RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

ZARZĄDZANIE KRYZYSOWE WOBEC NOWEGO TYPU ZAGROŻEŃ – SPOTKANIE EKSPERCKIE W RZĄDOWYM CENTRUM BEZPIECZEŃSTWA 3

DEZINFORMACJA – ROSYJSKA BROŃ STRATEGICZNA 6

ZJAWISKA MIGRACYJNE JAKO POTENCJALNE NARZĘDZIA WOJNY HYBRYDOWEJ 9

GLOBALNE ATAKI CYBERNETYCZNE 12

ZESPÓŁ CERT DLA SEKTORA ELEKTROENERGETYCZNEGO – DZIAŁANIA DLA REALNEJ OCHRONY INFRASTRUKTURY KRYTYCZNEJ W POLSCE I EUROPIE 16

NUMER 19 KWIECIEŃ – CZERWIEC 2017

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz – Zastępca Dyrektora RCB

Martyna Olejnik

Anna Zasadzińska-Baraniewska

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Zarządzanie kryzysowe wobec nowego typu zagrożeń – spotkanie eksperckie w Rządowym Centrum Bezpieczeństwa

Anna Zasadzińska-Baraniewska
Rządowe Centrum Bezpieczeństwa

11 maja 2017 r. w Rządowym Centrum Bezpieczeństwa odbyło się seminarium eksperckie zatytułowane ***„Odporność państwa na współczesne zagrożenia – wyzwania dla zarządzania kryzysowego”****.*

Fot. Dominik Mikołajczyk RCB

Tematyka spotkania, zorganizowanego wspólnie przez RCB i Wyższą Szkołę Policji w Szczytnie, koncentrowała się na nowego typu czynnikach niosących ryzyko destabilizacji szeroko pojętego środowiska bezpieczeństwa. Zagrożenia te, powszechnie określane jako hybrydowe, stanowią wyzwanie tym poważniejsze, że dotyczą wielu dziedzin i aspektów funkcjonowania państw i społeczeństw, od polityki, gdzie widoczne są próby wpływania na przebieg i wyniki procesów wyborczych, przez infrastrukturę narażoną na cyberataki aż po ochronę granic.

Wybrane elementy tej szerokiej problematyki omówione zostały przez ekspertów w ramach dwóch bloków tematycznych. Pierwszy dotyczył zagrożeń związanych z dezinformacją ze względu na skalę określaną często jako wojna informacyjna, oraz negatywnych zjawisk głównie z zakresu cyberbezpieczeństwa identyfikowanych jako poważny czynnik ryzyka dla ciągłości funkcjonowania systemów państwowych. Druga część seminarium poświęcona była problemom migracji w jej różnych aspektach – od nacisku migracyjnego i reakcji aparatu państwa na tę złożoną sytuację po działania podejmowane w zakresie ochrony granicy zewnętrznej Unii Europejskiej.

Dzięki uprzejmości ekspertów uczestniczących w spotkaniu, **dwa z poruszonych tematów możemy przedstawić Czytelnikom w aktualnym Biuletynie w pogłębiony sposób.** Na kolejnych stronach znajdą Państwo artykuł dr Jolanty Darczewskiej z Ośrodka Studiów Wschodnich omawiający zagadnienie dezinformacji jako rosyjskiej broni strategicznej oraz opracowanie płk SG Jacka Wysokińskiego analizujące zjawiska migracyjne, jako potencjalne narzędzia wojny hybrydowej. Podczas spotkania w RCB doradca Ministra Obrony Narodowej Kamil Basaj przedstawił na wybranych przykładach podstawowe techniki oddziaływania informacyjnego obcych ośrodków. Zwrócił uwagę przede wszystkim na wykorzystywanie ingerencji w sferę logicznego myślenia, zniekształcanie przestrzeni informacyjnej czy, bardziej

ogólnie, kształtowanie środowiska poznawczego poprzez działania rozproszone realizowane w różnorodnym środowisku informacyjnym. Osiąganie pożądanych skutków możliwe jest poprzez oddziaływanie informacyjne za pomocą narzędzi socjotechnicznych, językowych mechanizmów perswazji czy konsekwentne stosowanie zasady długotrwałego przekazu.

Ekspert reprezentujący Służbę Kontrwywiadu Wojskowego, Karol Molenda zaprezentował odnotowane w ostatnich miesiącach przykłady incydentów związanych z próbami ataków informatycznych na urzędy i instytucje administracji państwowej.

Z tematem tym wiąże się wyzwanie, jakim jest wzmacnianie odporności państwa, zwłaszcza w zakresie zapewnienia ciągłości funkcjonowania newralgicznych systemów i usług oraz zależności między ciągłością działania systemów infrastruktury krytycznej oraz ciągłością działania administracji państwowej. Zagadnienie to zostało wyczerpująco ujęte i usystematyzowane w wystąpieniu przedstawiciela Rządowego Centrum Bezpieczeństwa Adama Politowskiego. Podkreślił on, że odporny system, którego zbudowanie stanowi fundamentalny warunek zapewnienia bezpieczeństwa obywateli, powinien: efektywnie odpowiadać na incydenty, dostosowywać się do nowych warunków, funkcjonować zgodnie ze standardem na wcześniej ustalonym poziomie, po ewentualnym zakłóceniu powrócić do stanu normalnego funkcjonowania. Dodatkowo powinien charakteryzować się dostępnością, niezawodnością, zdolnością serwisowania oraz bezpieczeństwem technicznym.

Specyfika sytuacji na odcinku wschodnim zewnętrznej granicy Unii Europejskiej, związana ze zwiększoną presją migracyjną obserwowaną od kilkunastu miesięcy na przejściu granicznym Brześć – Terespol, była tematem wystąpienia płk SG Jacka Wysokińskiego, eksperta z Zarządu do Spraw Cudzoziemców Komendy Głównej Straży Granicznej. Nacisk grup obywateli Federacji Rosyjskiej, głównie narodowości czeczeńskiej, podejmujących wielokrotne próby wjazdu na terytorium RP i konieczność adekwatnej reakcji na to zjawisko w skomplikowanych warunkach geopolitycznych i prawnych, stanowią realne wyzwanie dla służb i instytucji państwa, odpowiedzialnych za kształtowanie właściwego środowiska bezpieczeństwa.

Z kolei Jarosław Truchan z Instytutu Bezpieczeństwa i Porządku Publicznego Wyższej Szkoły Policji w Szczytnie, przybliżył wybrane problemy z zakresu sytuacji migracyjnej na południu Europy, dzieląc się wnioskami z podróży studyjnej przedstawicieli WSPol na francuskim wybrzeżu Morza Śródziemnego i obserwacjami co do współdziałania służb francuskich i włoskich na południowym odcinku granicy UE.

Ryzyko dla bezpieczeństwa wewnętrznego państwa jakie stwarza wzrost nielegalnej migracji omówił ekspert Agencji Bezpieczeństwa Wewnętrznego Damian Szlachter. Ostatnie dane Europolu wskazują, że nielegalna migracja stała się jednym z najbardziej dochodowych i wyrafinowanych rodzajów aktywności kryminalnej prowadzonej przez zorganizowane grupy przestępcze na terenie Unii Europejskiej. Prawie każdy nielegalny imigrant docierający do UE jednym ze znanych szlaków migracyjnych korzysta na którymś z etapów swojej podróży z usług grup przestępczych. Problematyka nielegalnej migracji pozostaje w zainteresowaniu ABW przede wszystkim w związku z możliwością wykorzystania istniejących kanałów przerzutu nielegalnych imigrantów przez organizacje terrorystyczne i ekstremistyczne. Nielegalna migracja to także pole działalności przestępczej, której ofiarami stają się sami migranci. Jednym z najbrutalniejszych jej przejawów jest handel ludźmi. Analizę tego zagadnienia oraz narzędzia walki z procederem przedstawił podczas seminarium Michał Grzelec z Wydziału do walki z Handlem Ludźmi Biura Kryminalnego Komendy Głównej Policji.

Kończąca seminarium dyskusja była okazją do wymiany spostrzeżeń i doświadczeń prelegentów i zaproszonych gości, reprezentujących służby, instytucje i urzędy, w tym m. in. Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Zagranicznych, Ministerstwo Rozwoju, Urząd do spraw Cudzoziemców, Biuro Bezpieczeństwa Narodowego, Biuro Ochrony Rządu i Dowództwo Operacyjne Rodzajów Sił Zbrojnych.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Fot. Dominik Mikołajczyk RCB

Rządowe Centrum Bezpieczeństwa cyklicznie od 2012 r. organizuje seminaria eksperckie dotyczące szeroko rozumianego bezpieczeństwa narodowego, nowych czynników ryzyka i zmieniających się warunków bezpieczeństwa, a także innowacyjnych elementów systemu zarządzania kryzysowego. Spotkania takie pozwalają na uruchomienie synergii jaką daje wymiana informacji i współdziałanie urzędów administracji państwowej, instytucji, służb, ośrodków analitycznych i instytutów naukowo-badawczych. Wydaje się, że właśnie takie inicjatywy, oprócz podejmowanych konkretnych działań operacyjnych oraz rozwiązań w sferze legislacji, stanowią warunek stałego wzmacniania odporności państwa i społeczeństwa wobec zagrożeń współczesnego świata.

Fot. Dominik Mikołajczyk RCB

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Dezinformacja – rosyjska broń strategiczna

Jolanta Darczewska
Ośrodek Studiów Wschodnich

Dezinformując i manipulując rzeczywistością Moskwa prowadzi długofalowe działania destabilizacyjne, podsyca konflikty między poszczególnymi państwami NATO i UE, podważa demokratyczny proces wyborczy i europejski system wartości, osłabia projekt integracyjny UE i współpracę transatlantycką, uzasadnia swe prawo do budowania własnej strefy wpływów w Europie. Coraz więcej państw doświadcza konsekwencji tych działań dla bezpieczeństwa narodowego. Budzi to ich zdecydowaną reakcję; skłania państwa NATO i UE do wypracowania mechanizmów ostrzegawczych identyfikujących zagrożenie i przeciwdziałania mu.

Mimo wielu inicjatyw państwowych i społecznych temat pozostaje kontrowersyjny. Rosyjskie fake newsy i oparta na dezinformacji propaganda są bagatelizowane, jako że często trudno je brać na poważnie. W debacie naukowej i eksperckiej temat jest rozproszony, ujmowany jednowymiarowo. Dezinformację rozpatruje się na ogół w jej wąskim znaczeniu, jako sfabrykowane świadectwo, wprowadzające w błąd. Pomija się przy tym jej różnorodne formy organizacyjne jak prowokowanie wydarzeń czy akcji protestu, zakładanie prorosyjskich organizacji bądź portali informacyjnych. Problematyka bezpieczeństwa informacyjnego podlega ponadto swoistej modzie. W centrum uwagi znajduje się ochrona sfery cybernetycznej (pojawiające się strategie cyberbezpieczeństwa podkreślają zagrożenia płynące z cyberprzestrzeni, takie jak cyberszpiegostwo, cyberprzestępczość, cyberwojna, cyberterroryzm itp.), poszerzone ostatnio o cyberataki społecznościowe w internecie (trolling czy propaganda 2.0). Z pola widzenia znikają natomiast socjotechniczne aspekty oddziaływania dezinformacyjnego, zorientowane na wywieranie wpływu, a definiowane w takich terminach jak inspiracja, fortel, propaganda, decepcja, manipulacja, blef, kamuflaż, mistyfikacja i in. Warto też pamiętać, że zniekształcone dane, powodujące awarie urządzeń i obiektów infrastruktury krytycznej, mają wzmacniać wywołane wcześniej negatywne uczucia (lęk, obawa, strach), tj. w ostatecznym rozrachunku wpłynąć na psychikę człowieka.

W tym krótkim artykule podjęto próbę przedstawienia złożoności rosyjskiej strategii dezinformacji. W istocie stanowi ona pojęcie zbiorcze różnych metod wykorzystywanych w przestrzeni fizycznej i informacyjnej, jest syntezą znacznie subtelniejszych niż zwykłe oszustwo technik politycznych, wojskowych, wywiadowczych, biznesowych, dyplomatycznych, medialnych, cybernetycznych, służących realizacji długoterminowych celów polityki Kremla. Z tego choćby względu temat ten wymaga kompleksowego podejścia i oceny – nie z punktu widzenia poszczególnych fejków, ale strategicznych celów Rosji i oczekiwanych przez nią skutków, a także dalszych badań form organizacyjnych i metod dezinformacji, skuteczności rosyjskiego wpływu, jego zasięgu itp.

Obecne problemy państw demokracji zachodniej z dezinformacją wynikają po części z nieznajomości rosyjskiej strategii, po części z „przekładania" jej na własny system pojęć i język interpretacji. Tymczasem rosyjski model refleksji na ten temat jest zasadniczo odmienny od zachodniego. Przede wszystkim dezinformacja jest traktowana jako broń w konfrontacji informacyjnej z Zachodem oraz narzędzie wpływu, indoktrynacji i destabilizacji społeczeństw przeciwnika. Oznacza proces ciągły, polegający na systemowej zintegrowanej aktywności państwa na wielu frontach, prowadzonej różnymi kanałami (dyplomatycznymi, politycznymi, ekonomicznymi, militarnymi, społecznymi, medialnymi), zgodnie z celami i zasadami planowania strategicznego. Sprawia to, że nie ma jednego uniwersalnego modelu dezinformacji, zaś większość technik konfrontacji informacyjnej ma ponadto charakter niebezpośredni, trudny do uchwycenia. Aktywność ta jest nakierowana na realizację własnych celów strategicznych i wzmocnienie pozycji międzynarodowej Rosji oraz „rozbrojenie" przeciwnika, tj. doprowadzenie do sytuacji, w której aktorzy wewnętrzni będą realizować cele operatora zewnętrznego.

Rosyjska wizja podkreśla przy tym znaczenie akcji psychologicznej, socjotechnicznej – w rosyjskich dokumentach strategicznych nie znajdziemy np. terminu cyberprzestrzeń. Szersze pojęcie przestrzeń informacyjna oznacza tu przede wszystkim

przestrzeń cywilizacyjną, kulturową, duchową, czy językową. Eksploatowany przez Rosję wymiar kulturowy działań informacyjnych (podkreślający wyższość tradycyjnych rosyjskich wartości duchowych i norm moralnych) kamufluje ich wymiar polityczny. Akcentowanie płynących z przestrzeni informacyjnej zagrożeń (ekspansja obcych wartości, ingerencja Zachodu w sprawy wewnętrzne Rosji, degradacja zasobów społecznych, dziedzictwa kulturowego i historycznego itp.) służy indoktrynacji społeczeństwa, jego mobilizacji i militaryzacji, co Kremlowi pozwala utrzymać je w stanie podległości. Z drugiej strony, co istotniejsze z punktu widzenia omawianego tematu, poprzez obronę wartości „rosyjskiej cywilizacji" i osób posługujących się językiem rosyjskim, Moskwa legitymizuje możliwość ingerencji w politykę innych państw.

W informacyjnej konfrontacji z Zachodem Rosja ma zdecydowaną przewagę. Uwarunkowała to sama istota reżimu putinowskiego, która wyklucza postępowanie według norm prawa międzynarodowego. Moskwa wykorzystuje zdobycze systemów demokratycznych, które traktuje jako słabość Zachodu (np. przemienność władzy w wyborach demokratycznych, pluralizm opinii i wolność słowa). Ciągłość władzy umożliwia jej realizację określonych i niezmiennych od lat celów politycznych, które skłaniają do podejmowania działań ofensywnych. Strategiczną narrację zapewnia spójna podstawa ideowa (neoimperialna doktryna oparta na tzw. geopolitycznym światopoglądzie naukowym, stanowiąca zarazem określoną wizję „świata rosyjskiego" i kryterium „prawdy", tj. miernik prawdziwości idei swój – obcy). Ma koncepcje długofalowej konfrontacji informacyjnej dostosowane do specyfiki docelowego odbiorcy.

Rosja ma ponadto długą tradycję prowadzenia dezinformacji. Jej strategia, jak to wynika ze Słownika kontrwywiadowczego KGB z 1973 r., zawsze była konstruowana dwutorowo: jako wprowadzanie w błąd i jako wywieranie wpływu. Kluczową rolę w realizacji technik dezinformacyjnych pełniły (i pełnią nadal) służby specjalne, głównie z powodu posiadania informacji niezbędnych do formułowania strategicznych celów i zadań polityki Kremla, typowania zewnętrznych operatorów rosyjskiej dezinformacji i ich niejawnego finansowania. Pierwsze tzw. dezinformbiuro powstało w 1923 r. w ramach OGPU/NKWD. Odrębną komórką wyprofilowaną do działań dezinformacyjnych był wydział „D" (od ros. dieza, dezinformacja) powołany w 1959 r. w ramach I Zarządu Głównego KGB (wywiad), przekształcony z czasem w Służbę „A" (od ros. aktiwka, działania aktywne). Po rozwiązaniu KGB została ona przekształcona w Służbę „MS" (od ros. mieroprijatija sodiejstwija, środki, przedsięwzięcia wsparcia). Analogiczne struktury istniały w ramach wywiadu wojskowego (GRU), gdzie do 1991 r. działał VII Zarząd (specpropaganda). Praktyka unaocznia też znamienną ewolucję podejścia Kremla do strategii dezinformacji: od słowa do działania oraz od form miękkich do twardych (od dywersji informacyjnej do twardej dywersji).

Także współcześnie służby specjalne stanowią kluczową część zaplecza wykonawczego operacji wpływu, pełniąc funkcję informacyjną (rozpoznanie sytuacji), organizacyjną, zabezpieczającą, kontrolną, a także moderacyjną i inspiracyjną. Kanały służb służą do budowania sieci agentury wpływu i finansowania akcji wsparcia polityki Kremla. Generując fałszywe świadectwa, aktywizując opozycję wewnętrzną w krajach Zachodu i kreując tam kryzysy polityczne i społeczne, a także wydarzenia pożądane z punktu widzenia Kremla, działają pod jego nadzorem i kontrolą.

Szeroko ujmowana dezinformacja była przedmiotem wnikliwych badań na Zachodzie w czasie zimnej wojny. Znakomitą antologię tekstów jej teoretyków i praktyków pt. „Psychosocjotechnika, dezinformacja – oręż wojny" opracował francuski pisarz Vladimir Volkoff, opatrując je komentarzem precyzyjnie ukazującym cele, metody i środki sowieckich operacji wpływu na opinię publiczną i politykę obcych państw. Dezinformację Volkoff określał notabene mianem „doktryny" (systemem myślenia i postępowania), wprowadzanie w błąd traktując jako jedną z technik.

Bardziej wnikliwa analiza wskazuje, że repertuar współczesnych technik dezinformacyjnych niewiele odbiega od tych stosowanych w czasach zimnej wojny. Są one realizowane za pomocą słowa oraz działań (dywersja, prowokacja, akcje protestu, akcje o charakterze paramilitarnym itp.). Novum polega głównie na wykorzystaniu nowych kanałów komunikacyjnych, które poszerzyły możliwości Rosji w tym zakresie. Internet zniósł wcześniejsze bariery komunikacyjne, zapewnił dostęp do informacji w czasie rzeczywistym, umożliwiając służbom szybkie spenetrowanie informacyjne obiektu działań. Rozwój tzw. nowych mediów (media tradycyjne online i media społecznościowe) stworzył możliwości błyskawicznego upowszechniania spreparowanych treści

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

(ich emitowania na cały świat, powielania, wycinania treści niepożądanych, narzucania własnej interpretacji), zapewniając przy tym anonimowość nadawcy i dostęp do odbiorcy bez pośredników. Zapewnił też możliwości „wybielania" dezinformacji: odbiorca, szukając potwierdzenia podsuniętej mu informacji, uzyskuje ją z kilku innych dezinformujących źródeł. Sieć globalna dostarczyła skrzynki z nowymi narzędziami, co sprawia, że współczesne problemy z agresywną polityką zagraniczną Rosji są tylko wzmocnioną wersją starych.

Posiłkując się badaniami prowadzonymi w czasie zimnej wojny oraz uwzględniając możliwości jakie przyniosły nowe technologie informacyjno-komunikacyjne, współczesny aparat dezinformacji można przedstawić w następujący sposób:

Rodzaj	Techniki/formy organizacyjne
CZARNY (koordynowany przez służby specjalne)	➢ Pozyskiwanie agentury wpływu i instrumentalizowanie do realizacji celów Rosji osób tego nieświadomych. ➢ Fabrykowanie dowodów (fałszywki, fejki). ➢ Prowokacje, np. dewastacja pomników i miejsc pamięci. ➢ Dywersja. ➢ Organizowanie akcji protestu. ➢ Przekupstwo, korumpowanie, szantaż i oczernianie polityków. ➢ Ataki cybernetyczne i propaganda 2.0.
SZARY (koordynowany przez Kreml)	➢ Inspirowanie grup społecznych, w tym partii i organizacji skrajnych. ➢ Działania za pośrednictwem kontrolowanych organizacji międzynarodowych. ➢ Instrumentalizowanie rosyjskich fundacji i stowarzyszeń, np. Russkij Mir, Rosyjskie Towarzystwo Historyczne. ➢ Zakładanie prorosyjskich portali i ich wsparcie finansowe. ➢ Fabryki trolli i organizowanie prokremlowskich sieci. ➢ Ataki społecznościowe, trolling.
BIAŁY (koordynowany przez Kreml)	➢ Akcje informacyjne prowadzone za pośrednictwem państwowych agencji informacyjnych i multimedialnych (TV RT, Radio Sputnik, RIA Novosti). ➢ Działalność prowadzona poprzez wydziały informacyjne, oddziały Rossodrużestwa, RONIK-i (rosyjskie ośrodki nauki i kultury) przy ambasadach Federacji Rosyjskiej. ➢ Organizowanie wydarzeń o charakterze naukowym i kulturalnym (konferencje, wystawy, rajdy pamięci, stypendia i kursy językowe).

KOMENTARZ

Dezinformacja jest dla Rosji atrakcyjnym narzędziem z wielu względów: ma szeroki transgraniczny zasięg, niewiele kosztuje, jest anonimowa, pozwala ukryć tożsamość dezinformatora, umożliwia realizację celów polityki Kremla. Wielostronne akcje dezinformacyjne Rosji nie słabną. Ponadto obserwujemy tendencję do poszerzenia zaplecza wykonawczego i koncepcyjnego operacji wpływu. Oznacza to, że ich kryzysotwórcza rola będzie wzrastać, stanowiąc coraz większe zagrożenie dla bezpieczeństwa narodowego państw demokracji. Jego skuteczne odparcie będzie wymagać nie tylko zwiększonej uwagi podmiotów odpowiedzialnych za bezpieczeństwo państwa, ale i dalszych intensywnych badań dotyczących systemowych projektów organizacyjnych, idei je umożliwiających, technik wpływu, korupcyjnych mechanizmów finansowania jego zewnętrznych operatorów, a także wypracowania procedur pozwalających na szybkie, skuteczne zneutralizowanie rosyjskiej dezinformacji. Poszerzenie wiedzy o rosyjskiej dezinformacji pozwoli uniknąć myślenia, że agresor jest schematyczny – należy być przygotowanym na nowe, nieznane jeszcze metody konfrontacji informacyjnej.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Zjawiska migracyjne jako potencjalne narzędzia wojny hybrydowej

Jacek Wysokiński
Komenda Główna Straży Granicznej

Zarządzanie migracjami ma istotny wpływ na sprawność funkcjonowania państwa. Z jednej strony migranci są niezbędni do zaspokojenia potrzeby krajowego rynku pracy oraz stanowią znaczący element w rozwoju turystyki i handlu, z drugiej strony generują koszty związane z koniecznością zapewnienia właściwej obsługi administracyjnej oraz ich udziałem w programach socjalnych i integracyjnych, realizowanych przez państwo przyjmujące. Taka sytuacja jest korzystna dla każdej ze stron, państwu zapewnia stabilny rozwój, natomiast migranci mogą efektywnie realizować własne cele. Zachwianie tej równowagi jest wysoce niekorzystne przede wszystkim dla państwa, natomiast w mniejszym stopniu dla samych migrantów.

Odnosząc się do samej możliwości wykorzystywania zjawisk migracyjnych w wojnie hybrydowej należy wyraźnie podkreślić, że dotychczasowe kryzysy migracyjne nie były identyfikowane jako narzędzie wrogich działań jednego państwa wymierzonych w inne państwo. W związku z tym, charakter tego opracowania należy odbierać wyłącznie jako analizę zagrożeń migracyjnych dla państwa przyjmującego.

Oceniając krajową sytuację migracyjną trzeba mieć na uwadze położenie geopolityczne Polski. Obecność w strukturach Unii Europejskiej oraz NATO, położenie w centralnej części Europy, a przede wszystkim posiadanie najdłuższej, ochranianej, lądowej granicy UE (granica zewnętrzna) powoduje, że terytorium RP tworzy swego rodzaju pomost pomiędzy wysokorozwiniętymi gospodarkami krajów Europy Zachodniej i gospodarkami państw wschodnioeuropejskich, a w szczególności Ukrainy, Rosji i Białorusi. Dodatkowym czynnikiem przyciągającym cudzoziemców do Polski jest dynamicznie rozwijający się krajowy rynek pracy.

Wszystkie te elementy powodują, że Polska cieszy się coraz większym zainteresowaniem ze strony cudzoziemców, już nie tylko, jako kraj tranzytowy, ale coraz częściej, jako kraj docelowy. W Polsce dominują przede wszystkim różne formy czasowej migracji zarobkowej, chociaż rosnące znaczenie ma chęć podejmowania nauki w polskich uczelniach wyższych. Istotny jest również fakt, że Polska jest wybierana przez cudzoziemców pochodzących z krajów byłego ZSRS jako kraj, w którym składają oni wnioski o ochronę międzynarodową. Sytuacja ta jest spowodowana przebiegiem szlaków komunikacyjnych, gdzie kluczową rolę odgrywa połączenie kolejowe na trasie Moskwa – Mińsk Białoruski – Brześć – Terespol – Warszawa.

Jak już wspomniano, podstawowe zjawiska migracyjne mają charakter rosnący, co obrazuje poniższe zestawienie[1].

	2016	2015	wzrost (spadek)
Wydane wizy	1.895.005	1.525.551	24,22%
Kontrola graniczna cudzoziemców na wjazd do RP	17.062.852	14.675.442	16,27%
Wnioski o zezwolenia na pobyt	153.873	117.410	31,06%
Praca – liczba oświadczeń o zamiarze powierzenia wykonywania pracy cudzoziemcowi	1.314.127	782.222	68,00%
Ochrona międzynarodowa – liczba cudzoziemców objętych wnioskami	11.274	11.637	(-3,12%)
Odmowy wjazdu wydawane cudzoziemcom na granicy RP	118.202	53.144	144,42%
Nielegalny pobyt – liczba cudzoziemców, którym wydano decyzje o zobowiązaniu do opuszczenia terytorium RP	20.046	13 669	46,65%

[1] Dane statystyczne Ministerstwa Spraw Zagranicznych, Straży Granicznej, Urzędu do Spraw Cudzoziemców, Ministerstwa Rodziny, Pracy i Polityki Społecznej.

Jak widać z przedstawionych danych, liczba cudzoziemców, codziennie stawiających się do kontroli paszportowej w polskich przejściach granicznych oraz cudzoziemców już przebywających w kraju, stanowi znaczącą wielkość i tylko poprzez sam efekt skali może istotnie wpływać na sprawność funkcjonowania państwa.

W związku z tym można przypuszczać, że zjawiska migracyjne mogą być przedmiotem analiz pod kątem możliwości ich wykorzystania przez strony konfliktu, jako element wrogich działań, mogących destabilizować państwo w wielu obszarach, m.in. takich jak:

1. Ochrona granicy państwowej RP oraz dokonywanie kontroli ruchu granicznego – to elementy niezbędne do zachowania integralności terytorium państwa oraz wypełniania zobowiązań międzynarodowych w zakresie ochrony granicy zewnętrznej strefy Schengen.
2. Zarządzanie migracjami nielegalnymi. Ujawnianie cudzoziemców naruszających przepisy w zakresie wjazdu i pobytu na terytorium RP wpływa na bezpieczeństwo wewnętrzne państwa, natomiast efektywna realizacja polityki powrotowej wobec cudzoziemców naruszających polski porządek prawny świadczy o skuteczności działania aparatu państwa w zakresie zwalczania nielegalnej migracji.
3. Zabezpieczenie epidemiologiczne. Z uwagi na różny poziom zabezpieczenia sanitarno-epidemiologicznego w krajach pochodzenia migrantów oraz zagrożeń epidemiologicznych związanych z długotrwałą podróżą do kraju docelowego może zaistnieć konieczność izolowania cudzoziemców chorych na określone polskimi przepisami choroby zakaźne.
4. Odpowiednie warunki socjalne. Cudzoziemcy poszukujący ochrony międzynarodowej na terytorium RP od momentu zgłoszenia się do ośrodka recepcyjnego dla cudzoziemców (administrowanego przez Szefa Urzędu do Spraw Cudzoziemców) muszą mieć zapewnione zakwaterowanie oraz wyżywienie lub otrzymać świadczenie pieniężne na pokrycie we własnym zakresie kosztów pobytu na terytorium Polski. Dodatkowo ponadprzeciętny wzrost liczby cudzoziemców kierowanych do ośrodków spowoduje szybkie ich przepełnienie i konieczność poszukiwania nowych obiektów. Ponadto należy zapewnić odpowiednie środki finansowe na udział cudzoziemców w określonych programach socjalnych, np. „program 500+" dla cudzoziemców posiadających tytuł pobytowy, gwarantujący dostęp do krajowego rynku pracy.
5. Właściwy proces integracji. Poza nakładami finansowymi na ten cel należy pamiętać o kształtowaniu świadomości społeczeństwa przyjmującego, w celu uniknięcia konfliktów na tle narodowościowym, religijnym lub rasowym.
6. Potrzeby krajowego rynku pracy. Wroga wobec cudzoziemców retoryka spowoduje wzrost nietolerancji społeczności lokalnych, co w konsekwencji doprowadzi do odpływu pracowników cudzoziemskich do innych państw.
7. Wizerunek państwa na arenie międzynarodowej. Prowadzenie przez stronę przeciwną szerokich działań dezinformujących instytucje oraz społeczność międzynarodową, popartych np. incydentami o podłożu rasistowskim, może doprowadzić do marginalizacji państwa w polityce międzynarodowej oraz zarzutów niewłaściwej realizacji umów międzynarodowych.

Zapewnienie właściwej realizacji wszystkich ww. elementów wymaga odpowiednich nakładów finansowych oraz wdrożenia takich rozwiązań prawnych i organizacyjnych, które pozwolą na efektywne zarządzanie migracjami.

Oczywistym zagrożeniem migracyjnym jest tzw. masowa migracja. W celu wywołania masowej migracji istnieje konieczność stworzenia odpowiednich czynników wypychających, powodujących masowe ruchy migracyjne. Niezbędnymi działaniami w tym kierunku wydają się:

- destabilizacja sytuacji wewnętrznej w państwie pochodzenia migrantów,
- wskazanie kraju docelowego, poprzez informowanie o dogodnych drogach wyjazdu oraz kreowanie świadomości migranta o kraju przyjmującym, jako miejscu gwarantującym pełne bezpieczeństwo – w tym bezpieczeństwo socjalne,
- wywołanie efektu skali, poprzez wskazanie, że czas na migrację jest wyłącznie teraz. Dodatkowo można spotęgować ten efekt wskazując np. konkretny odcinek granicy lub konkretne przejście graniczne.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

W związku z powyższym należy mieć na uwadze rozwój wydarzeń w państwach sąsiadujących oraz w państwach, dla których Polska mogłaby stanowić naturalny rejon masowej migracji. Takie podejście zapewni niezbędny czas na przygotowanie państwa do zagrożenia, jakim jest masowa migracja.

W celu lepszego zobrazowania skutków wykorzystania migracji do działań obniżających sprawność funkcjonowania państwa można posłużyć się zjawiskiem masowej migracji. O efektach tego zjawiska można było się przekonać chociażby podczas kryzysu migracyjnego na Węgrzech w roku 2015. Również w realiach krajowych istnieje zagrożenie wystąpienia podobnej sytuacji, chociaż w tym przypadku zapewne byłyby to odmienne sposoby migracji i odmienne profile samych migrantów.

W przypadku masowego napływu cudzoziemców do Polski w pierwszej kolejności należy zapewnić właściwą obsługę ruchu granicznego oraz ochronę granicy państwowej przed nielegalną migracją. Działania te będą wiązały się z odmawianiem wjazdu cudzoziemcom niespełniającym warunków na wjazd i pobyt na terytorium RP, którzy zadeklarują cel podróży inny niż poszukiwanie ochrony. Natomiast wjazd i pobyt zostanie umożliwiony w przypadku cudzoziemców poszukujących ochrony. Już na tym etapie Straż Graniczna będzie zmuszona do wprowadzenia rozwiązań szczególnych, polegających na przesunięciu sił i środków na zagrożony odcinek granicy, osłabiając tym samy swoje zdolności operacyjne wewnątrz kraju oraz na pozostałych ochranianych odcinkach granicy. Kolejnym elementem opisywanego etapu działań będzie konieczność wzmocnienia sił Straży Granicznej siłami Policji, a nawet wojska.

Po przyjęciu przez Straż Graniczną wniosków o ochronę międzynarodową cudzoziemcy zostaną skierowani do ośrodków recepcyjnych Urzędu do Spraw Cudzoziemców, gdzie uzyskają zakwaterowanie. Wspomniane ośrodki, z uwagi na szybkie zapełnienie, będą lokalizowane w nowych miejscach na terenie całego kraju. W ramach tych działań należy spodziewać się znaczącego obciążenia służby zdrowia przez osoby, które odniosły obrażenia podczas ucieczki ze swojego kraju pochodzenia oraz przez osoby cierpiące na różnego rodzaju choroby, w tym choroby zakaźne.

Już w trakcie pobytu uchodźców na terytorium RP nie należy zapominać o takich elementach jak:

- zapewnienie właściwego poziomu bezpieczeństwa w ośrodkach dla cudzoziemców,
- zachowanie odpowiednich standardów sanitarnych,
- realizacja obowiązku szkolnego dla dzieci uchodźców,
- opieka medyczna.

Istotna jest kwestia związana z brakiem kontroli na granicach wewnętrznych strefy Schengen i pokusą podejmowania przez migrantów dalszej, nielegalnej podróży do krajów Europy Zachodniej. W takim przypadku cudzoziemcy, wobec których toczy się w Polsce postępowanie uchodźcze, a którzy zostaną ujawnieni w innym państwie, będą przekazywani ponownie do Polski, jako państwa właściwego do rozpatrzenia wniosku o ochronę międzynarodową. Rosnąca skala tego zjawiska może wywoływać niezadowolenie tych krajów i próbę wymuszenia na Polsce uszczelnienia systemu ochrony granicy wewnętrznej z czasowym przywróceniem kontroli granicznej włącznie.

Warto zwrócić uwagę na możliwość powstawania sytuacji konfliktowych, a nawet zamieszek na linii cudzoziemcy – społeczność lokalna. Przyczyną takiego stanu rzeczy mogą być przedłużające się postępowania administracyjne prowadzone wobec cudzoziemców, nasycenie miejscowego rynku pracy, brak akceptacji różnic kulturowych, nieefektywność programów pomocowych i integracyjnych adresowanych do cudzoziemców.

W przypadku wystąpienia zjawiska masowej migracji należy pamiętać o konieczności wprowadzenia mechanizmów określonych w Krajowym Planie Zarządzania Kryzysowego. Znacząco wzrosną obciążenia finansowe państwa w zakresie środków kierowanych bezpośrednio dla migrantów, środków koniecznych do zapewnienia sprawnego działania służb i instytucji państwowych oraz środków z tytułu realizacji świadczeń socjalnych i programów integracyjnych. Wyzwaniem będzie prowadzenie skuteczniej polityki informacyjnej adresowanej do społeczeństwa przyjmującego i społeczności międzynarodowej, jak również prowadzenia działań edukacyjnych, skierowanych do migrujących cudzoziemców.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Ponadto należy mieć na uwadze, że uwikłanie państwa w kryzys migracyjny znacząco osłabi jego działania w innych ważnych obszarach, co może wykorzystać strona zainteresowana osłabieniem pozycji swojego przeciwnika.

Czasami do ukierunkowania działań danego państwa wystarczy wyraźny sygnał o możliwości masowej migracji. Z taką sytuacją mieliśmy do czynienia w 2015 roku, kiedy to obywatele Syrii w celu przedostania się do Europy przekraczali rosyjsko-norweski odcinek granicy. Ponad 2 tys. Syryjczyków przekroczyło granicę w okolicach miasteczka Kirkenes, położonego prawie 1,4 tys. kilometrów na północny-wschód od Oslo[2]. W 2016 roku Polska również odnotowała niespotykaną dotychczas presję migracyjną ze strony obywateli Rosji narodowości czeczeńskiej, którzy podejmowali wielokrotne próby wjazdu na terytorium RP w kolejowym przejściu granicznym w Terespolu. Skala tego zjawiska przedstawia się następująco:

	styczeń	luty	marzec	kwiecień	maj	czerwiec	lipiec	sierpień	wrzesień	październik	listopad	grudzień
2016	**1145**	**2188**	**3728**	**3909**	**4666**	**12424**	**12444**	**17634**	**12312**	**7841**	**3840**	**2997**
2015	616	778	956	740	729	1453	1459	3575	4969	3393	2727	3963

KOMENTARZ

Zjawisko migracji jest doskonałym narzędziem do angażowania praktycznie całego potencjału państwa w celu rozwiązania rodzącego się lub już trwającego kryzysu migracyjnego. Wywołanie efektu masowej migracji, ukierunkowanej na terytorium wybranego państwa, przy jednoczesnym zastosowaniu innych metod, negatywnie wpływających na sprawność jego funkcjonowania, wydaje się być doskonałą bronią ofensywną, której trudno jest skutecznie przeciwdziałać.

Globalne ataki cybernetyczne

Michał Wątor

Rządowe Centrum Bezpieczeństwa

Wzrasta liczba ataków komputerowych infekujących systemy w celu okupu, tzw. ransomware. Ataki te mają charakter międzynarodowy, a ich skala może stanowić zagrożenie dla funkcjonowania instytucji, służb państwowych, co w konsekwencji przekłada się na bezpieczeństwo obywateli.

12 maja br., w piątek w godzinach porannych doszło do ataku WannaCry – złośliwego oprogramowania, blokującego dostęp do komputerów z systemem operacyjnym Windows – na urządzenia w wielu krajach, na kilku kontynentach. Działanie wirusa polegało na szyfrowaniu dysku twardego komputera i całkowitym odcięciu dostępu do znajdujących się na nim plików. Najszybciej zagrożenie zauważono w Hiszpanii i Wielkiej Brytanii.

O godz. 15.22 portal Independent poinformował o chaosie w brytyjskiej państwowej służbie zdrowia (National Health Service – NHS) spowodowanym potężnym atakiem cybernetycznym.

Źródło: Independent.co.uk /AFP/

[2] http://www.dw.com/pl/uchodźcy-z-syrii-szlakiem-polarnym-na-rowerze/a-18819905

Źródło: ZaufanaTrzeciaStrona.pl

Po zaatakowaniu komputera użytkownik otrzymywał komunikat zobrazowany na powyższej grafice. Okazało się, że atak objął ponad 70 krajów m.in. w Europie, Stanach Zjednoczonych i Azji. Dotknął systemy informatyczne zarówno firm jak i instytucji państwowych, w tym amerykańską firmę spedycyjną Fedex, rosyjskie Ministerstwo Spraw Wewnętrznych czy największy bank Rosji – Sbierbank. Eksperci zidentyfikowali zdarzenie jako atak ransomware w celu uzyskania okupu w wysokości równowartości 300 USD w kryptowalucie Bitcoin. Użycie tej popularnej kryptowaluty ma na celu uniemożliwienie prześledzenia przepływu płatności i namierzenia odbiorcy końcowego.

Incydent na tak wielką skalę uruchomił m.in. działania z zakresu reagowania kryzysowego. Władze brytyjskie zdecydowały o objęciu ochroną atakowanych instytucji przez Narodowe Centrum Cyberbezpieczeństwa (National Cyber Security Centre – NCSC).

Wokół cyberataku zaczęło pojawiać się coraz więcej niezweryfikowanych informacji. Między innymi portal WikiLeaks podał, że do uderzenia zostało wykorzystane oprogramowanie, które wyciekło z jednej z agend rządowych USA. W tym czasie eksperci z firmy Check Point zajmującej się cyberbezpieczeństwem określili, że użyta wersja ransomware pochodzi z lutego 2017 r.

W Polsce portal sekurak.pl poinformował o **godz. 17.40** o zmasowanym ataku na infrastrukturę IT i sieć telefoniczną brytyjskich szpitali oraz rozprzestrzenieniu wirusa na Portugalię, Hiszpanię, Rosję, Ukrainę i Tajwan. Sekurak skupił się na skutkach ataku na służbę zdrowia w Wielkiej Brytanii, gdzie doszło do częściowego wyłączenia systemów IT oraz do utraty dostępności niekrytycznych działań medycznych.

O godz. 18.30 firma Kaspersky Lab (securelist.com) opublikowała analizę przedstawiającą metodę przeprowadzenia ataku (wykorzystanie błędu w protokole SMB służącym udostępnianiu zasobów komputerowych), sposób działania wirusa, a także wykorzystanie sieci TOR (The Onion Router – wirtualna sieć komputerowa, zapobiega analizie ruchu sieciowego i w konsekwencji zapewnia użytkownikom prawie anonimowy dostęp do zasobów Internetu) do anonimizacji napastników. Podano także wykaz podatnych systemów, listę najbardziej dotkniętych atakiem krajów, zwrócono uwagę na wielojęzyczność komunikatów z żądaniami okupu oraz wymieniono rozszerzenia plików podlegających szyfrowaniu. Kaspersky Lab zapowiedział również prace nad deszyfratorem zarażonych systemów.

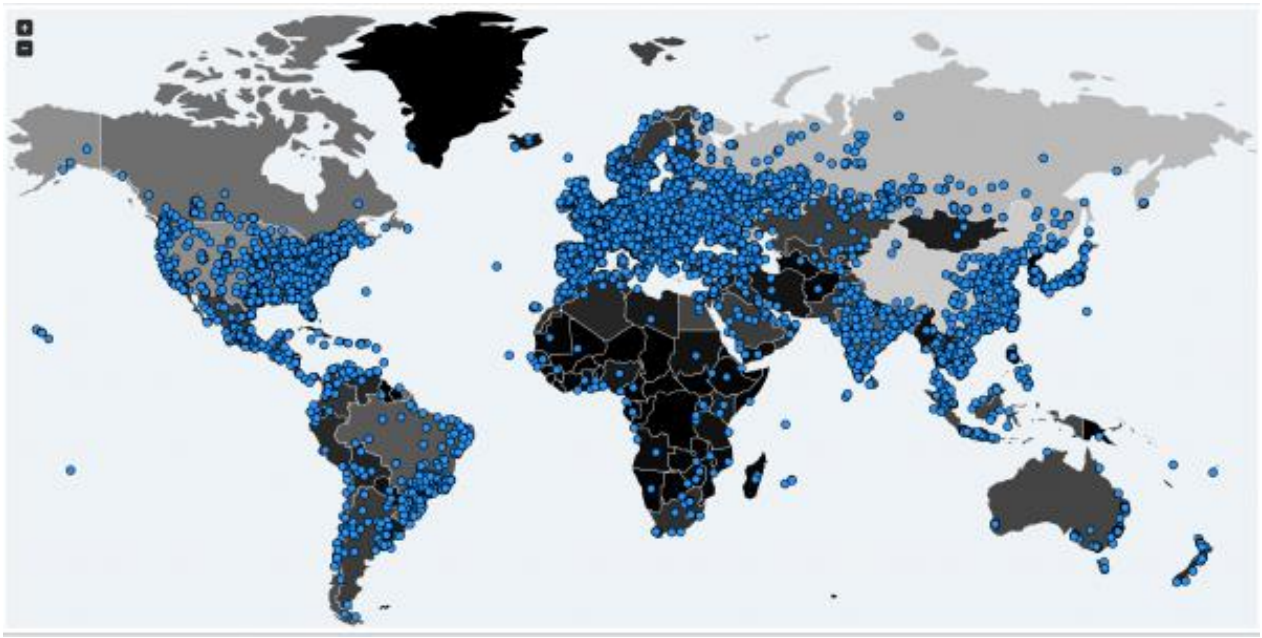
Tego samego dnia (12 maja), **grupa Cisco's Talos Intelligence Group Blog** zamieściła swoją analizę sytuacji. Wskazano m. in. na możliwość dalszego rozprzestrzeniania się wirusa poprzez skanowanie

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

wewnętrznych zakresów zainfekowanej sieci oraz wykorzystania luk w zewnętrznych domenach internetowych. Autorzy analizy zalecili niepłacenie okupu z powodu braku gwarancji zwrotu dostępu do plików. Przedstawili również swoje rekomendacje co do zastosowania środków bezpieczeństwa. Oprócz aktualizacji systemu operacyjnego i baz oprogramowania antywirusowego do zaleceń włączono m. in. blokadę komunikacji wychodzącej do węzłów sieci TOR.

Z kolei na blogu **blog.fox-it.com** poza dostępnymi już w Internecie informacjami o sposobie ataku i działaniach niezbędnych do zabezpieczenia się przed nim, pojawiło się doniesienie, że rozprzestrzeniający się złośliwy robak sam ma słabą stronę, wyłącznik (killswitch) dający szansę na zablokowanie wszystkich funkcji wirusa. Otóż – jak zauważył analityk z @MalwareTechBlog – WannaCry bezpośrednio po uruchomieniu na urządzeniu ofiary próbował łączyć się z domeną www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Skuteczne połączenie obezwładniłoby wirus, nie dopuszczając do szyfrowania plików i dalszego rozprzestrzeniania. Złośliwość robaka polegała jednak na tym, że adres domeny przez część programów antywirusowych identyfikowany był jako groźny, w związku z czym połączenie było automatycznie blokowane. W ten paradoksalny sposób zabezpieczenie antywirusowe umożliwiało rozprzestrzenianie się wirusa.

Ekspert, który dokonał odkrycia, niezwłocznie (o godz. 17:08:04) zarejestrował domenę o tym adresie i w ten sposób zatrzymał postęp epidemii. Analitycy zwrócili jednak od razu uwagę, że pozostawienie takiego „wyłącznika" w kodzie wirusa można interpretować zarówno jako niedopatrzenie programistów jak również jako celowy zabieg utrudniający analizę działania robaka w wydzielonym środowisku laboratoryjnym. Spośród polskich branżowych portali w piątek 12 maja o ataku wirusa informowały – sekurak.pl i zaufanatrzeciastrona.pl. W sobotę, 13 maja do akcji informacyjnej włączył się portal cyberdefence24, a następnie liczne polskie media. Około godz. 16:00 portal niebezpiecznik.pl opublikował obszerny artykuł obrazujący zasięg i skutki infekcji na całym świecie.



Źródło: niebezpiecznik.pl

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

W poniedziałek, 15 maja Rządowe Centrum Bezpieczeństwa rozesłało otrzymany od CERT Polska raport na temat ataku. Z danych wynikało, że w polskich adresach IP odnotowano ok. tysiąca wystąpień wirusa.

Od wtorku, 16 maja Narodowe Centrum Cyberbezpieczeństwa zaczęło docierać indywidualnie z informacją do operatorów sieci, z których odnotowano połączenia z adresem domeny blokującej działanie robaka.

W kolejnych dniach, w wyniku pogłębionej analizy zdarzenia, eksperci z firm Symantec i Kaspersky Lab stwierdzili, że za cyberatakiem stoi północnokoreańska grupa hakerska Lazarus. Grupa ta oskarżana jest o szereg cyberataków, do których dochodziło co najmniej od 2009 roku, m.in. o kradzież 81 milionów dolarów z banku centralnego w Bangladeszu, cyberatak na firmę Sony Pictures Entertainment z 2014 r., czy długoletnią negatywną kampanię przeciwko organizacjom demokratycznym z Korei Południowej.

Już w momencie opanowania sytuacji związanej z atakiem WannaCry analitycy podkreślali, że nie można wykluczyć potencjalnych zagrożeń, których charakter i zasięg może być jeszcze poważniejszy.

Tę prognozę potwierdziły zdarzenia z ostatnich dni czerwca. 27 czerwca br. między godziną 13:00 a 14:00 pojawiły się pierwsze informacje na Twitterze o nowym zmasowanym ataku na instytucje zlokalizowane na terenie Ukrainy. Ofiarami padły: ukraiński Gabinet Rady Ministrów, firmy sektora energetycznego, banki, firmy telekomunikacyjne, Ministerstwo Spraw Wewnętrznych, systemy w elektrowni w Czernobylu czy system ekranów informacyjnych na kijowskim lotnisku. Wśród ofiar w innych krajach jest Rosnieft, międzynarodowa firma spedycyjna Maersk, dostawca energii Ukrenergo, a także producent samolotów Antonov. Niektóre artykuły wspominają o setkach firm prywatnych. W Polsce ofiarami infekcji mogły paść takie firmy jak dom mediowy MediaCom i spółki z tej samej grupy kapitałowej, Kronospan, Intercars z branży motoryzacyjnej, Mondelez we Wrocławiu, TNT czy Raben z branży logistycznej.

Pierwsze opinie wskazywały na zmodyfikowaną odmianę znanego wcześniej robaka Petya. Efektem działania szkodliwego oprogramowania jest zaszyfrowanie sektora rozruchowego dysku twardego (MBR) oraz katalogów na dysku komputera, a następnie jego restart i brak możliwości uruchomienia. Dopiero po kilku godzinach ukazała się dodatkowa informacja z Ukrainy, że źródłem ataku było popularne oprogramowanie „M.E.doc", z którego korzystają ukraińskie instytucje i firmy do zarządzania elektronicznym obiegiem dokumentów. Hakerzy podmienili aktualizację tego oprogramowania na serwerze „upd.me-doc.com.ua (92.60.184.55)" na złośliwą, a ta poprzez funkcję automatycznej aktualizacji została zaciągnięta i uruchomiona w sieciach firm i instytucji będących użytkownikami programu. Atak na polskie sieci może być skutkiem ubocznym — część zaatakowanych firm podaje, że ma oddziały na Ukrainie i jest z nimi połączona wspólną siecią komputerową. Mogło to spowodować propagację robaka do Polski.

Z uwagi na kolejny w krótkim czasie i niepokojący ze względu na skalę atak, Premier Beata Szydło zwołała 28 czerwca br. w Rządowym Centrum Bezpieczeństwa posiedzenie Rządowego Zespołu Zarządzania Kryzysowego, w którym udział wzięli m. in. minister spraw wewnętrznych i administracji Mariusz Błaszczak, minister cyfryzacji Anna Streżyńska, minister obrony narodowej Antoni Macierewicz, minister spraw zagranicznych Witold Waszczykowski, minister – koordynator służb specjalnych Mariusz Kamiński i szefowie służb. Uczestnicy posiedzenia omówili sytuację związaną z atakami oraz działania prowadzone przez poszczególne instytucje. Agencja Bezpieczeństwa Wewnętrznego, na polecenie Koordynatora Służb Specjalnych, rozesłała do 70 instytucji rekomendacje działań dotyczących postępowania w związku z atakami teleinformatycznymi. Zalecenia dotyczą m.in.: tworzenia kopii bezpieczeństwa, uaktualniania systemów, a także prowadzenia szkoleń i ćwiczeń dla pracowników. Rządowe Centrum Bezpieczeństwa koordynuje przepływ informacji, tj. agreguje dane dotyczące zagrożeń pochodzące od trzech największych CERT-ów (Computer Emergency Response Team): CERT Polska, CERT ABW i CERT MON, a następnie przekazuje członkom Rządowego Zespołu Zarządzania Kryzysowego.

Źródła:

1. http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hospitals-hack-england-emergency-patients-divert-shut-down-a7732816.html
2. https://sekurak.pl/masowy-atak-na-publiczna-sluzbe-zdrowia-w-uk-chaos-ransomware-i-grozba-globalnego-ataku
3. https://zaufanatrzeciastrona.pl/post/masowa-niezwykle-skuteczna-kampania-ransomware-wylacza-cale-firmy/
4. https://zaufanatrzeciastrona.pl/post/komunikacja-polskich-instytucji-panstwowych-na-temat-wannacry-analiza

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

5. https://niebezpiecznik.pl/post/zamkniete-szpitale-i-zaklady-pracy-uderzenie-robaka-wannacry-i-olbrzymie-straty-na-calym-swiecie/
6. https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/
7. http://blog.talosintelligence.com/2017/05/wannacry.html
8. https://blog.fox-it.com/2017/05/12/massive-outbreak-of-ransomware-variant-infects-large-amounts-of-computers-around-the-world/
9. https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/
10. https://technet.microsoft.com/pl-pl/library/security/ms17-010.aspx
11. https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/
12. https://www.slideshare.net/nrc/cyber-securityreport2017
13. https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
14. http://businessinsider.com.pl/technologie/nowe-technologie/ransomware-wannacry-ekspert-wykryl-nowego-robaka-eternalrocks/5jtz3fb
15. http://www.bbc.com/news/technology-39901382
16. https://www.dobreprogramy.pl/WikiLeaks-ujawnia-hakerskie-narzedzia-CIA-zgodne-takze-z-Windows-10,News,81147.html
17. http://www.cyberdefence24.pl/595214,cyberatak-na-skale-swiatowa-paraliz-brytyjskiej-sluzby-zdrowia
18. https://www.greeneris.com/produktyuslug/bezpieczenstwo/cisco-umbrella-opendns/

KOMENTARZ

Ataki teleinformatyczne z ostatnich tygodni i ich konsekwencje dowodzą, że kwestia ochrony cyberprzestrzeni jest kluczowa, a działania powinny być prowadzone na wielu poziomach. Na szczeblu państwowym konieczne jest zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo w tym obszarze. Narzędziem do realizacji postulatu ma być, zgodnie z dokumentem pn. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej (KRPC RP) na lata 2017-2022, platforma zintegrowanego systemu wymiany informacji. W omawianym ataku ransomware bardzo przydatne byłyby atrybuty takiej platformy, w tym kompleksowa, następująca w czasie rzeczywistym, agregacja informacji o eskalacji zagrożenia. Do czasu wdrożenia projektowanej platformy przyśpieszenie prac nad systemem wymiany informacji powinno być realizowane równolegle ze zwiększaniem wykorzystania już dostępnych narzędzi automatycznej agregacji i współdzielenia informacji.

Jednocześnie niezbędne jest podjęcie działań edukacyjnych i informacyjnych w celu zwiększenia odporności społeczeństwa. Chodzi zwłaszcza o kształtowanie właściwych zachowań w komunikacji poprzez portale społecznościowe oraz pocztę email, jako najczęściej wykorzystywane kanały socjotechnicznych form ataków internetowych.

Zespół CERT dla sektora elektroenergetycznego – działania dla realnej ochrony infrastruktury krytycznej w Polsce i Europie

Jarosław Sordyl

Polskie Sieci Elektroenergetyczne S.A.

Rozwój zagrożeń dla systemów teleinformatycznych przybrał w ostatnich latach poziom na niespotykaną dotąd skalę. Codziennie napływają informacje o zagrożeniach, podatnościach na ataki oraz działaniach cyberprzestępców, które skutkują wymiernymi konsekwencjami dla bezpieczeństwa, w tym nierzadko międzynarodowego. Wywołane cyberatakami na całym świecie straty liczone są już w miliardach dolarów rocznie. Celem cyberprzestępców pozostają zarówno osoby fizyczne, przedsiębiorcy oraz urzędy, jak i wielkie międzynarodowe korporacje, bez względu na branżę czy miejsce prowadzenia działalności. Dla przykładu warto tu wspomnieć zdarzenia z Ukrainy, gdzie w 2015 i 2016 roku, motywowani politycznie i sponsorowani przez obcy rząd hakerzy dokonali ataku na jeden z systemów energetycznych, doprowadzając do jego wyłączenia na wiele dni. Ta sytuacja pokazuje, że cyberzagrożenia są realne i mogą mieć bezpośredni wpływ nawet na systemy krytyczne, a jedną z istotnych przyczyn ich powodzenia jest brak struktur zarządzających, monitorujących i reagujących na incydenty komputerowe.

Analiza zdarzeń dotyczących cyberbezpieczeństwa pokazuje, że utworzenie w strukturach, istotnych dla państwa i biznesu, organizacji Zespołów Reagowania na Incydenty Komputerowe – CERT (Computer Emergency Responce Team) jest nieodzownym elementem podnoszącym poziom bezpieczeństwa oraz przeciwdziałania cyberzdarzeniom.

Celem zespołów CERT jest reagowanie na zagrożenia dla systemów komputerowych, ich analiza, uzyskanie informacji o rodzaju oraz po źródłach zagrożenia, tworzenie rozwiązań i rekomendacji mających na celu ich uniknięcie lub wyeliminowanie w przyszłości, a także prowadzenie akcji uświadamiających użytkowników o istniejących zagrożeniach i ich skutkach. Zadania te wynikają m.in. z zaleceń wskazanych przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji – ENISA[1].

Ze względu na powagę zagrożeń w cyberprzestrzeni, w grudniu 2016 roku w PSE, decyzją Zarządu Spółki powołano jednostkę – CERT PSE. Celem jej utworzenia jest zwiększenie bezpieczeństwa teleinformatycznego organizacji w zakresie reagowania na zdarzenia i incydenty teleinformatyczne.

CERT PSE realizuje obecnie następujące działania:

- rejestruje i obsługuje zdarzenia naruszające bezpieczeństwo sieci,
- alarmuje użytkowników o wystąpieniu dla nich bezpośrednich zagrożeń,
- prowadzi działania zwiększające świadomość bezpieczeństwa teleinformatycznego,
- prowadzi badania i przygotowuje raporty dotyczące bezpieczeństwa korzystania z zasobów Internetu,
- niezależnie testuje produkty i rozwiązania z dziedziny bezpieczeństwa teleinformatycznego.

W CERT PSE zwraca się szczególną uwagę na wymianę informacji oraz współpracę pomiędzy podobnymi zespołami, powołanymi w innych organizacjach, w trakcie realizacji powierzonych zadań. Niejednokrotnie w przypadku ataków cybernetycznych o skuteczności podejmowanych działań decyduje to, kiedy informację o ataku otrzymał zespół bezpieczeństwa, który mógł podjąć działania zapobiegające temu atakowi. Dlatego powstał pomysł utworzenia sektorowego zespołu CERT realizującego typowe usługi zespołu bezpieczeństwa dla wskazanej grupy organizacji.

W ślad za tym, w marcu 2017 roku GK PSE i Grupa ENERGA podpisały porozumienie o współpracy zespołów CERT PSE i CERT ENERGA. Celem współpracy zespołów jest przede wszystkim wymiana informacji o zagrożeniach i podatnościach na ataki mogących mieć bezpośredni wpływ na bezpieczne funkcjonowanie systemów IT w obu organizacjach.

Obecnie zespół CERT PSE podejmuje dalsze działania mające na celu zwiększenie liczby zespołów funkcjonujących w ramach wspólnej platformy wymiany informacji w sektorze energetycznym. Założeniem PSE jest stworzenie możliwie jak najsilniejszej i najliczniejszej platformy współpracy, w oparciu o już funkcjonujące zespoły oraz zapewnienie szybkiej i skutecznej wymiany informacji na wypadek zdarzeń i cyberataków jakie do tej pory były notowane w innych krajach.

CERT PSE podejmuje także działania na rzecz współpracy w sektorze energetycznym w wymiarze międzynarodowym. Pierwsze porozumienie o współpracy jest obecnie negocjowane z norweskim KraftCERT, funkcjonującym w sektorze energetycznym.

W celu pokazania partnerom PSE, że osiągnięto dojrzałość organizacyjną oraz funkcjonalną do wykonywania i realizacji zadań, niezależnie od skali i obszaru objętego współpracą, CERT PSE zakończył proces akredytacji oraz w efekcie rozpoczął proces certyfikacji swojej struktury funkcjonowania w organizacji Trusted Introducer[2].

[1] https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-polish

[2] Trusted Introducer to inicjatywa mająca na celu wsparcie zespołów reagowania na incydenty bezpieczeństwa z Europy i sąsiednich krajów. Została zainicjowana w 2000 roku przez TF-CSIRT, największą europejską organizację promującą współpracę CERTów.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl