Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-07 | strony: 69–78

Jacek Buko
Uniwersytet Szczeciński
Wydział Zarządzania i Ekonomiki Usług
jacek.buko@wzieu.pl

Problematyka zagrożeń dla systemów informatycznych polskiej infrastruktury krytycznej

Kody JEL: H54, H56
Słowa kluczowe: infrastruktura krytyczna, zagrożenia informatyczne, bezpieczeństwo państwa
Streszczenie. Infrastrukturę krytyczną stanowią systemy, urządzenia, obiekty i usługi, kluczowe dla bezpieczeństwa państwa i jego obywateli. Powszechne zastosowanie technologii informatycznych czyni państwo sprawniejszym, a gospodarkę bardziej wydajną. Powstała w ten sposób powiązana informatycznie infrastruktura jest jednak w większym stopniu podatna na różnorodne zagrożenia. Celem rozważań podjętych w niniejszym artykule jest analiza zagrożeń dla informatycznych systemów infrastruktury krytycznej oraz próba scharakteryzowania i oceny systemowych działań podejmowanych w Polsce, w celu przeciwdziałania tego typu zagrożeniom.

Wprowadzenie

We współczesnym społeczeństwie, bazującym na daleko posuniętym podziale pracy, zaopatrzenie obywateli w dobra i usługi realizowane jest za pomocą skomplikowanej sieci systemów wytwórczych, dystrybucyjnych i administracyjno-zarządczych. Te spośród systemów tworzących przedmiotową sieć, które uznawane za najważniejsze dla zapewnienia bezpieczeństwa obywateli i państwa, określane są wspólnym mianem infrastruktury krytycznej[1]. W Polsce, podobnie jak w innych krajach, do systemów tych

[1] Określenie „infrastruktura krytyczna" zostało po raz pierwszy użyte w latach 90. XX wieku w Stanach Zjednoczonych, w dokumencie powstałym w związku z poważnymi awariami sieci przesyłu energii elektrycznej, tzw. Raporcie Marshalla. Awarie te wpłynęły negatywnie na inne kluczowe dla bezpieczeństwa obywateli i państwa systemy infrastrukturalne (Milewski, 2016, s. 107).

zalicza się przede wszystkim: zaopatrzenie w żywność, wodę, energię, paliwa i surowce energetyczne, zapewnienie ciągłości działania administracji publicznej, transportu, łączności, sieci teleinformatycznych, systemu finansowego, ochrony zdrowia i ratownictwa, a także produkcję, przesyłanie, stosowanie oraz przechowywanie substancji chemicznych i promieniotwórczych. Dla zapewnienia funkcjonowania każdego z tych systemów wykorzystywane są komponenty informatyczne, co czyni z nich newralgiczne elementy całej infrastruktury krytycznej. W dobie globalizacji systemy infrastruktury krytycznej są również coraz bardziej współzależne informatycznie w wymiarze międzynarodowym.

Zapewnienie bezpieczeństwa informatycznego infrastruktury krytycznej należy zatem uznać za kluczowe dla utrzymania jej wymaganej funkcjonalności. Zadanie to istotnie komplikuje fakt, że w skład informatycznego komponentu infrastruktury krytycznej wchodzą liczne oraz zróżnicowane punkty sterowania i centra przetwarzania danych, teletransmisyjne sieci wewnętrzne, a także sieci rozległe, które wraz z rozproszonymi punktami dostępowymi wychodzą poza obiekty własne, co sprawia, że nie może być nad nimi sprawowany kompleksowy nadzór.

Systemy informatyczne wykorzystywane w ramach infrastruktury krytycznej to dedykowane sterowaniu przemysłowemu systemy OT (*Operational Technology*) oraz systemy IT (*Information Technology*), do których zasadniczo przynależą wszystkie pozostałe systemy informatyczne wspomagające funkcjonowanie tej infrastruktury. Zagrożeniem dla funkcjonowania systemów OT są przede wszystkim zakłócenia dostępności procesu produkcyjnego, natomiast w przypadku systemów IT zagrożeniem jest utrata integralności, tj. kompletności, wiarygodności oraz poufności przetwarzanych przez te systemy danych.

1. Kategoryzacja zagrożeń dla systemów informatycznych infrastruktury krytycznej

Zagrożenia dla systemów informatycznych infrastruktury krytycznej mogą mieć różnorodne przyczyny, do których w ujęciu rodzajowym należy z pewnością zaliczyć:

- błędy ludzkie,
- presję obniżania kosztów,
- awarie sprzętu i oprogramowania,
- ataki fizyczne,
- ataki cybernetyczne,
- katastrofalne zdarzenia naturalne.

Błędy ludzkie to działania podejmowane bez założonego zamiaru wyrządzenia szkód, związane z brakiem świadomości zagrożeń, niedostatecznymi kompetencjami kierowniczymi, niedyspozycją psychofizyczną, brakiem staranności, lekceważeniem przepisów, jak również niewystarczającymi kwalifikacjami w zakresie obsługi coraz bardziej wyrafinowanych technologicznie systemów informatycznych. W Polsce głów-

nym powodem wykluczenia społecznego jest nie tylko brak dostępu do dedykowanych usług komunikacji elektronicznej, ale przede wszystkim brak kompetencji i umiejętności korzystania z usług w społeczeństwie informacyjnym (Budziewicz-Guźlecka, 2010, s. 241). Do kategorii błędów ludzkich należy zaliczyć ponadto brak prowadzenia przez decydentów odpowiedniej polityki bezpieczeństwa oraz wdrażanie niewłaściwych regulacji prawnych.

Kolejne zagrożenie wynika z presji ekonomicznej wywieranej na konkurujących między sobą dostawcach systemów informatycznych, którzy są kreatorami rynku e-commerce (Drab-Kurowska, 2013; Czaplewski, 2017). Efektem tej rywalizacji jest obniżanie kosztów wytworzenia i implementacji systemów informatycznych, uzyskiwane przede wszystkim w drodze unifikacji technologii informatycznych. Konstruowane na tej bazie systemy informatyczne mają powszechnie znaną architekturę i komponenty, co ułatwia ich potencjalną penetrację. Ponadto, w celu zoptymalizowania kosztów serwisowania, systemy te są niejednokrotnie serwisowane zdalnie, za pośrednictwem nieodseparowanych publicznych lub komercyjnych sieci teletransmisyjnych.

Przyczynami awarii sprzętu i oprogramowania mogą być wady producenckie, błędy technologiczne i projektowe, błędy konfiguracji i synchronizacji komponentów, niewłaściwa eksploatacja oraz konserwacja, jak również celowe działania. Te ostatnie należy wiązać z dwoma kolejnymi rodzajami zagrożeń, tj. atakami fizycznymi i cybernetycznymi.

Zarówno ataki fizyczne, jak i cybernetyczne są działaniami intencjonalnymi, których dokonywaniem zainteresowani mogą być m.in. obecni i byli pracownicy, podmioty konkurujące, pospolici przestępcy, hakerzy, terroryści oraz służby specjalne innych państw. Do motywów takich działań należą: kradzież, sabotaż, ideologia, terroryzm[2], niezadowolenie, łapownictwo, frustracja, wandalizm.

Atak fizyczny skierowany przeciwko systemowi informatycznemu infrastruktury krytycznej wymaga zazwyczaj bezpośredniego dostępu do przedmiotu ataku i powszechnie uznawany jest za trudniejszy do przeprowadzenia niż atak cybernetyczny, który może być dokonany zdalnie[3].

---

[2] Wymiar współczesnego terroryzmu postrzega się przede wszystkim przez pryzmat wojny cywilizacji, ale także kultur, narodów i religii (Budziewicz-Guźlecka, 2015, s. 79). O terroryzmie cybernetycznym można mówić wówczas, gdy cyberatak motywowany jest politycznie. W pozostałych przypadkach ataki tego rodzaju klasyfikuje się zazwyczaj jako przestępstwa cybernetyczne bez podtekstu politycznego. Z kolei próby zwrócenia uwagi opinii publicznej na określony problem społeczny bądź polityczny poprzez niedozwolone działania w sieci określa się jako haktywizm. Szerzej: Zuber (2014).

[3] Statystyki wskazują, że liczba zgłaszanych w Polsce fizycznych ataków przeciwko mieniu sukcesywnie zmniejsza się od co najmniej kilkunastu lat (*Przestępstwa przeciwko mieniu*), natomiast przestępczość cybernetyczna rośnie szybciej niż prawo Moore'a, tzn. podwaja się w niemal równych odcinkach czasu. Znamienne jest przy tym, że personalna identyfikacja sprawców ataków cybernetycznych jest niemal niemożliwa, podobnie jak pociągnięcie ich do odpowiedzialności. Należy również wskazać, że zdaniem specjalistów zaawansowane oprogramowanie antywirusowe jest przeciętnie w stanie zidentyfikować i zneutralizować jedynie połowę stosowa-

Jedyną formą fizycznego ataku, skierowanego selektywnie przeciwko komponentowi informatycznemu infrastruktury krytycznej i niewymagającego bezpośredniego kontaktu z atakowanym celem, jest użycie broni EMP (*Electromagnetic Pulse*). Działanie tej broni polega na wyemitowaniu krótkotrwałego i intensywnego impulsu promieniowania elektromagnetycznego, indukującego w urządzeniach zasilanych elektrycznie wysokie napięcie, wywołujące z kolei skokowy wzrost natężenia prądu zdolnego zniszczyć (przez przepięcie lub przegrzanie) niezabezpieczone struktury elektroniczne. Sztucznie stworzonym źródłem impulsu może być wybuch nuklearny lub emisja mikrofalowa z dedykowanego generatora. Efektywność broni bazującej na nienuklearnym EMP potwierdzają jej publiczne demonstracje dokonywane w ostatnich kilkunastu latach w Rosji i USA. Wskutek postępującej miniaturyzacji urządzeń emitujących nienuklearny EMP atak taką bronią może być współcześnie przeprowadzony nie tylko za pośrednictwem bomb lotniczych i rakiet, ale zapewne również przy użyciu ciężkiej artylerii lufowej. Atakowane mogą być zarówno obiekty wielkopowierzchniowe, np. bazy wojskowe, fabryki, elektrownie, jak i obiekty małe, przy unieszkodliwianiu których wymagane jest rażenie precyzyjne.

Zabezpieczenie struktur elektronicznych przed skutkami EMP jest możliwe poprzez ich całkowite odizolowanie od środowiska, w którym rozprzestrzenia się promieniowanie elektromagnetyczne. W praktyce jest to kosztowne, skomplikowane i ograniczone do urządzeń pozbawionych wszelkich zewnętrznych przyłączy w rodzaju zasilania elektrycznego, przewodów komunikacyjnych, anten itp.

Ataki *stricte* cybernetyczne mogą być dokonywane z wykorzystaniem systemów informatycznych oraz na systemy informatyczne i w cyberprzestrzeni. Do ataków tych wykorzystywane są podatności oprogramowania i transmisji oraz sabotaż komputerowy. Na infrastrukturę krytyczną dokonywane są najczęściej ataki zmasowane, mające na celu jak najdłuższe uniemożliwienie jej działania. Drugim typem ataków są ataki wyspecjalizowane. W przypadku systemów IT tego rodzaju ataki przeprowadzane są dla pozyskania określonych danych bądź przejęcia kontroli nad wybranym fragmentem systemu (Leśnikowski, 2011). W odniesieniu do systemów OT wyspecjalizowane ataki cybernetyczne mają najczęściej za zadanie dokonanie zmian parametrów w układach regulacji, zawieszanie działania zabezpieczeń, fałszowanie grafik synoptycznych, blokowanie bądź uszkadzanie urządzeń.

Do 2010 roku możliwość skutecznego ataku cybernetycznego na krytyczną infrastrukturę przemysłową rozpatrywana była jedynie teoretycznie, ze względu na stosowane tam najlepsze dostępne zabezpieczenia komercyjne. Zagrożenie to zaczęto postrzegać inaczej wraz z dokonanym przez służby amerykańskie atakiem na irański program nuklearny. Zastosowane wówczas algorytmy przełamały zwielokrotnione informatycznie zabezpieczenia instalacji wzbogacania uranu, stwarzając precedens, który uświado-

---

nego przez cyberprzestępców złośliwego oprogramowania, a luki w oprogramowaniu wykrywane są średnio dopiero po 200 dniach od zainfekowania systemów (*Blackout…*).

mił realność zagrożeń ze strony profesjonalnych zespołów walki cyberinformatycznej. Broń informatyczna znajdująca się na wyposażeniu służb specjalnych i armii takich państw jak USA, Rosja czy Chiny przewyższa o kilka poziomów komercyjne zabezpieczenia (Świrski, 2014).

W Europie poważne ataki cybernetyczne, identyfikowane jako dokonane przez profesjonalne służby innych państw, przeprowadzone zostały w minionych latach na infrastrukturę krytyczną m.in. Estonii (2007 r.), Gruzji (2008 r.), Ukrainy i Wielkiej Brytanii (2017 r.). Europejski Urząd Policji (Europol) szacuje, że w 2017 roku europejska infrastruktura krytyczna była dziennie celem ok. 4 tys. ataków cybernetycznych o zróżnicowanym stopniu stwarzanego przez nie zagrożenia (*Europol.*…).

W latach 2016 i 2017 w państwach europejskich obserwowane były cyberataki na takie systemy infrastruktury krytycznej, jak logistyczny, zdrowia i energetyczny. Przewiduje się, że w 2018 roku spektrum to może się poszerzyć o inne systemy, zwłaszcza wodny i transportowy. Ważnym elementem potencjalnych ataków będzie także ich zakładany międzynarodowy oraz międzysektorowy charakter (*Instytut Kościuszki.*…). Należy zaakcentować, że w 2017 roku Polska była szóstym najbardziej zagrożonym cyberatakami krajem w Europie (www.egospodarka.pl).

Ostatnią z wyszczególnionych w układzie rodzajowym przyczyn zagrożeń dla systemów informatycznych infrastruktury krytycznej są katastrofalne zdarzenia naturalne. Niszczące lub zakłócające funkcjonowanie infrastruktury krytycznej zdarzenia tego rodzaju mają z oczywistych względów jednoczesne destrukcyjne oddziaływanie na jej komponent informatyczny, natomiast żadne z nich nie ma zasadniczo na ten komponent wpływu selektywnego. W ograniczonym zakresie można tu jedynie rozpatrywać wywołane wybuchami plazmy słonecznej (koronalnymi wyrzutami masy) burze geomagnetyczne. Skutkami dostatecznie intensywnych burz tego rodzaju są czasowe zakłócenia funkcjonowania satelitów komunikacyjnych, nawigacji satelitarnej, łączności radiowej oraz telefonii komórkowej[4]. Negatywny wpływ tych zakłóceń można minimalizować uwzględniając w planowaniu pracy zagrożonych urządzeń informacje udostępniane przez monitorujące aktywność słoneczną agencje, np. NASA czy Space Weather Prediction Center (*Extreme space.*…). Agencje te publikują swoje ostrzeżenia z co najmniej kilkunastogodzinnym wyprzedzeniem w odniesieniu do zaistnienia przedmiotowego zagrożenia.

[4] Najbardziej na katastrofalne i bezpośrednie skutki burz słonecznych narażony jest system przesyłowy energii elektrycznej, gdyż indukowane w liniach przesyłowych prądy elektromagnetyczne są w stanie trwale uszkadzać transformatory. W 1859 r. wydarzyła się największa zidentyfikowana burza magnetyczna, która spowodowała rozległe awarie sieci telegraficznych w Europie i Ameryce. Współcześnie burza magnetyczna porównywalna do tej z 1859 r. mogłaby zniszczyć cały system energetyczny krajów uprzemysłowionych. Odbudowa tej infrastruktury zajęłaby od 4 do 10 lat – Eastwood i in. (2017).

2. Formalizacja ochrony systemów informatycznych polskiej infrastruktury krytycznej

Obowiązującymi w Polsce podstawowymi aktami prawnymi regulującymi kwestię ochrony infrastruktury krytycznej są: ustawa z 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 590) oraz ustawa z 2010 roku o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. 2010 nr 240, poz. 1600). Ustawy te nakazują realizację wszelkich działań zmierzających do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej. Ich przepisy określają również zasady sporządzania i aktualizacji tzw. Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), uwzględniającego rodzaje zagrożeń oraz zakres ochrony infrastruktury (*Narodowy Program…*). NPOiK jest dokumentem planistycznym o charakterze strategicznym, opracowywanym przez powołane w 2008 roku Rządowe Centrum Bezpieczeństwa. W dokumencie tym wskazano, że zapewnienie bezpieczeństwa infrastruktury krytycznej obejmuje jej ochronę: fizyczną, techniczną, osobową, teleinformatyczną, prawną oraz plany odbudowy. Aspekt zapewnienia bezpieczeństwa teleinformatycznego infrastruktury krytycznej sprowadzono w NPOiK do doprecyzowania, że jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania infrastruktury krytycznej w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne. Autorzy NPOiK zastrzegli, że dokument ten nie zawiera kompletu zasad i informacji na temat ochrony infrastruktury krytycznej, może natomiast posłużyć jako rozbudowana lista kontrolna tego, jak należy zorganizować system ochrony.

Kolejnym dokumentem planistycznym dedykowanym ochronie infrastruktury krytycznej jest Krajowy Plan Zarządzania Kryzysowego (KPZK), opracowywany przez Rządowe Centrum Bezpieczeństwa, we współpracy z ministerstwami, urzędami centralnymi i województwami (art. 5. Dz.U. 2007 nr 89, poz. 590). W dokumencie tym, zaktualizowanym w styczniu 2018 roku, scharakteryzowano zadania realizowane przez organy administracji publicznej w odniesieniu do 19 zagrożeń, w tym zdarzeń o charakterze terrorystycznym, zakłóceń w funkcjonowaniu sieci i systemów informatycznych oraz działań hybrydowych. Funkcjonalnie KPZK podzielony jest dwie części. Pierwsza poświęcona jest działaniom realizowanym na rzecz minimalizacji ryzyka wystąpienia sytuacji kryzysowej w ramach dwóch pierwszych faz zarządzania kryzysowego: zapobiegania i przygotowania. Część druga odnosi się do działań administracji po wystąpieniu kryzysu i zawiera rozwiązania stosowane podczas kolejnych faz: reagowania i odbudowy. W KPZK syntetycznie scharakteryzowano istotę, przyczyny, obszar występowania i najczęstsze skutki zagrożeń informatycznych oraz zadania i obowiązki uczestników zarządzania kryzysowego w tym zakresie.

W 2017 roku wszedł w życie uchwalony przez rząd dokument planistyczny pt. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej (KRPC) na lata 2017–2022 (*Strategia…*). W dokumencie tym określono blisko sto działań organów administracji rządowej odnoszących się do kwestii zapewnienia cyberbezpieczeństwa Polski

w przedmiotowym okresie. Wśród najistotniejszych zamierzeń ujęto opracowanie założeń ustawy o krajowym systemie cyberbezpieczeństwa oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego funkcjonowania państwa. Wskazano również na zamiar rozbudowy struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym Narodowego Centrum Cyberbezpieczeństwa oraz Narodowego CSIRT (*Computer Security Incident Response Team*), sektorowych zespołów reagowania na incydenty (CSIRT sektorowe), centrów wymiany i analizy informacji.

Realizacja działań opisanych w Krajowych Ramach Polityki Cyberbezpieczeństwa (KRPC) ma być finansowana przez poszczególne jednostki zaangażowane w ich wdrażanie, a także ze środów pochodzących z Narodowego Centrum Badań i Rozwoju i z funduszy Unii Europejskiej – „w miarę zaistnienia takich możliwości". Szacowanie wartości niezbędnych do wydatkowania w tym zakresie środków pieniężnych ujęto w tzw. Planie działań Krajowych Ram Polityki Cyberbezpieczeństwa, przedstawionym przez Ministra Cyfryzacji w styczniu 2018 roku. W planie tym zapisano m.in., że sam fakt zgłoszenia przez dany organ działania do Planu działań KRPC nie oznacza automatycznego zarezerwowania na ten cel środków budżetowych. Działania te będą realizowane w miarę uwzględnienia ich finansowania w budżecie państwa.

3. Ocena stanu systemowej ochrony komponentu informatycznego infrastruktury krytycznej w Polsce

Pomimo upływu blisko roku od formalnego wejścia w życie strategii cyberbezpieczeństwa, którą *de facto* stanowią Krajowe Ramy Polityki Cyberbezpieczeństwa na latach 2017–2022, w dalszym ciągu brak w Polsce jednego ośrodka decyzyjnego, koordynującego działania wszystkich instytucji publicznych w zakresie cyberbezpieczeństwa. Trudno uznać za taki ośrodek powołane w lipcu 2017 roku Narodowe Centrum Cyberbezpieczeństwa (działające w ramach NASK), które głównie pośredniczy w wymianie informacji o cyberzagrożeniach, a ponadto współpraca z nim nie jest obligatoryjna. Czynności z zakresu reagowania na incydenty są z różną skutecznością realizowane przez funkcjonujące niezależnie od siebie państwowe i prywatne zespoły CERT, zajmujące się swoimi własnymi obszarami oddziaływania. Na ten brak decyzyjnej koordynacji uwagę zwracała już Najwyższa Izba Kontroli, w której raporcie z 2015 roku (*Informacja…*) stwierdzono, że jest to kluczowy czynnik paraliżujący aktywność państwa w zakresie ochrony infrastruktury teleinformatycznej. Administracja publiczna nie wdrożyła również zintegrowanego i systemowego wspierania przez państwo badań w obszarze ochrony cyberprzestrzeni.

Równie aktualny jest wniosek z raportu NIK o braku stabilnego systemu finansowania działań związanych z ochroną polskiej cyberprzestrzeni, co znajduje potwierdzenie w niezabezpieczeniu w budżecie Ministerstwa Cyfryzacji na rok 2018 środków na wdrożenie Krajowych Ram Polityki Cyberbezpieczeństwa (*Ministerstwo cyfryzacji…*).

Zgodnie z przepisami ustawy o zarządzaniu kryzysowym obowiązek ochrony w zakresie zapewnienia bezpieczeństwa informatycznego ciąży na właścicielach infra-

struktury krytycznej oraz jej posiadaczach samoistnych i zależnych. W żadnych krajowych uregulowaniach prawnych nie określono jednak sankcji za niedopełnienie wskazanych obowiązków, co skutkuje niezadowalającą ochroną wielu elementów infrastruktury przed incydentami w zakresie bezpieczeństwa sieci i informacji. Przykładowo w 2016 roku jedynie 69% organizacji dokonało wymaganych prawem weryfikacji bezpieczeństwa systemów komputerowych (*Blackout*…). W 2017 roku tylko 8% przedsiębiorstw posiadło wysokie kompetencje w zakresie cyberbezpieczeństwa (do szczególnie dobrze zabezpieczonych należą przedsiębiorstwa z sektorów energetycznego i finansowego), natomiast 46% firm nie posiadło żadnych operacyjnych procedur reakcji na cyberincydenty (*Cyber-ruletka*…).

Dla oceny stanu gotowości państwa do obrony przed zagrożeniem cybernetycznym istotne jest także podkreślenie, że nie przeprowadzono dotychczas w Polsce inwentaryzacji rozproszonych w różnych aktach prawnych przepisów związanych z cyberbezpieczeństwem, co skutkuje chaosem definicyjnym, a w konsekwencji kompetencyjnym. Może to w praktyce oznaczać niedobór czy nawet brak aktywności ochronnej w jednym miejscu, natomiast w innym dublowanie takich działań, a przez to prawdopodobne marnotrawienie ograniczonych zasobów.

Podsumowanie

Systemy informatyczne infrastruktury krytycznej są wrażliwe na różnorodne zakłócenia ze względu na swoją wewnętrzną złożoność, a także dużą współzależność poszczególnych składników samej infrastruktury. Systemy te stanowią zarazem pierwszoplanowy cel cyberataków. Pomimo ewidentnego zagrożenia takim atakami, wynikającego m.in. z obecnej sytuacji geopolitycznej, świadomość ryzyka i konsekwencji z tym związanych wydaje się być w Polsce słabo rozpowszechniona. Skutkuje to jak dotychczas brakiem dostatecznej presji wywieranej przez polskie społeczeństwo na decydentów, w celu stworzenia realnych, rzetelnie finansowanych cyberzabezpieczeń infrastruktury krytycznej.

Należy wskazać, iż w ostatniej dekadzie powstało w Polsce wiele założeń, opracowań i dokumentów, mających być podstawą do stworzenia skutecznej, systemowej cyberobrony, co w praktyce nie przyniosło jednak oczekiwanych rezultatów. Istotnej zmiany w tym zakresie można obecnie upatrywać w ciążącym na państwie polskim obowiązku implementacji unijnej dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS, 2016). Przepisy tej dyrektywy, przewidziane do wprowadzenia w życie za pośrednictwem ustawy o cyberbezpieczeństwie (każdy kraj UE zobligowany jest uchwalić taką ustawę w ciągu 21 miesięcy od wejścia w życie dyrektywy NIS), narzucą państwu polskiemu wymóg regulacyjnego (sanacyjnego) zapewnienia realnych zdolności do w pełni skoordynowanych działań w zakresie zapobiegania, wykrywania, zwalczania oraz minimalizacji skutków cyberincydentów.

Literatura

Blackout po ataku na Ukrainę, ochrona infrastruktury i wsparcie państwa. Jak zabezpieczyć sieci energetyczne przed cyberatakiem? (2016). Pobrano z: www.energetyka24.com (29.11.2016).

Budziewicz-Guźlecka, A. (2010). Istota wykluczenia społecznego w społeczeństwie informacyjnym. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Informatyka Ekonomiczna, 17* (118), 241–249.

Budziewicz-Guźlecka, A. (2015). Uwarunkowania polityki gospodarczej. W; J. Buko (red.), *Polityka gospodarcza. Wybrane zagadnienia* (s. 77–108). Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście. (2018). 5. edycja Badania Stanu Bezpieczeństwa Informacji, PWC. Pobrano z: www.pwc.pl (30.01.2018).

Czaplewski, M. (2017). Wzmacnianie zaufania użytkowników e-commerce jako czynnik rozwoju tej formy handlu. W: K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *E-obywatel. E-sprawiedliwość* (s. 419–433). Warszawa: C.H. Beck.

Drab-Kurowska, A. (2013). Polityka konkurencji na rynku e-commerce. *Ekonomiczne Problemy Usług, 104* (t. 1), 501–511.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Eastwood J.P. i in. (2017). The Economic Impact of Space Weather: Where Do We Stand? *Risk Analysis*, *37* (2), 206–218.

Europol: 4 tys. cyberataków dziennie, narażona infrastruktura krytyczna (2017). Pobrano z: cyberdefence24.pl (14.11.2017).

Extreme space weather: impacts on engineered systems and infrastructure (2013). Pobrano z: www.raeng.org.uk (10.01.2018).

Informacja o wynikach kontroli. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej(2015). Pobrano z: www.nik.gov.pl (30.06.2015).

Instytut Kościuszki: W 2018 roku wzrośnie liczba cyberataków na infrastrukturę krytyczną (2018). Pobrano z: biznesalert.pl (3.01.2018).

konradswirski.blog.tt.com.pl (14.07.2014).

KPMG.pl (2018). *Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym*. Raport KPMG (29.01.2018).

Leśnikowski, W. (2011). *Cyberataki na infrastrukturę krytyczną jako tanie i skuteczne środki do paraliżowania rozwiniętych państw*. Bydgoszcz: Centrum Doktryn i Szkolenia Sił Zbrojnych.

Milewski, J. (2016). Identyfikacja infrastruktury krytycznej i jej zagrożeń, *Zeszyty Naukowe AON. Akademia Sztuki Wojennej, 4* (105).

Ministerstwo cyfryzacji nie ma środków na strategię cyberbezpieczeństwa? (2017). Pobrano z: cyberdefence24.pl (30.09.2017).

Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity (2015). Pobrano z: rcb.gov.pl (28.06.2016).

Polskie firmy narażone na cyberataki (2017). Pobrano z: www.pulshr.pl (23.03.2017).

Przestępstwa przeciwko mieniu (278–295) (2018). Pobrano z: statystyka.policja.pl. (10.01.1018).

Strategia cyberbezpieczeństwa przyjęta przez rząd (2017). Pobrano z: www.gov.pl (20.11.2017).

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym. Dz.U. 2007 nr 89, poz. 590.

Ustawa z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym. Dz.U. 2010, nr 240, poz. 1600.

W Polsce powstaje specsłużba do odpierania cyberataków. Ma liczyć tysiąc osób i kosztować dwa miliardy złotych (2018). Pobrano z: innowacje.newseria.pl (19.01.2018).

www.egospodarka.pl (07.07.2017).

Zuber, M. (2014). Infrastruktura krytyczna państwa jako obszaru potencjalnego oddziaływania terrorystycznego. *Rocznik Bezpieczeństwa Międzynarodowego*, *2*.

HAZARD PROBLEMS FOR SYSTEMS OF INFORMATION AND OPERATIONAL TECHNOLOGIES USED IN POLISH CRITICAL INFRASTRUCTURE

Keywords: critical infrastructure, threats for systems of information and operational technologies, state security

Summary. Critical infrastructure consists of systems, devices, facilities and services essential for the security of the state and its citizens. The widespread use of information technology makes the state more effective and the economy more efficient. However, the cyber infrastructure connected in this way is more vulnerable to various threats. The objectives of the considerations presented in this article are: to analyze threats for systems of information and operational technologies used in critical infrastructure, and then attempt to characterize and evaluate activities aimed at counteracting these types of threats in Poland.

Translated by Jacek Buko

Cytowanie

Buko, J. (2018). Problematyka zagrożeń dla systemów informatycznych polskiej infrastruktury krytycznej. *Ekonomiczne Problemy Usług*, *2* (131/1), 69–78. DOI: 10.18276/epu.2018.131/1-07.