie państwa są zmuszone do prowadzenia szerokich działań, mających na celu ochronę wrażliwych obszarów, które są kluczowe dla bezpieczeństwa. Konsekwencje cyberataków na Infrastrukturę Krytyczną mogą być podobne do strat wywołanych innymi zdarzeniami. Istotny jest fakt, że mogą one mieć wpływ nie tylko na system teleinformatyczny[14].

---

znaczenia?, http://www.tvp.info/18160728/korea-pld-atak-hakerski-na-elektrownie-jadrowa-wykradziono-informacje-bez-znaczenia [dostęp: 9.12.2017].

[12] [b.a], *Trzech zabitych po awarii w elektrowni atomowej w Korei Południowej*, https://www.polskieradio.pl/5/3/Artykul/1336081,Trzech-zabitych-po-awarii-w-elektrowni-atomowej-w-Korei-Poludniowej [dostęp: 9.12.2017].

[13] [b.a], *Korea Południowa: reżim Kim Dzong Una wykradł tajne plany wojny*, http://wiadomosci.onet.pl/swiat/korea-poludniowa-rezim-kim-dzong-una-wykradl-tajne-plany-wojny/fyme0y9 [dostęp: 9.12.2017].

[14] *Cyberataki mogą stać się kluczowym zagrożeniem dla infrastruktury krytycznej*, http://rcb.gov.pl/cyberataki-moga-stac-sie-kluczowym-zagrozeniem-dla-infrastruktury-krytycznej/ [dostęp: 9.12.2017].

Częstym celem ataków hakerów są również systemy bankowe współczesnych państw. Jest to bardzo istotny obszar z punktu widzenia państwa, ale i obywateli. Współcześnie instytucje bankowe odgrywają bardzo ważną rolę na wielu poziomach. Systemem bankowym określamy całokształt instytucji bankowych oraz normy, które definiują ich wzajemne zależności oraz powiązania z otoczeniem. W gospodarce rynkowej modelowym przykładem systemu bankowego jest tzw. dwuszczeblowy system bankowy. W skład tego systemu wchodzi bank centralny oraz szereg banków funkcjonujących na określonych rynkach finansowych. System bankowy jest częścią rynku finansowego.

Polski system bankowy składa się z trzech grup instytucji: stabilizujących, tworzących rynek oraz pomocniczych. Instytucjami stabilizującymi określamy te organy, które są odpowiedzialne za nadzorowanie właściwego funkcjonowania całego systemu. W skład instytucji stabilizujących wchodzi:

- bank centralny, w Polsce jest to Narodowy Bank Polski, który odpowiada za regulowanie płynności banków oraz wspieranie stabilności finansowej;
- organ nadzorujący (Komisja Nadzoru Finansowego), zajmująca się kontrolą dotyczącą prowadzenia działalności bankowej;
- instytucja gwarantująca wypłatę depozytów, którą jest Bankowy Fundusz Gwarancyjny.

Instytucjami tworzącymi system bankowy, które działają w ramach określonego porządku w Polsce, są: banki komercyjne, spółdzielcze oraz oddziały instytucji kredytowych. Instytucjami pomocniczymi określamy podmioty, które nie prowadzą działalności depozytowo-kredytowej, np. Związek Banków Polskich, instytucje ubezpieczające, Krajowy Depozyt Papierów Wartościowych[15].

Ataki na systemy bankowe stają się coraz bardziej popularne wśród cyberprzestępców. Skala zjawiska jest zdecydowanie większa niż przed kilkoma laty. Związane jest to z tym, że liczba osób korzystających z bankowości elektronicznej rośnie. Skuteczny atak na system bankowy może mieć bardzo poważne konsekwencje nie tylko dla zaatakowanej instytucji, ale i klientów.

W lutym 2017 r. media w Polsce, ale i poza jej granicami obiegła informacja o zmasowanym ataku na polski system bankowy. Zdaniem ekspertów do spraw bezpieczeństwa z firmy Symatec oraz BAE Systems, przeprowadzone ataki są powiązane z grupą Lazarus, która jest podejrzewana o szereg zma-

[15] *System bankowy*, https://www.nbportal.pl/slownik/pozycje-slownika/system-bankowy [dostęp: 9.12.2017].

sowanych akcji na całym świecie. Atak na polskie banki zaczął się od zainfekowania strony internetowej Komisji Nadzoru Finansowego. Rzecznik KNF potwierdził, że doszło do próby ingerencji w system informatyczny, który obsługiwał stronę internetową instytucji[16].

Atak został potwierdzony przez wiele banków. Nie istnieją dowody na to, by hakerzy w ramach ataku ukradli pieniądze klientów. Widoczny był jednak transfer danych. Według firmy Symatec zablokowano wiele innych ataków, które zostały przeprowadzone przy użyciu tych samych narzędzi, wykorzystanych do zainfekowania banków w Polsce. Tego typu ataki dotyczyły nie tylko Polski, ale również Urugwaju oraz Meksyku[17].

Do ataku wykorzystano tzw. taktykę wodopoju. Polega ona na zaatakowaniu konkretnej organizacji. Następnie hakerzy obserwują z jakich stron internetowych korzysta ofiara, by zainfekować te witryny szkodliwym oprogramowaniem. Powoduje to, że wirusy przenoszą się na kolejne komputery, które są celem ataku. Według KNF poszkodowanych zostało ponad dwadzieścia polskich banków. Nie jest wiadome kto stał za atakiem na polski system bankowy. Zdaniem ekspertów z „New York Times" akcję przeprowadziła Korea Północna[18].

Zmasowane ataki, które zagrażają stabilności państw powodują, że coraz częstsze są działania, które mają na celu sprawdzanie odporności systemu na wszelkiego rodzaju zagrożenia. W 2017 r. Bank Litwy przeprowadził ćwiczenia, w których sprawdzano odporność podmiotów będących częścią litewskiego systemu finansowego, na ataki cybernetyczne. W trakcie symulacji ataków sprawdzano jak chroniona jest infrastruktura oraz jak jest zabezpieczona dostępność usług elektronicznych. Sprawdzeniu podlegały również procedury zarządzania ryzykiem cybernetycznym oraz kwestia ich przestrzegania. Według

---

16 [b.a], *KNF potwierdza fakt ataku hakerskiego na stronę urzędu. Celem hakerów były dane instytucji finansowych, a nie pieniądze klientów?*, http://wgospodarce.pl/informacje/33274-knf-potwierdza-fakt-ataku-hakerskiego-na-strone-urzedu-ocenia-ze-system-bankowy-nie-jest-zagrozony [dostęp: 9.12.2017].

17 P. Paganini, *According to security experts from Symantec and BAE Systems, the recently discovered attacks aimed at Poland banks are linked to the Lazarus Group*, http://securityaffairs.co, http://securityaffairs.co/wordpress/56235/apt/lazarus-group-polish-bank.html [dostęp: 9.12.2017].

18 [b.a], *Cyberatak na KNF przez północnokoreańskich hakerów był bardzo wyrafinowany*, https://www.polskieradio.pl/42/1699/Artykul/1745452,Cyberatak-na-KNF-przez-polnocnokoreanskich-hakerow-byl-bardzo-wyrafinowany [dostęp: 9.12.2017].

specjalistki litewskiego banku centralnego tamtejsze systemy informatyczne komercyjnych banków poradziły sobie z imitowanymi atakami, co jej zdaniem potwierdza, że tamtejszy system jest przygotowany na tego typu zagrożenia[19].

Postępujący rozwój technologiczny oraz informatyzacja powodują, że wraz z wieloma udogodnieniami oraz możliwościami, pojawia się szereg nowych, kiedyś nieistniejących zagrożeń. W dobie powszechnych ataków hakerskich istotne z punktu widzenia państwa jest zabezpieczenie kluczowych obszarów, takich jak system bankowy oraz infrastruktura krytyczna. Wielość zagrożeń powoduje, że konieczną rzeczą staje się tworzenie wyspecjalizowanych komórek odpowiedzialnych za zajmowanie się cyberbezpieczeństwem. Jest to bardzo trudne zadanie, stojące przed współczesnymi państwami, którego realizacja staje się konieczna z punktu widzenia bezpieczeństwa i ochrony własnych interesów.

Summary

Nowadays hacker attacks on computers or smartphones of everyday users have become commonplace. Unfortunately, increasing number of sophisticated attacks are being targeted against critical infrastructure or banking systems. The threat from hackers is very serious. As a result, institutions exposed to the attacks are obliged to take action to repulse them, because the consequences of intrusions into internal systems can be far-reaching. Numerous cases of effective hacker activities are not rare, as shown by cases from recent years.

Keywords: critical infrastructure, banking system, hacker attack, operating system, safety

[19] K. Januszkiewicz, *Bank Litwy sprawdził odporność banków na ataki hakerskie*, https://lithuania.trade.gov.pl/pl/aktualnosci/251324,bank-litwy-sprawdzil-odpornosc-bankow-na-ataki-hakerskie.html#.WYAnNCxW57Q.facebook [dostęp: 9.12.2017].