Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny

Grzegorz Abgarowicz, Ryszard Antkiewicz, Piotr Ciepiela, Michał Dyk, Dominika Dziwisz, Zbigniew Fałek, Piotr Gajek, Rafał Kasprzyk, Włodzimierz Kotłowski, Mirosław Maj, Andrzej Najgebauer, Dariusz Pierzchała, Aleksander Poniewierski, Maciej Pyznar, Mirosław Ryba, Krzysztof Rzecki, Joanna Świątkowska, Zbigniew Tarapata, Agnieszka Wiercińska-Krużewska

Partner Główny

EY
Building a better working world

Partner Merytoryczny

RCB
Rządowe Centrum Bezpieczeństwa

Instytut Kościuszki

Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny

Grzegorz Abgarowicz, Ryszard Antkiewicz, Piotr Ciepiela,
Michał Dyk, Dominika Dziwisz, Zbigniew Fałek,
Piotr Gajek, Rafał Kasprzyk, Włodzimierz Kotłowski,
Mirosław Maj, Andrzej Najgebauer, Dariusz Pierzchała,
Maciej Pyznar, Aleksander Poniewierski,
Mirosław Ryba, Krzysztof Rzecki, Joanna Świątkowska,
Zbigniew Tarapata, Agnieszka Wiercińska-Krużewska

Instytut Kościuszki

Jeżeli doceniają Państwo wartość merytoryczną niniejszej publikacji, zachęcamy do finansowego wsparcia przyszłych inicjatyw wydawniczych Instytutu.

Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny

Maciej Pyznar, Grzegorz Abgarowicz, Agnieszka Wiercińska-Krużewska, Piotr Gajek, Joanna Świątkowska, Dominika Dziwisz, Mirosław Ryba, Aleksander Poniewierski, Włodzimierz Kotłowski, Piotr Ciepiela, Mirosław Maj, Ryszard Antkiewicz, Michał Dyk, Rafał Kasprzyk, Andrzej Najgebauer, Dariusz Pierzchała, Zbigniew Tarapata, Krzysztof Rzecki, Zbigniew Fałek.

Redakcja: Joanna Świątkowska

Pomoc w edycji: Anna Hojcak

Zespół Instytutu Kościuszki pracujący nad czynnikami wpływającymi na bezpieczeństwo oraz nad rekomendacjami przygotowanymi na bazie treści rozdziałów: Joanna Świątkowska, Zbigniew Fałek

Projekt i skład graficzny: Małgorzata Kopecka

W Rysunkach 7. i 11. użyto ikon z Noun Project: Arrow by Roman J. Sokolov, Skull and Crossbones by Andrew Cameron, Factory by Patrick Trouvé, Key by Márcio Duarte, Settings by Luis Rodrigues, Security by mohit arora, Route by Carlos Valério, Server Security by Roman Kovbasyuk, Laptop by Simple Icons, Analysis by Christopher Holm-Hansen, Network by Matthew Hawdon, Flow Chart by Jhun Capaya, Server by Jaime Carrion, Gears by Hysen Drogu, Computer by Simple Icons, Server by Alf.

Zamknięcie składu: sierpień 2014

Instytut Kościuszki
ul. Lenartowicza 7/4
31-138 Kraków
e-mail: ik@ik.org.pl
+48 12 632 97 24
www.ik.org.pl

ISBN: 978-83-63712-15-0

Spis treści

Nie wszystkie opinie wyrażone w niniejszej publikacji przez jej autorów odzwierciedlają oficjalne stanowisko programowe Instytutu Kościuszki oraz partnerów publikacji. Stanowią one wkład w debatę publiczną. Tezy zawarte w publikacji odzwierciedlają stanowiska poszczególnych autorów, niekoniecznie stanowiąc opinie pozostałych.

Wprowadzenie

Joanna Świątkowska, Zbigniew Fałek
– Instytut Kościuszki

Infrastruktura krytyczna (IK) jest kluczowym elementem z punktu widzenia bezpieczeństwa narodowego, stabilności i rozwoju gospodarczego, funkcjonowania społeczeństw oraz pojedynczych obywateli. Choć infrastruktura, mająca szczególne znaczenie dla funkcjonowania człowieka i tworzonych przez niego społeczności, istniała od czasów najdawniejszych, to wraz z rozwojem cywilizacyjnym jej znaczenie stale rosło. Coraz bardziej istotne, przede wszystkim w ostatnich latach, stawało się także zapewnianie jej bezpieczeństwa.

Punktem zwrotnym w debacie związanej z ochroną IK były zamachy terrorystyczne z 11 września 2001 r. mające miejsce w Stanach Zjednoczonych, a następnie te z 2004 r. z Londynu i Madrytu. Uświadomiły one, po pierwsze, jak dramatyczne konsekwencje mogą mieć ataki nakierowane na najbardziej newralgiczne infrastruktury; po drugie, jak bardzo poszczególne elementy infrastruktur są współzależne[1], oraz w końcu to, że zagrożeniem dla funkcjonowania państw mogą być nie tylko aktorzy państwowi, ale także podmioty niepaństwowe. W następstwie, poszczególne państwa i organizacje miedzynarodowe (np. Unia Europejska) zintensyfikowały swoje działania, których celem stała się ochrona IK.

Współcześnie jednak obserwujemy jeszcze jeden trend, kluczowy z punktu widzenia zapewniania ochrony IK – jest nim wzrost roli i wagi cyberbezpieczeństwa jako fundamentu funkcjonowania i bezpieczeństwa IK. To właśnie cyberbezpieczeństwo IK jest głównym tematem niniejszego raportu.

O rozwiązaniach teleinformatycznych w kontekście IK możemy mówić na dwa sposoby. Po pierwsze, w Polsce sieci teleinformatyczne to jeden z systemów należących do IK. Po drugie systemy teleinformatyczne są częścią różnych systemów IK wspierając, a często warunkując ich poprawne funkcjonowanie. Rozwiązania teleinformatyczne mogą zatem same w sobie stanowić IK, jak również mogą być częścią innych IK.

Co nam zagraża?

Wzrastające uzależnienie funkcjonowania IK od rozwiązań teleinformatycznych i zmiany jakie dokonują się w tym środowisku prowadzą do powstania nowych wyzwań dla zapewniania

1 Więcej: B. Hammerli, A. Renda, *Protecting Critical Infrastructure in the EU*. CEPS Task Force Report, 2010, s. 12.

bezpieczeństwa. Zagrożeniem mogą być zarówno możliwe usterki techniczne, błędy ludzkie, ale również intencjonalne, wrogie działania prowadzone w cyberprzestrzeni. Z co najmniej kilku powodów to właśnie ten ostatni rodzaj zagrożeń staje się coraz bardziej istotny.

Zakłócenie funkcjonowania IK lub doprowadzenie do jej zniszczenia mogą być efektem dokonania ataku na jej teleinformatyczne elementy. Działania w cyberprzestrzeni cechują między innymi relatywnie niskie koszty przygotowania i przeprowadzenia ataku przy jednoczesnym dużym potencjale zadania poważnych strat stronie zaatakowanej. Dodatkowym „atutem" jest trudność wykrycia sprawcy i udowodnienia mu winy,[2] skutkująca zarówno jego względnym bezpieczeństwem, rozumianym jako możliwość uniknięcia działań odwetowych, ale i szeroko pojętej odpowiedzialności. Potencjalna dotkliwość strat, łatwość dokonania ataku i przerzucenia odpowiedzialności sprawia, że cyberataki skierowane na IK mogą stać się kluczową bronią w rękach państw, ale także podmiotów niepaństwowych.

Jak wskazuje „The Cyber Index. International Security Trends and Realities", przygotowany pod auspicjami ONZ, gwałtownie wzrasta liczba państw, które oficjalnie w ramach sił zbrojnych tworzą specjalne podmioty dedykowane działaniu w cyberprzestrzeni (także mające zdolności ofensywne)[3]. Wszystko to pokazuje, że cyberprzestrzeń może w przyszłości stać się ważnym obszarem prowadzenia konfliktu. Cyberatak przeprowadzony na IK może zdestabilizować działania państwa w sytuacji napięcia politycznego, może stać się także ważnym elementem kampanii wojennej w sytuacji otwartego konfliktu.

Przygotowanie do przeprowadzenia potencjalnego ataku może mieć miejsce jeszcze w okresie pokoju. Doniesienia medialne coraz częściej wskazują, że gwałtownie wzrastają masowe działania cyberszpiegowskie, które skierowane są na podmioty z systemów powszechnie zaliczanych do IK[4]. Pomimo że w większości działania te są realizowane z pobudek finansowych, dają możliwość uzyskiwania wiedzy i dostępu do systemu, który w przyszłości może być celem ataku. Są także inne metody „przygotowujące grunt" pod potencjalne ataki. Wystarczy uświadomić sobie, że korzystamy z produktów teleinformatycznych (sprzęt, oprogramowanie itd.) produkowanych na terenach państw z całego świata. Nie trudno jest zatem implementować wrogie elementy, które aktywowane w odpowiednim momencie mogą doprowadzić do uszkodzenia funkcjonowania całego systemu.

Współcześnie inne państwa nie są jedynym źródłem zagrożenia. Choć dokonanie przez aktorów niepaństwowych[5] zmasowanego cyberataku na IK, mającego rozległe skutki w skali kraju wydaje się na tę chwilę mało prawdopodobne[6], z punktu widzenia pojedynczych infrastruktur – zagrożenie to jest już większe.

2 Problem atrybucji.

3 Center for Strategic and International Studies, Institute for Peace Research and Security Policy, *The Cyber Index. International Security Trends and Realities*, UNIDIR, 2013, s. 3.

4 Przykładowe zestawienie systemów, które obejmuje infrastruktura krytyczna w wybranych państwach znajduje się na przykład w Haemmerli, A. Renda, *CEPS Task Force Report. Protecting Critical Infrastructure in the EU*, 2010, http://www.ceps.eu/book/protecting-critical-infrastructure-eu, [dostęp: 05.03.2014].

5 Pojedynczy napastnicy, cyberterroryści, organizacje przestępcze, ale w tym kontekście nie wspierane przez państwa.

6 Z uwagi na brak zaawansowanej wiedzy koniecznej do dokonania takiego ataku, oraz innych wystarczających szeroko rozumianych zasobów.

W końcu, prócz potencjalnych zagrożeń intencjonalnych związanych z użyciem narzędzi cyfrowych, kluczowe pozostaje zapewnianie ochrony przed błędami, awariami technicznymi, ludzkimi czy nawet zagrożeniami o charakterze naturalnym.

Cele raportu i jego struktura

Dostrzegając fundamentalne znaczenie IK dla bezpieczeństwa państwa Instytut Kościuszki postanowił uczynić jej ochronę przedmiotem niniejszego raportu. Wzrastająca rola i znaczenie cyberbezpieczeństwa IK zdecydowało o tym, że aspekt ten stał się głównym elementem analizy. Naszą ambicją jest, aby niniejszy raport stanowił ważny wkład w toczącą się debatę nad ochroną IK, szczególnie w kontekście wymiaru związanego z cyberbezpieczeństwem.

Głównym celem raportu jest dostarczenie podmiotom bezpośrednio odpowiedzialnym za ochronę IK rekomendacji przyczyniających się do zwiększenia poziomu bezpieczeństwa. Rekomendacje zbudowane zostały na podstawie analizy czynników mających wpływ zarówno na ogólnie rozumianą ochronę IK oraz na bezpieczeństwo teleinformatyczne IK. Czynniki wyselekcjonowane zostały z poszczególnych rozdziałów raportu i stanowią ich najważniejsze elementy.

Struktura raportu odzwierciedla wyżej zarysowany cel i zadania postawione przed autorami. Raport podzielony został na dwie części. Pierwsza zawiera ogólne, systemowe rozważania związane z IK i zapewnianiem jej bezpieczeństwa. W sposób szczególny podkreślona została tematyka identyfikacji IK (co jest warunkiem bazowym skutecznej jej ochrony), prawnych aspektów związanych z bezpieczeństwem IK oraz współpracy prywatno-publicznej. Ta część raportu stanowi zatem materiał skierowany głównie do decydentów i podmiotów całościowo odpowiedzialnych za bezpieczeństwo państwa.

Część druga poświęcona została *stricte* wymiarowi teleinformatycznemu. Wskazane zostały najbardziej newralgiczne czynniki związane z cyberbezpieczeństwem IK oraz jednocześnie dobre praktyki i kierunki działań pozwalające prowadzić bardziej efektywne działania. Znaczna część rekomendacji zawiera propozycje zmian systemowych, część zaś zostało skierowanych[7] do właścicieli i operatorów IK i z uwagi na to, mają one charakter bardziej szczegółowy.

Część pierwszą otwiera rozdział przygotowany przez Macieja Pyznara i Grzegorza Abgarowicza z Rządowego Centrum Bezpieczeństwa. Nie tylko wprowadza on czytelnika w najważniejsze informacje związane z tym czym jest IK, ale także pokazuje najważniejsze, wybrane elementy systemu ochrony IK na poziomie państwa. Najważniejszym element rozdziału stanowią rozważania na temat procesu identyfikacji IK.

Rozdział drugi, który został przygotowany przez kancelarię prawniczą Wierciński-Kwieciński-Baher stanowi analizę uwarunkowań prawnych IK zarówno na poziomie krajowym, jak i międzynarodowym. W sposób szczególny analizie poddane zostały elementy finansowania działań z zakresu ochrony IK, problematyka zamówień publicznych oraz elementy budowania współpracy prywatno-publicznej.

7 Lub bezpośrednio ich dotyczy.

Rozdziały trzeci i czwarty części pierwszej, opracowane przez ekspertów Instytutu Kościuszki: Joannę Świątkowską i Dominikę Dziwisz, należy traktować komplementarnie. Oba poświęcone są problematyce współpracy prywatno–publicznej i czynnikom wpływającym na jej efektywność. Współcześnie większość IK znajduje się w rękach prywatnych lub jest przez sektor prywatny obsługiwana. Ponieważ efektywna współpraca na linii państwo – właściciel lub operator IK jest warunkiem podstawowym skutecznej ochrony, problematyka ta stanowi ważny element pierwszej części raportu.

Część drugą raportu rozpoczyna rozdział autorstwa Mirosława Ryby z firmy EY, pokazujący jaką rolę z punktu widzenia funkcjonowania i bezpieczeństwa IK odgrywają rozwiązania teleinformatyczne. Szczególnie uwzględnione zostało zastosowanie systemów informatycznych (IT) oraz systemów sterowania przemysłowego (OT).

Rozdział drugi, także przygotowany przez eksperta z firmy EY – Aleksandra Poniewierskiego, opisuje główne zmiany jakie dokonały się w obszarze funkcjonowania rozwiązań teleinformatycznych stosowanych w IK. Zmiany te dokonały się na poziomie ekonomicznym, technologicznym i organizacyjnym w sposób ścisły przekładają się na wyzwania związane z zapewnieniem bezpieczeństwa IK. Ich zrozumienie i uświadomienie jest konieczne, aby podejmować skuteczne działania.

Rozdział trzeci, napisany przez Włodzimierza Kotłowskiego z firmy MATIC, pokazuje w jaki sposób rozwiązania teleinformatyczne znajdują zastosowanie w efektywnej ochronie IK.

Rozdział czwarty, którego autorem jest Piotr Ciepiela z firmy EY, poświęcony jest bezpieczeństwu OT – newralgicznemu elementowi całego cyberbezpieczeństwa IK. Rozdział przedstawia nie tylko najważniejsze standardy związane z bezpieczeństwem OT (w mniejszym stopniu także IT), ale również wskazuje inne rozwiązania zapewniające i zwiększające bezpieczeństwo.

Cyberbezpieczeństwo IK wymaga także dobrze zorganizowanego procesu reagowania na incydenty. W rozdziale piątym, opracowanym przez Mirosława Maja – Prezesa Fundacji Bezpieczna Cyberprzestrzeń, przedstawione zostały dobre praktyki związane z tym wymiarem, a także krótka analiza incydentów, jakie zagrażają bezpieczeństwu teleinformatycznemu IK.

W rozdziale szóstym zaprezentowano autorską koncepcję pakietu narzędzi informatycznych zwiększających efektywność wykrywania, przeciwdziałania i neutralizacji skutków cyberzagrożeń przygotowaną przez Zespół pod kierownictwem profesora Najgebauera z Wojskowej Akademii Technicznej. Prezentowana koncepcja może mieć szerokie zastosowania wykraczające poza obszar stricte wojskowy, a obejmujący np. zarządzanie kryzysowe na różnych szczeblach administracji państwowej i samorządowej.

Ostatni rozdział przygotowany przez Krzysztofa Rzeckiego z Politechniki Krakowskiej zawiera analizę programu studiów wyższych w zakresie ochrony systemu sieci teleinformatyczne należącego do IK.

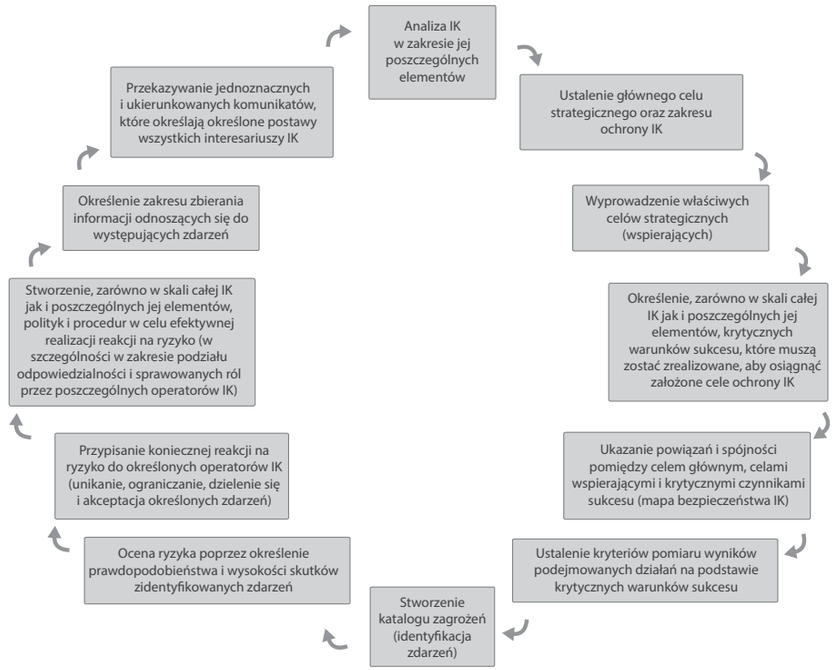
Raport zamykają rekomendacje.

Poniżej (patrz rysunek 1) przedstawiony został schemat procesu zawierający najważniejsze elementy związane z zapewnianiem bezpieczeństwa IK. Raport dotyka większości zaproponowanych elementów, jednak nie aspiruje on do bycia materiałem całkowicie wyczerpującym problematykę bezpieczeństwa IK. Jest to wynikiem przede wszystkim wynikiem rozległości tematyki związanej tak z IK w ogóle, jak i z wymiarem teleinformatycznym jej funkcjonowania.

Analiza czynników wpływających na bezpieczeństwo IK nie tylko pozwoliła przygotować zestaw podstawowych rekomendacji zawartych w raporcie, ale pokazała także elementy, które muszą stać się przedmiotem dalszych analiz. Mając świadomość braku wielu istotnych kwestii, które nie sposób było zawrzeć w jednym dokumencie, mamy nadzieję kontynuować pracę i rozwijać badania.

W końcu, z uwagi na fakt, że całość raportu przygotowana została w oparciu o jawne, ogólnodostępne źródła, czytelnik winien mieć świadomość, że nie dotyka on w pełni wszystkich informacji, które mogą mieć znaczenie z punktu widzenia bezpieczeństwa IK i może pomijać niektóre specyficzne dla danych zasobów czynniki.

Rysunek 1. Proces zapewniania bezpieczeństwa infrastruktury krytycznej – najważniejsze elementy.
Źródło: Opracowanie własne.



część I

1. Rola infrastruktury krytycznej w funkcjonowaniu państwa

Maciej Pyznar, Grzegorz Abgarowicz
– Rządowe Centrum Bezpieczeństwa

Rozwój infrastruktury i wzrost jej znaczenia

Rozwój technologiczny determinowany jest potrzebami człowieka. Proces oswajania natury poprzez ingerencję techniczną w otoczenie towarzyszył człowiekowi niemalże od samego początku. Rozwój rolnictwa wynikał z potrzeby zapewnienia pożywienia, rozwój przemysłu miał ułatwić człowiekowi egzystencję, zaś rozwój medycyny był odpowiedzią na zagrożenia życia. To właśnie człowieczeństwo determinuje chęć oraz potrzebę kreacji środowiska i jego ciągłej modyfikacji. W „Książeczce o człowieku" Roman Ingarden pisze: *ludźmi jesteśmy przez to, że żyjemy w pewnym sensie „ponad stan", że ponad wszystko co jest nam potrzebne do utrzymania naszego fizjologicznego życia (…) stwarzamy pewne „rzeczy", luksus dla życia fizjologicznego stanowiące (…). Jesteśmy ludźmi przez to, że przerastamy warunki biologiczne, w jakich znaleźliśmy się, i że na ich podłożu budujemy nowy, odmienny świat*[1].

Skutkiem aktywności człowieka, na ingardenowski dualizm: człowiek – natura zostaje nałożona warstwa nie tylko kultury, ale także technologii czy rozwiązań społecznych. Owymi „rzeczami" są zarówno państwo jak i infrastruktura. Ponieważ koncepcje społeczne czy kulturowe są niejako wpisane w człowieczeństwo i przez nie redukowane, ów dualizm przekształca się w triadę: człowiek – natura – technologia.

Człowiek przywykł do obecności infrastruktury w jego życiu i zdaje się nie zauważać, że dostęp do niej stał się powszechnie udziałem ludzkości całkiem niedawno. Początkiem takiego stanu rzeczy była rewolucja przemysłowa i technologiczna przełomu XIX i XX w. Rewolucja ta zapoczątkowała zmiany w całej strukturze społecznej, które były determinowane przede wszystkim poprzez rozbudowę miast. Wraz ze zwiększaniem się populacji ludności w miastach, gwałtownie zaczęły rosnąć potrzeby ludzi w nich zamieszkujących. Potrzeby te wypływały nie tylko z chęci zaspokojenia indywidualnych potrzeb mieszkańców, ale również z potrzeb zbiorowych populacji np. ochrony przed przestępczością czy chorobami, wzajemnej komunikacji czy transportu. W Polsce, choć obarczonej bagażem negatywnych doświadczeń historycznych, rozwój ten przebiegał podobnie jak w innych krajach. Dla zobrazowania fenomenu rozwoju technologicznego warto prześledzić ewolucje chociażby niektórych jego elementów.

1 R. Ingarden, *Książeczka o człowieku*, Wydawnictwo Literackie Kraków, Kraków 1987, s. 37.

W 1929 r. w Polsce czynnych było 57 elektrowni o mocy powyżej 5 MW i łącznej mocy 636 MW[2]. Ich łączna produkcja wynosiła 2355 GWh. Na dzień 30 września 2013 r. moc zainstalowana ogółem w polskich elektrowniach wynosiła 38490,1 MW[3], a produkcja energii elektrycznej w roku 2011 wyniosła 163 118 GWh[4] – prawie 70 razy więcej. Analizując te dane należy pamiętać, że przed II wojną światową elektrownie nie stanowiły połączonego systemu, gdyż nie powstała jeszcze ogólnopolska sieć elektroenergetyczna[5]. Systemy elektroenergetyczne w ich obecnym kształcie rozwinęły się dopiero po II wojnie światowej, czyli zaledwie 70 lat temu.

Na początku XIX w. szklanka zwykłej wody mogła ugasić pragnienie lub zabić. Bezpieczna woda pitna, którą obecnie traktuje się jako oczywisty element życia, nie była powszechnie dostępna, a śmiertelne choroby przenoszone przez wodę, takie jak cholera, dur brzuszny czy dyzenteria, były stałym i realnym zagrożeniem[6]. Pierwsza oczyszczona woda popłynęła do mieszkańców Warszawy 3 lipca 1886 r. W 2012 r. w kraju mieliśmy 8 748 przedsiębiorstw wodociągowo-kanalizacyjnych zaopatrujących w wodę ponad 37 mln ludności[7].

W 1927 r. firma Robert Bosch Gmbh wprowadziła do produkcji układ wtryskowy do silnika wysokoprężnego[8] (skonstruowanego przez Rudolfa Diesel'a w 1893 r.), co umożliwiło jego szerokie zastosowanie w motoryzacji i transporcie samochodowym. W tymże samym 1927 r. w Polsce było zaledwie 45 500 km bitych dróg[9], po których mogły się poruszać ciężarówki napędzane takim silnikiem. W 2011 r. w Polsce mieliśmy już 280 000 km dróg o utwardzonej powierzchni[10], którymi w 2012 r. przewieziono 1 545 mln ton towarów[11].

Od 1927 do 2012 r. długość linii kolejowych wzrosła z 17 146 km do 20 094 km[12]. Można byłoby wskazać, że to tylko 2 948 km więcej. Niemniej, trzeba jednak wziąć pod uwagę, że ponad połowa z tych linii jest zelektryfikowana[13], a koleją w 2012 przewieziono ponad 230 mln ton towarów (w 1927 r. 73,7 mln ton[14]).

2 *Mały rocznik statystyczny 1930*, tabl. 5, „Elektrownie w Polsce", s. 33, http://statlibr.stat.gov.pl/exlibris/aleph/a18_1/apache_media/4U9MMALMHKN1ENV6KTGHPGE9HDUFM8.pdf, [dostęp: 08.04.2014]. Największe elektrownie zawodowe około 1938 r. to: El. Powiśle 83 MW, El. Pruszków 31.5 MW, Łaziska 105 MW, Będzin 23.5 MW, Zabrze 70.3 MW, Szombierki 51.2 MW, Łódź 101 MW, Garbary w Poznaniu 42 MW, *Historia polskiej elektryki*, http://www.wnp.pl/artykuly/historia-polskiej-energetyki,5327.html, [dostęp: 08.04.2014]. Dla porównania moc elektryczna zainstalowana w elektrowni Bełchatów wynosi 5298 MW.

3 CIRE.pl, http://www.rynek-energii-elektrycznej.cire.pl/st,33,207,tr,75,0,0,0,0,0,0,podstawowe-dane.html, [dostęp: 10.04.2014].

4 Ibidem.

5 *Historia polskiej energetyki*, http://www.wnp.pl/artykuly/historia-polskiej-energetyki,5327.html, [dostęp – 08.04.2014].

6 *Greatest Engineering Achievements of the 20th Century*, http://www.greatachievements.org/?id=3610, [dostęp – 08.04.2014]. Dla unaocznienia jak młodym osiągnięciem jest dostarczanie czystej wody proponujmy prześledzić dokonania ludzkości na przedstawionej na przywołanej stronie osi czasu.

7 Główny Inspektorat Sanitarny, „Stan sanitarny kraju w 2012 r.", tabl. 22. „Struktura przedsiębiorstw wodociągowo-kanalizacyjnych w 2012 r.", s. 76. Ciekawie wygląda natomiast sytuacja w przypadku odprowadzania i oczyszczania ścieków. Jak podaje *Mały rocznik statystyczny Polski 2013* (s. 49) w 2012 r. oczyszczalnie ścieków obsługiwały tylko 69% ludności kraju (w miastach 92%, na wsi, gdzie mieszka ok. 39% ludności kraju, jedynie 33%).

8 F. DeLuca, *History of fuel injection,* http://www.disa.it/pdf/01HystoryOfDieselFuelInj.pdf, [dostęp: 08.04.2014].

9 *Mały rocznik statystyczny 1930 r.*, tabl. 8, „Drogi Bite w Polsce w latach 1925 – 1928", s. 55.

10 *Mały rocznik statystyczny Polski 2013*, tabl. 1 (237), „Sieć Komunikacyjna", s. 379.

11 Ibidem.

12 *Mały rocznik statystyczny Polski 2013*, tabl. 1 (237), „Sieć Komunikacyjna", s. 379 oraz *Mały rocznik statystyczny 1930 r.*, tabl. 1, „Długość linii i tabor w latach 1922 – 1928", s. 52.

13 *Mały rocznik statystyczny Polski 2013*, tabl. 1 (237), „Sieć Komunikacyjna", s. 379. Pamiętać należy również o tym, że elektryfikacja linii kolejowych w Polsce nastąpiła dopiero po II wojnie światowej.

14 *Mały rocznik statystyczny 1930 r.*, tabl. 3, „Przewóz pasażerów i towarów w latach 1922 – 1928", s. 52.

W 1928 r. w Polsce było 126 tys. abonentów telefonicznych, którzy ogółem wykonali 672 mln rozmów[15]. W całej Polsce w 1929 r. było 157 tys. aparatów telefonicznych[16], co oznacza, że aparatem telefonicznym dysponowało wtedy zaledwie około 0,5% populacji[17]. W 2012 r. z usług telefonii stacjonarnej korzystało blisko 7,4 mln abonentów (blisko 20% populacji[18]), a łączny wolumen ruchu osiągnął poziom 13 mld minut[19].

Oczywiście w przedwojennej Polsce, jak i w całym ówczesnym świecie, nie znano jeszcze wynalazku telefonii mobilnej. W 2012 r. w Polsce operatorzy mieli zarejestrowanych w swoich bazach łącznie ponad 53,9 mln kart SIM[20] (140% procent populacji), natomiast całkowity czas połączeń głosowych wychodzących w 2012 r. to ponad 69 mld minut[21].

O nowym medium łączności, jakim jest Internet, nie słyszano na świecie jeszcze na początku drugiej połowy XX w., a dziś w Polsce mamy ponad 11,6 mln abonentów usług dostępu do Internetu[22] (co odpowiada nasyceniu usługami Internetu w przeliczeniu na gospodarstwo domowe na poziomie 83,5%[23]). Nie można również zapomnieć o usługach, które narodziły się wraz z Internetem np. VoIP (VoIP – ang. *Voice over IP*). W 2012 r. z usługi tej skorzystało (odpłatnie) łącznie ponad 1,1 mln użytkowników[24].

Analizując, na przykładzie Polski, ilościowy i jakościowy rozwój infrastruktury należy jeszcze zwrócić uwagę na dwa determinanty.

Po pierwsze, w większości przypadków infrastruktura dostarczająca nam usługi jest od nas, w sensie geograficznym, oddalona[25]. Jej właścicielami są specjalnie do tego celu utworzone przedsiębiorstwa, a odbiorca usługi ma znikomy wpływ na jej pracę. Na taki stan rzeczy wpływ miały przynajmniej trzy czynniki:

- brak odpowiednich technologii do zastosowań jednostkowych – w przeszłości nie dysponowano technologiami umożliwiającymi pojedynczym gospodarstwom domowym na uniezależnienie się od infrastruktury (oczywiście nie można brać pod uwagę sytuacji, gdy, np. na terenach wiejskich, człowiek w ogóle nie korzystał z infrastruktury), a finansowanie rozwoju technologicznego było poza zasięgiem przeciętnego obywatela. Współcześnie, sytuacja ta ulega zmianie i coraz częściej dysponujemy taką technologią, np. ogniwa fotowoltaiczne generujące prąd, przydomowe oczyszczalnie ścieków, filtry jonowe do uzdatniania wody itp.;

15 Ibidem, tabl. 24, „Telefony w Polsce w latach 1924 – 1928", s. 61.

16 Ibidem, tabl. 27, „Stan liczbowy telefonów w niektórych państwach w 1929 r.", s. 62.

17 Populacja Polski na dzień 1 stycznia 1930 r. wynosiła 30,7 mln. *Mały rocznik statystyczny 1930 r.*, tabl. 6, „Ludność Polski w latach 1921 i 1930", s. 4.

18 Populacja Polski na 31 marca 2011 r. wynosiła 38512 tys. *Mały rocznik statystyczny Polski 2013*, tabl. 1 (62), Ludność na podstawie spisów, s. 116.

19 *Raport o stanie rynku telekomunikacyjnego w Polsce w 2012 roku*, Prezes Urzędu Komunikacji Elektronicznej, Warszawa, czerwiec 2013, s. 48 i 49.

20 Ibidem, s. 23.

21 Ibidem, s. 27.

22 Ibidem, s. 7.

23 Ibidem, s. 4.

24 Ibidem, s. 63.

25 Dla przykładu w Polsce jest zaledwie 20 elektrowni zawodowych, w których jest zainstalowanych ponad 80% mocy, *Elektrownie w Polsce*, http://www.rynek-energii-elektrycznej.cire.pl/st,33,200,tr,67,0,0,0,0,0,elektrownie-w-polsce.html oraz *Podstawowe dane*, http://www.rynek-energii-elektrycznej.cire.pl/st,33,207,tr,75,0,0,0,0,0,podstawowe-dane.html [dostęp 25.05.2014].

- koszty rozwoju technologicznego – budowa i utrzymanie infrastruktury jest kosztowne, dlatego też jej finansowanie przejmowało na siebie państwo, lokalne władze lub prywatni inwestorzy. Tylko te podmioty były w stanie ponieść koszty inwestycji w elektrownie, oczyszczalnie ścieków czy drogi;
- potrzeba zapewnienia dostępu do infrastruktury dużej ilości konsumentów – jedynym dostępnym w przeszłości sposobem zaspokojenia tej potrzeby była budowa scentralizowanej infrastruktury. Wynika to z faktu, iż dzięki owej centralizacji, pomimo dużych kosztów wybudowania i utrzymania infrastruktury, opłaty za dostęp do dostarczanych przez nią usług są relatywnie niskie i w związku z tym mogą być szeroko dostępne.

Po drugie, proces uniezależniania się człowieka od natury i nieprzewidywalnych konsekwencji jej działania poprzez rozwój technologiczny, będący wyrazem poszerzania niezależności człowieka oraz realizacji jego potrzeb, paradoksalnie wprowadził nowe zagrożenie – zależność od-technologiczną. Niemniej, bardziej lub mniej potencjalny brak dostępu do usług nie stanowi jedynej konsekwencji aktywności człowieka w tym obszarze. Sam fakt istnienia owej infrastruktury niesie ze sobą kolejne zagrożenia. Ze względu na zjawisko dyfuzji innowacyjności[26] zagrożenia te stają się jednymi z podstawowych zagrożeń dla współczesnego świata, tym bardziej, że procesu przyswajania nowinek technologicznych nie można już liczyć w dziesiątkach lat, ale w miesiącach. Tempo, w jakim zmienia się rzeczywistość poprzez pojawiające się nowe technologie, prowadzi do niemożności przygotowania się człowieka na ich konsekwencje. Taki stan jest pochodną nie tylko szybkości samych zmian, ale i nieprzewidywalności ich skutków. Rozwój technologiczny będący skutkiem poszukiwania coraz to nowszych środków zaspokajania potrzeb wykreował nie tylko nowe, nieznane dotąd zagrożenia, ale i nowe, wtórne w stosunku do pierwotnych, potrzeby. Ta swoista spirala rozwoju stała się dziś zjawiskiem tak naturalnym, że trudno wyobrazić sobie funkcjonowanie człowieka w oderwaniu od infrastruktury, a także dobrodziejstw i zagrożeń, które niesie ona ze sobą.

W konsekwencji to państwo musi wziąć na siebie odpowiedzialność, nie tyle za samo funkcjonowanie infrastruktury, ile za ciągłość dostaw oferowanych przez nią usług oraz skutki zagrożeń, które niesie dla zdrowia i życia ludzkiego czy środowiska naturalnego. Współczesne państwo realizując swoje podstawowe funkcje koncentruje się na tych kwestiach. Z sześciu obszarów wewnętrznej aktywności państwa połowa funkcji odwołuje się bezpośrednio do problematyki bezpieczeństwa i jest ściśle powiązana z infrastrukturą. Elementami tymi są: *zapewnienie porządku i bezpieczeństwa publicznego, ochrona mienia i zdrowia obywateli, działania na rzecz zapewnienia zewnętrznego bezpieczeństwa państwa*. Realizacja pozostałych tj. *zabezpieczenie występującego w państwie systemu własności, utrzymywanie i rozwijanie stosunków z innymi państwami, czy działania sprzyjające przepływowi informacji oraz kontaktom międzyludzkim*[27], jest pośrednio zależna od infrastruktury technicznej oraz stworzonego i gwarantowanego przez państwo systemu prawnego.

Można więc wskazać, że funkcjonowanie społeczeństwa i państwa jest zależne od infrastruktury, a stopień jej rozwoju wpływa na skuteczność i efektywność realizowanych przez to państwo zadań. W konsekwencji – rozwój technologiczny tworzy system współzależności i wzajemnego oddziaływania pomiędzy państwem a infrastrukturą.

26 Szerzej: A. Pomykalski, *Innowacje*, Wydawnictwo Politechniki Łódzkiej, Łódź 2001.

27 J. Oniszczuk, *Współczesne państwo w teorii i praktyce. Wybrane elementy*, Warszawa: Oficyna Wydawnicza SGH, Warszawa 2008, s. 401.

Z jednej strony państwo działając na rzecz bezpieczeństwa i porządku publicznego musi zabezpieczyć się przez zagrożeniami stwarzanymi przez tę infrastrukturę, a samo chcąc realizować swoje funkcje, będące od infrastruktury zależne, chronić ją. Z drugiej zaś, rozległe i rozbudowane systemy infrastruktury dążąc do zapewnienia ciągłości świadczonych przez siebie usług cedują część swojej odpowiedzialności za ich dostarczanie na państwo.

Obecnie trudno jest podważyć tezę, że możliwość sprawowania przez państwo swoich zadań (wszystkich jego funkcji) jest ściśle zależna nie tylko od poziomu rozwoju technologicznego, ale i jakości usług świadczonych przez poszczególne sektory infrastruktury. Świadomość tych zależności i ich konsekwencji doprowadziła do wyodrębnienia z całego systemu infrastruktury jej newralgicznych elementów – infrastruktury krytycznej (IK). Stąd taki nacisk kładzie się od kilkudziesięciu lat na stworzenie systemów służących ochronie tej infrastruktury.

Czym jest infrastruktura krytyczna i proces jej identyfikacji

Odnosząc się do kwestii roli, jaką IK pełni w stosunku do państwa, postrzegając przy tym państwo jako byt społeczny będący gwarantem bezpieczeństwa jego członków (obywateli), nie można nie odwołać się do pojęcia potrzeb. Jednym z czynników decydującym o wskazaniu infrastruktury jako kluczowego elementu systemu państwa jest uznanie jej za podstawowy instrument odpowiedzialny za dostarczanie usług zaspokajających potrzeby zarówno tegoż państwa jak i jego obywateli.

W literaturze możemy znaleźć przynajmniej kilka klasyfikacji potrzeb. Abraham Maslow wskazał na 5 grup potrzeb (fizjologiczne, bezpieczeństwa, miłości i przynależności, szacunku i uznania oraz samorealizacji), dokonując jednocześnie ich hierarchizacji[28]. Erik Allardt podzielił potrzeby ludzkie na trzy sfery: związane z posiadaniem (ang. *having*), ze stanami uczuciowymi (ang. *loving*) oraz z poczuciem istnienia (ang. *being*)[29]. Andrzej Luszniewicz wyróżnił z kolei 7 grup potrzeb materialnych i kulturalnych: wyżywienie, osłona (mieszkanie, odzież, obuwie), ochrona zdrowia, wykształcenie, rekreacja (czas wolny i jego wykorzystanie), zabezpieczenie społeczne i zagospodarowanie materialne[30]. W badaniach przeprowadzonych pod kierunkiem Aleksandra Zeliasia wykorzystano natomiast taksonomię 9 grup potrzeb, w tym: ochrony zdrowia i opieki socjalnej, funkcjonowania rynku pracy oraz stworzenia warunków bezpiecznego wykonywania pracy, adekwatnego wynagrodzenia i dochodów, odpowiednich warunków mieszkaniowych, a także bezpieczeństwa publicznego. Ponadto wskazano potrzeby oświaty i edukacji, rekreacji, kultury i zorganizowania czasu wolnego, komunikacji i łączności oraz ochrony przed skutkami degradacji środowiska naturalnego[31].

Przegląd powyższych klasyfikacji pozwala na konkluzję, że usługi dostarczane przez infrastrukturę są w stanie zaspokoić niemalże każdą z potrzeb, potwierdzając rolę IK. Perspektywa ta nie

28 M. Panek, *Podstawowe kategorie i klasyfikacje w badaniach poziomu i jakości życia*, http://kolegia.sgh.waw.pl/pl/KAE/struktura/ISiD/struktura/ZSS/zaklad/sklad/Documents/Statystyka_Tomasz_Panek/Statystyka_spoleczna/Podstawowe_kategorie_i_klasyfikacje_w_badaniu_poziomu_ijakosci_zycia.doc, [dostęp: 08.04. 2014].

29 Ibidem.

30 M. Dąbrowa, *Badanie poziomu życia – metodologia konstrukcji wybranych wskaźników – zeszyty naukowe MWSE w Tarnowie 2011*, nr 1(17), http://zn.mwse.edu.pl/dabrowa-maria-badanie-poziomu-zycia-metodologia-konstrukcji-wybranych-wskaznikow/, [dostęp: 08.04.2014].

31 Ibidem.

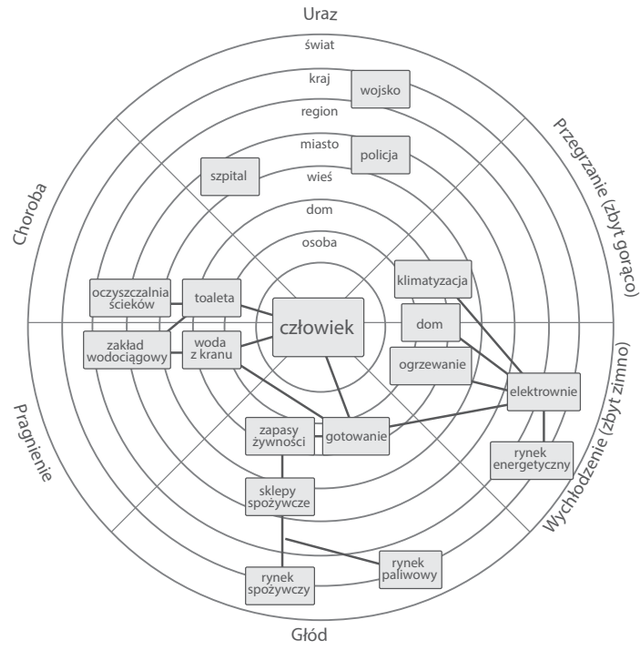
zapewnia jednak wskazania jej krytyczności. W związku z powyższym warte jest rozważenia inne podejście – definiowane poprzez wyodrębnienie wartości podstawowych, do których niewątpliwie zaliczyć należy życie ludzkie. Zasadniczo może ono zostać zagrożona z sześciu powodów (6WTD – ang. *6 ways to die*)[32]: przegrzania (zbyt gorąco), wychłodzenia (zbyt zimno), głodu, pragnienia, chorób oraz urazów.

W tym ujęciu podstawową rolą IK jest ochrona życia i zdrowia obywateli przed 6WTD. Zgodnie z tym modelem infrastrukturę można pogrupować na[33]:

1. zapewniającą schronienie i skuteczne funkcjonowanie tego schronienia, pod którą rozumie się najczęściej np.: ciepłownie, elektrownie;
2. towarzyszącą łańcuchowi dostaw, pod którą rozumie się infrastrukturę zabezpieczającą ten proces np.: infrastruktura drogowa, wodociągowa, rafinerie;
3. zapewniającą dostęp do podstawowych usług z zakresu bezpieczeństwa, pod którą rozumie się infrastrukturę pozwalającą dostarczyć usługi np.: centrale telefoniczne, elektrownie, rafinerie, bazy danych.

Należy zwrócić także uwagę, że ochrona przed 6WTD występuje na wielu poziomach, co najlepiej ilustruje poniższy rysunek:

Rysunek 2. Mapa infrastruktury krytycznej i jej poziomów. Źródło: M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe*.



32 M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe* – http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf. Więcej o pracach i projektach w których uczestniczy Vinay Gupta można przeczytać na stronie http://vinay.howtolivewiki.com/blog/about, [dostęp: 08.04. 2014].

33 Ibidem.

Patrząc na przedstawioną powyżej mapę można zauważyć, że nie obejmuje ona swoim zasięgiem IK, która nie łączy się bezpośrednio z ochroną przed 6WTD. Dlatego, aby otrzymać kompletną mapę infrastruktury istotnej dla państwa celowe wydaje się uzupełnienie koncepcji 6WTD o infrastrukturę niezbędną do realizacji podstawowych funkcji państwa wskazanych wcześniej.

Nakreślenie wzajemnych relacji pomiędzy IK a społeczeństwem i państwem pozwala na podjęcie próby zdefiniowania tego, czym jest sama IK. W Polsce pod tym pojęciem rozumie się *systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców*[34]. Porównując wskazaną definicję z definicjami IK stosowanymi w innych krajach można stwierdzić, że są one zbliżone. W większości przypadków, podobnie jak w Polsce, przez IK rozumie się infrastrukturę (wskazując przy tym np.: obiekty, usługi, systemy, sieci), której zniszczenie lub zakłócenie funkcjonowania miałoby poważne skutki dla obywateli i państwa (skutki te wskazywane są w różnych kategoriach np.: kluczowe funkcje społeczne, ekonomiczny dobrostan obywateli, bezpieczeństwo narodowe czy realizacja funkcji państwa)[35].

Zaletą zdefiniowania IK (poza nadaniem wspólnego znaczenia temu terminowi) jest również możliwość zawarcia w definicji narodowych celów i priorytetów działania[36]. Cécilia Gallais i Eric Filiol w swojej pracy "Critical Infrastructure: Where we Stand Today?"[37] wskazują na dwa brakujące elementy w definicjach IK, a mianowicie: pominięcie aspektu ludzkiego oraz brak odniesienia do politycznego i społecznego otoczenia IK. Zdaniem autorów żadna z definicji nie wspomina o ludziach jako jej części IK, choć są oni niezbędni do funkcjonowania każdej infrastruktury bez względu czy uznaje się jej krytyczność czy też nie. Żadna z nich nie uwzględnia również otoczenia IK jakim jest m.in. zależność od zewnętrznych podmiotów (podwykonawców, dostawców, centrów danych itp.). Autorzy jako konsekwencję tej sytuacji wskazują bardzo wąskie postrzeganie IK jako całkowicie wyizolowanej struktury. W celu usunięcia przedstawionych braków Gallais i Filiol proponują własną, szeroką definicję. Ich zdaniem IK mogą być przedsiębiorstwa, instytucje lub organizacje z poziomu regionalnego, krajowego lub międzynarodowego, których zakłócenie działania, uszkodzenie lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo lub dobrobyt gospodarczy obywateli lub efektywne funkcjonowanie rządów i innej zależnej od niej infrastruktury. Zawiera ona w sobie ludzi, których skorumpowanie, wykluczenie lub śmierć może prowadzić do zakłócenia jej działania. Ponadto obejmuje:

- instalacje (dostęp, budynki, teren itp.),
- wyposażenie (komputer, drukarka, dysk twardy itp.),
- zasoby, zarówno fizyczne jak i naturalne,
- sieci fizyczne (elektryczna, wodociągowa itp.) i wirtualne (Intranet, Internet itp.),

34 Art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 poz. 1166). Lista systemów infrastruktury krytycznej, która w przypadku Polski stanowi integralną część definicji, została pominięta celowo.

35 Szerzej: *Raport OECD: Protection of 'critical infrastructure' and the role of investment policies relating to national security*, Table 1. National Definitions of Critical Infrastructure, s. 4.

36 Należy przy tym zaznaczyć, że pomimo wymienionych zalet nie wszystkie kraje zdecydowały się na ten krok. Ochrona infrastruktury krytycznej jest realizowana poprzez ochronę założonych wartości np. kluczowych funkcji społecznych. Do tej grupy zaliczyć można m.in.: Francję, Szwecję, Estonię czy Włochy.

37 C. Gallais, E. Filiol, *Critical Infrastructure: Where we Stand Today?* http://www.tevalis.fr/images/ArticleICCWS2014.pdf, [dostęp: 08.04. 2014].

- dane, zarówno fizyczne, jak i wirtualne (poufne dane, takie jak hasła lub kody dostępu, procedury, schemat organizacyjny itp.),
- obiekty sektora technologii informacyjno-komunikacyjnych,
- usługi,
- procesy,
- aktywa, w tym wizerunek,
- systemy lub ich części,
- inną infrastrukturę, z którą istnieją połączenia (np. dostawcy usług lub produktów),

których zakłócenie, uszkodzenie, kradzież lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo lub dobrostan pracowników lub skuteczne funkcjonowanie IK. W rzeczywistości IK zawiera wszystkie elementy, które mógłby doprowadzić do zakłócenia jej funkcjonowania, uszkodzenia lub zniszczenia. Elementy te można także znaleźć w otoczeniu politycznym i kulturalnym infrastruktury.[38]

Wydaje się jednak, że zastosowanie tak szerokiej definicji IK nie jest konieczne. Pomijając fakt, że jej zastosowanie byłoby utrudnione ze względów praktycznych, należy zaznaczyć, że braki wskazane przez Gallais i Filiol, choć nie występują w powszechnie stosowanych, skompresowanych definicjach, są adresowane do każdego ze zorganizowanych systemów ochrony IK. Dla przykładu: w polskim „Narodowym Programie Ochrony Infrastruktury Krytycznej" określenie otoczenia IK, w tym wynikających z niego zależności i współzależności, stanowi element oceny ryzyka[39], a aspekt ludzki wskazywany jest w każdym z rodzajów ochrony IK[40]. Niemniej, rozważania przedstawione przez autorów „Critical Infrastructure: Where we Stand Today?" mogą być przydatne np. w procesie identyfikacji IK.

Bez względu bowiem na to czy w danym kraju zdecydowano się na zdefiniowanie pojęcia IK, czy nie, podstawowym i szczególnie ważnym procesem jest jej identyfikacja. Wiąże się on z szeregiem poważnych wyzwań. Pierwszym z nich jest opracowanie wspólnej lub zharmonizowanej metodyki, która może być wykorzystana w celu określenia poszczególnych elementów infrastruktury. Kolejnym wyzwaniem jest rozróżnienie elementów infrastruktury, które są krytyczne z punktu widzenia państwa, od infrastruktury, która może mieć kluczowe znaczenie na szczeblu lokalnym lub regionalnym, ale nie wymaga centralnej interwencji. Proces ten dodatkowo rodzi poważne konsekwencje związane z ochroną zebranych w ten sposób informacji, która często obejmuje nie tylko wykaz IK, ale również informacje dotyczące sposobów jej ochrony[41].

W procesie identyfikacji IK możemy zaobserwować dwa podejścia[42]. Pierwsze – „z dołu do góry" (ang. *bottom-up*) polega na zastosowaniu kryteriów do całej krajowej infrastruktury w celu oceny jej krytyczności. Drugie – „z góry do dołu" (ang. *top-down*) przewiduje zastosowanie wstępnie zdefiniowanej, podstawowej listy krytycznych sektorów, (systemów lub usług)[43] – to

38 Ibidem, s. 11.

39 Patrz *Narodowy Program Ochrony Infrastruktury Krytycznej – dokument główny* s. 30.

40 Patrz załącznik 2 do *Narodowy Program…*, op. cit – *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*.

41 Lord Jopling (special rapporteur), *Special report to NATO Parliamentary Assembly: The protection of critical infrastructures*.

42 *Good practices manual for CIP policies for policy makers in Europe* – praca w ramach projektu RECIPE (Recommended Elements of Critical Infrastructure Protection for policy makers in Europe).

43 Ibidem, s. 16. Lista krytycznych sektorów i podsektorów może być zawarta w samej definicji infrastruktury krytycznej lub w innych dokumentach wykonawczych.

podejście jest na świecie bardziej rozpowszechnione. Lista krytycznych sektorów jest silnie powiązana z określeniem wzajemnych relacji pomiędzy IK a społeczeństwem i państwem, czyli tym jaka rola w państwie została jej przypisana. Analiza wybranych przykładów pozwala na konkluzję, że lista krytycznych sektorów (systemów lub usług) w poszczególnych krajach jest bardzo zbliżona.

Tabela 1. Podział IK na sektory w Republice Francuskiej. Źródło: Opracowanie własne na podstawie Dekretu z 2 czerwca 2006 *ustanawiającego wykaz sektorów o zasadniczym znaczeniu oraz wyznaczaniu ministrów koordynatorów tych sektorów (Décret du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale)*.

Sektor	Minister Koordynator
Administracja państwowa	Minister Spraw Wewnętrznych
Sądownictwo	Minister Sprawiedliwości
Wojskowa działalność państwa	Minister Obrony Narodowej
Żywność	Minister Rolnictwa
Łączność elektroniczna i transmisja informacja	Minister właściwy do spraw łączności elektronicznej
Energia	Minister Przemysłu
Badania kosmiczne	Minister właściwy ds. badań
Finanse	Minister Gospodarki i Finansów
Gospodarka wodna	Minister Ekologii
Przemysł	Minister Przemysłu
Zdrowie	Minister Zdrowia
Transport	Minister Transportu

Tabela 2. Podział IK na sektory w Stanach Zjednoczonych Ameryki. Źródło: Opracowanie własne na podstawie Dyrektywy Prezydenta w Obszarze Bezpieczeństwa Narodowego nr 7 z dnia 17 grudnia 2003 *w sprawie identyfikacji, priorytetyzacji i ochrony infrastruktury krytycznej* (Homeland Security Presidential Directive-7 December 17, 2).

Sektor	Organ właściwy
Przemysł chemiczny Obiekty handlowe Zapory Usługi ratownicze Nuklearny	Departament Bezpieczeństwa Krajowego
Przemysł obronny	Departament Obrony
Rolnictwo i żywność	Departament Rolnictwa Departament Zdrowia i Usług Społecznych (w stosunku do żywności innej niż drób, mięso i produkcja jajek)
Telekomunikacja i technologie informacyjne	Biuro ochrony teleinformatycznej i telekomunikacji
Energia	Departament Energii
Bankowość i finanse	Departament Skarbu
Woda (zawiera również odprowadzanie ścieków)	Agencja Ochrony Środowiska
Dziedzictwo narodowe	Departament Spraw Wewnętrznych
Usługi pocztowe	Administracja Bezpieczeństwa Transportu
Ochrony zdrowia	Departament Zdrowia i Usług Społecznych
Transport	Administracja Bezpieczeństwa Transportu Straż Przybrzeżna USA (w zakresie transportu morskiego)
Obiekty rządowe	Służba Imigracyjna i Celna Federalna Służba Ochrony

Tabela 3 Podział IK na sektory w Królestwie Niderlandów. Źródło: Opracowanie własne na podstawie Raportu przygotowanego w 2005 r. przez Ministerstwo Spraw Wewnętrznych i Stosunków w Królestwie *ws. ochrony infrastruktury krytycznej* (Report on Critical Infrastructure Protection, 2005).

Sektor	Minister właściwy
Energia	Minister Gospodarki
Telekomunikacja i technologie informacyjne	
Zaopatrzenie w wodę	Minister Mieszkalnictwa, Gospodarki Przestrzennej i Środowiska
Przemysł chemiczny i nuklearny	
Żywność	Minister Rolnictwa i Jakości Żywności
Zdrowie	Minister Zdrowia i Sportu
Finanse	Minister Finansów
Porządek publiczny i bezpieczeństwo	Minister Spraw Wewnętrznych Minister Obrony Minister Spraw Zagranicznych
Administracja publiczna	
Porządek prawny	Minister Sprawiedliwości
Zapory oraz zarządzanie wodami powierzchniowymi	Minister Transportu, Robót Publicznych i Gospodarki Wodnej
Transport	

Tabela 4 Podział IK na sektory w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej. Źródło: Opracowanie własne na podstawie *Strategicznych Ram i Deklaracji Politycznej w sprawie poprawy odporności infrastruktury krytycznej na zakłócenia spowodowane zagrożeniami naturalnymi, 2010 (Strategic Framework and Policy Statement on Improving the Resilience).*

Sektor	Organ właściwy
Energia	Minister Energii i Zmian Klimatu
Łączność	Minister Przedsiębiorczości, Innowacyjności i Rozwoju Minister Kultury, Mediów i Sportu
Woda	Minister Środowiska, Żywności i Rolnictwa
Żywność	Minister Środowiska, Żywności i Rolnictwa Agencja ds. Jakości Żywności
Zdrowie	Minister Zdrowia i Sportu
Finanse	Minister Skarbu
Ratownictwo i ochrona zdrowia	Minister Spraw Wewnętrznych Minister Zdrowia Minister Samorządności i Społeczności Lokalnych
Administracja publiczna	Kancelaria Premiera Minister Samorządności i Społeczności Lokalnych
Transport	Minister Transportu

Dodatkowo, w ramach podejścia „z góry do dołu", autorzy poradnika „Good practices manual for CIP policies for policy makers in Europe" wymieniają trzy sposoby na wyłonienie IK. Pierwszy, oparty na usługach (ang. *service-based*), zakłada wykorzystanie kryteriów określających poziom wymaganej usługi np. liczby megawatów mocy, która powinna być dostarczona. Drugi, bazujący na operatorach IK (ang. *operator-based*), koncentruje się na wskazaniu krytycznych operatorów im pozostawiając wskazanie konkretnych obiektów (usług) IK. Trzeci, oparty na aktywach (ang. *asset-based*) wykorzystuje elementy obydwu wcześniejszych sposobów[44].

Wspólne dla obu podejść („z dołu do góry" oraz „z góry do dołu") jest zastosowanie kryteriów. Próba wyłonienia IK bazująca jedynie na skonfrontowaniu jej z definicją, biorąc pod uwagę generalny charakter tych definicji, obarczona byłaby zbyt dużą niepewnością co do końcowego rezultatu. Dlatego najczęściej stosowane są tzw. kryteria przekrojowe, dotyczące skutków zniszczenia lub zakłócenia funkcjonowania danego obiektu, usługi czy operatora. Kryteria te z reguły korespondują z definicją IK[45] i wskazanymi w niej obszarami zaangażowania państwa oraz możliwościami reakcji państwa na skutki zniszczenia lub zakłócenia funkcjonowania IK.

Drugim rodzajem stosowanych kryteriów są kryteria sektorowe, służące, jak wspomniano wcześniej, do określenia zapotrzebowania na daną usługę lub do określenia progów wstępnej selekcji infrastruktury z danego sektora, co ma docelowo zmniejszyć liczbę potencjalnych IK. Zarówno kryteria przekrojowe i sektorowe mogą być przedstawiane w sposób ilościowy (liczbowy) lub jakościowy (opisowy). Zaletą ilościowego przedstawiania kryteriów jest ich obiektywizm, wadą zaś mała elastyczność i w konsekwencji możliwość pomięcia w selekcji obiektów podprogowych, a mimo to krytycznych. Zaletą jakościowego (opisowego) przedstawiania kryteriów jest duża czułość na pozornie nieistotne, niedające się uchwycić w sposób ilościowy detale, wadą zaś zbyt duże pole do interpretacji opisu i możliwość braku zgody co do oceny pomiędzy uczestnikami procesu identyfikacji.

W praktyce, w celu kompensacji błędów w identyfikacji IK stosuje się mieszankę obydwu rodzajów kryteriów i sposobów ich przedstawiania. Nie rozwiązuje to jednak jednego z najpoważniejszych problemów procesu identyfikacji – dostępu do wiarygodnych informacji pozwalających na porównanie wartości przyjętego parametru z progiem. Odnosi się to przede wszystkim do kryteriów przekrojowych, przedstawianych tak w sposób ilościowy jak i jakościowy. W praktyce, jeśli nie są dostępne dane dotyczące historycznych zdarzeń, weryfikacja spełniania kryteriów oparta jest z konieczności na szacunkach, obarczonych mniejszym lub większym błędem. Błędem, którego granic często nie jesteśmy nawet w stanie ustalić.

W Polsce, w procesie identyfikacji IK zastosowano podejście „z góry do dołu", koncentrując się na usługach realizowanych przez infrastrukturę wymienionych w definicji IK systemów[46]. Zastosowane (tam gdzie to było możliwe w postaci ilościowej) zostały zarówno kryteria sektorowe jak i przekrojowe oraz definicja IK. Zgodnie z NPOIK procedura identyfikacji IK obejmuje[47]:

1. w etapie pierwszym – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, do infrastruktury systemu należy zastosować kryteria systemowe, właściwe dla danego systemu IK,

2. w etapie drugim – w celu sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w etapie pierwszym należy zastosować definicję zawartą w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym,

44 *Good practices manual…*, op. cit., s. 16.

45 W przypadku krajów, które nie stosują definicji, kryteria przekrojowe odnoszą się do założonych wartości, podlegających ochronie.

46 W art. 3 ust. 2 ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym wymienione zostały następujące krytyczne systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

47 *Narodowy Program…*, op. cit. s. 11 i 12.

3. w etapie trzecim – w celu oceny potencjalnych skutków zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w etapie pierwszym i drugim należy zastosować kryteria przekrojowe, przy czym potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe.

Warto przy tym zauważyć, że pomimo koncentracji na usługach dostarczanych przez infrastrukturę w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład IK w większości znalazły się określone, fizyczne obiekty. Obiekty, które są zarządzane przez konkretnych właścicieli i posiadają konkretną lokalizację, co pozwala na łatwiejszą implementację wciąż młodego systemu ochrony IK. Postulowane (i stosowane) przez niektóre kraje wskazywanie (np. Francję) jako IK całych systemów (np. systemu elektroenergetycznego) lub nawet procesów wydaje się w na chwilę obecną, w polskich warunkach zbyt wyrafinowane. System (proces) rozumiany jako np. łańcuch zaopatrzenia może być realizowany w wielu lokalizacjach i mieć wielu właścicieli. Zrodziłoby to określone problemy, w tym także prawne. Podobnie wygląda kwestia zależności i współzależności. Obecnie łatwiej jest je wskazać dla konkretnego obiektu niż dla systemu czy procesu. Prawdopodobne jest jednak, że wraz z rozwojem systemu ochrony IK i dojrzałością jego uczestników będzie zachodzić zmiana w tym obszarze.

Kolejny krokiem po zdefiniowaniu i identyfikacji IK jest jej ochrona. Można wyróżnić przynajmniej dwie metody zabezpieczenia IK – proceduralną i strukturalną. Proceduralna polega na organizacji systemu ochrony tych obiektów. Rozwiązanie to może przyjąć z kolei dwie drogi: obowiązkowego uczestnictwa w systemie ochrony lub uczestnictwa dobrowolnego. Metoda strukturalna zakłada zmniejszanie krytyczności infrastruktury. Efekt ten można osiągnąć poprzez dalszą rozbudowę infrastruktury, tak by w konsekwencji doprowadzić do sytuacji celowej nadmiarowości (redundancji) lub poprzez przybliżanie, w sensie geograficznym, wybranej infrastruktury do obywatela[48]. Koncepcja przybliżania zakłada wyposażanie jednostkowego obywatela lub mniejszych ich grup w infrastrukturę pozwalającą na niezależność od usług dostarczanych przez bardziej oddaloną infrastrukturę. Tym samym, niektóre usługi stałyby się mniej krytyczne z punktu widzenia państwa, gdyż zwiększyłaby się odporność i niezależność tej grupy obywateli od IK. Ten model zwiększa możliwości potencjalnej odpowiedzi służb państwowych na zakłócenie przybliżonej infrastruktury i kreuje stan, w którym liczba dotkniętych jednorazowo obywateli jest radykalnie mniejsza. Przykładami takiej infrastruktury mogą być: indywidualne źródła energii (słoneczne, wiatrowe) lub przydomowe oczyszczalnie ścieków. W przypadku miast i gęsto zaludnionych obszarów koncepcja ta zakłada budowę osiedlowych lub dzielnicowych infrastruktur obsługujących jednorazowo mniejszą liczbę mieszkańców[49]. W obydwu modelach zabezpieczenia infrastruktury, wyzwaniem staje się odpowiedź na pytanie: kto powinien wdrażać konkretne rozwiązania, a tym samym ponieść finansowy ciężar? oraz czy odpowiedzialność za ochronę ludności przez skutkami zakłócenia funkcjonowania IK spoczywa na podmiotach będących właścicielami lub zarządcami tej infrastruktury, czy na państwie?

48 M. Bennett, V. Gupta, op. cit.

49 W Polsce zaproponowano niegdyś budowę biogazowni w każdym mieście. Pomijając polityczny aspekt tej propozycji doskonale wpisuje się ona w przywołaną koncepcję i należy uznać ją za ciekawy głos w dyskusji o zwiększaniu odporności państwa i obywateli na sytuacje kryzysowe. Pomijamy również fakt, że we wzajemnie powiązanym systemie infrastruktury zmiana w jednym z nich może spowodować przeniesienie progu „krytyczności" w innym.

W Polsce, na etapie projektowania ustawy o zarządzaniu kryzysowym, oparto się na doświadczeniu i przykładach z krajów, w których budowę systemu ochrony infrastruktury kluczowej dla bezpieczeństwa obywateli i funkcjonowania państwa rozpoczęto wcześniej: Stanów Zjednoczonych Ameryki, Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, Królestwa Niderlandów, Republiki Francuskiej oraz Republiki Federalnej Niemiec. Wspólnymi cechami systemów ochrony IK w ww. krajach są:

- identyfikacja IK na podstawie kryteriów i wskazanie jej właściciela lub operatora jako odpowiedzialnego za jej ochronę;
- podział na krytyczne dla funkcjonowania państwa, społeczeństwa i gospodarki sektory (produkty lub usługi);
- wskazanie organów administracji odpowiedzialnych za koordynację działań w danym sektorze;
- konieczność opracowania przez właściciela IK (bądź nią zarządzającego) planów ochrony obiektów;
- współpraca pomiędzy właścicielami i operatorami IK, a właściwymi organami państwa odpowiedzialnymi zarówno za koordynację działań w danym sektorze, jak i tymi odpowiedzialnymi za ochronę ludności i zarządzanie kryzysowe.

Biorąc pod uwagę specyfikę i kulturę prawną w Polsce wybrano rozwiązanie regulacyjne, kładące akcent na metodę proceduralną i obowiązkowy udział w systemie ochrony IK tzn. w przepisach ustawy o zarządzaniu kryzysowym literalnie wskazany został obowiązek ochrony IK przez jej właścieli oraz posiadaczy samoistnych i zależnych, sporządzenia planu ochrony oraz wyznaczenia osoby do kontaktów z administracją. Natomiast w rozporządzeniu z dnia 30 kwietnia 2010 r. *w sprawie planów ochrony IK*[50] szczegółowo została wskazana zawartość planów oraz tryb i terminy ich uzgadniania oraz zatwierdzenia (mechanizm ten pozwala na realny wpływ organów na zawartość planu i system bezpieczeństwa danego obiektu IK). Rozwiązanie to bazuje na modelu francuskim[51], w którym występuje:

- wyznaczenie na operatora IK i obowiązek jej ochrony;
- obowiązek sporządzenia Planu Bezpieczeństwa Operatora;
- sankcje dla operatorów IK nierealizujących narzuconych obowiązków;
- obowiązek sporządzenia przez administrację publiczną Zewnętrznego planu bezpieczeństwa (pierwotnie w ustawie o zarządzaniu kryzysowym był obowiązek sporządzania „Krajowego Planu Ochrony Infrastruktury Krytycznej" (KPOIK) oraz „Wojewódzkich Planów Ochrony Infrastruktury Krytycznej" (WPOIK);
- określenie, które sektory uznane są za krytyczne, ze względu na kluczowe znaczenie dla procesów społecznych i gospodarczych.

W przeciwieństwie natomiast do rozwiązania zastosowanego we Francji, ale także w ustawie z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia*[52] nie przewidziano sankcji za niedopełnienie wskazanych obowiązków. Skuteczność tego rozwiązania okazuje się niezadowalająca. Represyjny charakter takiego podejścia przynosi skutki uboczne – głęboką niechęć wyko-

50 Rozporządzenie Rady Ministrów z dn. 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. nr 83, poz. 542).

51 Szerzej o systemie francuskim oraz systemach stosowanych w innych krajach europejskich w: *Study: Stock-Taking Of Existing Critical Infrastructure Protection Activities*, http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_stock_taking.pdf, [dostęp: 08.04.2014].

52 Ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia* (Dz. U. z 2005 r. nr 145, poz. 1221 z późn. zm.).

nawców do narzuconych zadań i w konsekwencji próby uchylania się od realizacji narzuconych obowiązków bądź wykonywanie ich minimalnym kosztem. Po stronie administracji natomiast wymusza budowę struktur, których zadaniem jest prowadzenie działalności kontrolnej oraz postępowań w przypadku naruszenia obowiązków. Oznacza to konieczność zatrudnienia kompetentnych pracowników (co wiąże się w obszarze ochrony z poważnymi trudnościami) oraz poniesienia znacznych nakładów finansowych. Podstawą tego podejścia było założenie, że zwiększenie skuteczności ochrony IK może nastąpić jedynie poprzez działania operatorów wspieranych przez możliwości i potencjał administracji publicznej. Oparto się przy tym na przekonaniu, że motywacja[53] do zachowania ciągłości biznesowej jest narzędziem skuteczniejszym niż sankcje w osiągnięciu wysokiego poziomu ochrony[54]. Operatorzy IK mają najlepszą wiedzę i narzędzia do ograniczenia zagrożeń dla ich działalności. Są również w stanie dokonać najwłaściwszego wyboru strategii minimalizacji skutków tych zagrożeń. Podejście nie przewiduje sankcji za niedopełnienie obowiązków określonych w ustawie. Brak sankcji nie oznacza jednak braku odpowiedzialności. Właściciele oraz posiadacze samoistni i zależni, którzy świadomie niedopełniają obowiązku ochrony IK narażają pracowników i innych ludzi na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu, mogące być skutkiem zakłócenia funkcjonowania IK, co jest zagrożone karą pozbawienia wolności do lat 3 (art. 160 § 1 Kodeksu karnego).

Bazując na doświadczeniach z funkcjonowania ustawy o zarządzaniu kryzysowym w 2009 r. dokonano jej nowelizacji. Co do zasady model ochrony IK nie uległ zmianie, przeniesiono jednak akcent jeszcze bardziej w kierunku właścicieli (zarządzających) IK. Zniesiono obowiązek opracowania KPOIK i WPOIK, w zamian wprowadzając obowiązek opracowania „Narodowego Programu Ochrony Infrastruktury Krytycznej" – dokumentu, który spina wysiłki na rzecz ochrony IK i stanowi pomoc dla operatorów IK oraz administracji. Ponadto, wychodząc z zasady współodpowiedzialności oraz skuteczności współpracy[55], w znowelizowanej ustawie na nowo podzielono obowiązki, wynikające z ochrony IK, pomiędzy administrację i operatorów IK. Obowiązkami operatorów są:

53 Motywacja to proces, który wywołuje, ukierunkowuje i podtrzymuje określone zachowania ludzi spośród innych, alternatywnych form zachowania, w celu osiągnięcia określonych celów. Jedna z teorii motywacji do pracy opracowana przez Douglasa McGregora (Massachusetts Institute of Technology) zakłada istnienie dwóch przeciwstawnych zestawów przekonań: X i Y. X zakłada, że przeciętna jednostka ludzka w sposób wrodzony nie lubi pracować i robi wszystko by jej uniknąć. Pracuje tylko dla zaspokojenia potrzeb materialnych. Y zakłada, że ludzie są w większości twórczy, posiadają bogatą wyobraźnie i pomysłowość. W odpowiednich warunkach człowiek taki nie tylko jest odpowiedzialny, lecz także oczekuje, że dana mu będzie odpowiedzialność za wykonanie jakiegoś przedsięwzięcia lub pracy. Wg McGregora zewnętrzne czynniki motywujące w postaci nagrody lub kary obniżają aktywność wewnętrznej motywacji. Dzieje się tak na sutek zmiany postrzegania i umiejscawiania przyczyn działania (na zewnątrz a nie wewnątrz podmiotu) oraz obniżenia związanego z tym poczucia sprawstwa, osobistego wpływu na sytuację.

54 Ujawnione przypadki naruszeń bezpieczeństwa wydają się potwierdzać, że występowanie sankcji nie gwarantuje skuteczności systemowi ochrony kluczowych obiektów: 03.07.2007 Bełchatów – aktywiści Greenpeace włamali się na teren elektrowni, wspięli się na chłodnię kominową i wykonali napis „Stop CO2", 03.12.2008 Konin – ekolodzy włamali się na teren elektrowni, wspięli się na komin i rozpoczęli protest przeciw emisji gazów cieplarnianych, 05.12.2011 Francja – działacze Greenpeace wtargnęli do czterech elektrowni atomowych. W Nogent-sur-Seine w ciągu zaledwie 15 minut dotarli do reaktora nuklearnego. Diagnozę tę potwierdzają również spływające do Rządowego Centrum Bezpieczeństwa raporty pełnomocników ds. ochrony infrastruktury krytycznej, powołanych w ramach realizacji ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. nr 65 poz. 404).

55 Szerzej: *Narodowy Program*…, op. cit.

1. ochrona IK, w szczególności poprzez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia (art. 6 ust. 5 ustawy) oraz

2. wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK (art. 6 ust. 5a ustawy).

Obowiązkiem administracji jest natomiast ujęcie zadań związanych z ochroną IK w planach zarządzania kryzysowego na każdym poziomie administracji – w przypadku poziomów niższych niż krajowy warunkiem umieszczenia tych zadań jest występowanie IK na obszarze objętym planem[56]. Dodatkowo, w ramach ochrony ludności przed skutkami awarii IK, oznacza to również system wsparcia operatorów celem skrócenia czasu odbudowy usług (zadań, funkcji) realizowanych przez IK.

Analizując rozwiązania przyjęte w Polsce[57] można wykazać, że znaleziono odpowiedzi przynajmniej na kilka postawionych wcześniej pytań. Czy to oznacza jednak, że przyjęty model się sprawdził? Jednoznaczna odpowiedź na tak postawione pytanie jest obecnie niemożliwa. Do dyspozycji wciąż pozostaje zbyt mało wiarygodnych danych. Doświadczenia Rządowego Centrum Bezpieczeństwa są zachęcające, lecz prawdziwym testem będzie ocena jakości planów ochrony IK, które dopiero zaczynają napływać do zatwierdzenia.

Podsumowanie

Nie sposób wyobrazić sobie dziś życia bez otaczającej nas infrastruktury czy rozwiązań, które ona ze sobą niesie. Tempo rozwoju technologicznego przynoszące praktycznie codziennie nowinki techniczne przestało już dziwić, a będące jego efektem powszechność i użyteczność usług – uzależniły. Jednak XXI wiek nie stawia przed człowiekiem pytań o sensowność tych zmian, ale o to: Jak przeżyć w świecie nasyconym technologiami? Jak ciesząc się zdobyczami współczesności nie stać się jednocześnie ich ofiarą[58]? Człowiek świadomy nowych zagrożeń coraz częściej kieruje w stronę państwa swoje oczekiwania zmniejszania ryzyka ich wystąpienia. To właśnie państwo i organizacje międzynarodowe, ze względu na rozległość infrastruktury, jej transgraniczność i powszechność, są predestynowane do wzięcia na siebie tej odpowiedzialności. Jednym z narzędzi pozwalających choćby w części kontrolować zagrożenia jest IK. Zwrócenie uwagi na wrażliwe elementy otoczenia człowieka oraz wskazanie ich charakterystycznych cech, a w konsekwencji stworzenie dedykowanych im szczególnych rozwiązań pozwoliło na ograniczenie ryzyka zaistnienia sytuacji dysfunkcji dostarczanych przez nie usług.

Każde rozwiązanie ma swoje ograniczenia. Również te przyjęte w tym zakresie w Polsce. Pomimo krótkiego czasu od wejścia w życie ustawy o zarządzaniu kryzysowym w Polsce

56 Art. 5 ust. 2 pkt 3 lit k i lit. l ustawy o zarządzaniu kryzysowym.

57 Szerzej: ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 poz. 1166) wraz z aktami wykonawczymi oraz *Narodowy Program Ochrony Infrastruktury Krytycznej*.

58 Wg Bennetta i Gupta skutki zakłócenia funkcjonowania zcentralizowanej infrastruktury mogą być większe niż pierwotne zagrożenie.

funkcjonuje komplementarny i powszechny system ochrony IK. Prezentowane w powyższym rozdziale rozważania wskazują jednoznacznie: dużo już zostało zrobione, ale i jeszcze dużo przed nami.

W przypadku Polski warto rozważyć uzupełnienie definicji IK w taki sposób, by nie pozostawiała wątpliwości, że obejmuje ona również infrastrukturę wirtualną (informacyjną), np. zbiory informacji z baz danych. W aktualnie obowiązującej definicji *systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi* nie wskazuje się tego w sposób jednoznaczny.

Należy dążyć do postulowanej w NPOIK rezygnacji z kryteriów sektorowych[59], a tym samym zbliżyć się do podejścia „z dołu do góry". Biorąc jednak pod uwagę trudności związane z zastosowaniem tego podejścia, powinno się w ramach obowiązującej procedury dążyć do jak największego zaangażowania w identyfikację IK lokalnych szczebli administracji i operatorów IK. Pozwoliłoby to zminimalizować możliwość pominięcia IK, która nie spełnia kryteriów.

W celu pozyskania informacji i danych historycznych na temat skutków występujących zakłóceń funkcjonowania infrastruktury wskazane byłoby zacieśnienie współpracy z lokalnymi szczeblami administracji, operatorami IK, a także innymi organami (np. regulatorami rynków), organizacjami (np. pozarządowymi), służbami i strażami, co może pozwolić na kalibrację kryteriów i ich dostosowanie do realnych warunków.

W przypadku braku efektów obecnie stosowanego, dobrowolnego podejścia do kooperacji, należałoby rozważyć bardziej sformalizowane rozwiązania oparte na obowiązku współpracy z Rządowym Centrum Bezpieczeństwa.

59 *Narodowy Program*…, op. cit., s. 12.

2. Prawne uwarunkowania ochrony infrastruktury krytycznej

Agnieszka Wiercińska-Krużewska, Piotr Gajek
– WKB Wierciński, Kwieciński, Baehr

Regulacje prawne dotyczące ochrony infrastruktury krytycznej (IK) zostały umiejscowione w licznych aktach prawnych rangi ustawowej i podustawowej, obejmujących różne dziedziny funkcjonowania państwa[60]. Pomimo, iż akty te nie odnoszą się bezpośrednio do IK, analiza używanych terminów, w tym dotyczących obiektów, wskazuje na ich zbliżone, a często wręcz tożsame znaczenie[61]. W tym przedmiocie wskazuje się na takie obszary działalności jak: działalność telekomunikacyjną, wytwarzanie i obrót paliwami oraz energią elektryczną, wykonywanie zadań obronnych przez przedsiębiorców, tworzenie rezerw strategicznych, uprawnienia ministra właściwego do spraw Skarbu Państwa czy ochronę osób i mienia[62]. Powyższe potwierdza, iż warunki formalno-prawne ochrony IK istniały jeszcze przed wejściem w życie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[63] (Ustawa).

Ustawa wprowadziła pojęcie IK oraz bardziej kompleksowo uregulowała problematykę ochrony IK. Zgodnie z Ustawą przez IK należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców (art. 3 pkt. 2 Ustawy). IK obejmuje łącznie 11 systemów (obiekty, urządzenia) niezbędnych do minimalnego funkcjonowania gospodarki i państwa tj.:

- zaopatrzenie w energię, surowce energetyczne i paliwa,
- łączność,

60 Przykładowo można wskazać na następujące akty prawne: ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia*, ustawa z dnia 23 sierpnia 2001 r. *o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców*, ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne*, ustawa z dnia 10 kwietnia 1997 r. *Prawo energetyczne*, ustawa z dnia 9 czerwca 2011 r. *Prawo geologiczne i górnicze*, ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze*, ustawa z dnia 29 października 2010 r. *o rezerwach strategicznych*, ustawa z dnia 18 marca 2010 r. *o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa* oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. *w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*. Uwzględniając, iż szczegółowe omówienie wskazanych aktów prawnych wykracza poza przedmiot niniejszego opracowania, w raporcie przedstawione zostały w szczególności uwarunkowania prawne wynikające z ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

61 W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, *Ochrona Infrastruktury krytycznej*, Akademia Obrony Narodowej, Warszawa 2012, s. 37.

62 K. Stec, *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, Bezpieczeństwo Narodowe 2011, nr 3, s.181-197.

63 Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz,U. 2013 r. poz. 1166).

- sieci teleinformatyczne,
- finanse,
- zaopatrzenie w żywność,
- zaopatrzenie w wodę,
- ochronę zdrowia,
- transport,
- ratownictwo,
- systemy zapewniające ciągłość działania administracji publicznej,
- produkcję, składowanie, przechowywanie i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Przez ochronę IK należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności IK w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

W celu realizacji założeń Ustawy podmioty, w których posiadaniu znajduje się IK, powinny podejmować aktywne działania w celu utrzymania jej w należytym stanie, ochrony przed zniszczeniami i dostępem osób, które mogłyby zagrozić bezpieczeństwu państwa. Podmioty te powinny czynić także inwestycje w celu stałego podnoszenia poziomu IK i jej stanu.

Działania właścicieli IK powinny być centralnie koordynowane, nie tylko w czasie wystąpienia zagrożenia, ale także w czasie wykonywania obowiązków związanych z utrzymaniem IK w stanie zapewniającym realizację zadań państwa w sytuacjach kryzysowych.

Jako że ochrona IK jest jednym z priorytetów stojących przed państwem, państwo powinno wprowadzić mechanizmy pozwalające na:
- monitorowanie i uaktualnianie listy elementów IK;
- ustalenie wzajemnych relacji pomiędzy elementami IK;
- ustalenie wzajemnych relacji pomiędzy dysponentami IK;
- tworzenie inicjatyw w zakresie ochrony IK;
- przeprowadzenie akcji edukacyjnych – uświadamiających rolę IK w bezpieczeństwie państwa;
- wspieranie podmiotów, w posiadaniu których znajduje się IK, w ponoszeniu kosztów jej budowy, utrzymania i ochrony.

Brak powyższych mechanizmów może doprowadzić do niewiedzy o wadze IK w bezpieczeństwie państwa, chaosie w działaniach koordynacyjnych, niechęci podmiotów prywatnych do ponoszenia kosztów związanych w IK.

Dopiero prawidłowe wypracowanie systemu wsparcia dla podmiotów uczestniczących w utrzymaniu IK daje podstawy do stworzenia systemu skutecznych sankcji. Elementami wsparcia dla podmiotów powinny być między innymi:
- formalna platforma do wymiany doświadczeń i wiedzy na temat ochrony IK;
- partnerstwo publiczno – prywatne;
- fundusze celowe;
- ułatwienia w stosowaniu aktów prawnych np. w stosowaniu ustawy o zamówieniach publicznych;
- wspieranie samoregulacji przedsiębiorstw dysponujących IK w zakresie przepływu informacji oraz ponoszenia nakładów na jej ochronę i utrzymanie.

Najwyższa Izba Kontroli (NIK) kilkukrotnie dokonywała kontroli działalności organów państwa w zakresie wykonywania obowiązków nałożonych przez Ustawę (ostatnie wyniki kontroli NIK z 20 czerwca 2013 r.). Kontrole NIK wykazały szereg nieprawidłowości w zakresie realizacji ustawowych zadań od wejścia w życie Ustawy, a szczególnie jej nowelizacji. NIK stwierdził, że ochrona IK opiera się w dużej mierze na działaniach doraźnych. Zdaniem NIK, biorąc pod uwagę konieczność aktualizacji resortowych i wojewódzkich planów zarządzania kryzysowego w zakresie realizacji zadań związanych z IK oraz konieczność opracowania przez operatorów poszczególnych obiektów IK planów ich ochrony, dokończenie budowy skutecznego systemu ochrony IK zostanie dokonane dopiero w dłuższej perspektywie czasowej.

Konstatacja NIK jest słuszna, ale jej przyczyna nie leży już, jak się wydaje, w braku regulacji i podstaw do dalszych prac. Takie ramy tworzy z całą pewnością powstały w 2013 r. „Narodowy Program Ochrony Infrastruktury Krytycznej".

Poziom Unii Europejskiej

Europejski Program Ochrony Infrastruktury Krytycznej / Dyrektywa

Podstawowym elementem „Europejskiego Program Ochrony Infrastruktury Krytycznej" (EPOIK) jest *Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*[64] (Dyrektywa). W tym dokumencie po raz pierwszy do porządku prawnego UE wprowadzono definicję IK, europejskiej infrastruktury krytycznej (EIK), ochrony IK oraz pojęcie właściciela (operatora) EIK. Głównym założeniem tego aktu prawnego jest określenie sposobu rozpoznawania i wyznaczania EIK oraz zdefiniowanie podstawowych obowiązków w zakresie ochrony EIK nałożonych na państwa członkowskie (oraz pośrednio na właścicieli IK).

Już w Dyrektywie podkreśla się wyraźnie, że *„zasadnicza i ostateczna odpowiedzialność za ochronę EIK spoczywa głównie na państwach członkowskich i właścicielach/operatorach tych infrastruktur", a „wspólnotowe podejście wymaga założenia pełnego zaangażowania sektora prywatnego z uwagi na bardzo istotny udział tego sektora w nadzorowaniu ryzyka, zarządzaniu ryzykiem, planowaniu ciągłości działania i w procesie przywracania stanu sprzed katastrofy"*. Dyrektywa wskazuje równocześnie na sektor ICT, jako przyszły sektor priorytetowy w zakresie ochrony IK. Sama Komisja Europejska również wiele uwagi poświęca wskazanemu sektorowi[65], o czym mogą świadczyć wydane przez nią dokumenty, w tym m.in.
- Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *w sprawie ochrony krytycznej infrastruktury*

64 Dz. Urz. UE. Z 23.12.2008 r., L 345/75.

65 T. Szewczyk, *Europejski program ochrony infrastruktury krytycznej*, Przegląd Bezpieczeństwa Wewnętrznego 6/12, s.157-168.

informatycznej „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności”[66] („Komunikat”);
- Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *w sprawie ochrony krytycznej infrastruktury teleinformatycznej* „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni”[67] oraz
- projekt Dyrektywy Parlamentu Europejskiego i Rady *w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*[68].

Należy jednak wskazać, że ani Dyrektywa, ani też żaden z pozostałych dokumentów wymienionych powyżej nie zawiera żadnych bezpośrednich regulacji w zakresie instrumentów prawnych, które mogłyby być użyte przez państwa członkowskie w celu zachęcenia podmiotów z sektora prywatnego do aktywnego uczestnictwa w inicjatywach dot. ochrony IK.

ENISA – partnerstwo publiczno prywatne

Równolegle do EPOIK prowadzone są działania zaplanowane w Komunikacie, gdzie po raz kolejny podkreślono, że chociaż ostateczną odpowiedzialność za określanie polityki związanej z krytyczną infrastrukturą teleinformatyczną (CII – ang. *Critical Information Infrastructure*) ponoszą państwa członkowskie, jej wdrażanie uzależnione jest w istocie od zaangażowania sektora prywatnego, który posiada lub kontroluje dużą liczbę CII. Z drugiej strony, rynki nie zawsze w wystarczającym stopniu zachęcają sektor prywatny do inwestowania w ochronę CII na poziomie odpowiadającym oczekiwaniom rządów[69].

W Komunikacie wskazuje się, iż *„aby rozwiązać ten problem dotyczący zarządzania, na szczeblu krajowym pojawiły się jako model odniesienia partnerstwa publiczno-prywatne („PPP”). Jednak mimo zgody co do tego, że PPP byłyby również pożądane na szczeblu europejskim, europejskie PPP jak do tej pory jeszcze nie zaistniały. Za pomocą europejskich wielostronnych ram zarządzania, w których zwiększoną rolę odgrywać może agencja ENISA70, można by wspierać zaangażowanie sektora prywatnego w określanie strategicznych celów polityki publicznej oraz priorytetów i środków operacyjnych. Ramy te zapełniłyby lukę między działaniami politycznymi na szczeblu krajowym a rzeczywistą sytuacją operacyjną w terenie*[71]*”*.

Właśnie w celu wspierania modeli takiej współpracy PPP, ENISA wydała przewodnik dotyczący efektywności dobrych praktyk w tym zakresie (Przewodnik). W Przewodniku wskazuje się, że:
- władze państwowe same nie dysponują odpowiednimi środkami finansowymi niezbędnymi do sprawowania efektywnej ochrony IK oraz, że
- prowadzenie takiej ochrony wymaga stworzenia mechanizmów, które pozwolą zaangażować sektor prywatny[72].

66 KOM (2009) 149 wersja ostateczna, 30.03.2009 r.
67 KOM (2011) 163 wersja ostateczna, 31.03.2011 r.
68 KOM (2013) 48 wersja ostateczna, 07.02.2013 r.
69 KOM (2009) 149 wersja ostateczna, 30.03.2009 r., pkt 3.4.2
70 Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji.
71 KOM (2009) 149 wersja ostateczna, 30.03.2009 r., pkt 3.4.2.
72 ENISA, *Cooperative Model for Effective Public Private Partnerships Good Practice Guide*, 2011, s. 18.

To właśnie w tym dokumencie zostały wskazane po raz pierwszy przesłanki, które mogą być kwalifikowane jako pośrednia zachęta do aktywnej współpracy sektora prywatnego z sektorem publicznym w zakresie ochrony IK (w ramach współpracy publiczno-prywatnej), tj.:
- zmniejszenie ryzyka narażania CII na uszkodzenia, które generują koszty po stronie operatorów / właścicieli IK;
- zmniejszenie kosztów realizacji obowiązków w zakresie zapewnienia odpowiednich standardów ochrony dla CII;
- zapewnienie dostępu do specjalistycznej wiedzy w zakresie ochrony CII;
- zapewnienie istotnego wpływu na ostateczne kształtowanie polityki państw członkowskich w zakresie ochrony CII, w tym na sposób sformułowania obowiązków nałożonych w powyższym zakresie na podmioty funkcjonujące w sektorze prywatnym (operatorzy/właściciele IK).

Powyższe przesłanki powinny być traktowane jako ogólne założenia, które mają w swoim zamierzeniu pełnić funkcję wspomagającą państwa członkowskie w zakresie implementacji bardziej konkretnych rozwiązań służących promocji PPP na poziomie krajowym.

Poziom krajowy

Ustawa o zarządzaniu kryzysowym

Dyrektywa powinna była zostać implementowana do krajowych porządków prawnych do dnia 12 stycznia 2011 r. Polska implementowała Dyrektywę poprzez nowelizację ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*[73], która jest głównym aktem prawnym dotyczącym ochrony IK. Jak zostało wskazane na wstępie, niezależnie od Ustawy, polski ustawodawca zawarł również przepisy szczególne dotyczące pośrednio ochrony IK w innych aktach prawnych, które dotyczą konkretnych sektorów gospodarki, takich jak np. telekomunikacja[74], czy też lotnictwo[75].

Wśród zadań z zakresu ochrony IK Ustawa wymienia m.in. współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń IK w zakresie jej ochrony. Ustawa nakłada na właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń IK obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony IK oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia. Z kolei na organy państwa (Radę Ministrów) został nałożony obowiązek przyjęcia „Narodowego Planu Ochrony Infrastruktury Krytycznej” (NPOIK, Program). Program został przyjęty 26 marca 2013 r.

Jednocześnie należy wskazać, że podobnie jak akty prawne na poziomie prawa UE, również i ustawodawstwo polskie nie wprowadza żadnych konkretnych regulacji, które mogłyby zostać zakwalifikowane bezpośrednio jako instrumenty motywujące (zachęcające) sektor

73 Ustawa z dnia 29 października 2010 r. *o zmianie ustawy o zarządzaniu kryzysowym* (Dz. U. Nr 240, poz. 1600).
74 Ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz.U. 2004 nr 171 poz. 1800).
75 Ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze*, (Dz.U. 2002 nr 130 poz. 1112).

prywatny do systematycznego polepszania standardów ochrony IK, co może ograniczać utrzymanie i rozwój IK. Jednak, również i w tym przypadku, takich instrumentów można próbować doszukać się w dokumentach o charakterze „miękkim".

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)

W Programie podkreśla się, że operatorami znacznej części IK są prywatni przedsiębiorcy niepowiązani z administracją publiczną. Program ustanawia ramy, w których administracja publiczna i operatorzy IK współpracują w celu zapewnienia ciągłości działania IK, chroniąc tym samym gospodarcze i społeczne fundamenty naszego kraju. Program zakreśla mechanizmy rozwoju partnerskich relacji między administracją publiczną i operatorami IK w zakresie ochrony IK[76]. Uwzględniając powyższe oraz obowiązek nałożony na operatorów IK przez Ustawę, Program adresowany jest także do tych podmiotów, a w szczególności do ich zarządów. Adresatem Programu automatycznie staje się każdy nowy operator IK. Operatorzy IK uczestniczą w działaniach na rzecz ochrony IK opisanych w Programie.

W Programie podkreśla się, że jednym z kluczowych elementów zapewniających sprawną i całościową ochronę IK, jest współpraca sektora publicznego z sektorem prywatnym[77], jak i współpraca wewnątrz tych sektorów, ze szczególnym uwzględnieniem współpracy przedstawicieli poszczególnych systemów w sektorze prywatnym. Ważnym elementem współpracy jest wypracowanie przejrzystych zasad i procedur między organami i służbami państwa a właścicielami oraz posiadaczami samoistnych i zależnych obiektów, instalacji lub urządzeń IK[78]. Należy jednak zaznaczyć, że PPP[79] w rozumieniu Programu (zakresie ochrony IK) oznacza jedynie rodzaj współpracy między jednostkami administracji publicznej a podmiotami prywatnymi, poprzez na przykład wymianę wszelkich informacji mogących mieć wpływ na osiągnięcie celów NPOIK. Takie partnerstwo nie przewiduje natomiast zawarcia jakiejkolwiek umowy, na podstawie której następowałaby realizacja za wynagrodzeniem przez partnera prywatnego przedsięwzięcia na rzecz podmiotu publicznego[80].

W tym przedmiocie zasadne jest, aby wyraźnie odróżnić nazewnictwo obu form współpracy tj. współpracy prywatno-publicznej, na którą wskazuje NPOIK, oraz współpracy w formie PPP w rozumieniu ustawy *o partnerstwie publiczno-prywatnym*[81] (Ustawa PPP). Wydaje się, że poza współpracą wskazaną w NPOIK, rozumianą jako pewien proces wymiany informacji, istotnym uzupełnieniem systemu ochrony IK mogłyby być również właśnie PPP w rozumieniu Ustawy PPP. W dalszej części opracowania, partnerstwo publiczno-prywatne w rozumieniu NPOIK będzie określane jako „WPP", natomiast partnerstwo publiczno-prywatne w rozumieniu Ustawa PPP jako „PPP". Z uwagi jednak, iż omówienie PPP wykraczałoby poza przedmiot niniejszego opracowania, nie będzie poddawane w tym miejscu bliższej analizie.

76 *Narodowy Program*…, op. cit., s. 6.

77 Szerzej na temat przyszłości współpracy prywatno-publicznej w Polsce patrz w rozdziale 3 – *Efektywna współpraca prywatni-publiczna – czynniki sukcesu*.

78 Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/?page_id=257, [dostęp: 12.06.2014].

79 Chodzi o partnerstwo publiczno-prywatne wskazane Narodowy Program…, op. cit. s.33. (współpraca).

80 *Narodowy Program*…, op. cit., s. 33.

81 Ustawa z dnia 19 grudnia 2008 r. *o partnerstwie publiczno-prywatnym*, (Dz. 2009, nr 19, poz. 100).

Jednakże wydaje się, że już samo uczestnictwo/przystąpienie do Programu, powinno być traktowane jako forma zachęty dla podmiotów należących do sektora prywatnego do podejmowania współpracy w zakresie ochrony IK. W szczególności, zachęcie tej miałaby służyć możliwość aktywnego działania tych podmiotów w ramach specjalistycznego forum WPP stworzonego na potrzeby Programu[82]. Do kluczowych celów tego forum ma bowiem należeć:

- stworzenie platformy sprzyjającej wymianie opinii jak i pracy nad delikatnymi kwestiami ochrony IK;
- zgłaszanie i wypracowywanie nowych rozwiązań prawnych dotyczących ochrony IK;
- wymiana opinii i uwag zainteresowanych podmiotów już na wczesnym etapie prac legislacyjnych w obszarze IK;
- organizacja warsztatów, seminariów i konferencji poświęconych tematyce ochrony IK;
- stworzenie bazy specjalistów w kwestiach związanych z tematyką IK w poszczególnych systemach – finansowym, łączności, sieci teleinformatycznych, zaopatrzenia w energię, surowce energetyczne i paliwa itd.

Wydaje się więc, że w powyższym zakresie, forum WPP stworzone w ramach Programu będzie w znacznej mierze powielało podstawowe założenia określone w Przewodniku. W konsekwencji, będzie ono stanowiło również instrument motywujący podmioty należące do sektora prywatnego do aktywności w zakresie polepszania standardów ochrony IK. Dzięki pracom forum powstanie baza specjalistów w kwestiach związanych z tematyką IK w poszczególnych systemach – finansowym, łączności i sieci teleinformatycznych, zaopatrzenia w energię i paliwa itd. Eksperci ci, będą współpracowali ze stroną rządową m.in. w trakcie prac podejmowanych na forum Unii Europejskiej w celu przedyskutowania z sektorem prywatnym propozycji legislacyjnych Unii. Funkcjonowanie bazy specjalistów przyspieszy proces konsultacji i jednocześnie pozwoli na korzystanie z doświadczenia i wiedzy, która w samej administracji publicznej może być niewystarczająca[83].

Podmioty uczestniczące w forum będą więc mogły:

- prowadzić aktywny dialog w zakresie kształtowania zasad ochrony IK;
- wywierać wpływ na ostateczny kształt konkretnych rozwiązań implementowanych w powyższym zakresie oraz
- korzystać na bieżąco z porad stałych ekspertów.

Wydaje się, iż efektem forum WPP mogłoby być m.in.:

- wypracowanie jasnych, przejrzystych zasad i procedury działania oraz wymiany informacji między organami państwa a partnerami prywatnymi;
- wypracowanie jednolitych, kompatybilnych sposobów gromadzenia i przetwarzania informacji dotyczących zagrożeń IK;
- opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń IK;
- wskazanie sposobów, mechanizmów ochrony oraz odtwarzania IK;
- opracowanie optymalnych sposobów zapewnienia bezpieczeństwa danym, otrzymanym od podmiotów prywatnych; utrzymywanie systemów rezerwowych;

82 Szerzej na temat metodyki zarządzania, struktury organizacyjnej, finansowania oraz komunikacji w ramach takich forów patrz rozdział 4 – *Metodyka zarządzania forami infrastruktury krytycznej*.

83 Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/?page_id=257, [dostęp: 12.06.2014].

- opracowanie procedur zapobiegania zakłóceniom funkcjonowania IK oraz przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na IK.

W celu realizacji przedstawionych powyżej zadań oraz osiągnięcia wskazanych rezultatów, konieczne jest podjęcie całego szeregu działań: edukacyjnych, planistycznych, koordynacyjnych i legislacyjnych. Działania te w pierwszej kolejności powinny być podejmowane przez Rządowe Centrum Bezpieczeństwa. W związku z tym, że NPOIK został opracowany dopiero w marcu 2013 r. (co było przedmiotem krytyki chociażby Najwyższej Izby Kontroli) trudno w tej chwili powiedzieć czy działania te będą sprawnie podejmowane. Zgodnie z informacjami udostępnianym przez Rządowe Centrum Bezpieczeństwa wykaz elementów infrastruktury powstał i jest uaktualniany, natomiast w związku z tym, że dostęp do niego ma wyłącznie ograniczony krąg osób, trudno wypowiadać się o jego kompletności. W chwili obecnej fakt istnienia Programu i wykazu IK pozwala na przystąpienie do dalszych prac szczegółowo regulujących mechanizmy efektywnego zarządzania i ochrony IK.

Finansowanie działań dotyczących ochrony IK w Polsce

W Programie podkreśla się, że działania z zakresu ochrony IK są finansowane ze środków własnych uczestników Programu i planowane w ich budżetach, w przypadku operatorów IK na podstawie art. 6 Ustawy. Zarówno Program, jak i Ustawa, nie wskazują bezpośrednio na możliwość ubiegania się przez właścicieli oraz operatorów IK o refinansowanie kosztów poniesionych na IK z budżetu państwa lub UE[84].

Jednakże, wśród instrumentów pośrednio finansujących działania z zakresu ochrony IK, Program wymienia Decyzję Rady z dnia 12 lutego 2007 r. ustanawiającą na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program: „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa"[85] – CIPS. Celem CIPS było umożliwienie wsparcia finansowego z budżetu Unii Europejskiej działań realizowanych m.in. w obszarze ochrony IK, takich jak:

- stymulowanie, promowanie i wspieranie ocen ryzyka dotyczących IK w celu modernizacji systemów bezpieczeństwa;
- stymulowanie, promowanie i wspieranie opracowania metodologii ochrony IK, szczególnie metodologii w zakresie oceny ryzyka;
- promowanie i wspieranie rozwoju standardów bezpieczeństwa oraz wymiany *know-how* i doświadczeń w zakresie ochrony ludności i IK;
- promowanie i wspieranie koordynacji i współpracy na skalę wspólnotową dotyczącą ochrony IK.

Jednocześnie, w ramach CIPS beneficjentami projektów odwołujących się do tematyki ochrony IK mogły być również podmioty z sektora prywatnego, które mogły ubiegać się o odpowiednie dofinansowanie inicjatyw zgodnych z podstawowymi celami tego programu. Program CIPS ustanowiony był w okresie od dnia 1 stycznia 2007 r. do 31 grudnia 2013 r. i obecnie częściowo ma zostać zastąpiony poprzez Fundusz Bezpieczeństwa Wewnętrznego, instrument finansowy na rzecz wspierania współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego (FBW)[86].

Wśród potencjalnych pośrednich źródeł, z których operatorzy IK mogą ubiegać się o finansowanie IK, należy wskazać również krajowe programy operacyjne, w ramach których wydatkowane są środki z funduszy europejskich[87] (obecnie w trakcie tworzenia na nową perspektywę finansową na lata 2014-2020) czy instrument finansowy na poziomie UE „Łącząc Europę" (CEF – ang. *Connecting Europe Facility*)[88]. CEF w zakresie celów związanych z infrastrukturą sieci telekomunikacyjnych wymienia m.in. wsparcie krytycznej infrastruktury teleinformatycznej.

Należy wskazać, iż oprócz wymiany informacji co do zagrożeń oraz szeroko pojętej współpracy prywatno-publicznej, kluczową kwestią pozostaje zapewnienie sposobu w jaki sektor prywatny podejmowałby aktywne działania w celu ochrony IK znajdującej się w jego posiadaniu, wykraczające poza podstawowe środki polegające wyłącznie na ochronie swoich zasobów. Słusznie bowiem stawia się pytanie o to, kto powinien odpowiadać za bezpieczeństwo IK, jeżeli sektor prywatny nie jest wystarczająco zmotywowany do inwestycji w bezpieczeństwo IK, a z drugiej strony państwo nie podejmuje niezbędnych inicjatyw w tym przedmiocie[89].

Podkreśla się, że istnieją niewielkie zachęty finansowe dla akcjonariuszy do inwestowania w bezpieczeństwo IK ponad ich interes w danej organizacji, a tym samym podmioty prywatne wspierają inwestycję w bezpieczeństwo IK tylko w zakresie, w jakim jest to niezbędne i zyskowne. Tak więc rynek sam w sobie nie generuje wystarczających zachęt do skutecznego zabezpieczenia IK[90]. Przykładowo wskazuje się, iż w dziedzinie energetyki, konieczność redukcji kosztów i zapewnienia bezpieczeństwa dostaw może prowadzić do sprzecznych celów polityki publicznej i niewystarczających zachęt po stronie podmiotów prywatnych do inwestowania w zwiększoną ochronę infrastruktury[91]. Z kolei poleganie wyłącznie na najlepszych praktykach i wewnętrznych regulacjach wprowadzonych przez poszczególne sektory (ang. *industry self-regulation*) może okazać się niewystarczające w dobie obecnych zagrożeń[92].

Wprowadzanie pewnych wymogów przez podmioty prywatne w danych sektorach, jest praktyką umożliwiającą m.in. podniesienie standardów branżowych. Samoregulacja jest środkiem, który pozwala na przekraczanie minimalnych wymogów prawnych, a także może wzmacniać zrozumienie i zgodność z obowiązującymi przepisami. W konkurencyjnym środowisku, współpraca wewnątrz-sektorowa jest silną zachętą dla przedsiębiorstw do ciągłego doskonalenia

84 Na tę kwestię wskazywano już w Studium Ministerstwa Infrastruktury w 2006 r., por. r. Piwowarczyk, *Ochrona Infrastruktury Krytycznej*.

85 Dz. Urz. UE z 24.02.2007 r., L 58/1.

86 Obecnie trwają pracę nad Rozporządzeniem Parlamentu Europejskiego i Rady (UE) ustanawiającym, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument finansowy na rzecz wspierania współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego.

87 W szczególności z Funduszu Spójności oraz Europejskiego Funduszu Rozwoju Regionalnego.

88 *Connecting Europe Facility*, http://ec.europa.eu/digital-agenda/en/connecting-europe-facility, [dostęp: 12.06.2014].

89 P. Auerswald, L.M. Branscomb, Todd, M. La Porte, E. Michel-Kerjan, *The Challenge of Protecting Criticial Infrastructure, Risk Management and Decision Process Center*, Wharton University of Pennsylvania, Working Paper # 05-11, October 2005, s. 4.

90 S. Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*, Matthew B Ridgway Center for International Security Studies, Pittsburgh, United States, 2005, s. 15.

91 CEPS, Task Force Report, *Protecting critical infrastructure in the EU*, Brussels 2010, s. 73.

92 Ibidem, s. 15.

standardów i ich podnoszenia, w celu zdobycia udziałów w rynku. Dobrowolne wprowadzanie pewnych wymogów przez podmioty prywatne, pozwala często uniknąć nakładania obowiązków i wymagań przez państwo.

Powyższe można odnieść również w kontekście problemu ochrony i bezpieczeństwa IK, dlatego podmioty prywatne z poszczególnych sektorów będące w posiadaniu IK powinny być zachęcane do wprowadzania samoregulacji w tym zakresie.

Należy zwrócić uwagę na potrzebę wypracowania dodatkowych, silniejszych zachęt na rzecz bardziej aktywnego zaangażowania sektora prywatnego w ochronę IK. W rozdziale 3 niniejszego raportu wskazano na potencjalne instrumenty, które państwo może w tym celu zastosować np.: ulgi podatkowe, dotacje (granty), ulgi ubezpieczeniowe, certyfikowanie firm, preferencyjne kredytowanie. Powinno się tworzyć również zachęty dla „oddolnego" podejmowania działań przez podmioty prywatne z poszczególnych sektorów (samoregulacji), na rzecz wypracowania i przestrzegania pewnych standardów i rozwiązań w zakresie ochrony i bezpieczeństwa IK.

Wydaje się, iż skuteczność systemu ochrony IK składającego się z elementów wyżej wskazanych tj. szeroko pojętej współpracy publiczno-prywatnej (WPP), w tym wymiany informacji, samoregulacji poszczególnych sektorów oraz zachęt fiskalnych oraz para fiskalnych, byłaby znacząco większa.

Kierunek zmian w zakresie wymogów dotyczących ochrony IK

Dotychczasowe podejście w zakresie ochrony IK oparte jest przede wszystkim na dobrowolnej współpracy sektora publicznego i prywatnego. W nowych regulacjach prawnych na poziomie UE można jednak dostrzec zmianę na rzecz podejścia regulacyjnego. Chodzi w szczególności o Dyrektywę Parlamentu Europejskiego i Rady *w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie UE*[93]*"* (Dyrektywa NIS). Celem proponowanej dyrektywy jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji. Obecnie trwają prace nad ostateczną wersją tego aktu prawnego.

W projekcie Dyrektywy NIS, Komisja Europejska przyjęła właśnie podejście regulacyjne (sankcyjne) uznając, iż stosowane dotychczas podejście oparte na dobrowolności doprowadziło do niejednolitego poziomu gotowości i ograniczonego poziomu współpracy. Uznano, iż obecny stan rzeczy w UE, który odzwierciedla czysto dobrowolne podejście, nie zapewnia wystarczającej ochrony przed incydentami w zakresie bezpieczeństwa sieci i informacji oraz przed zagrożeniami w obrębie całej UE.

W ocenie Komisji nieprawdopodobne jest, by wszystkie państwa członkowskie osiągnęły porównywalny krajowy poziom zdolności i gotowości niezbędny do poprawy bezpieczeństwa oraz umożliwienia współpracy i wymiany informacji poufnych na poziomie UE wyłącznie poprzez dobrowolne działania państw członkowskich oraz podmiotów prywatnych.

W ramach zaproponowanego w Dyrektywie NIS wariantu regulacyjnego, właściwe organy krajowe oraz zespoły reagowania na incydenty komputerowe mają stanowić element sieci służącej współpracy na poziomie UE. W obrębie tej sieci organy krajowe i zespoły reagowania na incydenty komputerowe prowadziłyby wymianę informacji oraz współpracę w celu zwalczania zagrożeń i incydentów w obszarze bezpieczeństwa sieci i informacji zgodnie z europejskim planem awaryjnym na wypadek incydentów cybernetycznych i europejskim planem współpracy, które musiałyby zostać uzgodnione przez państwa członkowskie. Komisja ma zamiar zobowiązać wszystkie państwa członkowskie do stworzenia przynajmniej minimalnych zdolności krajowych (zespoły reagowania na incydenty komputerowe, właściwe organy, krajowe plany awaryjne na wypadek incydentów cybernetycznych, krajowe strategie bezpieczeństwa cybernetycznego).

W uzasadnieniu Dyrektywy NIS wskazano, iż *„[…] podmioty zarządzające infrastrukturą krytyczną lub świadczące usługi niezbędne do funkcjonowania naszych społeczeństw nie są zobowiązane do przyjęcia środków przeciwdziałania zagrożeniom ani do wymiany informacji z właściwymi organami. Tak więc z jednej strony brakuje skutecznych bodźców, które zmusiłyby przedsiębiorstwa do odpowiedniego przeciwdziałania zagrożeniom, łącznie z przeprowadzaniem oceny zagrożeń i podejmowaniem odpowiednich kroków w celu zapewnienia bezpieczeństwa sieci i informacji."*[94]

Z tego względu Przedsiębiorstwa (z wyjątkiem mikroprzedsiębiorstw) w określonych branżach o znaczeniu krytycznym, takich jak bankowość, energetyka (energia elektryczna i gaz ziemny), transport, ochrona zdrowia oraz infrastruktura podstawowych usług internetowych, jak również organy administracji publicznej mają zostać zobowiązane do oceny zagrożeń, przed którymi stoją, oraz przyjęcia właściwych i proporcjonalnych środków w odpowiedzi na faktyczne zagrożenia. Podmioty te zostałyby ponadto zobowiązane do zgłaszania właściwym organom incydentów, które mają znaczny negatywny wpływ na funkcjonowanie ich sieci i systemów informatycznych, a tym samym niosą ze sobą istotne skutki dla ciągłości świadczenia usług i prowadzenia dostaw towarów, które są uzależnione od tych sieci i systemów.[95]

Przejawem powyższego podejścia jest proponowana treść m.in. art. 14 oraz 15 projektu Dyrektywy NIS (w brzmieniu po poprawkach Parlamentu Europejskiego[96]). Zgodnie z art. 14 ust. 1-3:

„1. Państwa członkowskie zapewniają zastosowanie przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu wykrywania zagrożeń, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne, skutecznego przeciwdziałania takim zagrożeniom i ich ograniczania. Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny i proporcjonalny do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydentom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług oraz bezpieczeństwo danych opartych na tych sieciach i systemach informatycznych.

93 COM(2013) 48 final, 2013/0027 (COD) 7.2.2013.

94 *Wniosek dotyczący środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*, SWD (2013) 31 final, 7.2.2013, s. 3.

95 Dokument Roboczy Służb Komisji, *Streszczenie Oceny Skutków*, Towarzyszący dokumentowi: *Wniosek dotyczący środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*, SWD (2013) 31 final, 7.2.2013, ss. 4-6.

96 Sprawozdanie PE z dnia 12 luty 2014 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady *w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii* (COM(2013) 48 – C70035/2013 – 2013/0027(COD)).

2. Państwa członkowskie dopilnowują, aby organy administracji publicznej oraz podmioty gospodarcze zgłaszały właściwym organom incydenty mające znaczące konsekwencje dla bezpieczeństwa świadczonych przez nie usług podstawowych.
a) Producenci oprogramowania komercyjnego są pociągani do odpowiedzialności pomimo zawartych w umowach z użytkownikami klauzul o braku odpowiedzialności, w przypadku wystąpienia poważnego zaniedbania w zakresie bezpieczeństwa i ochrony.

3. Wymogi zawarte w ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych i producentów oprogramowania świadczących usługi w obrębie Unii Europejskiej."

Z kolei zgodnie z art. 15 ust. 3 projektu Dyrektywy NIS *„państwa członkowskie zapewniają właściwym organom uprawnienia do wydawania wiążących instrukcji dla podmiotów gospodarczych i organów administracji publicznej".*

Powyżej powołane propozycje potwierdzają stanowisko organów UE, iż *„nieśmiałe, dobrowolne działania są nieskuteczne i że należy nałożyć na państwa członkowskie zdecydowane zobowiązania regulacyjne, by zapewnić harmonizację, zarządzanie i egzekwowanie w zakresie europejskiego NIS"*[97], a dzięki proponowanemu wariantowi regulacyjnemu możliwe będzie *„[…] istotne zwiększenie poziomu ochrony konsumentów, przedsiębiorstw i administracji publicznych w UE przed incydentami i zagrożeniami w obszarze bezpieczeństwa sieci i informacji."*[98]

Pomimo, iż przywołana powyżej dyrektywa dotyczy tylko pewnego obszaru IK, tj. IK związanej z bezpieczeństwem sieci i informacji, to nie można wykluczyć, iż podejście regulacyjne (sankcyjne) będzie miało w przyszłości zastosowanie również do ochrony IK w innych obszarach. Organy UE przyjmując podejście typu *„top-down"*, a więc regulacyjne, uznały, iż podejście czysto dobrowolne oraz typu *„bottom-up"* jest niewystarczające do osiągnięcia zakładanych celów.

Wątpliwość powstaje czy ten sposób „zachęcenia" podmiotów prywatnych do bardziej aktywnego działania w obszarze ochrony IK nie spowoduje podejścia minimalistycznego ze strony tych podmiotów tj. wypełniania obowiązków nałożonych przez prawo wyłącznie w zakresie w jakim jest to wymagane w celu uniknięcia sankcji, a zniechęci do podejmowania działań o charakterze *self-regulation*.

Problematyka zamówień publicznych w kontekście ochrony IK

Przepisy ustawy z dnia 29 stycznia 2004 r. *Prawo zamówień publicznych* (Dz. U. z 2013 poz. 907 z późn. zm., dalej „Pzp") nie odnoszą się wprost do zagadnień związanych z wystąpieniem zakłóceń w funkcjonowaniu IK[99]. Nie oznacza to jednak, iż Pzp nie zawiera rozstrzygnięć właściwych dla sytuacji o charakterze nadzwyczajnym, do których zaliczyć należy awarie, ataki i inne zdarzenia mogące prowadzić do zaburzeń w zakresie funkcjonalności, ciągłości działań czy integralności IK.

97 Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady *w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*, COM(2103) 48 final – 2013/0027 (COD), 22 maja 2013 r.

98 Dokument Roboczy Służb Komisji. *Streszczenie Oceny Skutków*, Towarzyszący dokumentowi: *Wniosek dotyczący środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*, SWD(2013) 31 final, 7.2.2013, s. 8.

99 Na marginesie zauważyć należy, iż ustawa o zarządzaniu kryzysowym również nie odwołuje się do przepisów Pzp

Kluczowym zagadnieniem z punktu widzenia zakłóceń funkcjonowania IK w kontekście systemu zamówień publicznych jest możliwość sprawnego i pozwalającego na ominięcie sformalizowanej i czasochłonnej procedury udzielania zamówień o charakterze interwencyjnym czy doraźnym. Jak wynika z danych opublikowanych przez Prezesa Urzędu Zamówień Publicznych średni czas trwania postępowania o udzielenie zamówienia publicznego (liczony od daty publikacji ogłoszenia o zamówieniu do zawarcia umowy) w 2012 r. (dane za 2013 r. nie zostały jeszcze opublikowane) prowadzonego w jednym z dwóch podstawowych trybów (przetarg nieograniczony oraz przetarg ograniczony) wynosił:

- *w przypadku postępowań prowadzonych wg procedury krajowej (o wartości nieprzekraczającej tzw. progów unijnych):*
  - 31 dni dla przetargu nieograniczonego
  - 60 dni dla przetargu ograniczonego,
- *w przypadku postępowań prowadzonych wg procedury unijnej (o wartości przekraczającej tzw. progi unijne)*:
  - 86 dni dla przetargu nieograniczonego
  - 112 dni dla przetargu ograniczonego.

Oczywiste jest więc, iż próby zapobiegania zakłóceniom funkcjonowania IK mogą się nie powieść, jeżeli zamawiający zmuszony będzie do skorzystania z czasochłonnej procedury przetargowej. Dlatego w Pzp zawarte zostały rozwiązania, które, po zaistnieniu określonych przesłanek, uprawniają zamawiającego do udzielenia zamówienia w sposób, który, adekwatnie do zaistniałej sytuacji, pozwala skrócić ustawowe terminy wymagane w ramach procedury przetargowej lub skorzystać z trybu niekonkurencyjnego. Rozwiązania te, w zależności od oceny nagłości zdarzenia i zapotrzebowania stanowiącego jego skutek, pozwalają zapobiegać sytuacjom o charakterze nadzwyczajnym.

Tabela przedstawia zestawienie ustawowych przesłanek umożliwiających skorzystanie przez zamawiającego z uprzywilejowania gwarantowanego przez Pzp (w zakresie poszczególnych trybów).

Tabela 5. Zestawienie ustawowych przesłanek umożliwiających skorzystanie przez zamawiającego z uprzywilejowania gwarantowanego przez Pzp. Źródło: Opracowanie własne.

	PRZESŁANKI
PRZETARG OGRANICZONY/ NEGOCJACJE Z OGŁOSZENIEM- PROCEDURA PRZYSPIESZONA	pilna potrzeba udzielenia zamówienia
NEGOCJACJE BEZ OGŁOSZENIA	pilna potrzeba udzielenia zamówienia potrzeba pilnego udzielenie zamówienia nie wynika z przyczyn leżących po stronie zamawiającego niemożność wcześniejszego przewidzenia konieczności udzielenia zamówienia brak możliwości zachowania terminów niezbędnych do przeprowadzenia postępowania w trybie przetargowym lub w trybie negocjacji z ogłoszeniem
WOLNA RĘKA	wyjątkowa sytuacja wyjątkowa sytuacja nie wynika z przyczyn leżących po stronie zamawiającego niemożność wcześniejszego przewidzenia zaistnienia wyjątkowej sytuacji brak możliwości zachowania terminów niezbędnych dla innych trybów udzielania zamówienia

Jeżeli spełnione zostały przesłanki warunkujące skorzystanie z jednego z powyższych trybów, to:

- w przypadku przetargu ograniczonego/negocjacji z ogłoszeniem prowadzonego w procedurze przyspieszonej – można ustanowić skrócone terminy składania wniosków o dopuszczenie do udziału w przetargu ograniczonym (min. 10 lub 15 dni, w zależności od formy przekazania ogłoszenia do publikacji Urzędowi Publikacji Unii Europejskiej, wobec min. 30 lub 37 dni przewidzianych w procedurze standardowej) oraz terminów składania ofert (min. 10 dni wobec min. 40 dni przewidzianych w procedurze standardowej);
- w przypadku negocjacji bez ogłoszenia – można prowadzić negocjacje z wybranymi przez siebie wykonawcami;
- w przypadku postępowania z wolnej ręki – można prowadzić negocjacje z jednym tylko wykonawcą.

Na uwagę zasługuje, iż w przypadku, gdy zamówienie zakwalifikowane jest jako sektorowe (tj. realizowane jest przez podmiot wskazany w art. 3 ust. 1 pkt 4 Pzp wykonujący zadania wskazane w art. 132 Pzp), przepisy Pzp znajdą zastosowanie jedynie, gdy jego wartość jest równa lub przekracza tzw. progi unijne (które aktualnie wynoszą 414.000,00 euro dla dostaw/ usług i 5.186.000,00 euro dla robót budowlanych). Natomiast jeżeli wartość zamówienia sektorowego oszacowana została na kwotę niższą, zamawiający nie jest zobowiązany do stosowania przepisów Pzp.

Podsumowując, przytoczone procedury (ze szczególnym uwzględnieniem negocjacji bez ogłoszenia oraz wolnej ręki) mogą okazać się niezwykle przydatne w przypadku zaistnienia stanu zakłócenia IK. Nie należy jednak zapominać, iż tryby niekonkurencyjne cechuje charakter wyjątkowy, a przesłanki uzasadniające ich zastosowanie nie mogą być interpretowane dowolnie. W przypadku korzystania przez zamawiającego z trybów niekonkurencyjnych zawsze dochodzi bowiem do naruszenia fundamentalnej z punktu widzenia systemu zamówień publicznych zasady konkurencyjności. Zamawiający musi być więc pewien, iż chronione przez niego dobro (życie, zdrowie, mienie) obiektywnie wymaga, aby, ze względu na jego doniosłość, przyznać mu pierwszeństwo przed konkurencyjnością[100]. Należy również pamiętać, iż zastosowanie jednego z powyższych trybów uzasadnione jest jedynie w odpowiedzi na ziszczenie się określonego zagrożenia. Nie będzie natomiast podstaw do udzielenia zamówienia w trybie negocjacji bez ogłoszenia lub z wolnej ręki, gdy zamawiający, chcąc zapobiec bliżej nieokreślonemu przyszłemu zjawisku zrealizuje zamówienia, które mogłyby zostać udzielone w procedurze konkurencyjnej.

Zwolnienie ze stosowania przepisów Pzp

Niezależnie od opisanych powyżej procedur zauważyć należy, iż w przypadku wystąpienia stanu zakłócającego funkcjonowanie IK potencjalnie możliwe jest także skorzystanie z przesłanki uprawniającej do odstąpienia od stosowania przepisów Pzp w sytuacji, gdy *wymaga tego istotny interes bezpieczeństwa państwa lub ochrona bezpieczeństwa publicznego* (art. 4 pkt 5 Pzp).

100 W. Dzierżanowski, Ochrona konkurencji w prawie zamówień publicznych, Wolters Kluwer Polska Sp. z o.o., 2012, s. 156

Zgodnie z interpretacją Prezesa Urzędu Zamówień Publicznych celem ustawodawcy była m. in. ochrona bezpieczeństwa wewnętrznego. Należy mieć na uwadze, iż pomiędzy odstąpieniem od stosowania przepisów Pzp a istnieniem istotnego interesu bezpieczeństwa zachodzić musi związek przyczynowo-skutkowy. Problemów może dostarczać wykładnia nieostrego sformułowania *istotny interes bezpieczeństwa państwa*. Zgodnie ze stanowiskiem Prezesa UZP z zamówieniem dotyczącym istotnego interesu bezpieczeństwa państwa będziemy mieli do czynienia w szczególności, gdy dotyczy ono takich wartości jak suwerenność, międzynarodowa pozycja, niepodległość, nienaruszalność terytorium czy obronność państwa. O ile więc zakłócenie w funkcjonowaniu IK wywierać będzie wpływ na powyższe wartości, rozważyć należałoby odstąpienie od stosowania Pzp. Wydaje się jednak, iż, jakkolwiek nie wspomina o tym Pzp, zakłócenie to musi mieć charakter rzeczywisty, a nie jedynie potencjalny.

Procedura odwoławcza

Kontrowersje może wywołać korzystanie w postępowaniu prowadzonym w związku z zakłóceniem funkcjonowania IK z procedury odwoławczej. Podkreślić bowiem należy, iż regułą jest, że wniesienie odwołania powoduje, że do czasu ogłoszenia przez KIO wyroku lub postanowienia kończącego postępowanie odwoławcze zamawiający nie może zawrzeć umowy. Procedura odwoławcza może więc spowodować znaczące przedłużenie postępowania prowadzącego do podpisania umowy, co, w przypadku zagrożeń funkcjonowania IK, których immanentną cechą zdaje się być nagłość, może negatywnie wpłynąć na podjęte przez zamawiającego działania. Podkreślić jednak należy, iż Pzp przewiduje mechanizm zapobiegający negatywnym skutkom odnoszącym się do okresu zawieszenia związanego z wniesionym odwołaniem. Zamawiający jest bowiem uprawniony do przedłożenia do KIO wniosku o uchylenie zakazu zawarcia umowy. KIO natomiast może przychylić się do powyższego wniosku, o ile niezawarcie umowy mogłoby spowodować negatywne dla interesu publicznego skutki, przewyższające korzyści związane z koniecznością ochrony wszystkich interesów, w odniesieniu do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez zamawiającego w postępowaniu o udzielenie zamówienia. Wydaje się, iż w przypadku zagrożeń dotyczących IK uzasadnienie przedmiotowego wniosku nie powinno być problematyczne (a jak wynika z praktyki KIO istnieje duże prawdopodobieństwo uwzględnienia takiego wniosku). Jednocześnie podkreślenia wymaga, iż odwołanie do KIO może być wniesione jedynie wówczas, gdy postępowanie o udzielenie zamówienia publicznego prowadzone jest w reżimie Pzp (niezależnie od wybranego przez zamawiającego trybu). W przypadku więc, gdy dane postępowanie, czy to z uwagi na wartość zamówienia, czy wyłączenie, o którym mowa w art. 4 ust. 5 Pzp, prowadzone jest z pominięciem Pzp, postępowanie przed KIO nie może być prowadzone (odwołanie podlega odrzuceniu).

Pzp nie przewiduje jakichkolwiek mechanizmów (oprócz wskazanych powyżej), które ułatwiałyby (przyspieszały) procedurę zamówieniowa w odniesieniu do utrzymania (budowy) IK w sytuacjach niekryzysowych. Przewidziane przez Pzp tryby nadzwyczajne zaczerpnięte są wprost z dyrektywy UE. Dlatego też bez zmiany dyrektywy wprowadzenie dodatkowych uproszczeń dla zamawiających wydaje się na obecnym etapie niemożliwe. Najnowsze regulacje unijne powielają dotychczasowy system w zakresie radzenia sobie z nadzwyczajnymi sytuacjami, jak zawarte w starych dyrektywach (co też pośrednio świadczy o tym, że zdaniem ustawodawcy unijnego aktualne rozwiązania należy ocenić jako wystarczające). Potencjalnie

można jedynie rozważać wprowadzenie do ustaw szczególnych wyłączenia stosowania Pzp w pewnych zdefiniowanych sytuacjach. Takie rozwiązania w Polsce funkcjonują (np. ustawa *o inwestycjach w zakresie terminalu regazyfikacyjnego skroplonego gazu ziemnego w Świnoujściu* przewiduje, że jeżeli wymaga tego istotny interes bezpieczeństwa państwa, dopuszcza się realizowanie zamówień zgodnie z art. 4 ust. 5 Pzp, czyli, *de facto*, z pominięciem Pzp).

Podsumowanie

Ustawodawstwo krajowe nakłada na właścicieli i operatorów IK konkretne obowiązki, które mogą się w praktyce wiązać z dużymi nakładami finansowymi. Jednocześnie, zgodnie z regulacją Ustawy, koszty związane z realizacją tych obowiązków ponoszą odpowiednio właściciele i operatorzy IK.

Wydaje się jednak, że takie podmioty powinny mieć możliwość ubiegania się o dofinansowanie przynajmniej części nakładów poniesionych w związku z utrzymaniem IK, Wśród potencjalnych źródeł, z których operatorzy IK mogą ubiegać się o finansowanie IK, należy wskazać np. krajowe programy operacyjne, w ramach których wydatkowane są środki z funduszy europejskich, instrument finansowy CEF, który w zakresie celów związanych z infrastrukturą sieci telekomunikacyjnych wymienia m.in. wsparcie krytycznej infrastruktury teleinformatycznej.

Podstawowych zachęt dla operatorów IK do aktywnego współdziałania z organami państwowymi w zakresie ochrony IK należy się natomiast dopatrywać nie tyle w wiążących przepisach prawa, ile w samych skutkach nawiązanej współpracy z administracją publiczną, takich jak np.:

- uzyskanie dostępu do specjalistycznej wiedzy;
- identyfikacja najlepszych praktyk i standardów w zakresie ochrony IK;
- możliwość udziału w kształtowaniu i wpływaniu na politykę państwa w zakresie ochrony IK, a tym samym na ostateczne ukształtowanie obowiązków związanych z tą ochroną.

Wydaje się, że już powyższe mogłoby przyczynić się do zmniejszenia kosztów operatorów IK w pewnych obszarach, niemniej jednak istotną zachętę do bardziej aktywnego udziału operatorów IK (poza obowiązkami ustawowymi) mogłoby stanowić chociażby częściowe refinansowanie ponoszonych przez operatorów IK kosztów, wynikające wprost z obowiązujących przepisów prawa.

Natomiast obecnie w obowiązujących aktach prawnych większy nacisk kładzie się na potrzebę ochrony IK i obowiązek zaangażowania w ten proces podmiotów z sektora prywatnego, a nie na konkretne instrumenty (w tym finansowe, PPP), które mogłoby zachęcić te podmioty do aktywnego udziały w systemie ochrony IK.

Przepisy Pzp przewidują mechanizmy ułatwiające skrócenie albo wręcz wyeliminowanie procedur konkurencyjnych w przypadku sytuacji nadzwyczajnych oraz w sytuacji pewnych konkretnych zamówień sektorowych. Jednakże na etapie utrzymania i ochrony IK, ustawodawca nie przywiduje ułatwień w zakresie nabywania towarów lub usług.

3. Efektywna współpraca prywatno-publiczna – czynniki sukcesu

Joanna Świątkowska – Instytut Kościuszki

Współcześnie, znaczna część infrastruktury krytycznej (IK) znajduje się w rękach podmiotów prywatnych. Tym samym, w wielu przypadkach państwo nie ma wyłącznego wpływu na bezpieczeństwo i ciągłość działania IK. W celu zmaksymalizowania skuteczności ochrony infrastruktury zapewnione muszą być mechanizmy współpracy pomiędzy podmiotami prywatnymi i publicznymi. Celem niniejszego rozdziału jest wskazanie elementów, które wzmacniają efektywność takiej kooperacji, pokazanie potencjalnych trudności wraz z rekomendacjami jak je pokonać. Komplementarną częścią tego artykułu jest rozdział czwarty, przedstawiający dobre praktyki w zakresie metodyki zarządzania forami IK.

Warunki bazowe efektywnej współpracy

Warunkiem wstępnym efektywnej kooperacji między podmiotami publicznymi i prywatnymi, a w konsekwencji ważnym składnikiem bezpieczeństwa IK, jest obopólna świadomość i przekonanie o współdzieleniu odpowiedzialności za bezpieczeństwo państwa i dobro wspólne. Z jednej strony, państwo powinno traktować podmioty prywatne jako kluczowego aktora i partnera, którego zaangażowanie jest niezbędne z punktu widzenia osiągnięcia założonego celu. Z drugiej strony zaś, same podmioty prywatne powinny mieć świadomość jak ważną rolę odgrywają w procesie zapewniania bezpieczeństwa zarówno państwa, jak i jego poszczególnych obywateli. Ciąży na nich bowiem olbrzymia odpowiedzialność, na którą muszą być przygotowani. Uświadomienie tych okoliczności jest warunkiem rzetelnie podjętych działań, koniecznych do zapewniania bezpieczeństwa IK.

Współpraca prywatno-publiczna jest częstym „zwrotem wytrychem", używanym w większości debat o ochronie IK. Nie zawsze jednak sprecyzowane zostaje to, co kryje się w jego ramach[1]. W niniejszym tekście współpraca prywatno-publiczna oznacza przede wszystkim realizowanie inicjatyw nakierowanych na szeroko rozumianą wymianę informacji (między samymi

1 Często na przykład w kontekście współpracy publiczno-prywatnej można znaleźć odwołanie do partnerstw prywatno-publicznych. Jeśli PPP zgodnie z ustawą (Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym), rozumiemy, jaką wspólną realizacja przedsięwzięcia (bardzo formalnie określoną), to zgodnie z duchem przyjętych rekomendacji, nie będzie to najbardziej efektywna forma współpracy. Jednym z powodów jest to, że PPP są zorientowane na projekt, tymczasem bezpieczeństwo musi być traktowane w kategoriach procesu.

podmiotami prywatnymi oraz między podmiotami prywatnymi a publicznymi przy wsparciu władzy) oraz wdrażanie przez podmioty prywatne, rekomendowanych przez państwo rozwiązań, wpływających na większy poziom bezpieczeństwa (wyrażonych na przykład w formie standardów). Wymiana informacji winna być rozumiana jako proces gromadzenia, analizy i wymiany informacji, najczęściej dotyczących zagrożeń, wrażliwości infrastruktury, dobrych praktyk, rekomendacji itp.

Pomimo zogniskowania rozważań na procesie wymiany informacji, rekomendacje przedstawione w niniejszym rozdziale mogą być pomocne także w kontekście innych form kooperacji np. wspólnych ćwiczeń, w ramach których testowane są procedury, sprawdzany jest poziom zabezpieczeń i inne ważne dla bezpieczeństwa elementy.

Czynniki efektywnej współpracy oraz potencjalne wyzwania

Jednym z największych wyzwań stojących przed efektywną współpracą prywatno-publiczną jest różnica w perspektywie rozumienia celów i priorytetów przez obie strony. Podmioty publiczne w centrum swoich działań stawiają zapewnienie jak najwyższego stopnia bezpieczeństwa państwa i jego obywateli. Współcześnie przyjmuje się, że jest to warunkiem dobrobytu i rozwoju. Podmioty prywatne, z kolei, przede wszystkim zorientowane są na ciągłe polepszanie wyników finansowych. Tymczasem zapewnianie bezpieczeństwa wymaga nakładów materialnych m.in. w postaci inwestycji, opłacenia pracy, wdrożenia zabezpieczeń, kontroli, monitoringu itd. Kosztowne inwestycje w bezpieczeństwo są zatem dodatkowym obciążeniem, które podmioty prywatne muszą ponieść. Niekoniecznie wydatki tego typu zgodne są ze strategią finansową. Istnieje zatem zagrożenie, że podmioty te będą minimalizować wydatki na bezpieczeństwo, albo świadomie wliczając potencjalne straty w ryzyko, albo licząc, że problematyczna sytuacja nie zaistnieje.

Kluczem do rozwiązania tego problemu i jednocześnie podstawowym zadaniem państwa, jest zatem uświadamianie podmiotom prywatnym, właścicielom i użytkownikom IK, że ciąży na nich dużo większa odpowiedzialność, niż wyłącznie ta związana z wynikiem finansowym. Odwoływanie się do argumentów etycznych czy emocjonalnych ma małe szanse osiągnięcia rezultatów i jest obarczone dużym ryzykiem, dlatego warto skupić się na naświetlaniu ekonomicznych konsekwencji, będących efektem zaniedbań w obszarze bezpieczeństwa.

Dobrą praktyką jest przekonanie o konieczności inwestycji w bezpieczeństwo przedstawicieli firmy z najwyższego stopnia hierarchii (najlepiej na poziomie zarządu). Istotne jest wskazanie im potencjalnego ryzyka, które może być zminimalizowane za pomocą akceptowalnych zasobów i jest w stanie znacząco wpłynąć na bezpieczeństwo.

Ilustracją może być tutaj często niewłaściwy poziom zabezpieczeń związanych z cyberbezpieczeństwem. Uświadomienie przedstawicielom zarządu, często niemającym świadomości zagrożeń, jak powszechnym i kosztownym problemem są cyberzagrożenia ma szansę przynieść skutek[2]. Przydatne jest pokazanie częstotliwości wystąpienia problemów oraz tego, jak wielkie szkody finansowe, wizerunkowe oraz utrata zaufania, są ich następstwem. Zderzenie z obrazem potencjalnych konsekwencji, wraz ze wskazaniem, że inwestycja w bezpieczeństwo może uchronić firmę przed wieloma stratami i zabezpieczyć wynik finansowy, jest skutecznym instrumentem. W tym kontekście szczególny nacisk powinien położony zostać na zaprezentowanie zalet prewencyjnego podejścia do bezpieczeństwa zamiast przyjęcia reaktywnej postawy.

Inną taktyką jest skierowanie podobnych działań do akcjonariuszy firmy. Założenie powinno być takie, że wiedza, którą otrzymają, sprawi, że niejako „wymuszą" oni na zarządzie podjęcie działań, alternatywnie wyrażą konieczność inwestycji w bezpieczeństwo.

Poza istnieniem odmiennej perspektywy związanej z celami, skuteczność współpracy między podmiotami prywatnymi i publicznymi warunkowana jest rozwiązaniem innych potencjalnych trudności. Należą do nich między innymi: zbudowanie wzajemnego zaufania między współpracującymi stronami oraz przekonanie ich o celowości i istnieniu wartości dodanej wynikającej z podejmowanej współpracy. Ilustracją mogą być tutaj procesy, których przedmiotem jest wymiana informacji. W kontekście zaufania[3], zaangażowane podmioty muszą mieć pewność, że samo przekazywanie informacji jest „bezpieczne". Podmioty muszą mieć gwarancję, że nie dostanie się ona w niepowołane ręce, nie zostanie bez ich zgody ujawniona, nie zaszkodzi ich wizerunkowi i nie wpłynie na zmniejszenie zaufania klientów. Analogicznie, nie mogą się obawiać, że spotka je kara w wyniku ujawnienia jakichkolwiek danych. Zapewnienie bezpieczeństwa musi zostać dopełnione na poziomie umów, wzajemnych zobowiązań, ale także w formie technicznych zabezpieczeń kanałów wymiany informacji. Poza zaufaniem, zaangażowane podmioty muszą mieć pewność, że uczestniczenie w inicjatywach związanych z wymianą informacji ma sens i przyniesie określony skutek[4]. W przeciwnym razie zaangażowanie ocenione zostanie jako bezproduktywna strata czasu. Komunikacja musi mieć charakter dwukierunkowy, a informacje zwrotne, otrzymywane przez podmioty prywatne, muszą przekładać się na korzyści związane z realnym zwiększaniem bezpieczeństwa. Tylko poczucie celowości działań sprawi, że podmioty rzetelnie zaangażują się w działania.

W końcu, w ramach dyskusji nad skuteczną formą kooperacji prywatno-publicznej, najwięcej emocji wywołuje spór między zwolennikami i przeciwnikami stosowania dobrowolnej oraz obligatoryjnej współpracy. Pierwsza strategia bazuje na chęci uczestnictwa w danych inicjatywach i przekonaniu o jej wartości. W ramach drugiego wariantu uważa się, że za pomocą groźby szeroko rozumianych sankcji można sprawić, że przedstawiciele podmiotów prywatnych będą angażowali się w dane procesy lub będą na przykład wdrażali rozwiązania związane z bezpieczeństwem (m.in. określone standardy)[5].

Przeciwnicy obligatoryjnego podejścia wskazują, że „wymuszone" formy współpracy niszczą zaufanie, a podmioty wykonują zadania tylko po to by uniknąć kary. Działania prowadzone

2 Istnieją dobre praktyki związane z metodyką prowadzenia wyżej opisanego procesu uświadamiania, pochodzą one między innymi z doświadczeń holenderskich. Przede wszystkim, proces uświadamiania jest niezwykle skuteczny, gdy odbywa się w ramach bezpośrednich rozmów między firmą, a przedstawicielami podmiotów publicznych, lub z nimi związanych. W ramach takiego spotkania można zachęcić do wykonania krótkiego testu wiedzy, który pokazuje z jednej strony czy zarząd ma świadomość i wiedzę w zakresie stosowania w firmie mechanizmów zabezpieczeń oraz z drugiej, daje szansę zweryfikowania tego czy są one wdrażane. Zadanie prostych pytań opracowanych według wystandaryzowanego kwestionariusza może przynieść dobre efekty.

3 Dobre praktyki w tym zakresie są ściśle związane z metodyką prowadzenia i zarządzania forum i zostaną przedstawione w rozdziale 4.

4 O tym więcej także w rozdziale 4.

5 Kwestią sporną jest nawet czy taką formę można w ogóle nazwać współpracą.

są z minimalnym zaangażowaniem, tylko w celu wykonania zadania i często nie przynoszą założonych skutków. Przykładem niebezpieczeństwa jest tutaj rutynowe stosowanie podejścia określanego przez angielskie słowo *compliance*. Poszczególne podmioty otrzymują zestaw standardów, wymagań, które muszą spełnić. Nie skupiają się na faktycznych zagrożeniach czy niebezpieczeństwach (ang. *risk based approach*), a jedynie, często bezrefleksyjnie „odhaczają" działania jakie muszą wykonać by uzyskać zgodność ze standardem. Zgodność z wytycznymi jest w tej sytuacji błędnie traktowane jako cel sam w sobie.

Jako argument przeciwko obowiązkowemu działaniu, wskazywane są także udane formy dobrowolnej współpracy. Przykładem może być działalność funkcjonujących m.in. w USA i Wielkiej Brytanii tak zwanych Self Storage Associations[6]. Celem tych organizacji jest przede wszystkim tworzenie wspólnych, dobrowolnych standardów. Wartością nadrzędną jest fakt, że są one wypracowywanie wspólnie w oparciu o praktyczną wiedzę i doświadczenia poszczególnych podmiotów. Mając przekonanie co do ich wartości, podmioty same zaczynają je stosować i wdrażać.

Z kolei zwolennicy współpracy obowiązkowej odwołują się do argumentu o niewystarczającej sile rozwiązań rynkowych, które nie skłaniają podmiotów do zapewniania bezpieczeństwa, a nawet co więcej, często promują podejmowanie ryzyka. Wiele rzeczywistych przypadków zaniedbań w zapewnianiu bezpieczeństwa wzmacniają argument, że bardziej „inwazyjna" forma wpływu państwa często znajduje uzasadnienie. Należy przy tym mieć na uwadze, że ryzyko wynikające z podejścia opartego włącznie na zaufaniu jest ogromne w kontekście wagi i roli, jakie z perspektywy bezpieczeństwa państwa spełnia IK.

W dodatku, jak wskazują eksperci tacy jak James Andrew Lewis z CSIS, wprowadzenie zaledwie kilku bardzo prostych rozwiązań niekiedy drastycznie wzmacnia bezpieczeństwo. W takim kontekście warto zastanowić się nad wprowadzeniem regulacji, które wymuszą ich wdrożenie[7].

Podsumowując rozważania o obligatoryjnym i dobrowolnym podejściu, wydaje się, że nie jest możliwe dokonanie jednoznacznej oceny, które z nich jest słuszne. Jest to jeden z najtrudniejszych aspektów efektywnej współpracy publiczno-prywatnej, także dlatego, że odwołuje się do kwestii światopoglądowych. W ramach niniejszej publikacji rekomenduje się zastosowanie oceny sytuacji i wyboru strategii za pomocą metody *case by case*. Rozwiązania „szyte na miarę", a niepolegające na stosowaniu zawsze jednolitych rozwiązań mogą przynieść pożądany skutek. Z kolei „mieszane" podejście daje możliwość wyboru i zastosowania obowiązkowych mechanizmów w najbardziej kluczowych sektorach[8], gdzie ryzyko jest największe.

Niezależnie od wybranej opcji warto zadbać o spełnienie podstawowych zasad, takich jak wskazanie celowości działań i pokazanie przekładania się czynów na rezultaty[9]. Przede wszystkim jednak, wszelkie formy współpracy winny zostać połączone z wprowadzaniem przez państwo mechanizmów stymulujących zainteresowanie współpracą, jak i wpływających na efektywność i zaangażowanie uczestników.

Bodźce wpływające na efektywność współpracy publiczno-prywatnej

Istnieje szeroki wachlarz instrumentów, które państwo może zastosować w celu zachęcenia podmiotów prywatnych do współpracy i rzetelnego wykonywania zadań związanych z bezpieczeństwem (np. wprowadzania konkretnych standardów). Poniżej przedstawiony jest katalog wybranych narzędzi:

Ulgi podatkowe – przeznaczone dla podmiotów, które biorą udział w inicjatywach, związanych między innymi z wymianą informacji, bądź stosują rozwiązania związane z bezpieczeństwem zgodne z określonymi standardami[10].

Granty – wprowadzenie systemu grantów przeznaczonych na badania i innowacyjne działania związane z bezpieczeństwem. Przykładem może być grant amerykańskiej organizacji Enviornmental Protection Agency w wysokości 51 milionów dolarów przeznaczony dla właścicieli wodociągów na pomoc w przygotowaniu oceny podatności i planów ochrony[11]. System grantowy może także działać na dwa sposoby. Po pierwsze, jako sama w sobie możliwość uzyskania środków finansowych na działania bezpośrednio związane z bezpieczeństwem. Po drugie, w sposób pośredni, mogą one wpływać na większy poziom ochrony. Określone działania związane z bezpieczeństwem, na przykład wdrażanie standardów, mogą bowiem być warunkiem dopuszczającym do wzięcia udziału w interesujących dla firm konkursach grantowych. Z jednej strony zatem firmy wdrożą pewne rozwiązania, wezmą udział w inicjatywach (warunkiem może być np. aktywne uczestnictwo w forach wymiany informacji), by móc ubiegać się o dofinansowanie, a dodatkowo mają szansę pozyskać środki na realne działania. Powyższe mechanizmy, alternatywnie wobec grantów, mogą przybrać formę warunku dopuszczenia do wzięcia udziału w przetargach, lub na przykład w dofinansowanych przez państwo programach szkoleniowych, wzmacniających konkretne umiejętności itd.

Stworzenie rynku ubezpieczeń[12] związanego ze stosowaniem działań nakierowanych na bezpieczeństwo. Sprowadzałby się on do tego, że firmy, które wykonywałyby działania zwiększające bezpieczeństwo (np. wypełniając standardy, wprowadzając określone procedury, biorące udział w pracach związanych z wymianą informacji), uzyskiwałyby znaczne ulgi na ubezpieczenia.

6 Zob. http://www.azselfstorage.org/, http://www.ssauk.com/.

7 Choć autor odwołuje się *stricte* do rozwiązań związanych z zapewnianiem systemami teleinformatycznymi, warto rozważyć jego argumentacje zarówno w tym konkretnym odniesieniu jak i w kontekście ogólnych rozwiązań w całym systemie IK. Zob. J. A. Lewis, *Raising the Bar for Cybersecurity*, 12 luty 2013. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf, [dostęp: 13.04.2013].

8 S. Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*, http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf, [dostęp: 13.04.2013].

9 Co w dobrowolnym podejściu, wobec braku efektu groźby sankcji, jest absolutną koniecznością.

10 Tu podkreślić należy konieczność, aby standardy spełniały kryterium aktualności i elastycznie dostosowały się do panujących warunków. Sztywność i dezaktualizacja standardów, w połączeniu z minimalnym wypełnianiem narzuconych rozwiązań może przynieść katastrofalne skutki (m.in. fałszywego poczucia bezpieczeństwa).

11 S. Eckert, op.cit.

12 Ten element potencjalnego „systemu zachęt" wymaga najbardziej pogłębionej analizy potencjalnych skutków. Samo stworzenie rynku ubezpieczeń może być bardzo trudne. Szczególnie na początku zatem warto rozważyć system publicznego wsparcia dla tych działań na przykład w postaci reasekuracji.

Certyfikowanie firm lub oznaczenie ich w sposób rozpoznawalny dla klientów, tak by było wiadomo, że są to podmioty, które postępują zgodnie ze standardami, procedurami i działają na rzecz wzmocnienia bezpieczeństwa. Można także zastosować gradację oznaczeń. Firma może w różnym stopniu stosować działania zabezpieczające, im bardziej zaawansowane działania, tym wyższy stopień byłby przyznawany.

Kredyty – mechanizm może działać w taki sposób, że firmy, które bądź biorą udział w forach wymiany informacji, bądź stosują określone środki bezpieczeństwa, mają dostęp do atrakcyjnych propozycji kredytowania lub pomocy finansowej w odtwarzaniu uszkodzeń, zniszczeń czy strat, jeśli dojdzie do jakiegoś zdarzenia.

Powyższe propozycje odnosiły się w dużej mierze do finansowych form zachęcania podmiotów prywatnych do angażowania się w działania nakierowane na bezpieczeństwo. Istnieje także wiele innych czynników pozafinansowych, które mogą mieć duże znaczenie.

Pytanie więc brzmi – co, poza powyższymi mechanizmami finansowymi może sprawić, że podmioty będą aktywnie i rzetelnie angażowały się w działania na rzecz bezpieczeństwa? Przykłady przedstawione zostaną w odniesieniu do partycypacji w inicjatywach związanych z wymianą informacji.

Jak zostało wskazane wcześniej, najważniejszym czynnikiem zachęcającym dane podmioty do współpracy jest przekonanie o wartości dodanej i celowości działań. Aktywne zaangażowanie w platformy wymiany informacji powinno nieść za sobą obietnicę uzyskiwania danych, które przełożą się na lepsze i bezpieczniejsze funkcjonowanie ich firm. Informacje muszą być więc przydatne, aktualne i na czas. Dodatkowo, uczestnictwo w wybranych mechanizmach wymiany może być premiowane dostępem do informacji przekazywanych ze strony rządu, przede wszystkim tych, których nie można byłoby uzyskać nigdzie indziej. Zachętą może stanowić też doradztwo, dzielenie się wiedzą, (techniczną, prawną etc.) między ekspertami związanymi z podmiotami publicznymi oraz podmiotami prywatnymi. Analogicznie, ofertą ze strony władz może być zapewnienie podmiotom zaangażowanym specjalistycznej pomocy w sytuacji problematycznej. Wartościowe może okazać się także przekonanie uczestników, że udział w inicjatywach to możliwość prowadzenia dialogu, dającego szansę dyskusji na temat przyszłych decyzji podejmowanych przez podmioty publiczne. Podmioty prywatne, poprzez branie udziału w takiej dyskusji, miałyby możliwość lobbowania pożądanych kierunków zmian oraz wskazywania możliwych negatywnych skutków potencjalnych decyzji. Finalnie, podmioty biorące udział w forach wymiany informacji, ale także w innych inicjatywach (na przykład ćwiczenia), mogą uzyskać możliwość partycypacji w treningach i szkoleniach – organizowanych lub finansowanych przez państwo. Mogą być one bardzo atrakcyjną formą zachęty, bowiem wzmacniają kompetencje, umiejętności i zwiększają poziom wiedzy.

W ramach podsumowania informacji związanych z efektywnym, dającym obopólne korzyści, angażowaniem się we współpracę podmiotów prywatnych i publicznych warto odwołać się do modelowej inicjatywy holenderskiej znanej jako ICT RB (ang. ICT Response Board)[13]. Jest to ciało składające się z przedstawicieli sektora prywatnego i publicznego, które powoływane jest ad hoc w sytuacji kryzysu związanego z cyberzagrożeniami[14]. Głównym celem ICT RB jest dostarczanie wsparcia dla odpowiednich podmiotów – elementów systemu zarządzania kryzysowego, ale także dla podmiotów prywatnych. Konkretnymi działaniami jakie podejmuje ICT RB jest sygnalizowanie potencjalnych zagrożeń, ich identyfikacja i interpretacja, koordynacja działań, gdy sytuacja kryzysowa zaistnieje, doradztwo dla podmiotów dotkniętych incydentem lub zagrożonych, gromadzenie informacji i dzielenie się nimi wśród interesariuszy. Dodatkowo podmioty zaangażowane w inicjatywę organizują wspólne ćwiczenia na bazie przygotowanych scenariuszy, podczas których mają możliwość testowania procedur, konkretnych rozwiązań i działań.

13 ICT Response Board, https://www.ncsc.nl/english/services/crisis-management-reinforcement/ict-response-board.html, [dostęp: 13.04.2013].

Przyszłość współpracy prywatno-publicznej w Polsce

NPOIK przygotowany przez RCB preferuje bezsankcyjne podejście do ochrony kluczowych składników infrastruktury państwa[15]. Wyżej przedstawione propozycje mają szansę przyczynić się do wzmocnienia efektywności dobrowolnych form współpracy, jak również zwiększyć szansę rzetelnego realizowania wielu inicjatyw.

Jednocześnie warto zwrócić uwagę, że w najbliższym czasie rozwiązania międzynarodowe, które Polska najprawdopodobniej będzie musiała implementować, wymuszą regulację pewnych obszarów współpracy. Chodzi tutaj o dyrektywę w sprawie bezpieczeństwa sieci i informacji[16], która w czasie gdy powstawał ten rozdział, została przegłosowana przez Parlament Europejski i w następnym kroku jej ostateczny tekst negocjowany będzie z Radą UE. Jeśli zostanie ona przyjęta w obecnym kształcie, nałoży obowiązkowe elementy współpracy między podmiotami prywatnymi i publicznymi. Przede wszystkim dyrektywa narzuci dokonanie przez właścicieli IK[17]wdrożenia właściwych środków zwiększających bezpieczeństwo i raportowanie incydentów zagrażających bezpieczeństwu informacji i sieci[18]. Oczywiście, należy mieć świadomość, ze dyrektywa odnosi się do wycinka zadań związanych z bezpieczeństwem IK – konkretnie z bezpieczeństwem teleinformatycznym. Jest to jednak ingerencja w sposób budowania współpracy między podmiotami prywatnymi i publicznymi, która w przyszłości może dotykać innych obszarów.

Jeśli dyrektywa wejdzie w życie, Polska będzie musiała zastosować elementy sankcyjnego podejścia. Wiąże się to z obawą, że podmioty prywatne będą realizowały zadania narzucone z góry wyłącznie po to, aby uniknąć kary i na minimalnym poziomie zaangażowania. W celu złagodzenia wszystkich możliwych, negatywnych form sankcyjnej współpracy (tej narzuconej przez dyrektywę, jak również możliwych innych przyszłych), warto rozważyć połączenie ich z zastosowaniem wyżej przedstawionego katalogu działań wspierających prywatny sektor. Dyrektywa może być implementowana do porządku prawnego państw w elastyczny sposób, warto zatem zabezpieczyć efektywność jej wdrażania poprzez stymulację skutecznej współpracy prywatno-publicznej.

14 Lub w sytuacji zagrożenia kryzysem.
15 RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej*, s. 6., s.7.
16 *Directive of The European Parliament and of The Council concerning measures to ensure a high common level of network and information security across the Union*, COM(2013) 48 final.
17 Zob. COM(2013) 48 final, Annex II.
18 COM(2013) 48 final, art. 14 pkt. 1; art 14. pkt. 2.

Podsumowanie

Efektywna współpraca publiczno-prywatna musi opierać się na zrozumieniu różnicy w perspektywie definiowania celów i priorytetów związanych z bezpieczeństwem jakie często cechuje dwie strony. Warunkiem bazowym jest także zagwarantowanie korzyści dla obu sektorów we wszystkich wspólnych inicjatywach. Jest to szczególnie istotny postulat zwłaszcza w kontekście dobrowolnych inicjatyw. Podejście obowiązkowe powinno być decyzją przemyślaną, opartą o analizę *case-by-case*, ze szczególnym uwzględnieniem sektorów najbardziej narażonych. W końcu, podmioty prywatne powinny być zachęcane do współpracy poprzez katalog bodźców – finansowych i niefinansowych, które zwiększą prawdopodobieństwo efektywnego zaangażowania.

4. Metodyka zarządzania forami współpracy w zakresie ochrony infrastruktury krytycznej

Dominika Dziwisz – Instytut Kościuszki

Większość istniejących form współpracy między partnerami publicznymi i prywatnymi ukierunkowanych jest na ułatwianie wymiany informacji na temat ryzyka, słabości, zagrożeń, podatności na atak, a także najlepszych praktyk i rekomendacji w zabezpieczeniu infrastruktury krytycznej (IK). Aby była ona skuteczna, powinna być organizowana na trzech poziomach: krajowym, systemowym i regionalnym[1]. Na każdym z tych poziomów wymiana informacji musi być prowadzona na bieżąco, najlepiej przez bezpośrednie kontakty stron, tak aby umacniać i utrzymywać stałe relacje między partnerami.

Podstawową formą wymiany informacji prowadzącą do zwiększenia bezpieczeństwa IK, są wspólne spotkania uczestników współpracy publiczno-prywatnej[2] w ramach forów ochrony IK. Dlatego w 2013 r. Rządowe Centrum Bezpieczeństwa (RCB) zarekomendowało utworzenie sieci forów, których celem będzie identyfikacja kluczowych problemów z zakresu ochrony IK oraz opracowanie propozycji rozwiązań[3].

Jak zidentyfikowane zostało w raporcie ENISA, badającym efektywność funkcjonowania forów, jedną z największych barier, a jednocześnie wyzwaniem w ich budowaniu jest, obok niskiej jakości informacji i źle dobranych zachęt do współpracy[4], niewłaściwe zarządzanie forami[5].

Artykuł stanowi uzupełnienie rekomendacji RCB o propozycje konkretnych rozwiązań w zakresie zarządzania forami IK, a także wskazuje najważniejsze problemy z tym związane. Analiza została oparta na przykładach skutecznych rozwiązań zastosowanych w Stanach

1 RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej*, http://rcb.gov.pl/?page_id=261 [dostęp: 10.04.2014].

2 Istnieje wiele mechanizmów zarządzania ochroną IK. Od takich, gdzie rząd określa zasady jakich należy przestrzegać, czyli pełni rolę jedynej władzy, która ustala standardy bezpieczeństwa oraz egzekwuje ich właściwe spełnianie, aż po takie, gdzie rząd pozostawia bezpieczeństwo infrastruktury krytycznej mechanizmom rynkowym. Pomiędzy tymi rozwiązaniami istnieje wiele innych pośrednich form współpracy. Różnią się one stopniem ingerencji państwa w działanie tej części IK, która jest własnością prywatną. Z tego powodu autorka zrezygnowała z używania zwrotu „partnerstwo publiczno-prywatne", które jest tylko jedną formą współpracy, na rzecz pojęcia szerszego „współpracy publiczno-prywatnej". W podjętym temacie, przez współpracę publiczno-prywatną w zakresie bezpieczeństwa IK należy rozumieć inicjatywy nakierowane na gromadzenie, przetwarzanie i wymianę istotnych dla bezpieczeństwa IK informacji między sektorem rządowym a prywatnym, a także między samymi podmiotami prywatnymi.

3 *Narodowy Program*…, op. cit.

4 Niewspółmiernych z ponoszonym ryzykiem.

5 ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, 2010.

Zjednoczonych Ameryki, a przede wszystkim na obserwacjach i propozycjach Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA – ang. European Network and Information Security Agency) – centrum wymiany doświadczeń i informacji w zakresie bezpieczeństwa cybernetycznego między państwami i instytucjami Unii Europejskiej. W raportach z 2010 i 2011 r.[6] ENISA porównała różne modele zarządzania współpracą publiczno-prywatną stricte w zakresie ochrony teleinformatycznej infrastruktury krytycznej (CIIP – ang. Critical Information Infrastructure Protection). Jednak obserwacje i rekomendacje ENISA znajdują zastosowanie w ustalaniu ogólnych reguł i struktury współpracy wykorzystywanych w ramach inicjatyw związanych z wymianą informacji.

Na zakończenie, autorka chciała zwrócić uwagę, że poniższe obserwacje i rekomendacje odnoszą się przede wszystkim do zarządzania forami sektorowymi.

Organizacja forum

Z założenia, aby zapobiec sytuacji uprzywilejowania jednej ze stron, współpraca publiczno-prywatna powinna opierać się na zasadzie równości wszystkich partnerów publicznych i prywatnych. Z uwagi na to, organizując forum wymiany informacji, wszystkie zaangażowane podmioty powinny mieć podobne uprawnienia, obowiązki, możliwości działania i odpowiedzialność za bezpieczeństwo „klienta" (państwowego i prywatnego). Jednocześnie, nawet jeśli założymy równość współpracujących stron, to tak jak w każdej organizacji, niezbędne jest wybranie jednostki odpowiedzialnej za zarządzanie i koordynację działań.

Pierwsza i najczęściej występująca w praktyce forma zarządzania to kierowanie przez jednego z uczestników partnerstwa z sektora prywatnego lub rządowego, czyli od wewnątrz. Sprawdza się ona najlepiej, kiedy forum służy wymianie informacji między partnerami tego samego sektora IK. Są oni bowiem w pełni zaznajomieni ze specyfiką własnej działalności i świadomi możliwych problemów z nią związanych.

Druga, mniej popularna forma to kierowanie przez specjalnie do tego utworzony organ. Takie rozwiązanie sprawdza się w zarządzaniu współpracą pomiędzy poszczególnymi forami sektorowymi. Może ono zapobiec sytuacji, w której partycypujący, którzy posiadają szczegółowe informacje w ramach własnego sektora, nie są w stanie przeciwdziałać potencjalnym zagrożeniom z powodu braku całościowej perspektywy. Tym samym, organ koordynujący, świadomy kompleksowości problemu potrafi w sposób najbardziej optymalny ukierunkować działania wszystkich uczestników.

W przypadku amerykańskich Centrów Wspólnej Wymiany i Analizowania Informacji (z ang. Information Sharing and Analysis Center – ISAC) taką funkcję pełni powołana w 2003 r. Narodowa Rada ISAC (National Council of ISACs). Rada jest złożona z reprezentantów sektorowych ISAC i spotyka się raz w miesiącu w celu rozwijania współpracy między nimi, umacniania wzajemnego zaufania, a także odniesienia się do bieżących problemów i opracowania strategii reagowania na zaistniałe zagrożenia. Dodatkowo, Rada organizuje szkolenia i jest łącznikiem między sektorem prywatnym a Narodowym Centrum Koordynacji Infrastruktury (National Infrastructure Coordinating Center, NICC) w ramach Departamentu Bezpieczeństwa Krajowego (U.S. Department of Homeland Security) w sytuacji kryzysów o znaczeniu państwowym. Rada sponsoruje także doroczny Kongres Bezpieczeństwa Infrastruktury Krytycznej (Critical Infrastructure Protection (CIP) Congress).

Trzecia forma zarządzania forami to demokratyczne zarządzanie przez wszystkich jego uczestników. W praktyce, ta forma jest najmniej efektywna, a przy tym najbardziej konfliktogenna, dlatego też rzadko stosowana. Podejmowane są natomiast próby „demokratyzacji" zarządzania np. przez rotacyjne wybieranie przewodniczącego, aby nie dopuścić do sytuacji, kiedy jeden z uczestników posiada dominującą pozycję i faktycznie zarządza siecią.

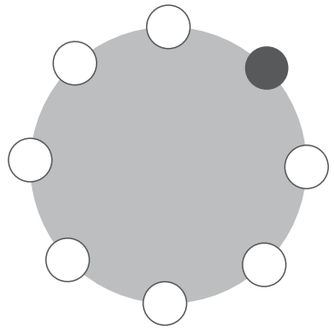
Poziomy organizacji forum

Jak zaznaczono we wstępie, aby wymiana informacji w zakresie bezpieczeństwa IK była skuteczna, powinna być organizowana na kilku poziomach: krajowym, systemowym i regionalnym. Ponownie przykładem dobrej organizacji i zarządzania siecią partnerów publicznych i prywatnych są amerykańskie ISAC. Centra zajmują się gromadzeniem danych z dziedziny bezpieczeństwa informacyjnego i ich udostępnianiem instytucjom współtworzącym dane centrum. Zgodnie z początkowym projektem miał powstać tylko jeden ISAC wspólny dla wszystkich sektorów gospodarki. W praktyce takie rozwiązanie okazało się nieskuteczne. Dlatego dla każdego z sektorów wymienionych w Dyrektywie Prezydenckiej 63 (PDD 63) utworzono oddzielne centrum[7].

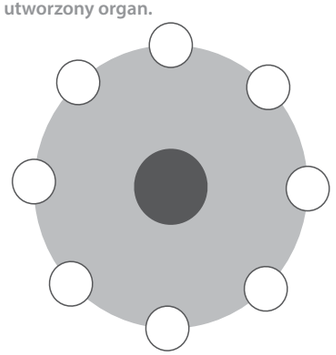
Decyzja o tym, aby każdy sektor IK miał swój własny, odrębny ISAC była kluczową dla skuteczności działania sieci ISAC. Ze względu na specyfikę różnych sektorów IK utworzenie jednego „kolektywnego" ISAC dla wszystkich sektorów miało małe szanse na powodzenie. Utworzenie ogólnych standardów współpracy byłoby nieefektywne choćby z uwagi na to, że każdy sektor ma swoją specyfikę funkcjonowania. Dlatego lepszym rozwiązaniem było utworzenie odrębnych ISAC, gdzie każdy odpowiada za bezpieczeństwo danego sektora. Amerykańskie ISAC były jednymi z pierwszych forów sektorowej wymiany informacji. Obecnie, w innych państwach, które wielokrotnie wzorowały się na ISAC

Rysunek 3, 4, 5. Typy zarządzania forum. Źródło: Opracowanie własne na podstawie ENISA, *Desktop Reserach on Public Private Partnerships*, 2011.

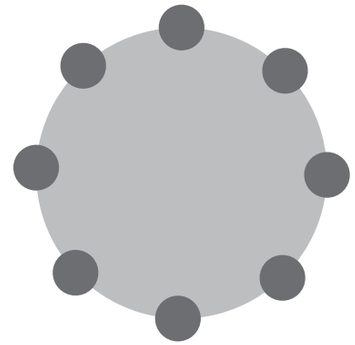
Forum zarządzane od wewnątrz.



Forum zarządzane przez specjalnie do tego utworzony organ.



Forum zarządzane demokratycznie.



6 ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, 2010, ENISA, *Cooperative Models for Effective Public Private Partnerships. Desktop Research Report*, ENISA, 2011.

7 *Presidential Decision Directive 63*, 22.05.1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, [dostęp: 10. 12. 2013].

przyjęto podobne rozwiązania[8]. Na gruncie polskim, Rządowe Centrum Bezpieczeństwa (RCB) zarekomendowało utworzenie oddzielnych forów systemowych dla każdego sektora IK, które będą się zbierać przynajmniej dwa razy do roku lub częściej, zależnie od okoliczności. RCB projektując fora wymiany informacji korzystało z międzynarodowych standardów opierających się na sektorowości. Jest to rozwiązanie, które z wyżej wymienionych powodów, ma szansę przynieść równie pozytywne efekty co rozwiązania amerykańskie.

Zarządzanie hierarchiczne vs. zarządzanie sieciowe

Problem budowy skutecznych form współpracy wiąże się ze zderzeniem dwóch kultur zarządzania. Sektor prywatny angażuje wielu udziałowców, jest otwarty, podatny na zmiany i zarządzany horyzontalnie. Natomiast sektor publiczny jest często mniej elastyczną strukturą, zarządzaną hierarchicznie[9] i dlatego wykazuje mniejszą reaktywność w obliczu zmian. Ma za to większe możliwości rozwiązywania złożonych problemów w dłuższych okresach czasu. Obecnie, w związku z relatywnie dużą siłą działania sektora prywatnego, ustalenie zasad współpracy z rządem jest przyczyną wielu nieporozumień[10]. *Sytuację komplikuje fakt, że każda z zainteresowanych grup chce pełnić wiodącą rolę*[11].

Niektórzy specjaliści wskazują, że rozwiązaniem może być zrezygnowanie z „tradycyjnych" form współpracy i zarządzania na rzecz zarządzania sieciowego (ang. *network governance*). Zgodnie z tą koncepcją odchodzi się od hierarchicznej organizacji ról, w której podmioty nadzorują resztę przymusowych uczestników pod rygorem sankcji karnych, na rzecz bardziej skomplikowanych systemów sieciowych. Cechują się one wieloma centrami decyzyjnymi, równym statusem uczestników i ich współodpowiedzialnością za podjęte inicjatywy, oraz dobrowolnym wypracowywaniem rozwiązań na rzecz obopólnych korzyści. W przypadku forów wymiany informacji oznaczałoby to zrezygnowanie z myślenia o monopolu rządu na zarządzanie nimi, czyli wydawanie instrukcji i monitorowanie zadań przez jeden podmiot, a co za tym idzie zastosowanie bardziej rozproszonego modelu podejmowania decyzji. Należy stworzyć warunki, w których „administracja publiczna staje się drużyną sportową, motywowaną przez perswazje, negocjacje i wzajemne zaufanie. Porozumienie i komplementarne współdziałanie na równych zasadach pozwoli osiągnąć cele zarówno sektorowi prywatnemu jak i publicznemu, co z reguły jest utrudnione, a czasem niemożliwe przy kontroli i regulacjach sprawowanych przez jeden podmiot"[12]. W praktyce oznacza to utworzenie niewielkich i stosunkowo homogenicznych sieci współpracy, w ramach których uczestnicy, we własnym interesie, będą wypełniać zadania publiczne[13]. Wszyscy uczestnicy, prywatni i publiczni, organizują się w tym zakresie *quasi* niezależnie. Ustalają zasady wspólnych działań, a także przypisują odpowiedzialność i zobowiązania poszczególnym uczestnikom. Te różne sieci same monitorują własne działania. Innymi słowy, zadania publiczne są wykonywane przez wiele niezależnych, samoregulujących się sieci. Swoją „reprezentację" ma sektor publiczny i prywatny, ale reprezentanci sektora publicznego rezygnują ze specjalnego, uprzywilejowanego statusu. Sieć będzie funkcjonować tylko wtedy, kiedy decyzje będą podejmowane w ramach negocjacji, a każda strona będzie równoprawnym uczestnikiem.

Finansowanie forum

Ważną kwestią związaną z organizacją forum wymiany informacji jest finansowanie jego działania. Forum może być finansowane z budżetu rządowego albo sami uczestnicy zobowiązują się do wniesienia opłaty członkowskiej. W pierwszym przypadku, kiedy rząd pokrywa koszty administracyjne, jest to zachętą i dodatkowym bodźcem do uczestnictwa dla sektora prywatnego. Przykład amerykańskich ISAC, których funkcjonowanie jest subsydiowane albo w niektórych przypadkach w całości finansowane z budżetu federalnego, jest dowodem na to, że brak opłat po stronie uczestników sektora prywatnego sprawdza się jako forma motywacji do działania. Natomiast nie jest to powszechnie przyjętą praktyką. W raporcie ENISA wykazano, że 24 proc. przeanalizowanych organizacji egzekwuje od uczestników opłaty za członkowstwo na pokrycie kosztów administracyjnych[14].

Fora i inne formy wymiany informacji są także finansowane na inne sposoby. Na przykład, uczestnicy mogą płacić za usługi posiadające realną wartość, takie jak dostęp do opracowań eksperckich albo w formie mieszanej, gdzie członkowie ponoszą koszty własnego czasu i wydatków, a rząd ponosi koszty koordynacji, lokalu, itp.

Formy komunikacji

Kolejnym zagadnieniem zarządzania forami jest wybór formy komunikacji między partnerami. Wymiana informacji może odbywać się tradycyjnie, czyli w trakcie regularnych lub nieregularnych spotkań „twarzą w twarz". Praktyka wskazuje, że taki sposób jest najbardziej skuteczny i efektywny. Można także korzystać z dobrodziejstw nowoczesnych technologii, w tym przede wszystkim Internetu, który umożliwia organizowanie wideokonferencji albo rozsyłanie informacji na prywatne listy dystrybucyjne. Uczestnicy mogą także zamieszczać istotne dla bezpieczeństwa IK informacje na specjalnie utworzonych w tym celu platformach internetowych. Taka platforma może być zbudowana z określonych grup (pokoi) systemowych oraz eksperckich[15]. Koordynacja i administrowanie forum może być prowadzone wirtualnie, ale najważniejsze decyzje w zakresie współpracy powinny być podejmowane w czasie bezpośrednich spotkań uczestników. Zgodnie z raportem ENISA, bezpośrednie kontakty uczestników forum pozwalają na efektywną wymianę informacji.

8 Między innymi, sektorowe fora wymiany informacji działają w Australii. Australijskie Trusted Information Sharing Network (TISM) są forami wymiany informacji między właścicielami i operatorami infrastruktury krytycznej. W ramach TISM działa siedem Grup Sektorowych (Sector Groups), dwie Doradcze Grupy Eksperckie (Expert Advisory Groups), a także Wspólnoty Interesów (Communities of Interest, CoL) i Rada Doradcza ds. Infrastruktury Krytycznej (Critical Infrastructure Advisory Council, CIAC). Grupy Sektorowe stanowią pomost między sektorem rządowym a sektorem prywatnym. Za: ENISA, Cooperative *Models for Effective Public Private Partnerships. Good Practice Guide*, 2011, s. 49.

9 J. Healey, *Preparing for Cyber 9/12*, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=966c9813-6e74-4e0b-b884-8ed9f3f0978c&lng=en&id=143486, [dostęp: 01. 04. 2014].

10 Ibidem.

11 Ibidem.

12 M. D. Cavelty, M. Suter, *Public-Private Partnerships are no silver bullet: An expanded governance for Critical Infrastructure Protection*, „International Journal of Critical Infrastructure Protection" 2009, doi:10.1016/j.ijcip.2009.08.006, s. 5.

13 Ibidem.

14 ENISA, *Cooperative Models for Effective Public Private Partnerships. Desktop Research Report*, 2011.

15 Narodowy Program…, op. cit.

Zaufanie między uczestnikami forum

Podstawową przeszkodą funkcjonowania forum może być brak zaufania między jego uczestnikami, a szczególnie między przedstawicielami sektora prywatnego i sektora publicznego. Przedsiębiorstwa prywatne obawiają się niewystarczającego poziomu poufności i bezpieczeństwa przekazywanych danych, co może mieć negatywny wpływ na wizerunek i konkurencyjność firm. Obawy występują także po stronie rządowej. „Kultura tajemnicy" i ugruntowany przez lata niepokój wobec dzielenia się informacjami z podmiotami pozarządowymi stwarzają ryzyko impasu w wymianie informacji.

W związku z tym, budowa obustronnego zaufania oraz zapewnienie możliwie najwyższego poziomu bezpieczeństwa przesyłanych informacji są priorytetem i największym wyzwaniem dla efektywnej współpracy. Budowa zaufania powinna być rozumiana jako stopniowy i długotrwały „proces", podczas którego kontakty między uczestnikami forum są stale umacniane. Do wzrostu poziomu zaufania można doprowadzić na wiele sposobów.

Po pierwsze, niezbędne jest określenie przez członków forów typu wymienianych informacji, które muszą być bieżące, rzeczowe i użyteczne z punktu widzenia całej grupy. W sytuacji, gdy uczestnicy forum sami określą zasady z tym związane minimalizowane jest ryzyko zaistnienia wątpliwości co do możliwości ujawniania innych niż określone informacji na forum. Jednocześnie należy zapewnić procedury usuwania z baz danych wszelkich informacji personalnych i adresowych dotyczących wrażliwych danych.

Po drugie, przeszkodą w budowie relacji i zaufania pomiędzy uczestnikami forum może być także jego rozmiar. Jeśli grupa będzie za duża trudniej będzie zbudować zaufanie między jej uczestnikami. Często bowiem wzrost liczby uczestników idzie w parze z większą różnorodnością, odmiennymi celami, priorytetami utrudniającymi osiągnięcie konsensusu. Jednocześnie nie łatwo jest znaleźć wspólne, tak samo ważne dla wszystkich uczestników, korzyści współpracy. Trudno jest jednak określić ilu uczestników powinno mieć wzorcowe forum. Zależy to m.in. od specyfiki danego sektora IK, a przede wszystkim od zgodnej decyzji partnerów.

Po trzecie, istnieje ryzyko, że niektóre wymieniane informacje mogą zostać wykorzystane w celach komercyjnych. Dlatego warto rozważyć, czy obok specjalistów z zakresu bezpieczeństwa i ekspertów technicznych w forach sektorowych powinny uczestniczyć osoby odpowiedzialne za sprzedaż i marketing. Jak wykazano w raporcie ENISA, ryzyko komercyjnego wykorzystania poufnych informacji jest przeszkodą w budowie wzajemnego zaufania. Dlatego niezbędne jest dokładne określenie preferencji odnośnie uczestników forów oraz ich zgoda na podjęcie współpracy w proponowanym składzie.

Po czwarte, trwałość i ciągłość działania forum są podstawą zaufania. Dlatego niezbędna jest implementacja zasad gwarantujących ciągłość członkostwa, takich jak: szczegółowe reguły uczestnictwa w forum podparte konkretnymi zachętami do współpracy, zasady rzetelnego wykonywania zadań, deklaracja praw i obowiązków oraz przepisy regulujące proces wykluczania podmiotu z członkowstwa. Nie można dopuścić do sytuacji, w której jedni członkowie będą biernie korzystali z wyników pracy innych, przy znikomym wkładzie własnym. Jednocześnie zapobiegać należy niezdrowemu współzawodnictwu. Każdy z uczestników forum powinien być świadomy wagi swojej działalności, dążyć do optymalizowania własnych starań i tym samym wypracowywania wartości dodanej dla całej grupy.

Po piąte, wybór sposobu kontaktowania się między uczestnikami forum ma bezpośredni wpływ na zaufanie w grupie. Wymiana informacji przez Internet, np. poprzez platformę internetową, wirtualne konferencje, czy pocztę elektroniczną są skutecznymi narzędziami, które budują poczucie stabilności i dają pewność szybkiej reakcji ze strony jednostek współpracujących. Jednak to osobiste spotkania uczestników forum mają tę niepodważalną zaletę, że redukują bariery niepewności i braku zaufania, związane z nieznajomością reszty członków. Osobiste spotkania budują także wiedzę na temat wspólnych celów oraz strategii działania, na bazie której członkowie mogą perspektywicznie przewidywać dalsze kierunki działań. Dlatego, jak już wcześniej zaznaczono, komunikacja „twarzą w twarz" powinna być podstawową formą kontaktów między uczestnikami forum.

Elastyczność wyboru formy współpracy

Na zakończenie warto wziąć pod uwagę, że ze względu na specyfikę i różnice między sektorami IK forma współpracy nie powinna być z góry narzucona. Po raz kolejny, bazując na amerykańskim projekcie kooperacji można zauważyć, że ISAC cechują się dużą różnorodnością budowy swych struktur dzięki niezależności od agencji rządowych. Każdy sektor ma specyficzne problemy, dlatego taka forma elastyczności w organizacji partnerstwa umożliwia projektowanie rozwiązań jak najlepiej odzwierciedlających charakterystykę każdego z sektorów i najlepiej odpowiadających jego potrzebom. To właśnie potrzeby danego sektora oraz jasno wytyczone cele partnerstwa, a nie konwencje przyjęte w innych rozwiązaniach w ramach współpracy publiczno-prywatnej, powinny wpływać na strukturę i reguły obowiązujące członków w ramach forum.

Podsumowanie

Budując forum współpracy w zakresie bezpieczeństwa IK należy od samego początku założyć równość współpracujących stron, a jednocześnie wybrać najlepszą możliwą formę zarządzania i koordynacji forum w zależności od tego, czy wymiana informacji jest prowadzona między uczestnikami tego samego czy różnych sektorów IK. Ważne, aby każdy sektor IK, ze względu na własne specyficzne problemy, miał oddzielne forum systemowe. Utworzenie jednego forum dla wszystkich sektorów IK w praktyce okaże się nieskuteczne. Jednak, dla uzyskania pełnego obrazu sytuacji i zrozumienia złożoności różnych problemów, powinien istnieć podmiot do zarządzania współpracą między poszczególnymi forami sektorowymi. Na gruncie polskim tę funkcję może pełnić RCB.

Organizując i zarządzając forum należy także zrezygnować z historycznie ugruntowanego nastawienia, że niektóre rozwiązania są możliwe tylko na poziomie rządowym. Innymi słowy, powinno się porzucić myślenie w kategorii hierarchicznego podporządkowania na rzecz elastyczności i zarządzania sieciowego, które w praktyce okazuje się dużo bardziej efektywne. Inne równie ważne czynniki, mające wpływ na sprawność działania forum wymiany poglądów to dobranie skutecznych narzędzi jego finansowania, rodzajów komunikacji, a także pozwolenie na elastyczność wyboru formy współpracy dla każdego sektora. Jednak najważniejszym warunkiem skuteczności forum jest wzajemne zaufanie jego uczestników oraz sama chęć wymiany informacji, oparta na wierze w znaczenie, skuteczność, powodzenie i bezpieczeństwo partnerstwa. Nawet jeśli założymy, że uczestnictwo jest obowiązkowe, to przy braku chęci i zaufania wszelkie inicjatywy zakończą się fiaskiem.

część II

5. Rola elementów teleinformatycznych w funkcjonowaniu infrastruktury krytycznej

Mirosław Ryba – EY

Fakt rozwoju technologii teleinformatycznych (digitalizacji) nie dziwi już dzisiaj nikogo. To raczej tempo tego rozwoju budzi podziw, a niekiedy nawet niedowierzanie. Dawniej zmiana technologiczna zachodziła na przestrzeni lat, dzisiaj modyfikacja w systemach teleinformatycznych realizuje się na przestrzeni pojedynczych miesięcy. Rozwiązania, które 10 lat temu wydawały się pomysłami z kategorii *science–fiction*, obecnie zaczynają wchodzić do użytku militarnego, a niejednokrotnie również komercyjnego. Przykładem mogą być testowane współcześnie na szeroką skalę autonomiczne samochody[1], które według zapowiedzi producentów mają wkrótce wejść do komercyjnego użytku, nie mówiąc już o wprowadzanych co kilka tygodni na rynek urządzeniach mobilnych, z których każde posiada moc obliczeniową większą niż ta, którą dysponowała NASA wysyłając po raz pierwszy człowieka na Księżyc (np. zaprojektowany w tym celu na MIT komputer AGC był wyposażony w 64 kilobajty pamięci i taktowany był z częstotliwością 43kHz).

Rozwiązania teleinformatyczne, tak powszechne w życiu codziennym, w sposób naturalny znalazły również swoje zastosowanie w rozwiązaniach systemów infrastruktury krytycznej (IK), i dzisiaj nikt już nie kwestionuje, że IK nie może sprawnie funkcjonować bez należytego wsparcia z ich strony.

Systemy teleinformatyczne wykorzystywane w IK

Systemy teleinformatyczne wykorzystywane w ramach IK można podzielić na dwie grupy rozwiązań – systemy informatyczne (IT – ang. *Information Technology*) oraz systemy sterowania przemysłowego (OT – ang. *Operational Technology*). Zastosowanie tych rozwiązań ściśle zależy od branży, a dokładniej obszaru funkcjonowania IK, w której są one wykorzystywane. Systemy IK zorientowane na usługi dla obywatela (finanse, komunikacja, ratownictwo etc.), czyli takie, gdzie teleinformatyka wspiera proces biznesowy lub wykorzystywana jest do gromadzenia i przetwarzania danych, szeroko wykorzystują rozwiązania IT. Natomiast we wszystkich obiektach IK związanych z procesami technologicznymi (wydobycie, wytwarzanie, przetwórstwo etc.) kluczową rolę odgrywają rozwiązania OT, mianowicie urządzenia i aplikacje służące do zarządzania urządzeniami produkcyjnymi oraz procesem technologicznym.

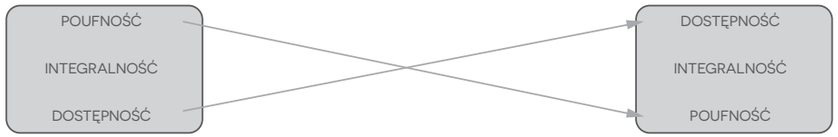
1 Autonomiczne samochody (ang. *autonomous* car lub *driverless car*) – zrobotyzowane, samosterujące samochody potrafiące nawigować i reagować na zmiany w otoczeniu (inne pojazdy, przeszkody, sygnalizacja świetlna, etc.) bez jakiejkolwiek potrzeby ingerencji człowieka.

Jako kluczowe różnice pomiędzy IT a OT można wskazać kwestie związane z wydajnością i dostępnością tych rozwiązań. O ile w przypadku rozwiązań IT przerwa w ciągłości działania systemu jest akceptowalna (choć niejednokrotnie kosztowna biznesowo), o tyle w OT mamy do czynienia z rozwiązaniami typu *real-time*, gdzie reakcja na zmiany zachodzące w środowisku produkcyjnym muszą być natychmiastowe, a wszelkiego rodzaju opóźnienia są nieakceptowalne[2]. Fakt ten spowodowany jest czynnikami ekonomicznymi (nieplanowane przerwanie ciągłości działania niektórych instalacji produkcyjnych skutkuje wielomilionowymi stratami finansowymi), ale przede wszystkim czynnikami związanymi z bezpieczeństwem ludzi. Zapewnienie kontroli nad środowiskiem produkcyjnym bezpośrednio wpływa na bezpieczeństwo ludzi (ich zdrowie, niekiedy nawet życie), a także na bezpieczeństwo środowiska naturalnego.

Kolejną kluczową różnicą pomiędzy rozwiązaniami IT a OT jest okres działania, na jaki rozwiązania te są projektowane. Dla rozwiązań IT średni czas eksploatacji systemów/komponentów to 3 do 5 lat, podczas gdy rozwiązania OT planowane są na minimum dekadę, gdzie średnia to ok. 15 lat. Zatem przy takim czasookresie funkcjonowania, należy liczyć się z faktem, że rozwiązania OT nie będą podlegały tak częstym zmianom jak rozwiązania IT, oraz że w środowisku OT spotykali będziemy technologie dawno już przestarzałe i dłużej nierozwijane. Skutkuje to również ograniczonymi zasobami (w rozumieniu wydajności procesorów, pamięci, dysków etc.), dostępnymi z poziomu komponentów sprzętowych, co niejednokrotnie uniemożliwia rozbudowę systemu OT (bądź zainstalowanie dodatkowych komponentów bezpieczeństwa) i w przypadku potrzeby aktualizacji bądź rozbudowy wymusza wymianę całego środowiska.

Różny obszar zastosowania IT i OT powoduje również różnice w postrzeganiu aspektów bezpieczeństwa pomiędzy IT a OT. Z perspektywy bezpieczeństwa rozwiązań IT kluczowe jest zapewnienie poufności danych (biznesowych), podczas gdy z perspektywy rozwiązań OT najistotniejszym jest zapewnienie dostępności procesu produkcyjnego. Zależność tą pokazuje poniższy rysunek.

Rysunek 6. Priorytety atrybutów bezpieczeństwa dla IT i OT. Źródło: Opracowanie własne.



W tym miejscu należy zwrócić uwagę, że o ile rozwiązania IT wchodziły do świata IK (np. do telekomunikacji) podążając za rewolucją technologiczną mającą miejsce u schyłku XX wieku, o tyle świat rozwiązań OT pozostawał hermetyczny przez długie lata. Dopiero początek XXI wieku, przyniósł gwałtowne zmiany w świecie OT, polegające na przenoszeniu rozwiązań IT do świata OT, dążeniu do standaryzacji OT, odchodzeniu od zamkniętych protokołów komunikacyjnych, wprowadzaniu do OT rozwiązań wirtualnych oraz mobilnych, czy wreszcie wdrażaniu narzędzi bezpieczeństwa teleinformatycznego. Jednak należy mieć na względzie, że wdrażanie

2 Nawet tak prozaiczna czynność z perspektywy IT jak restart [ang. *Reboot*] komponentów systemu, w przypadku rozwiązań OT bardzo często jest całkowicie nieakceptowana.

dowolnego rozwiązania, w tym teleinformatycznego w ramach IK, musi być efektem świadomej decyzji adresującej zarówno korzyści, jakie ta technologia przynosi, jak również jakie zagrożenia może spowodować w istniejącym środowisku.

Opierając się na podziale IK na systemy, zaprezentowanym w „Narodowym Programie Ochrony Infrastruktury Krytycznej"[3], należy podkreślić, że rola, charakter, jak również rodzaj rozwiązań teleinformatyki wykorzystywanych w poszczególnych systemach IK są diametralnie różne. Poniżej przedstawiona została ogólna charakterystyka rozwiązań teleinformatycznych wykorzystywanych w poszczególnych systemach IK oraz zasad ich działania.

Rozwiązania IT i OT wykorzystywane w poszczególnych systemach IK

Obszarem najbardziej uzależnionym od rozwiązań OT jest system zaopatrzenia w energię, surowce energetyczne i paliwa, w ramach którego wyróżnić należy wytwarzanie, przesył i dystrybucję energii elektrycznej i cieplnej oraz gazu ziemnego, przesył i przetwarzanie ropy naftowej, a także wydobycie węgla. Kluczową rolę w podmiotach z tych sektorów odgrywają systemy OT odpowiedzialne za monitorowanie i sterowanie procesami technologicznymi – takie jak SCADA (SCADA – ang. *Supervisory Control and Data Aquisition*), DMS (DMS – ang. *Distribution Management System*) czy EMS (EMS – ang. *Energy Management System*) w przypadku energetyki. Instalacje produkcyjne (np. bloki energetyczne w elektrowniach czy instalacje w rafineriach) sterowane są z kolei za pomocą rozwiązań DCS (DCS – ang. *Distributed Control System*) będących kompleksowymi zintegrowanymi systemami odpowiadającymi za sterowanie i wizualizację procesu przemysłowego.

Niekiedy, w celu zwiększenia wydajności procesu produkcyjnego stosowane są rozwiązania klasy APC (APC – ang. *Advanced Process Control*), w szczególności związane z ograniczaniem czasów niedostępności, optymalizacją procesu utrzymania instalacji oraz lepszym dostosowaniem wolumenu i rodzaju produkcji do chwilowych potrzeb makroekonomicznych.

Bardzo podobne rozwiązania wykorzystywane są w systemie produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych oraz w ramach systemu zaopatrzenia w wodę, gdzie nad całością procesu technologicznego, nadzór sprawują systemy SCADA.

W ramach systemu zaopatrzenia w żywność w zakładach przetwórczych, poszczególne maszyny przemysłowe sterowane są za pomocą dedykowanych sterowników PLC (PLC – ang. *Programmable Logic Controller*) realizujących zadaną funkcję produkcyjną. W bardziej zaawansowanych zakładach nad całością procesu czuwają rozwiązania MES (MES – ang. *Manufacturing Execution System*), zbierające w czasie rzeczywistym dane ze sterowników PLC, co umożliwia podejmowanie na bieżąco właściwych decyzji pozwalających na efektywne sterowanie procesem produkcyjnym, jego optymalizację oraz reagowanie na ewentualne nieprawidłowości pojawiające się w czasie procesu produkcyjnego.

3 RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej*, http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf, [dostęp: 06.06.2014].

Zupełnie inne wyzwania stoją przed rozwiązaniami teleinformatycznymi wykorzystywanymi w ramach systemu finansowego. Tutaj podstawą jest zapewnienie poufności danych finansowych oraz posiadanie mechanizmów kontrolnych, gwarantujących integralność przechowywanych i przetwarzanych danych. Jak pokazuje praktyka i ostatnie awarie systemów informatycznych największych banków w Polsce, chwilowy brak dostępności usług finansowych – bądź to dostępu do środków na rachunku lub możliwości realizowania transakcji za pośrednictwem kart kredytowych – staje się zjawiskiem powszechnym i nie budzi już zaniepokojenia czy zaskoczenia wśród dużej części użytkowników.

Ponadto, rozwiązania IT wykorzystywane w systemie bankowym mają za zadanie przetwarzanie dużych wolumenów danych transakcyjnych, a w szczególności muszą posiadać bogate możliwości analityczne, tak aby na podstawie zgromadzonych danych o użytkownikach, instytucje finansowe mogły podejmować świadome decyzje co do kategoryzacji klientów i ich stratyfikacji. Podobne wyzwanie stoi przed podmiotami telekomunikacyjnymi, które na podstawie danych o aktywnościach użytkowników sieci telekomunikacyjnej podejmują decyzje dotyczące podejścia do różnych grup klientów, ale przede wszystkim, co jest kluczowe z perspektywy IK, decydują o rozwoju infrastruktury telekomunikacyjnej.

Kolejnym obszarem, gdzie duże znaczenie odgrywają obecnie technologie teleinformatyczne to system ciągłości działania administracji publicznej. Jednak mnogość rozwiązań IT, wykorzystywanych w poszczególnych jednostkach administracji, przy jednoczesnym braku należytego, kompleksowego podejścia do bezpieczeństwa dla całej administracji (np. opartego o uznaną na całym świecie metodykę SABSA – ang. *Sherwood Applied Business Security Architecture*) prowadzi do punktowych – a przez to nieskutecznych i niezwykle kosztownych – rozwiązań bezpieczeństwa. Oczywiście należy tu pamiętać, że nie wszystkie systemy teleinformatyczne wykorzystywane w administracji są równie istotne, niemniej jednak część z nich (przykładem mogą być systemy ZUS, przechowujące dane o oszczędnościach emerytalnych milionów Polaków) wymaga zastosowania zaawansowanych mechanizmów kontrolnych, wspartych efektywnym procesem reakcji na ewentualne zdarzenia noszące znamiona zdarzeń niepożądanych. Niemniej jednak, brak całościowego spojrzenia na aspekty zabezpieczenia systemów teleinformatycznych wspierających funkcjonowanie państwa doprowadzi do nieuchronnych w dłuższej perspektywie, skutecznych ataków na tą infrastrukturę i osłabienia jej funkcji.

Postęp technologii wymusza nie tylko konieczność ciągłej aktualizacji rozwiązań wykorzystujących rozwiązania teleinformatyczne w ramach IK, ale również generuje potrzebę ciągłego dostosowywania, przez rząd i regulatorów, legislacji do zmieniającego się otoczenia. Wspomniane na wstępie autonomiczne samochody będą bezużyteczne, jeżeli nie zostaną wprowadzone zmiany legislacyjne dopuszczające je do ruchu drogowego. Ale taka zmiana to nie decyzja chwili – jej wprowadzenie musi zostać poprzedzone szeregiem analiz i decyzji, co do docelowego modelu jej funkcjonowania. Konieczne będzie na przykład udzielenie odpowiedzi na pytania związane z odpowiedzialnością cywilną (co się stanie jeśli samochód autonomiczny będzie sprawcą kolizji drogowej). Skoro więc samochody autonomiczne staną się powszechne, a przez to miara ryzyka związanego z przejęciem kontroli nad takim pojazdem wzrośnie, to czy zintegrowane systemy komunikacyjne, zbudowane w oparciu o samochody autonomiczne, zostaną zaklasyfikowane jako element IK? Dlatego mówiąc o ochronie IK należy mieć na uwadze: z jakich komponentów IK na chwilę obecną się składa, jak jest wspierana rozwiązaniami organizacyjnymi, procesowymi czy technicznymi (w tym teleinformatycznymi) i w jaki sposób zdefiniować mechanizmy kontrolne zapewniające jej bezpieczeństwo, a pośrednio bezpieczeństwo wszystkich obywateli.

Podsumowanie

Rozdział prezentuje dwie grupy rozwiązań teleinformatycznych wykorzystywanych w ramach IK – IT i OT, których niezakłócone funkcjonowanie jest kluczowe z punktu widzenia bezpieczeństwa IK. W rozdziale opisane są też podstawowe istotne różnice pomiędzy IT a OT (czyli systemami odpowiedzialnymi za procesy sterowania przemysłowego) szczególnie istotne z punktu widzenia ochrony IK. Rozdział pokazuje także w jaki sposób w poszczególnych systemach zaliczanych do IK wykorzystywane są poszczególne rozwiązania IT i OT.

6. Zagrożenia dla bezpieczeństwa infrastruktury krytycznej w kontekście zaawansowanego zastosowania rozwiązań teleinformatycznych – wyzwania dla państwa

Aleksander Poniewierski – EY

Przed dokonaniem analizy zagrożeń dla infrastruktury krytycznej (IK), a w zasadzie jej elementu teleinformatycznego, należy przedmiot rozważań osadzić w realiach zmian technologicznych, jakie dokonały się w przeciągu ostatnich trzech dekad. Zmiany te mają fundamentalne znaczenie dla zrozumienia istoty i powagi zagrożeń w dzisiejszym świecie technologicznym, zarówno w kontekście technologii informacyjnej (IT – ang. *Information Technology*), służącej automatyzacji procesów informacyjnych oraz decyzyjnych, jak i technologii operacyjnej (OT – ang. *Operational Technology*) służącej monitorowaniu oraz sterowaniu automatyką przemysłową. Owe zmiany należy rozważać z trzech głównych perspektyw:

- zmiany ekonomicznej;
- zmiany technologicznej;
- zmiany organizacyjnej.

Oczywiście istnieje szereg innych czynników mogących wprowadzić zagrożenia dla systemów teleinformatycznych IK, lecz wymienione powyżej mają fundamentalny i kluczowy wpływ na dzisiejszy poziom ryzyka. W tym miejscu zaznaczyć należy, że zjawisko to dotyczy nie tylko naszego kraju, lecz ma charakter globalny i dotyczy większości instalacji, przedsiębiorstw i państw na całym świecie.

Zmiana ekonomiczna

Rozwój technologii po II wojnie światowej, a w szczególności w latach 70-tych i 80-tych minionego stulecia szedł w parze ze stopniowym odchodzeniem od przeznaczania dużych nakładów na badania i rozwój, jakich dokonywano w USA, Europie Zachodniej, Japonii oraz krajach bloku wschodniego, skutkujących „patentowaniem" pełnych rozwiązań technologicznych przy równoczesnym stałym koszcie ich nabycia. Ten skomplikowany opis świata automatyki ery zimnej wojny można sprowadzić do uproszczenia, wedle którego państwo lub koncern wydaje potężne pieniądze na wynalezienie lub udoskonalenie danej technologii. W wyniku wieloletnich badań pojawia się kompletne (słowo to ma zasadnicze znaczenie) i samowystarczalne rozwiązanie technologiczne. Instalowane w danym przedsiębiorstwie, zawiera w sobie specyficzne dla danego producenta rozwiązania z zakresu automatyki przemysłowej, jak również rozwiązania sterowania, modelowania i kontroli. Niejednokrotnie wypracowane podczas procesu badania i rozwoju rozwiązania IT i OT są specyficzne dla danej technologii

w określonej wersji. To powoduje, że wspominając o koszcie instalacji na przykład nowej centrali telefonicznej, nowego bloku energetycznego lub nowego systemu do hydrokrakingu, mówimy o technologii danego producenta „pod klucz". Co więcej, technologia ta sprzedawana i dostarczana jest w całym okresie amortyzacji i funkcjonowania, czyli nie ma tu mowy o instalacji, a następnie utrzymywaniu jej przez wewnętrzne służby odpowiedzialne za IT i OT przedsiębiorstwa. Można powiedzieć, że jakakolwiek ingerencja przez takie służby skutkuje brakiem gwarancji poprawnego działania lub odmową usuwania uszkodzeń. Tak więc, do połowy lat 80-tych XX wieku ekonomia stosowania rozwiązań IT i OT dotyczyła całości technologii, nie zaś pojedynczych jej komponentów informatycznych i automatyki przemysłowej.

Dodatkowo, w latach 90-tych i na początku XXI wieku następuje bardzo silny nacisk na obniżanie kosztów oraz, co ważniejsze, wygasać zaczęły patenty na technologie. Z tego to ekonomicznego powodu (presja ceny – presja kosztu) pojawia się silna potrzeba poszukiwania oszczędności w rozwiązaniach technologicznych. Następuje potężna fala unifikacji rozwiązań IT i OT. Zamiast dedykowanych systemów operacyjnych i języków programowania wprowadzane są klasyczne, ogólnodostępne systemy korporacyjne, zamiast dedykowanych rozwiązań łączności i separowanych galwanicznie sieci transmisyjnych wykorzystywane zostają sieci korporacyjne oraz publiczne. Ta zmiana w sposób bardzo zasadniczy ogranicza koszty rozwiązania zarówno nabycia, jak i utrzymania. Dodatkowo, następuje bardzo silna tendencja poszukiwania taniej produkcji na rynkach wschodnich – początkowo w kierunkach: Tajlandia, Malezja, a finalnie Chiny. Daje to nie tylko kolejną obniżkę cen, za sprawą mniejszego kosztu wytworzenia, lecz co najważniejsze daje zaczątek powstawania taniego substytutu w całości produkowanego przez chińskie lub koreańskie koncerny. Tym samym można powiedzieć, że zmiana ekonomiczna (presja ceny) całkowicie zmieniła rynek technologiczny i miała kluczowe znaczenie dla kształtu technologii OT i IT w systemach IK.

Zmiana technologiczna

Powyżej przeanalizowane zostały zagadnienia zmiany ekonomicznej, skutkującej modyfikacjami technologicznymi IT i OT w IK. W tym miejscu omówiona zostanie zmiana technologiczna dotyczącą aspektu skali i szybkości obliczeniowej. Jest to zagadnienie często pomijane w analizach poświęconych bezpieczeństwu rozwiązań IT i OT. Ponieważ jednak wpływ tych zmian na bezpieczeństwo jest znaczny, należy problematyce tej przyjrzeć się bliżej. Wspomniana powyżej, szybka zmiana technologiczna, zachodzącą w okresie zimnej wojny, była swoistym wyścigiem zbrojeń. Blokady wymiany technologicznej Wschód – Zachód (COCOM – ang. *Coordinating Committee for Multilateral Export Controls*) miały ograniczać dostęp do technologii, w szczególności branży IT i OT, będącej dziś fundamentem IK w państwach. Wokół poszczególnych instalacji (zakładów produkcyjnych) budowane były rozwiązania technologiczne IT i OT specyficzne dla danej fabryki lub rafinerii. Działając przez wiele lat wytwarzały one specyficzne zmiany technologiczne (wnioski racjonalizatorskie), adoptowane przez producentów danej technologii i przenoszone na inne instalacje. Niestety postęp i potrzeba szybkiego, nagłego wzrostu ilości instalacji (w szczególności po uwolnieniu rynku wschodniego oraz przeniesienia produkcji do krajów azjatyckich) powodują konieczność odmiejscowienia ekip serwisujących rozwiązania zarządzające, w szczególności systemy IT i OT. Wprowadzany jest nadzór zdalny nad instalacjami, i co najważniejsze, tworzone są ogólno producenckie bazy konfiguracji (CDB – ang. *Configuration Data Base*), zawierające informacje o wszystkich elementach instalacji. Konieczne staje się również wprowadzanie w pełni mobilnych instalatorów wyposażonych w laptop i urządzenia mobilne oraz współdzielenie wyżej opisanych systemów teleinformatycznych. Z tego tez powodu (tj. skali i mobilności oraz różnorodności ekip serwisowych), dąży się do standaryzacji protokołów (ich publikacji) oraz otwartości centralnych serwerów zarządzających sygnałami (SCADA). Dodając do tego ekonomicznie wymuszoną zmianę specyficznych dla technologii systemów operacyjnych i baz danych na ogólnie dostępne rozwiązania rynkowe, mamy pełen obraz bardzo wrażliwego na zakłócenia i ingerencje środowiska technologicznego, zamienionego w sposób niekontrolowany na niespójny architektonicznie konglomerat połączeń. W dodatku, panuje powszechne przekonanie o odseparowaniu tego środowiska i jego wysokiej niezawodności. Jest to jeden z najbardziej mylnych obrazów środowiska technologicznego IT i OT, który w dodatku stanowi podstawę dla zapewniania bezpieczeństwa IK państw.

Zmiana organizacyjna

Wielokrotnie w powyższych opisach sygnalizowana była warstwa organizacyjna. Zmiana w tym obszarze jest szczególnie istotna w kontekście bezpieczeństwa IK. Ponownie odwołując się do czasów sprzed pół wieku, organizacją utrzymującą rozwiązania technologiczne była niejako linia jej użytkowników, która sprowadzana była przez producentów owej technologii do roli ekip wykonujących polecenia z listy dostępnej w danym zakładzie i dostarczonej przez dostawcę. Drugą stronę procesu stanowiła dedykowana, wysoko wykwalifikowana, grupa inżynierów na bieżąco kontrolująca daną instalacje i działająca na zasadzie ciągłej zmiany środowiska.

W takiej organizacji, samokontrolujący się organizm, wyposażony w punkty kontrolne oraz okna serwisowe, działał w sposób ciągły. Organizacja dbała tylko o jeden element, mianowicie, aby utrzymać kulturę „mistrz – uczeń". Ten kształt organizacyjny w procesie edukacyjnym był elementem koniecznym i wystarczającym dla zapewnienia ciągłości działania instalacji. W praktyce oznaczało to, że po stronie firmy powstawały szkoły zawodowe (przysposobienia zawodowego), kształcące pod okiem mistrzów z zakładu pracowników nowego pokolenia (linia operatorów) oraz uczelnie inżynieryjne (głównie związane z producentami technologii, a wiec zakładane na Zachodzie), kształcące kadrę znającą daną technologię i posiadającą potencjał do jej rozwoju. Niestety w chwili obecnej oba te elementy, edukacyjny i organizacyjny, zostały zachwiane, co ma bezpośredni wpływ na poziom bezpieczeństwa.

Współczesne zagrożenia związane z systemami teleinformatycznymi IK

Współczesne zagrożenia są w dużej mierze związane z wyżej opisanymi zmianami. Należy uświadomić sobie źródło zagrożeń, aby wiedzieć, w jaki sposób dochodzić do wypracowania mechanizmów zabezpieczenia. Bez tej wiedzy i świadomości wszystkie działania na rzecz bezpieczeństwa będą nieskuteczne. Przedstawiony poniżej schemat zagrożeń i ich klasyfikacja stanowi wybór szczególnie istotnych grup zagrożeń, które z kolei można rozwinąć na dalsze, bardziej specyficzne dla rozwiązań i obszarów IK grupy. Celem tego tekstu nie jest dokonanie systematycznego i kompletnego opisu wszystkich grup zagrożeń, a jedynie tych, które stanowią najistotniejszy element, wobec którego należy podjąć działania.

Jako pierwsze i najistotniejsze zagrożenie dla bezpieczeństwa systemów IT i OT IK wymienić należy brak świadomości i edukacji w tym zakresie. Właściciele instalacji – obiektów IK, maja bardzo małą świadomość zagrożeń i ryzyka w zakresie teleinformatycznym IT i OT. Brak świadomości wpływu na bezpieczeństwo zmian ekonomicznych, technologicznych i organizacyjnych, a co za tym idzie, brak wiedzy w zakresie ich konsekwencji dla prawidłowego funkcjonowania IK, są podstawowymi czynnikami ryzyka. Są to kwestie warte podkreślenia, bowiem brak świadomości wpływa bezpośrednio na niewystarczające zainteresowanie tematem, na brak przeznaczania funduszy na poprawne zabezpieczenie IK oraz na brak zrozumienia skali powiązań pomiędzy obiektami IK. To zaś w konsekwencji, przy niezabezpieczonym choćby jednym elemencie łańcucha, czyni go słabym w całości. Niestety, wspomniany już brak świadomości jest też domeną rządzących (w dużej części właścicieli przedsiębiorstw będących częścią IK) oraz kadry kierowniczej i wykonawczej. Wniosek z tego jest taki, że na wszystkich poziomach niewystarczająca świadomość powoduje stan pozornego bezpieczeństwa – najgorszy scenariusz dla zarządzających ryzykiem. Bardzo mocno z tym zagrożeniem związany jest brak systemowej edukacji wspomnianych powyżej poziomów. Mowa tu zarówno o edukacji systemowej (szkolnej i uniwersyteckiej) kształcącej kadry zarządcze, ale również kadry mającej zdolność przeciwdziałania zagrożeniom dla IK np. działaniom antysabotażowym lub hackerskim. Należy pamiętać, że cykl edukacyjny to ok. 7 lat, wiec są to działania długoterminowe i niemożliwe do zrealizowania w krótkim okresie czasu.

Drugą grupą zagrożeń są zagadnienia związane z zarządzaniem zmianą. Pod pojęciem tym należy rozumieć szereg działań związanych ze zmianą zarówno technologii, organizacji lub własności systemów IT i OT, ale również całokształt czynników związanych ze zmianą kultury organizacji. Te drugie są następstwem przejęć i połączeń pomiędzy firmami lub wynikiem zmian legislacyjnych i regulacyjnych. Szczególnie istotnymi zmianami, mającymi duży wpływ na bezpieczeństwo IK, są zmiany projektowe wprowadzające całkowicie nowe, rozwiązania i technologie do łańcucha IK. Mowa tu np. o rozwiązaniach otwartych (w zakresie IT i OT) lub technologiach inteligentnych (ang. *smartgrid*). Skala zmian pośrednich na sieć IT i OT jest tak duża, że bez całościowego planowania architektonicznego nie sposób jest jej przeanalizować i odpowiednio nią zarządzić. Ostatnią kategorią grupy zagrożeń związanych ze zmianą są zagadnienia związane z testowaniem jej wyników. W chwili obecnej kwestie testów IK IT i OT są problemem o najwyższym poziomie złożoności i krytyczności. Brak odpowiedniej metodyki testowania zarówno rozwiązań, jak i zachowań organizacji w sytuacji niespodziewanego błędu stanowią poważny problem w skali globalnej.

Trzecia grupa zagrożeń związana jest ze zmianą paradygmatu ekonomicznego i rzeczowego bezpieczeństwa IT i OT. Ujmując kwestie ogólnie, zagrożenie polega na radykalnym obniżeniu poziomu możliwych i uzasadnionych ekonomicznie środków finansowych przeznaczonych na zabezpieczenie IT i OT. Wraz ze zmianą (obniżeniem) kosztów infrastruktury IT i OT zmienia się uzasadniony ekonomicznie koszt zabezpieczeń[1]. Przy opisanym wcześniej zjawisku zmian ekonomicznych i technologicznych możliwe koszty przeznaczone na zabezpieczenia zmniejszają się, a równocześnie gwałtownie, aby nie powiedzieć radykalnie, zwiększają się potrzeby wynikające z niejednorodnej architektury. W konsekwencji mamy przed sobą problem, który będzie ujawniał się wraz z biegiem czasu coraz bardziej, a wycenione w sposób klasyczny, konieczne do zastosowania zabezpieczenia minimalizujące ryzyko będą liczone w dziesiątkach milionów złotych. Równocześnie, wartość samej infrastruktury (rzeczowa) będzie o wiele niższa. Będziemy stawali przed dylematem czy zabezpieczać czy może wymieniać poszczególne fragmenty infrastruktury. Będziemy też (co już się dzieje) stawiani przed dylematem czy aplikować rozwiązania tanie dla głównych zastosowań (technologii) np. chmura obliczeniowa, stosować rozwiązania zunifikowane, czy też patrzeć na nie przez pryzmat ryzyka. Aby zrozumieć skale tego zagrożenia należy wyobrazić sobie jak bardzo zmienia się potrzeba zabezpieczeń przy zastosowaniu przetwarzania w chmurze.

Czwarta grupa zagrożeń fundamentalnych dla IT i OT to upowszechnienie się technologii i jej ogólnodostępność. W latach, kiedy instalacje IK posiadały specjalistyczne i sobie tylko specyficzne rozwiązania, zagrożenia dla ich bezpieczeństwa mogły przyjść ze strony przypadkowych błędów w produkcji, nieprawidłowego użytkowania systemów teleinformatycznych lub celowego sabotażu ze strony osób mających autoryzowany dostęp. Dziś możliwe jest (bez większych problemów) przejęcie kontroli nad poszczególnymi elementami IK bez fizycznej obecności przy instalacji. Istnieje możliwość przejęcia kontroli nad systemem produkcyjnym lub poszczególnymi jego komponentami nawet przez średnio wyspecjalizowane osoby oddalone o setki lub tysiące kilometrów. Co więcej, działania takie prowadzone przez organizacje zorganizowane państwowo, lub przez państwo wspierane (oficjalnie, nieoficjalnie), ale także organizacje i podmioty niepaństwowe stanowią realne zagrożenie dla bezpieczeństwa państw. I właśnie ta grupa zagrożeń (upowszechnienie technologii) jest dziś najbardziej „widowiskowa" i przemawia do decydentów. Istotą jej zrozumienia są opisane powyżej kwestie. Ta grupa zagrożeń ma także bardziej skomplikowany i nieznany wymiar, a mianowicie źródło wytwarzania. Ten enigmatycznie brzmiący zwrot szeroko rozpowszechniony w świecie IT i OT sprowadza się do jednego – kto jest twórcą technologii i kto kontroluje jej rozwój, ten ma wiedze o potencjalnych problemach z nią związanych oraz potrafi użyć luk związanych z jej bezpieczeństwem. To zagadnienie (transparentności technologii) będzie w najbliższych latach wzbudzało wiele kontrowersji i obaw. Jest to kluczowy problem.

Ostatnią grupą zagrożeń dla systemów teleinformatycznych IK są same rozwiązania teleinformatyczne. Przez to, że systemy OT i IT są krytyczne dla jej funkcjonowania oraz nie mają należytej opieki (zarówno związanej z brakiem edukacji, ale i stosowanych rozwiązań zabezpieczających i monitorujących), stanowią najsłabsze ogniwo całej IK państw. Czyni je to w sposób szczególny narażonymi na zagrożenia, które mogą płynąć ze strony terrorystów, wrogich rządów i organizacji przestępczych. Celem może być paraliż funkcjonowania IK, jej destabilizacja, a w skrajnej sytuacji nawet zniszczenie.

Wniosek może wydawać się odważny, ponieważ, obrazowo rzecz ujmując – dlaczego by przypuszczać, że najsłabszym ogniwem nowej wersji luksusowego BMW lub Ferrari miałaby być elektronika w nim zastosowana? Zgodnie z zasadami bezpieczeństwa, największe zagrożenia wprowadza komplikacja i brak transparentności. Boimy się tego, czego nie rozumiemy i nie potrafimy w pełni używać nie mając wiedzy. Wówczas, zagrożeniem jest sam przedmiot użycia. Ta ostatnia grupa zagrożeń, nieco prowokacyjna, jest często poruszana na zagranicznych konferencjach oraz na forach ekspertów, gdzie padają pytania o skalę zastosowania rozwiązań

1 Paradygmat ekonomiczny bezpieczeństwa przewiduje, że koszty zabezpieczeń mogą być, co najwyżej, równe wartości straty, a powinny być mniejsze.

teleinformatycznych w IK. Pytania dotyczą tego, jaka jest przyszłość tych rozwiązań oraz w jaki sposób skutecznie je zabezpieczyć i monitorować. Te pytania, to w rzeczywistości pytania o zagrożenia.

Podsumowanie

W niniejszym rozdziale autor dokonuje analizy trzech zmian jakie dokonały się w środowisku rozwiązań teleinformatycznych mających dzisiaj zastosowanie w IK. Na bazie tych właśnie zmian, wyróżnione zostały cztery główne grupy zagrożeń, którym należy przeciwdziałać. Odnoszą się one do niskiej świadomości zagrożeń i ryzyka w zakresie teleinformatycznym IT i OT; są związane z problematyką zmiany, dalej z upowszechnieniem się technologii i jej ogólnodostępnością, ekonomicznymi kalkulacjami prowadzącymi do obniżania wydatków na bezpieczeństwo, w końcu są związane z wyzwaniem jakie wprowadzają rozwiązania teleinformatyczne same w sobie.

7. Teleinformatyczne elementy ochrony infrastruktury krytycznej

Włodzimierz Kotłowski – MATIC

Skuteczna ochrona infrastruktury krytycznej (IK) dotyczy przede wszystkim zachowania integralności i ciągłości działania procesów, które dana infrastruktura bezpośrednio zapewnia lub pośrednio wspiera w łańcuchu powiązanych działań z zewnętrznymi strukturami. Nowoczesne rozwiązania teleinformatyczne (ICT – ang. *Information and Communitcation Technology*) znajdują zastosowanie w budowie optymalnej ochrony IK. Poziom współczesnej ochrony zależy od szybkości wykrycia negatywnego zdarzenia oraz szybkości i kompletności odpowiedzi na zaistniałe zdarzenie w aspekcie zachowania ciągłości działania istotnych procesów. Włączenie ICT do ochrony IK powoduje, że w procesie identyfikacji zasobów krytycznych danej infrastruktury rozważać należy również zasoby ICT użyte do jej ochrony zgodnie z istniejącymi dla nich zagrożeniami i wykrytymi podatnościami oraz skutkami biznesowymi w przypadku wystąpienia negatywnych scenariuszy.

Ochrona IK wspierana przez ICT

Wśród zagadnień ochrony IK wspieranych przez ICT wymienić można następujące działania:

- inwentaryzacja i zarządzanie zasobami IK;
- monitorowanie i zarządzanie dostępem fizycznym (ochrona perymetryczna obszaru z IK, ochrona wewnętrzna, zarządzanie dostępem dla osób uprawnionych);
- monitorowanie i zarządzanie dostępem logicznym do zasobów ICT;
- zbierania danych z monitorowanych procesów/obiektów, również wybrane dane przesyłane z automatyki przemysłowej;
- zbieranie danych z otoczenia biznesowego;
- automatyczna analiza zebranych danych w czasie rzeczywistym;
- przechowywanie i archiwizacja zebranych danych (w tym działania z zakresu informatyki śledczej (*forensic*);
- zarządzanie negatywnymi zdarzeniami i sytuacjami kryzysowymi;
- ocena ryzyka i zarządzanie nim;
- planowanie odbudowy (scenariusze zdarzeń i odpowiadające im procedury postępowania);
- testowanie planów odbudowy;
- ochrona informacji (poufność, dostępność, integralność);
- utrzymanie IK (konserwacja, naprawy, przeglądy);

- komunikacja (koordynacja działań, włączenie instytucji zewnętrznych);
- szkolenia w zakresie ochrony i planów ciągłości działania.

Trudno dziś sobie wyobrazić, w jaki inny sposób realizować działania ochronne bez wdrażania rozwiązań ICT równolegle do istniejących w przemyśle systemów ICS (ICS – ang. *Industrial Control Systems* – oprogramowanie będące częścią systemów OT – np. SCADA). Należy również rozważyć czy konieczna jest wymiana danych pomiędzy systemami ICT a ICS. W przypadkach konieczności takiej wymiany niezbędne jest odpowiednie zabezpieczenie takich wzajemnych powiązań komunikacyjnych.

W tabeli nr 1 znajdującej się w Aneksie nr 1 przedstawiono ramowe podejście do ochrony IK zgodnie z metodyką dla podnoszenia bezpieczeństwa systemów ICS („Framework for Improving Critical Infrastructure Cybersecurity") wydaną przez amerykańską agencję NIST (NIST – ang. *National Institute of Standard and Technology*) w lutym 2014 r. W kolumnie „Odnośniki informacyjne" przytoczono odpowiadające danemu zagadnieniu standardy bezpieczeństwa ICT oraz ICS.

Wszystkie wymienione w tabeli funkcje i procesy zarządzania bezpieczeństwem IK obsługiwane mogą być w całości przez dedykowane oprogramowanie wraz z funkcją centralnego zarządzania, przydzielania i kontroli zadań wyznaczonym osobom, zgodnie z wcześniej zdefiniowanymi rolami w systemie bezpieczeństwa.

Przenośne stacje robocze i urządzenia mobilne w ochronie infrastruktury krytycznej

Natychmiastowa reakcja służb (wewnętrznych jak i zewnętrznych, jeśli dotyczy) interweniujących w przypadku zaistnienia negatywnych zdarzeń związanych z bezpieczeństwem chronionej IK byłaby bardzo utrudniona lub wręcz niemożliwa (głównie ze względu na wymaganą reakcję w określonym reżimie czasowym), gdyby cała dokumentacja wraz z planami odbudowy była w postaci papierowej lub na nośniku cyfrowym w izolowanej zamkniętej sieci.

Służby odpowiedzialne za ochronę IK wyposażone powinny być w sprzęt stacjonarny (nadzór, monitorowanie) oraz w urządzenia mobilne umożliwiające połączenia głosowe oraz wymianę określonych danych (mapy, plany, procedury i inne), przewidzianych do obsługi negatywnych scenariuszy zdarzeń często dynamicznie zmiennych w czasie i wymagających przemieszczania się.

Sprawna i bezpieczna komunikacja mobilna oprócz zapewnienia bezpiecznych połączeń (również szyfrowanych, jeśli wynika to z przeprowadzonej analizy ryzyka) wymaga posiadania oprogramowania do zarządzania wszystkimi urządzeniami mobilnymi (MDM – ang. *Mobile Device Management*) działającymi w sieci właściciela IK.

Oprogramowanie MDM powinno spełniać wymogi zawarte w opracowanej i wdrożonej polityce bezpieczeństwa do zarządzania mobilnymi urządzeniami przenośnymi (tablety, smartfony, laptopy), zapewniającą:

- scentralizowaną kontrolę nad wszystkimi terminalami mobilnymi w sieci;
- zarządzanie zasobami mobilnymi – rozpoznawanie, przechowywanie i raportowanie danych o urządzeniach mobilnych (również zarządzanie sprzętem z wieloma systemami operacyjnymi);
- zarządzanie konfiguracjami – zdalna konfiguracja połączeń sieciowych;
- zarządzanie aplikacjami – centralne repozytorium aplikacji, zdalna dystrybucja i instalacja aplikacji oraz łatek oprogramowania i upgradów dla zdefiniowanych użytkowników;
- ochronę przesyłanych danych siecią mobilną (zachowanie atrybutu poufności, integralności i dostępności tylko dla osób upoważnionych) wraz z automatycznym uwierzytelnianiem uprawnionego użytkownika (stosowanie kilku poziomów uwierzytelnień wynikających z analizy ryzyk); mechanizmy do zapobiegania wyciekom wrażliwych danych (DLP – ang. *Data Leak Prevention*);
- automatyczny *backup* danych – kopie zapasowe najważniejszych danych dostępnych na urządzeniu mobilnym;
- zarządzanie bezpieczeństwem – definiowanie, aktualizowanie i zdalne przesyłanie polityk bezpieczeństwa na urządzenia mobilne (w tym zdalne blokowanie urządzeń, kasowanie danych, zmiany konfiguracyjne, zmiany uprawnień i inne przewidziane w polityce).

Monitoring zagrożeń i podatności jako niezbędny krok do zapewniania bezpieczeństwa

Wdrażane rozwiązania ICT oraz ICS są narażone na zagrożenia, które ze względu na przyczyny możemy podzielić na naturalne, przypadkowe i umyślne. Zagrożenia naturalne (jak np. pożar, zalanie i inne) nie wywołują w nas niepokoju, znamy je od początku istnienia naszej cywilizacji i potrafimy im zapobiegać. Niepokoją nas nieznane, przypadkowe i umyślne zagrożenia wynikające z aktualnie istniejących podatności zasobów lub z podatności, które za chwilę się pojawią wraz z nowymi zagrożeniami. Już to sformułowanie rodzi niepokój – podatności, które zależą od dynamicznie zmieniającego się otoczenia zewnętrznego jak i wewnętrznego, które również może być źródłem zagrożenia (np. zbuntowany pracownik). Dodajmy do tego szczególną klasę podatności związaną z używanym systemem operacyjnym, oprogramowaniem, jak również bazami danych. Znajomość tych ostatnich wymienionych podatności jest wykorzystywana przez osoby przeprowadzające różnego rodzaju ataki na zasoby ICT lub ICS. Często tego rodzaju naruszenia bezpieczeństwa pozostają niewykryte.

Pozyskiwanie wiedzy o istniejących zagrożeniach i skojarzonych z nimi podatnościami zasobów ICT lub ICS jest podstawowym zadaniem osób odpowiedzialnych za bezpieczeństwo zasobów krytycznych. Jeżeli bezpieczeństwo IK zależy wprost od bezpieczeństwa zasobów ICT i ICS to konieczne jest stałe monitorowanie podatności tych zasobów. Zalecana częstotliwość przeprowadzanych testów podatności powinna wynikać z analizy ryzyk.

Zalecane cechy narzędzi testujących podatności zasobów ICT są następujące:

- narzędzia testujące powinny być bezpieczne dla naszych systemów (nie powinny wprowadzać zmian i uszkadzać zasobów);
- do przeprowadzania testów należy używać wyłącznie narzędzia znanych światowych *vendorów* (dostawców);
- *vendor* oferujący narzędzia do testowania powinien dysponować odpowiednio dużą bazą opisanych podatności wraz z bazą zawierającą istniejące zagrożenia skojarzone z daną podatnością, plus dodatkowe wskazówki niwelujące działanie podatności dla administratora w przypadku aktualnego braku łatek oprogramowania;
- narzędzia testujące powinny zapewniać wykrywanie podatności typu *„zero-days"* (natychmiast po pierwszym pojawieniu się na świecie, przy braku łatki oprogramowania);
- narzędzia testujące powinny dostarczać wyniki testów czytelne dla osoby nieposiadającej głębokiej wiedzy z dziedziny informatyki;
- narzędzia testujące powinny podlegać stałej aktualizacji (wymagana jest stała komunikacja narzędzi z bazą wiedzy lub centrum kompetencji; aktualizacja bazy raz w tygodniu może nie być wystarczająca) zgodnie z dynamicznie zmieniającą się wiedzą na temat zagrożeń i podatności przy szerokiej gamie stosowanego oprogramowania;
- narzędzia testujące powinny podlegać stałej aktualizacji (wymagana jest stała komunikacja narzędzi z bazą wiedzy lub centrum kompetencji; aktualizacja bazy raz w tygodniu może nie być wystarczająca) zgodnie z dynamicznie zmieniającą się wiedzą na temat zagrożeń i podatności przy szerokiej gamie stosowanego oprogramowania.

Metody testowania podatności zasobów ICS należy starannie dobierać adekwatnie do wymagań danego środowiska IK, jego rozwiązań technologicznych, architektury systemów sterowania, użytych systemów operacyjnych, oprogramowania i technik przesyłania danych. Testy nie mogą spowodować niestabilności systemu ICS, muszą zapewniać ciągłość działania procesów IK.

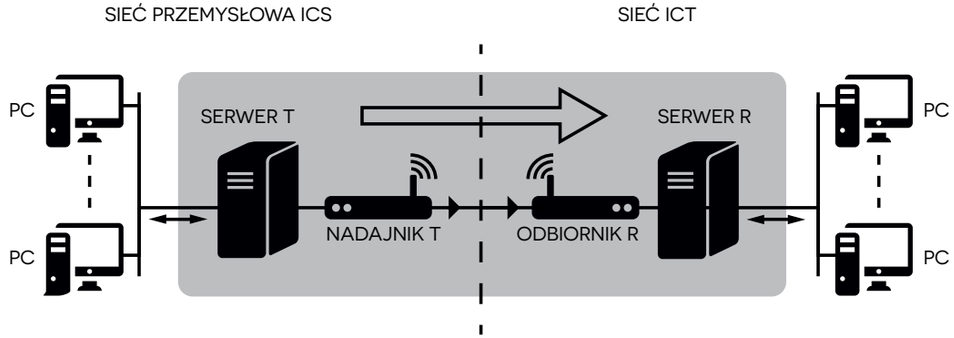
Przy tak sformułowanych wymaganiach dotyczących budowania wiedzy o zagrożeniach i podatnościach wypływających ze stosowanych systemów operacyjnych i oprogramowania należy zastanowić się nad budową krajowego centrum kompetencji w tej dziedzinie, czyli polskiej firmy dysponującej wiedzą i narzędziami testującymi na światowym poziomie. Pozostaje tylko pytanie, czy nas na to stać i w jakim czasie zostanie to zbudowane. Można rozpatrywać również wariant budowania aliansu ze światowym *vendorem* w tej dziedzinie lub wariant wspólnej ochrony krytycznych zasobów ICT w ramach istniejących porozumień obronnych (UE lub NATO).

Bezpieczna integracja rozwiązań ICT przedsiębiorstwa oraz systemów nadzoru przemysłowego ICS IK

Czy jest konieczne całkowite odizolowanie rozwiązań ICT od systemów nadzoru przemysłowego (ICS)? Jeśli rozwiązania ICT mają zapewniać ochronę IK w czasie rzeczywistym dodatkowo eliminując lub zmniejszając w znacznej mierze zaangażowanie obsługującego personelu, to budowanie całkowicie odseparowanych systemów ICT od ICS nie jest uzasadnione. Konieczne powiązania i stąd wynikające kanały i sposoby komunikacyjne powinny być poddane szczegółowej analizie ryzyka. Wnioski z tej analizy powinny decydować o zastosowanej architekturze rozwiązań i sposobach wzajemnej komunikacji. Poniżej przedstawiono możliwe sposoby budowania wzajemnych powiązań ICT z ICS.

Wariant 1
Zastosowanie jednokierunkowego przepływu danych (tzw. dioda danych), które zapewnia całkowitą ochronę przed atakami internetowymi od sieci zewnętrznych.

Rysunek 7. Jednokierunkowy przepływ danych (tzw. dioda danych) Oznaczenia: Nadajnik T– laser emitujący światło do światłowodu, można wysyłać dane, ale nic nie może wrócić do chronionej sieci przemysłowej; Odbiornik R – fotodioda odbiorcza. Źródło: opracowanie własne, ikony pochodzą ze strony www.nounproject.com



Wariant 2
- Zastosowanie firewalli typu SCADA (gwarantują w sposób fizyczny – konstrukcja elektroniki i optoelektroniki – komunikację określonego typu);
- zastosowanie rozproszonych firewalli funkcjonujących wewnątrz całości sieci automatyki w taki sposób, że atak w pojedynczym punkcie nie daje dostępu do całości sieci automatyki (dobrą analogią dla architektury rozproszonych firewalli są grodzie w łodzi podwodnej);
- szyfrowanie za pomocą rozwiązań sprzętowych (szyfratorów i de-szyfratorów);
- zastosowanie wielopoziomowych metod uwierzytelniania;
- automatyczne ostrzeganie przy jednoczesnym monitorowaniu parametrów *Quality-of-Service* (QoS) w sieci wewnętrznej.

Rozwiązanie przedstawione w Wariancie 1 (stosowane od wielu lat w technice wojskowej) z przełączaniem kierunkowości łącza można stosować również w wielu procesach związanych

z utrzymaniem krytycznej infrastruktury ICT lub ICS (uaktualnianie oprogramowania, zarządzanie łatkami programowania, testy podatności i inne). Przełączanie można zaplanować w wybranych przedziałach czasowych wraz z dodatkowymi zabezpieczeniami monitorującymi i ochronnymi.

Budując bezpieczne kanały komunikacji pomiędzy ICT a ICS zawsze należy przeprowadzić analizę ryzyk, a następnie wybrać rozwiązanie adekwatne do wartości chronionych zasobów i procesów.

Podsumowanie

Rozdział pokazuje, że wraz z włączeniem elementów teleinformatycznych do ochrony IK, w procesie identyfikacji zasobów krytycznych danej infrastruktury rozważać należy również owe zasoby teleinformatyczne. Istotne jest aby prowadzić działania w odniesieniu do istniejących dla nich zagrożeń i wykrytych podatności oraz w połączeniu ze skutkami biznesowymi, w przypadku wystąpienia negatywnych scenariuszy. Autor poruszył także m. in. problematykę przenośnych stacji roboczych i urządzeń mobilnych w ochronie IK.

8. Bezpieczeństwo systemów nadzoru przemysłowego

Piotr Ciepiela – EY

Ochrona infrastruktury krytycznej (IK) stała się w ostatnich latach jednym z najważniejszych aspektów związanych z szeroko pojętym bezpieczeństwem na świecie. Pod pojęciem IK częściej rozumiane były same instalacje, budynki i infrastruktura bez warstw automatyki przemysłowej, która faktycznie nimi steruje oraz zarządza, i w obecnych czasach *de facto* stanowi integralną część całości środowiska przemysłowego. Obszar ten jednak jest coraz częściej brany pod uwagę i wprost zaliczany do IK. Takie podejście zostało niedawno wprowadzane również w Polsce.

Bezpieczeństwo OT (OT – ang. *Operational Technology*) – to sprzęt, oprogramowanie (systemy ICS np. SCADA/DCS), personel i wszelkie działania, które maja na celu wykrywanie lub wprowadzanie zmian w procesach technologicznych poprzez kontrolę fizycznych urządzeń (takich jak pompy, zawory itp.). Jest ono ostatnimi czasy traktowane jako priorytetowe z punktu widzenia całościowej ochrony IK, która do tej pory sprowadzała się często do ochrony fizycznej. Stało się tak, dlatego że systemy sterowania zostały zauważone jako absolutnie krytyczny element IK, a przy tym najbardziej wrażliwy i łatwy do zaatakowania. Dodatkowo, atak może zostać przeprowadzony w sposób anonimowy, zdalny i praktycznie bez ryzyka poniesienia konsekwencji przez atakującego, który może być na drugim końcu świata. Cyberbezpieczeństwo IK pojawiło się w rezultacie na liście priorytetowych działań wielu krajów świata, o czym świadczą m.in. inicjatywy legislacyjne zarówno w Stanach Zjednoczonych, na poziomie Unii Europejskiej, jak i w poszczególnych krajach członkowskich.

Przyczyn tego, że zabezpieczeniem cybernetycznym systemów OT zajęto się dopiero niedawno jest kilka. Przede wszystkim, systemy OT pracowały wcześniej w odizolowanych środowiskach, gdzie nie zagrażały im takie problemy jak ataki czy infekcje wirusami z Internetu, do którego po prostu nie były podłączone. Z drugiej strony były to konstrukcje zamknięte, budowane przez każdego producenta inaczej, z wykorzystaniem dedykowanych protokołów komunikacyjnych (innych niż w tradycyjnym IT) i praktycznie „uszyte na miarę" konkretnego przedsiębiorcy. Dostępność takich systemów stanowiła jedyny wyznacznik bezpieczeństwa. Przede wszystkim z racji ekonomicznych nastąpiła w środowisku automatyki przemysłowej zmiana technologiczna, powodująca coraz większą otwartość systemów i zbliżenie świata automatyki przemysłowej do świata IT głównie poprzez konwergencje na poziomie infrastruktury (np. serwery i stacje dyspozytorskie), komunikacji (protokoły przemysłowe zastępowane przez

standard TCP/IP) czy systemów operacyjnych. Rozwój systemów oraz nowa sytuacja wymusiła niejako potrzebę wprowadzenia nowych standardów dotyczących kwestii bezpieczeństwa tak mocno rozwiniętego np. w obszarze IT.

Standardy w zakresie OT/ ICS dla IK

Systemy przemysłowe działają na świecie od ponad 40 lat. Standardy i zestawy wytycznych dotyczące ich ochrony zaczęły jednak powstawać dopiero w ostatnich kilku latach, w wyniku wspomnianych wcześniej zmian środowiskowych. W krótkim czasie transformacje te doprowadziły do gwałtownego wzrostu liczby zagrożeń dla systemów OT, które zupełnie nie były na to przygotowane.

Prekursorem działań były Stany Zjednoczone i do tej pory państwo to jest największym producentem standardów w OT. Zauważyć warto także, że to właśnie w USA zrodziło się samo pojęcie Infrastruktury Krytycznej (1995 r. „Raport Marshalla"). Działania związane z ochroną IK w Stanach Zjednoczonych są tak zaawansowane, że w najważniejszych sektorach, tj. energetyce i petrochemii, wprowadzono regulacje wymuszające na operatorach infrastruktury wdrażanie określonych rozwiązań bezpieczeństwa.

Drugim źródłem regulacji są międzynarodowe organizacje zrzeszające m.in. użytkowników systemów OT (np. firmy petrochemiczne, energetyczne).

W końcu, trzecim źródłem są dostawcy rozwiązań OT, którzy poziom bezpieczeństwa swoich systemów rozpoznali jako obszar przewagi konkurencyjnej, a przede wszystkim obszar strategiczny z punktu widzenia konsekwencji PR-owych. Kolejne doniesienia medialne o atakach na IK z wykorzystaniem podatności takiego czy innego systemu, który przy tego typu informacjach prasowych coraz częściej wymieniany jest z nazwy, może bardzo negatywnie wpłynąć na wizerunek dostawców.

Zaczynając od standardów rządowych, jedną z pierwszych, bardzo konkretnie i poważnie traktujących kwestie bezpieczeństwa w systemach nadzoru, jest publikacja z roku 2011 agencji amerykańskiej NIST (NIST – ang. *National Institute of Standard and Technology* – Narodowy Instytut Standaryzacji i Technologii) o numerze 800-82 pt. „Guide to Industrial Control Systems (ICS) Security"[1]. Ten obszerny dokument przez lata stanowił standard w podejściu do bezpieczeństwa w tym obszarze. Nie przedstawiał jedynie wytycznych technicznych, choć bardzo duży nacisk położono na kwestie bezpieczeństwa sieciowego, ale również poświęcał wiele uwagi kwestiom zarządzania środowiskiem, podnoszenia świadomości i szkoleniom pracowników. Dość sporym mankamentem wszystkich tego typu „wytycznych" jest jednak ich modelowość. Środowiska automatyki przemysłowej są zwykle skomplikowane (występują na przykład różne klasy systemów, od różnych dostawców, z różnych „epok technologicznych"), a przy tym praktycznie nierozerwalne i niełatwe do zmodyfikowania ze względu na wymaganie ciągłej dostępności. Dostosowanie do prezentowanych modeli było i nadal jest przedsięwzięciem zdecydowanie trudniejszym niż zbudowanie samego modelu. Warto jeszcze zwrócić uwagę na rozszerzenie, jakie wprowadził NIST do swojej sztandarowej publikacji 800-53 „Recommended Security Controls for Federal Information Systems and Organizations" – dodatek dedykowany dla systemów przemysłowych (Appendix I – „ICS Security Controls, Enhancements, And Supplemental Guidance"). Publikacja stanowi zbiór kontroli bezpieczeństwa możliwych do zastosowania w środowisku ICS.

Zwieńczeniem działań NIST jest wydana w lutym 2014 r. metodyka dla podnoszenia bezpieczeństwa systemów OT/ICS („Framework for Improving Critical Infrastructure Cybersecurity"). Metodyka ta została zamówiona bezpośrednio przez prezydenta Baracka Obamę („Executive Order 13636"), po to, aby niezależna grupa ekspertów stworzyła ogólne wytyczne dotyczące tego, jak operatorzy IK mogą w sposób systemowy podejść do stworzenia wewnętrznego programu cyberbezpieczeństwa.

Pierwszym sektorem, który otrzymał formalne wytyczne, m.in. dotyczące bezpieczeństwa automatyki przemysłowej, jest amerykański sektor chemiczny. Sektor ten jest kontrolowany przez DHS (ang. *Department of Homeland Security* – Departament Bezpieczeństwa Krajowego), który stworzył CFATS („Chemical Facilities Anti-Terrorism Standards"). CFATS miało zapewnić, że każda organizacja, która produkuje, przechowuje lub transportuje niebezpieczne substancje chemiczne ma wdrożone nie tylko zabezpieczenia fizyczne, ale również teleinformatyczne. Niespełnienie wymagań standardu może spowodować natychmiastowe zamknięcie działalności danego przedsiębiorstwa. Co ciekawe, DHS zakładało pierwotnie, że standard uda się w pełni wdrożyć w ciągu 2 lat, tymczasem po ponad 10 latach nadal jest on w fazie implementacji. Pokazało to, jak trudnym obszarem jest bezpieczeństwo systemów sterowania i jak kompleksowo należy planować jego wdrożenie.

Kolejnym tzw. regulowanym sektorem w Stanach Zjednoczonych jest sektor energetyczny. Specjalnie dla niego agencja NERC (NERC – ang. *North American Electrical Reliability Corporation*) stworzyła CIP (CIP – ang. *Critical Infrastructure Protection*), zbiór zasad dotyczących bezpieczeństwa IK zawierających również wytyczne dla systemów sterowania (potocznie nazywany NERC-CIP). Pierwsza wersja publikacji składała się z kilku bardzo wysokopoziomowych wytycznych (obecnie dostępna jest wersja 5. standardu). Głównym celem było zwrócenie uwagi zarządów i managementu na fakt istnienia takiej infrastruktury, systemów przemysłowych i konieczności ich zabezpieczenia. Nie były to wytyczne bardzo szczegółowe, a dużą bolączką stała się wielość możliwości interpretacyjnych. Warto zwrócić uwagę, że NERC-CIP jest w amerykańskim sektorze energetycznym bezwzględnym wymogiem. Wdrożenie tych zasad jest weryfikowane poprzez badanie zgodności, a brak spełnienia wymagań może przynieść przedsiębiorcy karę nawet do 1 mln USD za każdy dzień niezgodności.

Z punktu widzenie podejścia sektorowego warto wymienić jeszcze dwa zestawy wytycznych:

Dla sektora rafineryjnego opracowane przez American Petroleum Institute i tu głównie tzw. „API-1164 – Pipeline SCADA Security" oraz "API-1165 – Recommended Practice for Pipeline SCADA Displays". Stanowią one zbiór zasad dla bezpieczeństwa systemów ICS, który można z powodzeniem stosować również w innych sektorach. Dla sektora gazowego natomiast został stworzony przez American Gas Association tzw. „AGA-12" (*SCADA encryption).* Cały standard traktuje jedynie o szyfrowaniu, co może dziwić, gdyż sektor gazowy nie ma dodatkowych specjalnych wymagań w tym obszarze. Jest to raczej przykład na to, że każdy sektor starał się stworzyć wytyczne dla bezpieczeństwa automatyki przemysłowej niekoniecznie o podobnym

1 W wolnym tłumaczeniu tytuł brzmi „Wytyczne bezpieczeństwa dla Przemysłowych Systemów Sterowania".

zakresie. Biorąc pod uwagę czas powstania publikacji (rok 2005), ówczesny stan systemów oraz brak formalnego wymogu zgodności ze standardem wdrożenie tych wytycznych pozostało na niskim poziomie.

Na poziomie Unii Europejskiej warto zaznaczyć działalność ENISA (ENISA – ang. *European Union Agency for Network and Information Security*), czyli agencji Wspólnoty zajmującej się kwestiami bezpieczeństwa. ENISA wydała na przełomie 2011 oraz 2012 „Protecting Industrial Control Systems – Recommendations for Europe and Member States", dokument, który opisuje ówczesną sytuację bezpieczeństwa systemów przemysłowych oraz 7 głównych kroków jak podnieść poziom bezpieczeństwa w takim środowisku. W publikacji zwrócono szczególną uwagę na potrzebę stworzenia państwowych oraz paneuropejskiej strategii bezpieczeństwa systemów OT/ICS oraz konieczność edukacji i podnoszenia świadomości społeczeństwa w tym zakresie.

Inne kraje członkowskie również rozwijają swoje wewnętrzne standardy np. Niemcy i Wielka Brytania mają swoje dojrzałe regulacje, co więcej, sam rząd Estonii sponsoruje operatorom IK przeglądy bezpieczeństwa automatyki przemysłowej.

Największym obecnie przedsięwzięciem, które na światową skalę zrzesza niezależnych ekspertów z dziedziny automatyki przemysłowej, cyberbezpieczeństwa czy przedstawicieli producentów rozwiązań klasy ICS, jest zdecydowanie stowarzyszenie ISA (ISA – ang. *Instruments, Systems and Automation Society*). W szczególności ISA99 jest ciałem powstałym w celu stworzenia zestawu standardów dla bezpieczeństwa automatyki przemysłowej. Normy te tworzone są więc przez osoby pracujące z systemami ICS i jednocześnie doskonale rozumiejące specyfikę tego obszaru. Dotychczasowo powstałe wytyczne są na tyle popularne i skuteczne, że staną się one oficjalną serią standardów IEC (IEC – ang. *International Electrotechnical Commission* – Międzynarodowa Komisja Elektrotechniczna) o sygnaturze IEC 62443. Do tej pory ISA wydała w obszarze bezpieczeństwa OT:

- "ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models";
- "ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems";
- "ANSI/ISA–99.02.01–2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program".

W fazie opracowania znajduje się, najbardziej przez wszystkich oczekiwany standard ISA 99.03.03 – „Security For Industrial Automation And Control Systems – System Security", dotyczący konkretnie bezpieczeństwa systemów przemysłowych.

Rozwiązania zapewniające i zwiększające bezpieczeństwo

Opisywane standardy mają zapewnić w pewnym sensie ustrukturyzowane podejście do poszczególnych obszarów bezpieczeństwa systemów przemysłowych. W większości nie są jednak one uniwersalne dla wszystkich rozwiązań i sektorów. Całkowite zapewnienie bezpieczeństwa w zróżnicowanych technologicznie środowiskach o często dużym stopniu skomplikowania i wysokiej dostępności nie jest celem łatwym do osiągnięcia, jeżeli w ogóle możliwym. Jednym ze sposobów zwiększenia bezpieczeństwa jest zastosowanie filozofii *defence in depth,* znanej chociażby ze świata IT. Oczywiście przenoszenie rozwiązań IT do świata OT bez adekwatnej zmiany jest o wiele bardziej niebezpieczne niż pozostawienie *statusu quo*. Czasem jednak na poziomie filozofii możemy posłużyć się znanym rozwiązaniem. W rzeczonym *defence in depth* niezależnie od rodzaju środowiska staramy się zapewnić ochronę na kilku warstwach. Najlepiej jednak rozpatrywać taką ochronę dla 3 podstawowych wymiarów: technologicznego, organizacyjnego i procesowego. Każdy z tych wymiarów musi być zabezpieczony na odpowiednim poziomie, w przeciwnym razie może dojść do łatwego zaburzenia procesu technologicznego.

Wymiar technologiczny to zabezpieczenie sprzętowe począwszy od najniższej warstwy, czyli urządzeń występujących na instalacji, przechodząc do sterowników (PLC/RTU) mających bezpośredni kontakt z instalacjami, do systemów przemysłowych. Nie można również zapomnieć o zabezpieczeniu wymiany danych pomiędzy poszczególnymi elementami środowiska, a więc odpowiednim zabezpieczeniu warstwy sieciowej (zarówno protokołów przemysłowych jak i urządzeń sieciowych). Najbardziej zbliżonym do IT obszarem technologicznym jest zabezpieczenie serwerów i stacji roboczych wraz z wykorzystywanymi systemami operacyjnymi. Ostatnią istotną kwestią jest bezpieczeństwo fizyczne instalacji, czyli dotychczas najbardziej rozpowszechniony sposób ochrony infrastruktury. Niezależnie od znacznego zwiększenia zagrożeń cybernetycznych cały czas niezbędna jest ochrona przed zwykłym wandalizmem za pomocą przysłowiowego „młotka".

Wymiar organizacyjny to stworzenie odpowiedniej struktury organizacyjnej osób odpowiedzialnych za bezpieczeństwo w przedsiębiorstwie: przydzielenie ról, zarządzanie wiedzą i budowanie kompetencji, dostarczenie odpowiedniego poziomu wiedzy i budowanie świadomości. To także odpowiednie zarządzanie personelem, np. weryfikacja czy dany pracownik nie stworzył zagrożenia dla systemów przemysłowych u poprzedniego pracodawcy (referencje pracownicze).

Wreszcie, wymiar procesowy to zidentyfikowanie i zdefiniowanie procesów technologicznych wraz z procesami zarządczymi. Następnie stworzenie i efektywne wdrożenie zestawu wewnętrznych polityk, procedur i standardów technicznych opisujących zasady działania w środowisku automatyki przemysłowej. Do procedur, które należy wziąć pod uwagę jest odpowiednie zarządzanie zmianą w środowisku, zarządzanie użytkownikami, incydentami, zarządzanie dostawcami czy zapewnienie ciągłości procesu.

Tak wygląda ogólny model podejścia do zwiększenia bezpieczeństwa. Niezależnie jednak od przyjętego modelu, dobrze jest zwrócić uwagę na trzy najbardziej podstawowe obszary problemowe.

1. Pierwszy z nich to identyfikacja i możliwa eliminacja tzw. SPOF (SPOF – ang. *Single Point of Failure*), czyli pojedynczych punktów awarii. Odpowiednia redundancja kluczowych elementów infrastruktury musi uniemożliwiać sytuację, w której awaria małego przełącznika potrafi doprowadzić do przestoju całej instalacji. Jak się okazuje, rzadko które przedsiębiorstwo faktycznie wykonało taką analizę i niejednokrotnie jest zależne od potencjalnie mało istotnych elementów infrastruktury.

2. Następny obszar to separacja od świata zewnętrznego rozumianego jako sieci zewnętrzne, takie jak Internet i sieć biurowa. Nie oznacza to tzw. galwanicznego odseparowania – to jest filozofii, która towarzyszyła środowiskom automatyki przemysłowej w latach 80-tych i 90-tych, kiedy takie systemy były faktycznie całkowicie odseparowane. Jednakże, na skutek ewolucji technologicznej, integracji sieci lub po prostu zwykłych biznesowych wymagań natychmiastowego otrzymywania informacji zarządczej z produkcji, sieci te w większości przypadków są, lub w najbliższym czasie zostaną, połączone z siecią biznesową. Tego trendu nie da się odwrócić. Oznacza to wykonie trudnego zadania architektonicznego, odpowiedniego uporządkowania i zabezpieczania kanałów komunikacji ze światem biurowym, jak również kontrolę wszelkich prób zdalnego dostępu do systemów ICS.

3. Ostatni punkt to po części kwestia organizacyjna, a po części kwestia poziomu świadomości użytkowników systemów ICS. Historycznie bardzo często dostarczenie całego środowiska, realizującego specyficzną funkcjonalność, leżało po stronie konkretnego dostawcy danego systemu. Nie byłoby w tym nic dziwnego i niepokojącego – w końcu dbał o system i jego wysoką dostępność, jednak w konsekwencji, aktualnie w przedsiębiorstwie może zabraknąć faktycznej wiedzy o architekturze systemu, możliwościach jego konfiguracji, rozwoju itp. Doprowadzić to może, np. w przypadku bankructwa dostawcy, do braku możliwości rozwoju systemu, a nawet wprowadzenia najprostszych zmian konfiguracyjnych. Nie wspominając już o kompletnym paraliżu w sytuacji awarii. Kolejna skrajna sytuacja to tzw. *vendor lock*, gdzie dostawca kluczowego systemu za każdą modyfikację czy zmianę konfiguracyjną każe płacić wygórowane ceny, a ze względu na brak dostępu do kodu źródłowego oraz znajomości logiki systemu żadna inna firma nie jest w stanie wykonać tego typu zadań.

A zatem niezbędna jest znajomość swoich własnych systemów i jakakolwiek forma kontroli nad dostawcami np. poprzez dostęp poprzez *escrow* do kodów. W skrócie jest to zabezpieczenie interesów spółki, polegające na powierzeniu stronie trzeciej kodów źródłowych danego rozwiązania informatycznego. W przypadku bankructwa dostawcy oprogramowania strona trzecia przekazuje kod źródłowy spółce. Warto rozważyć tego typu zabezpieczenia gdyż mówimy o systemach stanowiących IK, a więc mających wpływ na znaczną część obywateli państwa.

Techniki i metodologie tworzenia zintegrowanego modelu zarządzania bezpieczeństwem IK dla OT i IT

Wprowadzenie rozwiązań bezpieczeństwa bez odpowiedniej warstwy zarządzania nim nie będzie przynosiło skutku w dłuższej perspektywie czasowej. Bezpieczeństwo to proces i trzeba ciągłe upewniać się, że jest odpowiednio zdefiniowany oraz zarządzany. Budowa zintegrowanego modelu zarządzania bezpieczeństwem jest więc tematem jak najbardziej aktualnym. Wracając do porównań z obszarem IT mamy dobrze znany wzorzec jakim jest norma ISO27001, która daje wytyczne jak stworzyć system zarządzania bezpieczeństwem informacji. Niestety jest to norma stworzona z myślą o IT (z naciskiem na przetwarzaną informację) i w kontekście automatyki przemysłowej nie może być w pełni wykorzystana. Przede wszystkim, w świecie IT bezpieczeństwo to głównie poufność informacji, podczas gdy w OT zabezpieczamy proces przemysłowy – jego ciągłość i integralność. Pierwszą różnicą może być więc kwestia ochrony przed oprogramowaniem złośliwym. O ile w IT takie rozwiązania powinno się używać wszędzie ze znaczną automatyzacją procesu uaktualniania i usuwania zagrożeń, o tyle w świecie OT usunięcie, a nawet zwykła kwarantanna plików może skończyć się zatrzymaniem instalacji przemysłowej. Innym przykładem jest choćby tak prosta kwestia jak zmiana haseł. O ile jest to idea jak najbardziej słuszna, rodzi ona pewne problemy. Zwykła zmiana hasła w systemie SCADA może okazać się problematyczna, gdyż konto ze standardowym hasłem jest wykorzystywane np. raz na pół roku i w newralgicznej sytuacji może nie zadziałać. Skomplikowanie haseł też jest kwestią wymagającą dużego przemyślenia – bardzo często od odpowiednio szybkiego wpisania takiego hasła zależeć będzie życie ludzkie zagrożone awarią na instalacji. W sytuacji zagrożenia ludzie popełniają częściej błędy, wpisanie trzykrotnie błędnego hasła i zablokowanie konta może więc przynieść więcej szkody niż pożytku. To samo się tyczy automatycznego zamykania sesji na stacjach operatorskich.

Jeżeli chodzi o architekturę sieciową, czyli praktycznie jeden z kluczowych aspektów bezpieczeństwa OT, to również wprost nie znajdziemy wymagań co do jej tworzenia w ISO27001. Dodatkowo ISO 27001 nie wspomina o urządzeniach na poziomie serwerów czy stacji roboczych. Podobieństw świata OT i IT jest sporo, kiedy jednak przejdziemy do sterowników i protokołów wymiany danych między nimi, to różnice w podejściu do bezpieczeństwa będą znaczne.

Co do zasady, normę ISO27001 można traktować jako dokument pomocniczy, nie należy jednak wprowadzać zasad normy bez wcześniejszej, bardzo krytycznej analizy adekwatności do świata OT.

Patrząc na dostępną literaturę tworzenie systemu, czy też programu bezpieczeństwa opisane jest np. we wspomnianym wcześniej NIST 800-82, ale faktyczny opis ustanowienia systemu zarządzania bezpieczeństwem dla automatyki przemysłowej znajduje się w standardzie „ISA-99.02.02 Security for industrial automation and control systems – Operating and IACS Security Program". Co ciekawe, pod względem filozoficznym podobnie jak w ISO27001 zalecane jest wprowadzenie systemu na bazie tzw. Cyklu Deminga (*Plan/Do/Check/Act*). Natomiast cykl, jak i same wytyczne, rozwijane były z myślą o systemach automatyki przemysłowej i bezpieczeństwa procesu technologicznego. Poszczególne sekcje dokumentu opisują, w jaki sposób ustanowić organizację, jak wykonać segmentację sieci, jak podejść do aktualizacji systemów itp. Według ogólnie przyjętej zasady:

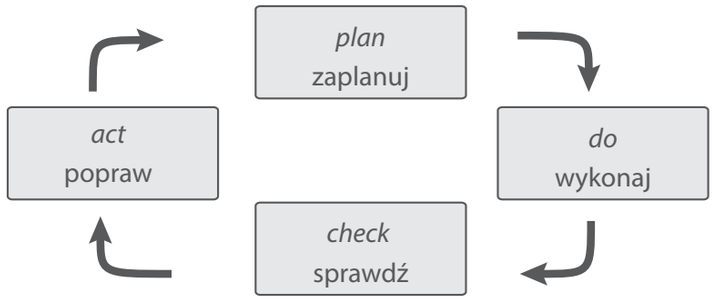
Plan – ustanowienie polityki systemów zarządzania bezpieczeństwem (SZB) dla systemów ICS wraz z adekwatnymi celami, procesami i procedurami umożliwiającymi zarządzanie ryzykiem i podnoszenie poziomu bezpieczeństwa;

Do – wdrożenie i wykorzystanie SZB dla systemów ICS w rozumieniu wdrożenia procesów, polityk, procedur;

Check – ocena, pomiar efektywności procesu i odpowiednie raportowanie rezultatów;

Act – wprowadzenie działań naprawczych na podstawie wyników przeglądów i audytów działania SZB systemów ICS w celu ciągłego poprawiania stanu SZB.

Rysunek 8. Cykl Deminga. Źródło: Opracowanie własne



Podstawą jest jednak, aby odpowiednio zidentyfikować wymagania dotyczące cyberbezpieczeństwa systemów ICS, oraz ustanowić odpowiedni zestaw procedur i wytycznych. Należy wdrożyć kontrole, które umożliwiają zarządzanie ryzykami związanymi z automatyką przemysłową, jako częścią składową ryzyk biznesowych przedsiębiorstwa. W końcu trzeba monitorować efektywność systemu zarządzania bezpieczeństwem i stale udoskonalać system bazując na stopniu osiągnięcia danego celu.

Organizacja i środki podnoszenia świadomości

Znaczące podniesienie świadomości bezpieczeństwa systemów automatyki przemysłowej musi zostać zrealizowane zarówno na poziomie państwa (ochrona własnej IK), jak również i przedsiębiorstwa (ochrona własnych zasobów).

Rolą państwa jest między innymi: wprowadzanie działania w ramach edukacji obejmującej wprowadzenie i uaktualnienie odpowiednich programów kształcenia informatycznego w szkołach i na wyższych uczelniach.

Ponadto państwo, jako interesant bezpieczeństwa IK, powinno motywować jej bezpośrednich właścicieli i operatorów do jej zabezpieczania, co leży w interesie wszystkich. Motywacja taka, idąc za wzorem najbardziej w tym obszarze rozwiniętych państw, powinna się opierać na zachęcaniu przedsiębiorców do inwestowania w bezpieczeństwo (np. ulgi podatkowe, obniżenie składek ubezpieczeniowych, sponsorowanie szkoleń i wsparcia eksperckiego dla przedsiębiorstw np. na wzór Estonii), ale również do sankcjonowania pewnych przynajmniej podstawowych standardów, które później będą sukcesywnie rozwijane i dostosowywane do rosnącej skali zagrożeń. Budowa świadomości jest niezbędna, z drugiej jednak strony należy rozważyć wprowadzenie obligatoryjnych wymagań bezpieczeństwa np. na kształt NERC-CIP. Nie są one skomplikowane, a zwracają uwagę na problem bezpieczeństwa Zarządów spółek przy jednoczesnych karach finansowych dla braku zgodności z normą. Życie pokazuje, że sama świadomość istnienia zagrożenia rzadko przekłada się na praktykę w takim zakresie, w jakim byśmy tego chcieli. Bez istnienia kodeksu drogowego i sankcji za jego nieprzestrzeganie, na drogach sytuacja byłaby dużo gorsza niż jest obecnie. Powinniśmy iść zatem za przykładem krajów najbardziej rozwiniętych.

Przedsiębiorstwa powinny stanowić główny punkt szkoleniowy i *de facto* dla każdej spółki powinno być ważne, aby takie szkolenia przeprowadzić. Prewencja i świadomość personelu skutkuje znacznym zmniejszeniem strat finansowych. Na poziomie spółki powinny być również rozważone zabezpieczenia technologiczne i organizacyjne, uniemożliwiające lub ograniczające do minimum zestaw działań do tych niezbędnych. Konieczne jest również odpowiednie monitorowanie środowiska, zarówno w celu pełnej znajomości własnej infrastruktury, jak również identyfikacji wszelkich zmian i odpowiedniej reakcji na nie. Szczególnym rodzajem przedsiębiorstw są dostawcy rozwiązań ICS. To na nich powinno nakładać się twarde wymagania regulacyjne, dotyczące spełnienia standardów bezpieczeństwa. Jak pokazują liczne przykłady to niefrasobliwość i, w pewnym sensie, niezrozumiałe zaufanie do własnych rozwiązań doprowadziły do znanych obecnie incydentów i powstania cyberbroni, skierowanych na instalacje przemysłowe. Przez lata producenci mogli zapewniać swoich klientów, że ich rozwiązania są bezpieczne, licząc na to, że są na tyle specyficzne i mało rozpoznawalne, że nie wzbudzą zainteresowania cyberprzestępców. Ta era się jednak skończyła.

Podsumowanie

Rozdział systematyzuje informacje dotyczące standardów podnoszących bezpieczeństwo OT w IK. Dodatkowo omówione zostały rozwiązania zapewniające i zwiększające bezpieczeństwo w trzech wymiarach: technologicznym, organizacyjnym, procesowym. Autor odnosi się także do takich zagadnień jak eliminacja pojedynczych punktów awarii, kluczowych z punktu widzenia funkcjonowania IK, separacja od świata zewnętrznego, oraz działania związane z podnoszeniem świadomości.

9. Reagowanie na incydenty w obszarze infrastruktury krytycznej

Mirosław Maj – Fundacja Bezpieczna Cyberprzestrzeń*

Domena teleinformatycznej infrastruktury krytycznej (TIK) wymaga dobrze zorganizowanego procesu reagowania na incydenty. Praktyka wykazała, że nadzorowanie i sterowanie urządzeniami odpowiedzialnymi za utrzymanie tej infrastruktury narażone jest na niemalże wszystkie bezpośrednio przychodzące z sieci Internet zagrożenia. Seria poważnych naruszeń bezpieczeństwa w systemach SCADA na całym świecie udowodniła, że problem jest realny, a jego zamiatanie pod dywan może być wyjątkowo niebezpieczne. Dowodem na to są najbardziej spektakularne przypadki – np. wirus Stuxnet. Wraz z rozwojem technik i procesów związanych z zabezpieczeniem teleinformatycznym, eksperci uznają, że reagowanie na incydenty z czasem staje się coraz ważniejsze i nie powinno być zaniedbywane w odniesieniu do działań profilaktycznych.

Obserwacja trendów związanych z reagowaniem na incydenty (IR – ang. *Incident Response*) dla TIK wskazuje na istnienie dwóch ścieżek realizacji tego zadania i kształtowanie się trzeciej.

Po pierwsze, funkcję IR przypisuje się bardzo często jako zadanie dla CERT-ów rządowych lub CERT-ów wojskowych. Tak jest na przykład w Hiszpanii, na Litwie, w Luksemburgu, Finlandii, Danii, Słowenii, czy Gruzji. Jak widać głównie w Europie. Tak jest też w Polsce, gdzie rządowy CERT.GOV.PL informuje, że „obszarem działania CERT.GOV.PL oraz podstawowymi „odbiorcami" usług (ang. *constituency*) oferowanych przez zespół są użytkownicy systemów teleinformatycznych administracji państwowej (domena *.gov.pl), a także podmioty należące do tzw. „krytycznej infrastruktury teleinformatycznej państwa".

Ten trend europejski związany jest z historyczną ważną rolą europejskich CERT-ów, które przez swoje aktywne i skuteczne działanie sprawiły, że najważniejsze tematy dotyczące bezpieczeństwa IT przypisywane są właśnie tego typu komórkom. W sytuacji kiedy idea CERT-ów została przejęta również przez administrację państwową praktycznie większości państw, również w administracji te najważniejsze zadania trafiają do komórek CERT-owych.

Drugi sposób podejścia do tematu reagowania w obszarze TIK to sposób amerykański i typowe dla Amerykanów zadaniowe ujęcie problemu. Takie podejście doprowadziło do

* Materiał częściowo ukazał się w magazynie CIIP fokus wydawanym przez RCB.

powstania nowego podmiotu, ściśle zajmującego się powierzonym zadaniem. Podmiotem tym jest ICS-CERT, czyli Industrial Control Systems-CERT. CERT ten, w odróżnieniu od CERT-ów rządowych, zajmuje się tylko i wyłącznie sprawami związanymi z ochroną TIK. W Stanach Zjednoczonych, które, przypomnijmy, są ojczyzną idei CERT-owej, istnieje też CERT rządowy – US-CERT oraz odgrywający bardzo ważną rolę w działaniach na rzecz bezpieczeństwa teleinformatycznego państwa – CERT Coordination Center – pierwszy CERT jaki powstał na świecie (1988r.).

Warto jeszcze zauważyć inny trend, który wskazuje na przypisanie roli IR dla TIK nowopowstałym organizacjom skupiającym w danym kraju wszelkie funkcje związane z ochroną cyberprzestrzeni. Tak jest na przykład w Holandii, gdzie tamtejszy CERT rządowy GOVCERT.NL wyewoluował w kierunku organizacji o nazwie National Cyber Security Centrum.

Nie wchodząc w ocenę poszczególnych modeli, co byłoby możliwe tylko w przypadku przeprowadzenia szczegółowych badań nad skutecznością poszczególnych rozwiązań, warto przyjrzeć się rozwiązaniu amerykańskiemu. Wybór ten, jak wspominamy, nie stanowi wyróżnienia tego modelu, ale jest podyktowany powodami praktycznymi – dzięki zawężonemu i precyzyjnemu określeniu oczekiwań w stosunku do ICS-CERT zajmuje się on praktycznie tylko tym, czym CERT odpowiedzialny za IR w TIK zajmować się powinien. W rezultacie obserwacja poczynań takiego CERT-u daje szanse na rozpoznanie najważniejszych zadań.

Zadania związane z reagowaniem na incydenty na przykładzie działalności ISC-CERT

ISC-CERT jest częścią Departamentu Bezpieczeństwa Krajowego Stanów Zjednoczonych (ang. *Department of Homeland Secuirty*). Jego powstanie i funkcjonowanie jest częścią „Programu Ochrony Informatycznej Infrastruktury Krytycznej" (PCII Program – „Protected Critical Infrastructure Information Program") oraz „Programu Bezpieczeństwa dla Systemów Kontroli" (CSSP – „Control System Security Program"). Właśnie ten program jest częścią spinającą inne inicjatywy wokół tematu ochrony TIK, w tym reagowania na incydenty. W programie uczestniczy też amerykański CERT rządowy – US-CERT. Główne cele tego programu to:

- analiza i zabezpieczanie IK i chronionych systemów;
- identyfikacja słabości systemowych i ocena ryzyka;
- wypracowywanie wsparcia dla procedur ciągłości działania i odtwarzania atakowanych zasobów i serwisów.

Program ma również zapewniać przedstawicielom sektora prywatnego, do którego jak wiadomo należy zdecydowana większość IK, dzielenie się poufną informacją dotyczącą bezpieczeństwa TIK, w taki sposób, aby zachować bezpieczeństwo przekazywania tej informacji, w szczególności nie ujawnianie jej, co mogłoby zdaniem autorów programu zwiększyć ryzyko. Oprócz samej wymiany informacji, chodzi również o wymianę doświadczeń i wspólne prace nad poprawą bezpieczeństwa i lepszą koordynację odpierania zagrożeń. To jest już konkretne zadanie dla ICS-CERT-u.

Dla realizacji powyżej wspomnianych celów stworzono dwie grupy robocze:

- Industrial Control Systems Joint Working Group (ICSJWG)[1] – właśnie dla współpracy z sektorem prywatnym;
- Control Systems Security Working Group (CSSWG) – dla przedstawicieli instytucji federalnych.

ICS-CERT jest aktywny w obydwu najważniejszych obszarach działań CERT-ów – w obsłudze incydentów naruszających bezpieczeństwo, jak również w stałym prowadzeniu działań ostrzegawczych, uświadamiających i analitycznych. Niektóre z tych usług realizuje poprzez inne podmioty. Przede wszystkim zgłoszenia dotyczące słabości systemowych oraz złośliwego oprogramowania są zgłaszane do CERT Coordination Center specjalizującego się w tych dwóch dziedzinach. Natomiast incydenty związane z *phishingiem* są „odsyłane" do US-CERT. Sam ISC-CERT skupia się na incydentach związanych bezpośrednio z TIK. Swoją drogą ten przykład pokazuje, że zadaniowe podejście i tworzenie nowych struktur jest możliwe między innymi dzięki bardzo precyzyjnemu przypisaniu zakresu odpowiedzialności.

Jeśli chodzi o działania ostrzegawcze, analityczne i uświadamiające, warto aby to zespół odpowiedzialny za IR publikował informacje z następujących obszarów:

- porady (*advisories)*, które zawierają informacje o bieżących słabościach i występowaniu *exploitów* je atakujących;
- ostrzeżenia (*alerty*), które są szczególnymi alertami w sytuacjach wymagających szczególnej uwagi i reakcji;
- *newslettery*, które są wynikiem gromadzenia informacji w szczególny sposób poruszających wybrane tematy. Są one skierowane bezpośrednio do personelu zaangażowanego w ochronę TIK;
- raporty uświadamiające, czyli wszelakie materiały i informacje (np.: o różnych przewidzianych inicjatywach czy konferencjach) będące cennym materiałem do stałego podnoszenia świadomości związanej z koniecznością zapewnienia bezpieczeństwa dla TIK;
- techniczne raporty z analiz zagrożeń;
- raporty okresowe (w tym roczne).

Uzupełnieniem takich działań proaktywnych powinny być szkolenia organizowane przez zespół CERT-owy (szkolenia *online* lub szkolenia stacjonarne).

Rodzaje incydentów związanych z TIK

Aby przedstawić rodzaje incydentów, które w największym stopniu dotyczą TIK posłużyliśmy się danymi dotyczącymi dwóch ważnych obszarów – krajów członkowskich Unii Europejskiej oraz Stanów Zjednoczonych. W pierwszym przypadku są to dane odnotowane przez Europejską Agencję Bezpieczeństwa Sieci i Informacji (ENISA – ang. European Network and Information Security Agency). Dotyczą one incydentów zgłoszonych do ENISA w 2012[2], które wynikały z realizacji zapisów tzw. Artykułu 13a[3]. Na początku warto zwrócić uwagę, że to już

1 ICS-CERT, https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG, [dostęp:05.25.2014].

2 Raport stanowi najnowszą publikację ENISA na ten temat (tj: kwiecień 2014).

3 Pełna treść raportu jest dostępna na stronach ENISA: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012 [dostęp:05.25.2014].

drugi raport od momentu wprowadzenia obowiązku zgłaszania takich przypadków w europejskiej dyrektywie telekomunikacyjnej. Ten obowiązek dotyczy operatorów telekomunikacyjnych, którzy muszą raportować do krajowych władz regulujących rynek telekomunikacyjny.

W 2012 r. do Agencji zgłoszono 51 takich przypadków (dotyczyły one 2011 r.), zaś w 2013 r. tych przypadków było 79. Jednak przyrost nie jest tak dynamiczny jak wskazują te liczby, ponieważ jest on mocno uwarunkowany liczbą krajów, które raportowały. W zeszłym roku było ich 20, zaś w tym już 28. Nie wszystkie raportujące kraje odnotowały poważne incydenty. Tych, które je odnotowały było tylko 18. Nie znamy jednak szczegółów co do tego, który z krajów raportował, a który nie, który i ile miał incydentów, i jakie to były incydenty. Wszelkie szczegóły objęte są tajemnicą.

Tak jak to już było wspomniane na początku, raportowanie odbywa się do krajowych władz regulujących[4]. Zgodnie z przyjętym schematem regulator powinno się dzielić tymi danymi z ENISA oraz swoimi odpowiednikami w innych krajach, w sytuacji kiedy naruszenie bezpieczeństwa ma charakter transgraniczny i obowiązkowo raz na rok przekazywać ENISA dane zbiorcze. To co powinno się raportować określane jest jako „incydenty naruszające bezpieczeństwo, które miały znaczący wpływ na ciągłość świadczenia usług teleinformatycznych".

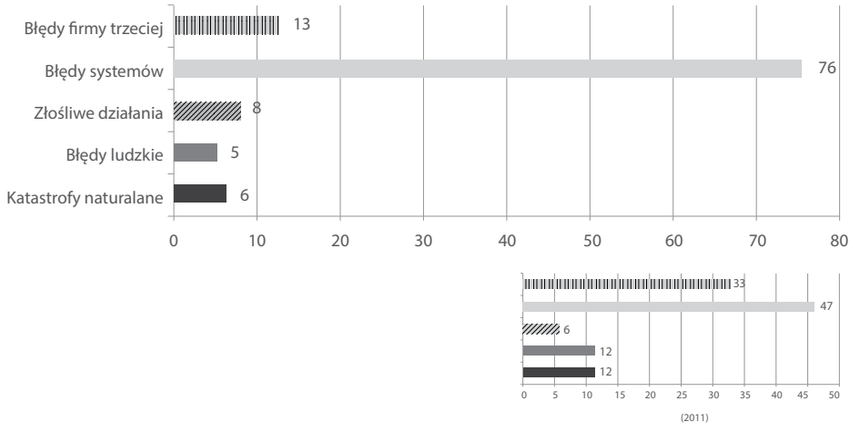
Przykłady zgłaszanych incydentów są następujące:

- przy przejściu ze świadczenia usług w oparciu o sieć tymczasową na sieć docelową, usługi głosowe VoIP były niedostępne dla 400 tys. użytkowników;
- aktualizacja jednego z głównych routerów była błędna, co spowodowało wyłączenie ruchu IP i w konsekwencji niedostępność wielu serwisów, w tym połączenia alarmowego 112. Incydent doprowadził do awarii trwającej 17 godzin i dotyczył 3 mln użytkowników;
- sieć światłowodowa została przecięta przy okazji kradzieży kabla. Incydent spowodował niedostępność usług telefonii stacjonarnej przez 10 godzin dla 70 tys. użytkowników i kablowej sieci internet dla 90 tys. użytkowników;
- seria ataków DDoS (DDoS – ang. *Distributed Denial of Service*, skierowana na usługę DNS (DNS – ang. *Domain Name Service*) spowodowała niedostępność sieci Internet przez 1-2 godziny dla 2,5 mln użytkowników;
- operator telekomunikacyjny zaimplementował aktualizacje systemowe dla HLR (HLR – ang. *Home Location Register*), co spowodowało awarię i w konsekwencji niedostępność mobilnej telefonii i usługi dostępu do sieci Internet. Incydent dotyczył połowy klientów operatora i trwał 8 godzin.

Jak widać z powyższych przypadków zgłoszenia w dużej mierze dotyczą problemów wynikających z sytuacji nie wywołanych działaniem intencjonalnym. Nie mniej jednak i takie występują, o czym świadczy przypadek ataków DDoS na system DNS. W raporcie pojawia się 5 głównych przyczyn incydentów, w kolejności najczęściej występujących: awaria systemu (76%), błąd u dostawcy zewnętrznego (13%), złośliwe działanie (8%), zjawiska naturalne (6%), których swoją drogą usuwanie trwa najdłużej – średnio 36 godzin i błędy ludzkie (6%). Co ciekawe w tej kategorii nastąpiła dość istotna zmiana w stosunku do roku poprzedniego, w którym błędy u dostawców zewnętrznych dotyczyły co trzeciego przypadku (33%).

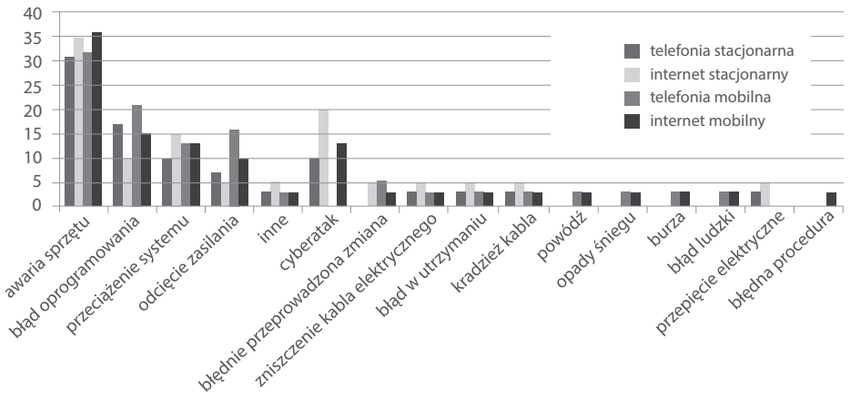
4 W Polsce jest to Urząd Komunikacji Elektronicznej.

Rysunek 9. Przyczyny powstawania incydentów naruszających bezpieczeństwo. Źródło: ENISA Annual Incidents Report 2012



Jeśli chodzi o incydenty związane z atakami komputerowymi, to choć nie jest ich dużo, warto dokonać ich krótkiej analizy. W naturalny sposób odnajdujemy je w kategorii działanie złośliwe (dla przypomnienia – to 8% przypadków). Jeśli sięgniemy do statystyk pokazujących szczegółowe przyczyny incydentów to znajdziemy tam informację, że *„cyber attacks"* były przyczyną 6 incydentów i jest to VI miejsce wśród przyczyn. Warto jednak zwrócić uwagę, że jeżeli rozważania ograniczymy do ataków na sieć Internet to cyberataki są drugą najczęstszą przyczyną incydentów. We wszystkich kategoriach jako przyczyna incydentu zdecydowanie dominuje awaria sprzętu.

Rysunek 10. Szczegółowe przyczyny incydentów w odniesieniu do poszczególnych serwisów. Źródło: 14 ENISA Annual Incidents Report 2012.

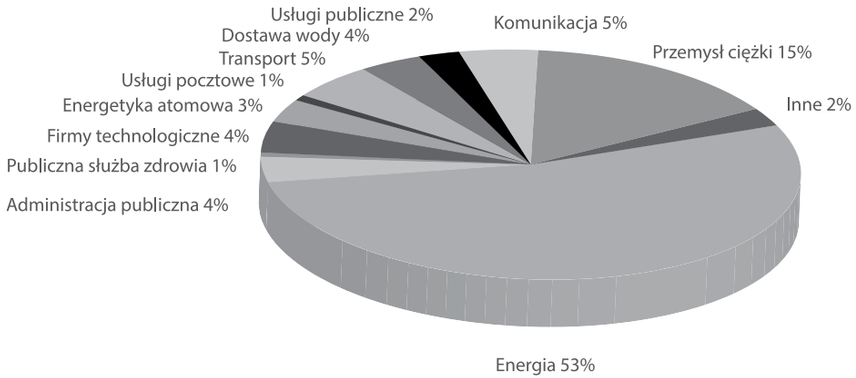


W swoim raporcie ENISA podaje również kryteria, jakie powinny obowiązywać w przypadku zgłaszania incydentów. Dzięki temu operatorzy telekomunikacyjni i narodowi regulatorzy rynku telekomunikacyjnego mają podpowiedź jak rozpatrywać swoje przypadki. Zgodnie ze wskazówkami zgłaszany powinien być każdy z incydentów, który powoduje przerwę

w świadczeniu usługi dłuższą niż 8 godzin (nawet jeśli dotyczy tylko 1% użytkowników) lub dotyczy więcej niż 15% użytkowników tego serwisu (nawet jeśli trwa tylko 1 godzinę), powinien być zgłoszony. To są bazowe kryteria dla tych dwóch cech (czas trwania i zasięg oddziaływania). Występują one również w kombinacji długości trwania awarii i jej zasięgu, a odpowiednią tabelę przedstawiającą te kombinacje można znaleźć w raporcie.

Jeśli chodzi o incydenty zgłaszane do amerykańskiego zespołu ICS-CERT to w 2012 r. do zespołu zgłoszono 198 incydentów, natomiast w 2013 r., już w pierwszym półroczu fiskalnym (październik 2012 r. – maj 2013 r.), zgłoszono 200 incydentów. Ponad połowa z nich (53%) dotyczy sektora energetycznego, a najczęściej spotykane ataki to SQL *Injection, spear-phishing,* czyli dedykowany *phishing* na konkretne osoby oraz *„watering hole*[5]*"* atak dla tych, którzy są „odporni" na *„spear-phishing"*. Jak widać w przypadku amerykańskim mamy bardziej szczegółowe dane dotyczące natury ataku.

Rysunek 11. Podział incydentów obsłużonych przez ICS-CERT w I połowie 2013 r. Podział w odniesieniu do poszczególnych sektorów. Źródło: ICS-CERT Monitor, Kwiecień, Maj, Czerwiec 2013.



Podsumowanie

Treść rozdziału odnosi się do zadań jakie stoją przed podmiotami odpowiedzialnymi za reagowanie na incydenty mające miejsce w systemach teleinformatycznych IK. W tym celu dokonane zostało odwołanie do przykładu amerykańskiego. Autor analizuje także rodzaje incydentów odnotowanych w teleinformatycznym środowisku TIK odwołując się do danych ENISA. Pokazują one, że w dużej mierze dotyczyły one problemów wynikających z sytuacji nie wywołanych działaniem intencjonalnym. Na podstawie amerykańskich danych wskazane zostały także sektory IK w których odnotowano najwięcej incydentów. Analiza pokazała, że sektor związany z energią był tym, w którym wystąpiło najwięcej incydentów.

5 Zob. RSA, *Lions at the Watering Hole – The "VOHO" Affair*, https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/.

10. Koncepcja rozwoju zdolności w obszarze cyberbezpieczeństwa infrastruktury krytycznej państwa

Ryszard Antkiewicz, Michał Dyk, Rafał Kasprzyk, Andrzej Najgebauer, Dariusz Pierzchała, Zbigniew Tarapata – Zespół Badawczy Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Konfliktowych i Kryzysowych, Instytut Systemów Informatycznych, Wydział Cybernetyki, Wojskowa Akademia Techniczna, Mirosław Maj – Fundacja Bezpieczna Cyberprzestrzeń

W rozdziale przedstawiono koncepcję pakietu narzędzi informatycznych zwiększających efektywność wykrywania, przeciwdziałania i neutralizacji skutków cyberzagrożeń. Narzędzia te powinny umożliwić skuteczną identyfikację i klasyfikację zagrożeń płynących z cyberprzestrzeni oraz analizę podatności, w oparciu o dane gromadzone przez sieć sensorów oraz skanery podatności, a następnie ułatwiać efektywne wykorzystanie mechanizmów przeciwdziałania i neutralizacji niebezpieczeństwa. Fundamentem prezentowanej koncepcji jest propozycja budowy autorskiej taksonomii oraz modeli formalnych i wzorców cyberzagrożeń. Będzie to podstawą opracowania metod: ich identyfikacji i klasyfikacji, wykrywania i analizy podatności systemów teleinformatycznych, optymalizacji zarówno sieci sensorów, jak i wykorzystania mechanizmów przeciwdziałania i neutralizacji skutków cyberzagrożeń. Prezentowana koncepcja wpisuje się w obszar obronności i bezpieczeństwa państwa w zakresie osiągania nowych zdolności obronnych – obrona cyberprzestrzeni państwa (ang. *Cyber Defence*) – i może mieć szerokie zastosowania wykraczające poza obszar *stricte* wojskowy, a obejmujący np. zarządzanie kryzysowe na różnych szczeblach administracji państwowej i samorządowej.

Cyberprzestrzeń

Początek XXI wieku zdominowany został przez procesy globalizacji oraz gwałtowny rozwój Internetu i innych sieci telekomunikacyjnych. Zauważalne staje się coraz większe uzależnienie administracji państwowej, instytucji prywatnych i całego społeczeństwa od prawidłowego funkcjonowania sieci komunikacyjnych i systemów informatycznych. Sam Internet coraz częściej postrzegany jest jako infrastruktura niezwykle wrażliwa, od której zależy bezpieczeństwo państwa. Aby przeprowadzić skuteczny atak na tę infrastrukturę krytyczną (IK) nie trzeba mobilizować sił zbrojnych. Człowiek wyposażony w standardowe technologie komputerowe,

* Kierownikiem Zespołu jest prof. WAT, dr hab. inż. Andrzej Najgebauer.

posiadający odpowiednią wiedzę, może przeprowadzić cyberatak o skutkach wręcz katastrofalnych dla współczesnego systemu polityczno-gospodarczego. Dlatego niezwykle ważne jest, aby umieć w porę wykryć, przeciwdziałać i neutralizować skutki tego typu zagrożeń.

Pojęcie cyberprzestrzeni pojawiło się po raz pierwszy w 1982 r. w opowiadaniu „Burning Chrome" Williama Forda Gibsona, a następnie w jego noweli „Neuromancer", do określenia „strefy mimowolnej halucynacji" (ang. *mass consensual hallucination*) generowanej przez sieci komputerowe. Cyberprzestrzeń rozumiana była przez Gibsona jako przestrzeń wypełniona danymi i/lub informacją, do której fizycznie mogli się przedostać bohaterowie. Obecnie mianem cyberprzestrzeni określa się przede wszystkim wirtualną przestrzeń otwartego komunikowania się za pośrednictwem sieci komputerowych lub innych mediów cyfrowych (np. telefonii komórkowej). Definicję taką sformułował Pierre Levy w tekście „Deuxieme Déluge" („Drugi Potop"). Trudno jednak mówić o powszechnie obowiązującej definicji cyberprzestrzeni. Wskazuje się natomiast pewne cechy, które ją charakteryzują: płynny, plastyczny, niematerialny charakter; brak możliwości jednoznacznego/wyraźnego określenia granic; zdecentralizowanie; brak ośrodka kontroli i nadzoru nad jej całością; powszechna dostępność; cyfrowe przetwarzania informacji i dokonywanie obliczeń w czasie rzeczywistym z dużą dokładnością; numeryczny, hipertekstowy, interaktywny i wreszcie wirtualny charakter.

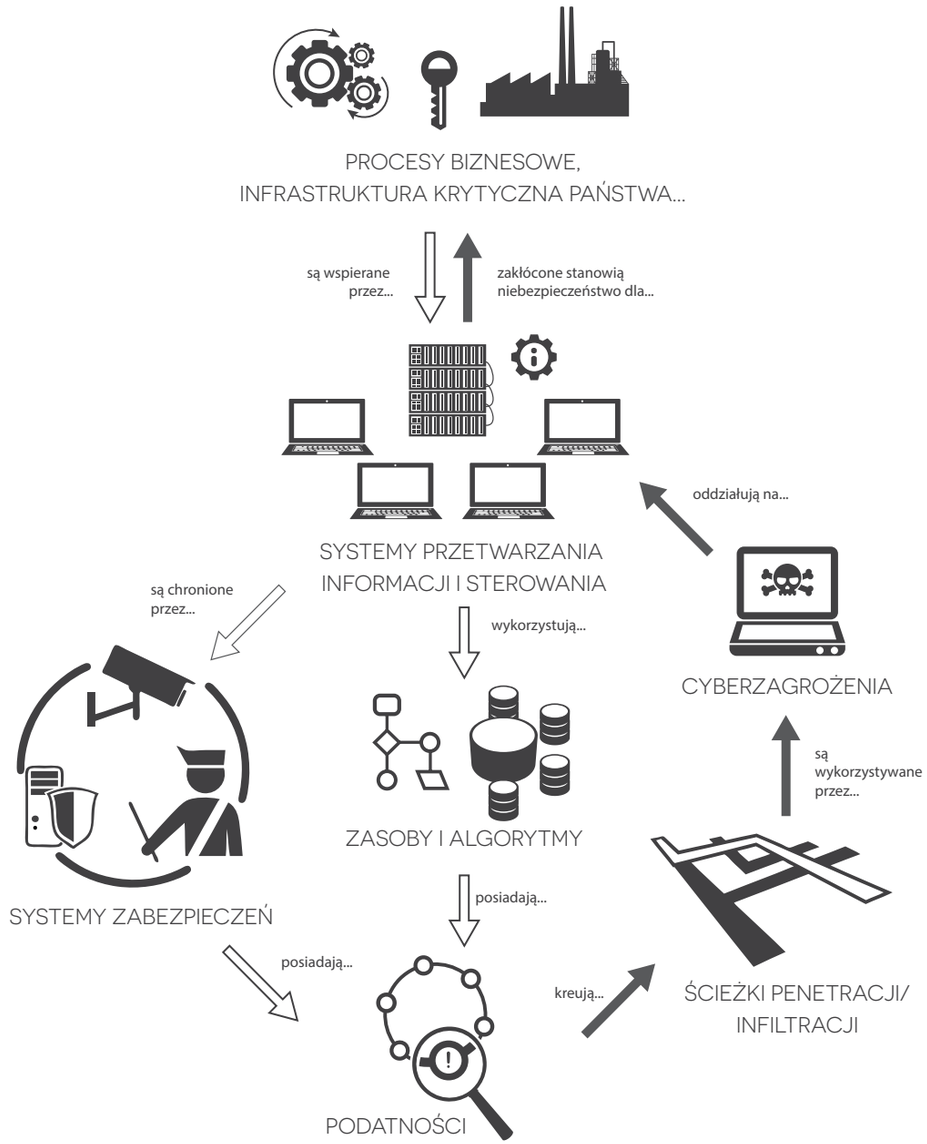
Kluczowym czynnikiem determinującym powodzenie realizacji prezentowanej koncepcji będzie więc definicja podstawowych pojęć związanych z cyberprzestrzenią i zjawiskami w niej zachodzącymi, jak również ustalenie zależności między tymi elementami. W ramach koncepcji szczególny nacisk położony zostanie na budowę taksonomii i modeli matematycznych cyberzagrożeń. Idea tego podejścia została przedstawiona na Rys.12.

Cyberprzestrzeń została spopularyzowana przez gwałtowny rozwój Internetu (dlatego też obydwa terminy są często stosowane zamiennie). W tym kontekście cyberprzestrzeń może być rozumiana jako przestrzeń wytwarzania, gromadzenia, przetwarzania i wymiany informacji, która jest „generowana" przez współpracujące ze sobą systemy teleinformatyczne. Jest ona również postrzegana jako nowy typ przestrzeni społecznej, w której „spotykają" się ludzie. Ze względu na wymienione wyżej cechy, cyberprzestrzeń coraz częściej postrzegana jest jako przestrzeń niezwykle wrażliwa na ataki. Zwraca się szczególną uwagę na fakt, że Internet nie może być traktowany jako podmiot prawa i nie jest też jego przedmiotem, co powoduje że nie istnieje żadna osoba fizyczna bądź prawna odpowiedzialna za to, co się dzieje w sieci jako całości. Nie można wykluczyć jako cyberagresora zarówno podmiotów państwowych (cyberwojna), jak i pozapaństwowych (cyberprzestępcy, cyberterroryści), co stanowi olbrzymie wyzwanie dla większości współczesnych państw.

Warto dodać także, że na gruncie polskim obowiązuje definicja cyberprzestrzeni zgodnie z ustawą z dnia 30 sierpnia 2011 r. *o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (Dz. U. z 2011 r. Nr 222, poz. 1323)[1].

1 Przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.3), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

Rysunek 12. Schemat zależności między podstawowymi pojęciami z obszaru cyberprzestrzeni.
Źródło: opracowanie własne, ikony pochodzą z The Noun Project.



Koncepcja realizacji pakietu narzędzi informatycznych zwiększających efektywność wykrywania, przeciwdziałania i neutralizacji skutków cyberzagrożeń

Zdolności do zapewnienia cyberbezpieczeństwa IK państwa obejmują dysponowanie przygotowanym personelem, procedurami, organizacją, narzędziami i doktryną. Prezentowana koncepcja dotyczy jedynie opracowania narzędzi i procedur. Osobnym zagadnieniem, wymagającym uzupełnienia, jest opracowanie doktryny ich wykorzystania, stosownej organizacji w skali państwa i poszczególnych instytucji oraz szkolenia i utrzymania w gotowości odpowiedniego personelu.

Proponowany pakiet narzędzi informatycznych opiera się zasadniczo na wykorzystaniu modeli matematycznych zagrożeń w cyberprzestrzeni i podatności chronionych systemów, oraz metod matematycznych pozwalających na identyfikację i ocenę zagrożeń, ocenę stopnia podatności oraz optymalizację struktury, parametrów i sposobu działania systemu zapewnienia cyberbezpieczeństwa. Wykorzystanie wspomnianych modeli i metod w obszarze bezpieczeństwa w cyberprzestrzeni nie jest podejściem całkowicie nowym. Jednak, wydaje się, że proponowana koncepcja wyróżnia się kompleksowością oraz uwzględnieniem zagadnień do tej pory słabo rozpoznanych, takich jak: optymalizacja sieci sensorów oraz mechanizmów przeciwdziałania atakom cybernetycznym czy ulepszanie mechanizmów neutralizacji skutków wystąpienia cyberataków.

Opracowanie takiego pakietu narzędzi informatycznych możliwe będzie poprzez realizację następujących zadań cząstkowych:

Zadanie. 1: Opracowanie taksonomii oraz założeń do modeli formalnych cyberzagrożeń

W ramach zadania dokonany zostanie przegląd istniejących taksonomii oraz ich ocena pod kątem przydatności do budowy narzędzi informatycznych zwiększających efektywność wykrywania, przeciwdziałania i neutralizacji skutków cyberzagrożeń. Wynikiem przeglądu będzie rekomendacja jednej z przeanalizowanych taksonomii, jej adaptacja lub propozycja autorskiego katalogu cyberzagrożeń, będącego podstawą realizacji kolejnych zadań. Przeanalizowane powinny zostać między innymi takie klasyfikacje jak: eCSIRT.net (ang. *The European CSIRT Network*), CVE (ang. *Common Vulnerabilities and Exposures*), *Common Language for Incident Response*, CAPEC (ang. *Common Attack Pattern Enumeration and Classification*). W procesie analizy i oceny standardów możliwych do wykorzystania przy modelowaniu zagrożeń uwzględnione powinny zostać ponadto następujące standardy: OVAL (ang. *Open Vulnerability and Assessment Language*), XCCDF (ang. *Extensible ConfigurationChecklist escription Format*), OCIL (ang. *Open Checklist Interactive Language*), IODEF (ang. *Incident Object Description Exchange Format*), CCE (ang. *Common Configuration Enumeration*), CPE (ang. *Common Platform Enumeration*).

Prezentowana koncepcja zakłada, że w ramach zadania opisane zostaną również schematy/procedury realizacji wybranych rodzajów ataków (najistotniejsze z punktu widzenia bezpieczeństwa państwa, w szczególności ukierunkowane na IK) z opracowanego katalogu cyberzagrożeń.

Zadanie 2: Opracowanie modeli formalnych i wzorców dla wybranych cyberzagrożeń

Realizacja zadania polegać będzie na opracowaniu modeli matematycznych wybranych (istotnych z punktu widzenia bezpieczeństwa państwa) cyberzagrożeń z katalogu cyberzagrożeń (wynik zadania 1), które będą stanowiły podstawę metod identyfikacji i klasyfikacji cyberzagrożeń (wynik zadania 4). Budowa modelu matematycznego wymaga rozpoznania „taktyk, technik i procedur" – TTP (ang. *Tactics, Techniques and Procedures*) stosowanych w cyberprzestrzeni do przeprowadzania ataków, w szczególności zidentyfikowanych i opisanych w zadaniu 1 oraz podatności systemów teleinformatycznych (wynik zadania 3).

Szczegółowa analiza metod ataków wymaga dostępu do danych historycznych na temat zaistniałych i zidentyfikowanych ataków oraz udziału ekspertów z obszaru bezpieczeństwa teleinformatycznego. Pozwoli to na ustalenie istotnych parametrów modeli matematycznych, będących podstawą identyfikacji i klasyfikacji cyberzagrożeń. Kolejnym krokiem będzie opracowanie wzorców (sparametryzowanych modeli) dla wybranych rodzajów cyberzagrożeń. Zakłada się również, że opracowane modele matematyczne i wypracowane wzorce powinny zostać wykorzystane do opisu i identyfikacji nowych cyberzagrożeń. Pozwoli to na uwzględnienie także niespotykanych wcześniej zagrożeń, stanowiących swego rodzaju anomalie (odstępstwo od wzorców sytuacji „normalnych/typowych").

Zadanie 3: Opracowanie metod analizy podatności systemów IT na cyberataki

Opracowanie metod analizy podatności systemów teleinformatycznych musi być poprzedzone zdefiniowaniem modelu formalnego, opisującego podatności dla wybranych warunków pracy systemów teleinformatycznych. Model ten pozwoli na konstrukcję wzorców podatności (sygnatur). Na tej podstawie zostaną opracowane metody skutecznego wykrywania podatności, jednocześnie generujące niewielką liczbę zgłoszeń typu *false-positive*. Metody identyfikowania podatności będą uwzględniały warunki pracy systemów teleinformatycznych (w szczególności: rodzaj środowiska teleinformatycznego oraz rodzaje cyberzagrożeń). Oprócz standardowych środowisk sieci LAN, należy rozważyć systemy teletransmisyjne i informatyczne występujące w sieciach obsługujących IK, w tym systemy sterowania przemysłowego – SCADA (ang. *Supervisory Control And Data Acquisition*).

Metody analizy podatności pozwolą na szacowanie konsekwencji skutecznego wykorzystania konkretnych podatności przy uwzględnieniu rodzaju zagrożenia oraz specyfiki środowiska, w którym podatność może występować.

W ramach realizacji zadania przeanalizowane powinny zostać wykorzystywane standardy opisu podatności, które mogą wpłynąć na model formalny i metodę analizy podatności, m.in.: CVSS (ang. *Common Vulnerability Scoring System*), CCSS (ang. *Common Configuration Scoring System*).

Zadanie 4: Opracowanie metod identyfikacji i klasyfikacji cyberzagrożeń

Realizację zadania rozpocząć należy od przeglądu istniejących metod oraz narzędzi identyfikacji i klasyfikacji cyberzagrożeń. Prezentowana koncepcja przewiduje w szczególności rozważenie wykorzystania metod opartych na analizie szeregów czasowych, sieci stochastycznych, a w tym sieci bayesowskich oraz ukrytych modeli Markowa (ang. *Hidden Markov Model*), sieci Petriego, modeli grafów ataku, modeli sieci społecznościowych (w aspekcie modelowania botnetów) oraz modeli growych. Ważnym wyróżnikiem prezentowanego podejścia jest naturalne założenie, że cyberzagrożenia mogą mieć charakter złożony. Oznacza to, że w tym samym czasie przeciwko ustalonemu systemowi mogą być realizowane dwa (lub więcej) różne ataki. Jeden z tych ataków może mieć zadanie zaabsorbowania uwagi zespołu chroniącego system i ułatwić realizowanie drugiego, właściwego ataku. Istotny wpływ na ostateczną postać metod identyfikacji i klasyfikacji cyberzagrożeń będzie miał opracowany katalog cyberzagrożeń (wynik zadania 1) oraz modele formalne i wzorce wybranych (istotnych z punktu widzenia bezpieczeństwa państwa) rodzajów cyberzagrożeń (wynik zadania 2).

Opracowane algorytmy identyfikacji i klasyfikacji cyberzagrożeń będą determinowały prace w zadaniach związanych z zasadami funkcjonowania sensora (zadanie 5), zarządzaniem (zadanie 6) i optymalizacją (zadanie 8) siecią sensorów.

Zadanie 5: Opracowanie zasad funkcjonowania sensora

W ramach zadania dokonany powinien zostać przegląd urządzeń i technologii wykorzystywanych do realizacji funkcji sensora sieciowego. Rozważa się wykorzystanie pasywnych sond typowych dla systemów o funkcjonalnościach HIDS (HIDS – ang. *Host Intrusion Detection System*) oraz NIDS (NIDS – ang. *Network Intrusion Detection System*), jak również metod zbierania reprezentatywnych próbek podejrzanego ruchu sieciowego np. z wykorzystaniem technik typu „garnek miodu". Sensory powinny zbierać dane istotne z punktu widzenia metody identyfikacji i klasyfikacji cyberzagrożeń, a z drugiej strony metoda identyfikacji i klasyfikacji cyberzagrożeń powinna być w stanie skutecznie działać w oparciu o dane, które sensory są w stanie dostarczyć – stąd niezwykle istotna jest koordynacja zadań 4 i 5.

Rozważa się dwie podstawowe funkcje sensorów tj. związane z analizą ruchu sieciowego i śledzeniem wykonywania oprogramowania. Pierwsza z nich powinna umożliwić np. badanie zawartości przesyłanych pakietów, wykrywania ruchu/komunikacji z określonymi adresami w sieci (w szczególności z tzw. *„darknetem"*, czyli tym obszarem Internetu, który nie powinien występować w ruchu sieciowym), czy w końcu wskazywać zmianę charakterystyki ruchu.

Druga funkcja powinna z kolei umożliwić np. wykrywanie nietypowych lub niedozwolonych wywołań systemowych, które wskazywałyby na przejęcie kontroli nad procesem i modyfikację jego właściwego trybu wykonania.

W wyniku realizacji zadania wypracowane zostaną również rekomendacje, co do możliwych i właściwych miejsc rozmieszczenia sensorów w monitorowanej sieci teleinformatycznej.

Zadanie 6: Opracowanie metody zarządzania siecią sensorów

Zasady funkcjonowania sensora opracowane w zadaniu 5 będą podstawą do opracowania metody zarządzania siecią sensorów. Zorganizowanie pojedynczych elementów w sieć wymaga opracowania mechanizmów, które obejmować powinny metody komunikacji pomiędzy sensorami, zarządzanie ich zasobami oraz sposób pozyskiwania danych z sieci jako całości. Kluczowe dla komunikacji pomiędzy sensorami jest opracowanie algorytmów trasowania oraz efektywnych metod pozyskiwania danych (obserwacji), tak aby nie było konieczności „odpytywania" pojedynczych sensorów. Zakłada się wprowadzenie pewnej hierarchii w sieci z wyróżnionymi węzłami stanowiącymi swego rodzaju koncentratory danych gromadzących i udostępniających dane z sensorów „podległych".

Istotną determinantą metody zarządzania siecią będą metody identyfikacji i klasyfikacji cyberzagrożeń (wynik zadania 4). Właściwe funkcjonowanie sieci sensorów powinno bowiem pozwolić na pozyskiwanie i gromadzenie danych, które są danymi wejściowymi niezbędnymi do identyfikacji i klasyfikacji cyberzagrożeń. Z kolei sama metoda ich identyfikacji i klasyfikacji, przy założeniu posiadania danych z sieci sensorów, sprowadzać się będzie do fuzji zgromadzonych danych, a w konsekwencji wykorzystania opracowanych algorytmów wnioskowania o zaistniałym niebezpieczeństwie i algorytmów klasyfikacji zidentyfikowanych cyberzagrożeń.

Prace nad tym zadaniem oraz zadaniami 7 i 8 wymagają ścisłej koordynacji, gdyż algorytmy optymalizacji sieci sensorów (wynik zadania 8) będą miały bezpośredni wpływ na metody (algorytmy) jej zarządzania.

Zadanie 7: Opracowanie modelu matematycznego sieci sensorów

Model matematyczny sieci sensorów może zostać zdefiniowany z wykorzystaniem języka teorii grafów i sieci. Struktura tej sieci modelowana mogłaby być z wykorzystaniem grafu, a do opisu ilościowego wykorzystane byłyby grafy opisane ilościowo (tzw. grafy ważone, sieci formalne). Elementami struktury będą wówczas sensory (reprezentowane przez węzły grafu) i kanały komunikacyjne między nimi (reprezentowane przez krawędzie/łuki grafu).

Parametry pracy sensorów i kanałów komunikacyjnych opisywane będą przez funkcje opisane odpowiednio na węzłach i krawędziach/łukach grafu (sieci formalnej). Wspomniane parametry wynikać będą z technicznej realizacji sieci sensorów opisanej w ramach zadań 5 i 6. Istotnym

elementem modelu będzie również matematyczny opis samego środowiska pracy sensorów, którym jest istniejąca infrastruktura sieciowa, a także rozmieszczenie sensorów (sieci sensorów) w tym środowisku.

Model ten stanowił będzie podstawę m.in. do opracowania algorytmów optymalizacji sieci sensorów (zadanie 8), zatem finalnie wpłynie na postać metody zarządzania siecią sensorów (zadanie 6).

Zadanie 8: Opracowanie algorytmów optymalizacji sieci sensorów

Zakłada się, że opracowywane algorytmy dotyczyć będą optymalizacji sieci sensorów, której zasadniczym zadaniem ma być zbieranie danych na potrzeby wczesnego identyfikowania i klasyfikowania potencjalnych cyberzagrożeń (zadanie 4). Optymalizacja powinna obejmować zarówno etap planowania struktury sieci (w tym rozmieszczenia węzłów sieci), jak również parametrów oraz ilościowych charakterystyk jej pracy. Wykorzystany powinien zostać grafowo-sieciowy model matematyczny sieci sensorów opracowany w zadaniu 7, teoria kolejek, jak również symulacja komputerowa, której zastosowanie pozwala na rozwiązanie wielu praktycznych problemów, w szczególności, kiedy ich złożoność uniemożliwia uzyskanie rozwiązania analitycznego (klasycznymi metodami).

Opracowane algorytmy powinny umożliwiać optymalizację sieci sensorów z punktu widzenia takich kryteriów, jak m.in.: niezawodność (zdolność do działania mimo występowania awarii), odporność na niszczenie czy zakłócenia sensorów i kanałów komunikacyjnych, koszt budowy oraz efektywność zbierania danych o incydentach (symptomach cyberzagrożeń). Koniecznym jest więc sformułowanie i rozwiązanie wielokryterialnego zadania optymalizacji struktury sieci sensorów. Ulepszanie parametrów i charakterystyk pracy sieci o zoptymalizowanej strukturze dotyczyć powinno przede wszystkim szybkości przesyłania danych (zagadnienia routingu), co wymaga również sformułowania i rozwiązania wielokryterialnego zadania optymalizacji parametrów pracy sieci.

Zadanie 9: Opracowanie mechanizmów przeciwdziałania możliwości realizacji cyberataku

Po wykryciu cyberzagrożenia, w oparciu o metody identyfikacji i klasyfikacji cyberzagrożeń (wynik zadania 4) konieczne jest podjęcie działań mających na celu przeciwdziałanie czy też przerwanie możliwości realizacji cyberataku.

Przeciwdziałanie zagrożeniom rozumiane jest jako zespół czynności związanych z reagowaniem na sytuacje, w których zostało zidentyfikowane ryzyko cyberataku, natomiast sam atak jeszcze nie nastąpił. Przedmiotem zadania, oprócz mechanizmów mających na celu przeciwdziałanie zagrożeniom, będą również mechanizmy mające na celu przerwanie ataku na chronione obiekty. Zarówno w przypadku przeciwdziałania, jak i przerywania cyberataku należy założyć, że będą możliwe działania aktywne strony zaatakowanej Przykładowymi mechanizmami tego typu są m.in.: przerywanie trwających połączeń TCP; generowanie reguł filtrowania pakietów w czasie zbliżonym do rzeczywistego, czy przerywanie pracy wybranych procesów systemowych.

Należy zwrócić szczególną uwagę na fakt, że koniecznym jest wypracowanie nie tylko technicznych, ale również organizacyjnych procedur reagowania. Przeciwdziałanie możliwości realizacji cyberataku będzie skuteczne tylko w przypadku precyzyjnego i możliwego do stosowania w praktyce (w tym uwzględniającego wszelkie regulacje prawne) określenia zasad współpracy pomiędzy różnymi podmiotami, np.: operatorami telekomunikacyjnymi, dostawcami treści, firmami hostingowymi, centrami danych i zespołami reagującymi. Jest to konieczne chociażby dla skutecznego wykorzystania efektywnej metody *„notice and take-down"* (powiadomienie o naruszeniu bezpieczeństwa i likwidacja zagrożenia w przypadku zasadnego zgłoszenia).

Zadanie 10: Optymalizacja mechanizmów przeciwdziałania możliwości realizacji cyberataku

Zadanie optymalizacji mechanizmów (technicznych i organizacyjnych) przeciwdziałania możliwości wystąpienia wybranych rodzajów cyberzagrożeń bazuje na wynikach zadania 9. Należy je ocenić z punktu widzenia różnego rodzaju kryteriów (efektywność, koszt wdrożenia, koszt wykorzystania, czas potrzebny na wykorzystanie mechanizmu, itp.). Kryterium efektywności należy tu rozumieć dwojako. Z jednej strony istotna jest ocena skuteczności zapobiegania zagrożeniom. Jednak wprowadzanie różnych mechanizmów ochrony (np. filtrów sieciowych – *firewall*), powoduje opóźnienia w realizacji zasadniczych zadań chronionych systemów. Zatem istotna jest również ocena wpływu tych mechanizmów na efektywność (opóźnienia, przepustowość) realizacji podstawowych funkcji systemu. Kryteria te należy wykorzystać do optymalizacji posiadanych mechanizmów przeciwdziałania możliwości wystąpienia wybranych rodzajów cyberzagrożeń. Zatem celem powinien być taki dobór mechanizmów oraz wypracowanie takiej ich konfiguracji, która będzie optymalna z punktu widzenia wybranych kryteriów przy zadanych zasobach (zwykle ograniczonych) i w określonych warunkach pracy systemu. Koniecznym jest więc sformułowanie i rozwiązanie wielokryterialnego zadania optymalizacji mechanizmów przeciwdziałania możliwości realizacji wybranych rodzajów cyberataków.

Zadanie 11: Opracowanie mechanizmów neutralizacji skutków wystąpienia cyberataków

Zadanie dotyczące opracowania mechanizmów do neutralizacji skutków wystąpienia wybranych rodzajów cyberataków jest zadaniem analogicznym do zadania 9. Zasadnicza różnica pomiędzy tymi zdaniami polega na tym, że większość działań neutralizujących skutki ataku przeprowadzana jest w obszarze tzw. ciągłości działania (ang. *constituency*) poszkodowanego oraz na konieczności uwzględnienia faktu, że mamy do czynienia z sytuacją, w której cyberatak okazał się skuteczny. Przykładowymi technicznymi mechanizmami neutralizacji ataków są np.: generowanie listy kryptograficznych skrótów plików binarnych i konfiguracyjnych; porównywanie list pomiędzy zadanymi punktami czasowymi; generowanie listy zmodyfikowanych plików, które powinny zostać przywrócone z kopii zapasowej, itp.

Przy tym należy zwrócić uwagę, że skutki cyberataku mogą się diametralnie różnić w zależności od sposobu reagowania na jego wystąpienie. Pierwsze fazy udanego natarcia zazwyczaj są przygotowaniem do fazy zasadniczej eksploracji systemów i nie wywołują jeszcze realnych strat. Dopiero brak prawidłowej reakcji na te ataki, co w sposób oczywisty wiąże się z umiejętnością ich wykrywania, może okazać się krytycznie niebezpieczny dla funkcjonowania podmiotu atakowanego i wymagać użycia mechanizmów neutralizacji skutków cyberzagrożeń.

W ramach zadania wypracowane powinny być nie tylko techniczne, ale również organizacyjne procedury neutralizacji skutków cyberzagrożeń, które są w szczególności istotne dla dużych podmiotów, w tym zarządzających IK państwa.

Zadanie 12: Optymalizacja mechanizmów neutralizacji skutków wystąpienia cyberataków

Zadanie optymalizacji mechanizmów neutralizacji skutków wystąpienia wybranych rodzajów cyberzagrożeń bazuje na wynikach zadania 11. Posiadając zbiór możliwych do zastosowania mechanizmów neutralizacji cyberzagrożeń, należy ocenić je z punktu widzenia różnego rodzaju kryteriów (efektywność, koszt wdrożenia, koszt wykorzystania, czas potrzebny na wykorzystanie mechanizmu, itp.). Kryteria te należy wykorzystać do optymalizacji posiadanych mechanizmów neutralizacji skutków wybranych rodzajów cyberzagrożeń, czyli celem powinien być taki dobór mechanizmów oraz wypracowanie takiej ich konfiguracji, która będzie optymalna z punktu widzenia wybranych kryteriów przy zadanych zasobach (zwykle ograniczonych) i w określonych warunkach pracy systemu. Koniecznym jest więc sformułowanie i rozwiązanie wielokryterialnego zadania optymalizacji mechanizmów neutralizacji skutków wybranych rodzajów cyberataków.

Podsumowanie

W rozdziale przedstawiono koncepcję pakietu narzędzi informatycznych zwiększających efektywność wykrywania, przeciwdziałania i neutralizacji skutków cyberzagrożeń. Tego typu rozwiązania stanowić powinny wsparcie dla właściwych służb państwowych oraz organizacji o charakterze CERT-owym. Wykorzystanie tego pakietu narzędzi powinno przyczynić się do uzyskania efektu synergii dzięki wsparciu koordynacji działań właściwych służb oraz automatyzację przepływu informacji.

Kluczowym dla umożliwienia wczesnego wykrycia zagrożenia jest właściwe rozmieszczenie sensorów (czujników, elementów filtrujących), co pozwoli na efektywne wykrywanie symptomów zagrożenia, a w konsekwencji również przeciwdziałanie zagrożeniom i neutralizacje ich skutków. Z tego też powodu, w przypadku realizacji opisanej w rozdziale koncepcji należałoby dodatkowo dokonać szczegółowej analizy uwarunkowań i ograniczeń prawnych mających wpływ na sposób rozmieszczenia sensorów. Jedną z wielu korzyści odpowiedniego ich rozmieszczenia jest możliwość identyfikacji komputerów korzystających z anonimizujących serwerów Proxy lub sieci TOR.

11. Analiza programu studiów wyższych w zakresie ochrony systemu sieci teleinformatycznych należącego do infrastruktury krytycznej

Krzysztof Rzecki – Politechnika Krakowska

Celem niniejszego rozdziału jest analiza programu studiów na kierunku informatyka pod kątem edukacji z zakresu ochrony sieci teleinformatycznych jako systemu IK. Sieci teleinformatyczne to jeden z jedenastu systemów należących do IK zdefiniowanych w Ustawie z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590, z późn. zm. zwana dalej: ustawą o zarządzaniu kryzysowym). Każdy z opisanych w Ustawie systemów składa się ze ściśle powiązanych ze sobą funkcjonalnie obiektów (w tym budowlanych), urządzeń, instalacji i (kluczowych) usług przez nie dostarczanych. Sieci teleinformatyczne są także elementem innych systemów IK wspierając, a często warunkując ich poprawne funkcjonowanie.

Teleinformatyka (ICT, ang. *Information and Communication Technologies*) to dziedzina nauki i techniki łącząca osiągnięcia informatyki i telekomunikacji w zakresie zagadnień związanych z szeroko rozumianym przesyłaniem informacji elektronicznej z użyciem różnych mediów oraz sterowaniem tej transmisji między urządzeniami sieciowymi.

Ochrona systemu sieci teleinformatycznych składa się z ochrony (systemów przetwarzania) informacji oraz ochrony systemów produkcyjnych i oba podejścia muszą być brane pod uwagę. Mimo bliskiego powiązania systemu sieci teleinformatycznych oraz systemu łączności, ten drugi nie będzie przedmiotem analizy z uwagi na dystans dzielący go od tematyki studiów kierunku informatyka. Przynależność danego elementu do systemu będzie zależała od konkretnego zastosowania tego elementu, a w szczególnych przypadkach dany element może należeć nawet do więcej niż jednego systemu.

Klasyfikacja przynależności poszczególnych części danej infrastruktury jako obiekt, urządzenie, instalacja czy usługa dla każdego systemu powinna być ściśle określona, lecz ze względu na powiązania i wielofunkcyjność tych części, klasyfikacja ta może być utrudniona. W przypadku sieci teleinformatycznych obiektami mogą być budynki wraz z wyposażeniem (zabezpieczeniami fizycznymi, ochroną ppoż., awaryjnym zasilaniem, itp.) zawierające serwerownie, węzły teleinformatyczne, centra obliczeniowe, itp. W zestawie urządzeń znajdą się zarówno urządzenia jak i oprogramowanie implementujące funkcjonalności sieci teleinformatycznych, a także sprzęt służący do ochrony tych sieci w omawianym zakresie. Instalacjami mogą być

zestawione urządzenia teleinformatyczne wraz z oprogramowaniem udostępniając określoną funkcjonalność, realizując określone procesy. Usługi teleinformatyczne polegają bowiem na przesyłaniu, przechowywaniu, przetwarzaniu, itp. danych.

Podstawa prawna

Ustawa z dnia 27 lipca 2005 r. *Prawo o szkolnictwie wyższym*[1] jest podstawowym, wyjściowym dokumentem określającym zasady funkcjonowania uczelni wyższych. Ustawa definiuje Krajowe Ramy Kwalifikacji dla Szkolnictwa Wyższego jako „opis, przez określenie efektów kształcenia, kwalifikacji zdobywanych w polskim systemie szkolnictwa wyższego". Z kolei efekty kształcenia to „zasób wiedzy, umiejętności i kompetencji społecznych uzyskanych w procesie kształcenia przez osobę uczącą się". Na podstawie oceny osiągniętych przez daną osobę efektów kształcenia, uprawniona instytucja wydaje dokument (dyplom, świadectwo, certyfikat lub inny dokument), który poświadcza kwalifikacje tej osoby. Kwalifikacje odnoszą się do określonego profilu kształcenia, czyli „profil praktyczny, obejmujący moduł zajęć służących zdobywaniu przez studenta umiejętności praktycznych albo profil ogólnoakademicki, obejmujący moduł zajęć służących zdobywaniu przez studenta pogłębionych umiejętności teoretycznych".

Krajowe Ramy Kwalifikacji dla Szkolnictwa Wyższego wydawane są w drodze rozporządzenia Ministra Nauki i Szkolnictwa Wyższego. W aktualnym rozporządzeniu z 2 listopada 2011 r. znajduje się załącznik 5, który dotyczy opisu efektów kształcenia w zakresie nauk technicznych, do których zaliczany jest m.in. kierunek Informatyka. Opis tych efektów uogólniony jest do wszystkich nauk technicznych, a zgodnie z zapisami Ustawy każda uczelnia ma prawo do „ustalania planów studiów i programów kształcenia, uwzględniających efekty kształcenia zgodnie z Krajowymi Ramami Kwalifikacji dla Szkolnictwa Wyższego [...]". Zatem autonomicznie senat każdej z uczelni drogą uchwały określa efekty kształcenia dla prowadzonych kierunków studiów.

Jeszcze do niedawna, przez wiele lat Ministerstwo Nauki i Szkolnictwa Wyższego udostępniało przygotowane standardy kształcenia. Standardy te służyły jako podstawa do określenia zakresu wiedzy na poszczególnych kierunkach studiów prowadzonych przez daną uczelnię wyższą. Mimo, że obecnie rolę standardów przejęły efekty kształcenia, to w licznych przypadkach efekty kształcenia są wynikiem płynnego przejścia właśnie z tych standardów i te właśnie były źródłem informacji poddanej do analizy.

Standardy kształcenia

Na liście kierunków studiów, dla których MNiSW przygotowało standardy kształcenia nie ma kierunku teleinformatyka, natomiast znajdują się tam dwa kierunki dotyczące informatyki:
- informatyka,
- informatyka i ekonometria.

W opracowaniach tych nie ma zapisów dotyczących edukacji bezpośrednio z zakresu IK, a w szczególności dotyczących sieci teleinformatycznych.

1 Ustawa z dnia 27 lipca 2005 r. *Prawo o szkolnictwie wyższym* (Dz. U. z dnia 21 kwietnia 2011 r. Nr 84, poz.455).

Z tematyki zbliżonej do tematyki ochrony IK znajdziemy:

- dla kierunku informatyka, w grupie treści kierunkowych dla studiów pierwszego stopnia treści kształcenia w zakresie technologii sieciowych zawierające „Bezpieczeństwo w sieciach komputerowych i kryptografia",

- dla kierunku informatyka i ekonometria w grupie treści podstawowych studiów pierwszego stopnia treści kształcenia w zakresie informatyki ekonomicznej zawierające „Bezpieczeństwo informacji i systemów informacyjnych",

- dla kierunku informatyka i ekonometria w grupie treści kierunkowych studiów pierwszego stopnia treści kształcenia w zakresie baz danych zawierające „Bezpieczeństwo danych".

Kierunki studiów, dla których MNiSW opracowało standardy kształcenia obejmujące zagadnienia związane z ochroną IK to:
- bezpieczeństwo narodowe,
- bezpieczeństwo wewnętrzne,
- inżynieria bezpieczeństwa.

W opracowaniu dla kierunku bezpieczeństwo narodowe, dla drugiego stopnia studiów w grupie treści podstawowych znajdują się treści kształcenia w zakresie prawa obronnego Rzeczypospolitej Polskiej zawierające „Prawo obronne w obszarze zapewnienia bezpieczeństwa i porządku publicznego, ochrony ludności, ochrony granicy państwowej, porządku konstytucyjnego, ochrony gospodarki i infrastruktury krytycznej." W opracowaniu dla kierunku bezpieczeństwo wewnętrzne, dla drugiego stopnia studiów w grupie treści kierunkowych znajdują się treści kształcenia w zakresie ochrony ludności i obrony cywilnej zawierające „Ochrona infrastruktury krytycznej" oraz „Zadania wynikające z zobowiązań sojuszniczych, ratyfikowanych umów i konwencji międzynarodowych w zakresie zarządzania kryzysowego, ratownictwa, ochrony ludności, planowania cywilnego oraz ochrony infrastruktury krytycznej". W opracowaniu dla kierunku inżynieria bezpieczeństwa, dla pierwszego stopnia studiów w grupie treści kierunkowych znajdują się treści kształcenia w zakresie modelowania zagrożeń zawierające „Prognozowanie zagrożeń związanych z infrastrukturą krytyczną, zatrucie ujęć wody". W tym samym opracowaniu dla pierwszego stopnia studiów, w grupie treści kierunkowych znajdują się treści kształcenia, które w całości odnoszą się do ochrony systemów IK, dotyczą zakresu technicznych systemów zabezpieczeń.

Na podstawie przedstawionej analizy standardów kształcenia stwierdzić można, że choć na kierunkach studiów związanych z informatyką MNiSW nie przewiduje kształcenia w zakresie zagadnień związanych z ochroną IK bezpośrednio, to w niewielkim zakresie treści kształcenia zawierają zagadnienia związane z bezpieczeństwem informacji. Natomiast treści kształcenia zawarte w standardach kształcenia dla kierunku inżynieria bezpieczeństwa omawiają problematykę ochrony systemów IK poświęcając temu jeden cały rozdział treści kształcenia.

Zarys zakresu wiedzy w edukacji dotyczącej ochrony systemu sieci teleinformatyczne

Aby możliwe było wskazanie właściwego zakresu wiedzy, która powinna stanowić materiał dydaktyczny dotyczący systemu sieci teleinformatyczne do przedstawienia na studiach wyższych kierunku informatyka, konieczne jest spojrzenie na system z perspektywy elementów, które wchodzą w jego skład. Zauważyć można wówczas, że podstawą ochrony obiektów będą aspekty najmniej związane z informatyką. Podobnie będzie w przypadku urządzeń, dla których ochrona stanowi pochodną ochrony obiektów. Dopiero instalacje, a najbardziej usługi stanowią elementy, które najsilniej związane są z informatyką i w których dobrze przygotowani absolwenci tego kierunku będą najlepiej przygotowaną kadrą do ochrony systemu sieci teleinformatyczne.

W innych rozdziałach tego opracowania przedstawiono różne aspekty i oraz zasadnicze różnice między dziedziną IT (IT – ang. *Information Technology*), a dziedziną OT (OT – ang. *Operational Technology*). W tym miejscu wskazane zostaną najbardziej podstawowe zagadnienia z nimi związane, na których bazują protokoły, procesy, technologie, itp. związane z ochroną systemu sieci teleinformatyczne. Podstawy te charakteryzują zakres wiedzy, który powinien być dostarczany studentom kierunku informatyka.

Zakres wiedzy w edukacji o ochronie informacji (systemy IT)

Operacje związane z informacją obejmują operacje proste, jak jej zmienianie, ale też bardziej złożone, jak jej pozyskiwanie, analizowanie, oczyszczanie, zaciemnianie, transformowanie, przetwarzanie, przechowywanie, backup, archiwizację, przesyłanie, itp. W przypadku, kiedy informacja ma znaczenie dla bezpieczeństwa treści, którą ta informacja niesie, każda z wymienionych operacji może uwzględniać aspekty bezpieczeństwa.

Ochronę sieci teleinformatycznych w rozumieniu ochrony informacji rozumieć należy z punktu widzenia podmiotu (osoba, instytucja, program komputerowy, itp.), którego celem jest dostęp do określonego zasobu (informacja, program komputerowy, itp.). Ochrona tego typu opiera się o kilka powiązanych ze sobą zagadnień stanowiących procesy (w skrócie):

- identyfikacja, czyli deklaracja tożsamości danego podmiotu,
- uwierzytelnianie, czyli potwierdzenie zadeklarowanej tożsamości,
- autoryzacja, czyli stwierdzenie czy i w jakim zakresie podmiot ma dostęp do zasobów,
- integralność, czyli stwierdzenie czy informacja posiada oryginalną postać,
- poufność, czyli zapewnienie, że nikt nieautoryzowany nie ma dostępu do informacji,
- niezaprzeczalność, czyli brak możliwości wyparcia się autorstwa informacji.

Do realizacji każdego z powyższych procesów stosuje się techniki związane z kryptografią, protokołami i algorytmami kryptograficznymi itp. Implementacja danego zagadnienia może być zarówno rozwiązaniem sprzętowym, jak i programowym. Na podstawie wymienionych procesów można projektować i budować rozwiązania na wyższym poziomie abstrakcji.

Zakres wiedzy w edukacji o ochronie systemów produkcyjnych (systemy OT)

Podstawowa wiedza o ochronie systemów produkcyjnych rozpoczyna się od umiejscowienia ich w gronie systemów wchodzących w skład typowej infrastruktury informatycznej przedsiębiorstwa. Szeregowanie to ma na celu zwrócenie uwagi na zależności z pozostałymi systemami, które mają (niekoniecznie bezpośredni) wpływ na procesy produkcyjne. Wymieniając od najwyższego stopnia zarządzania przedsiębiorstwem mamy:

- EIS, ang. *Executive Information System* – system informowania kierownictwa.
- SCM, ang. *Supply Chain Management* – zarządzanie łańcuchami dostaw.
- ERP, ang. *Enterprise Resource Planning* – zarządzanie zasobami przedsiębiorstwa.
- MRP, ang. *Manufacturing Resource Planning* – planowanie zasobów produkcyjnych.
- MES, ang. *Manufacturing Execution System* – system realizacji produkcji.
- LIMS, ang. *Laboratory Information System* – system komunikacji z laboratorium.
- PCS, ang. *Process Control System* – system kontroli procesu.
- SCADA, ang. *Supervisory Control & Data Aquisition* – system nadzorczy procesu produkcyjnego.
- DCS, ang. *Distributed Control System* – rozproszony system sterowania.
- PLC, ang. *Programmable Logic Controller* – system sterowania maszynami.

Można wymienić jeszcze inne systemy, ale przedstawiony zestaw wydaje się być najbardziej uogólnionym zbiorem. Biorąc pod uwagę, że chodzi o systemy znajdujące się na ścieżce związanej z procesami produkcyjnymi, pominięte zostały systemy takie jak HRM (ang. *Human Resource Management*), czy CRM (ang. *Customer Relationship Management*).

Za najważniejsze, z punktu widzenia IK, wskazywane są systemy klasy SCADA (i bezpośrednio z nimi powiązane, jak DCS i PLC). Jest to wynik dynamicznego charakteru działania tych systemów, a więc wrażliwości ich podatności na czynniki zewnętrzne.

Operacje wykonywane przez dany system komputerowy obejmują bardzo zróżnicowane czynności ściśle uzależnione od przeznaczenia danego systemu. W kwestiach związanych z bezpieczeństwem będą to przede wszystkim wszelkie aspekty, które obejmują:

- rozliczalność, czyli rejestrowanie zdarzeń w celu wskazania autora danej aktywności;
- monitorowanie, czyli bezinwazyjne obserwowanie przez analizowanie rejestrów zdarzeń;
- anonimowość, czyli własność systemu odwrotna do rozliczalności;
- dostępność, czyli udzielenie dostępu określonemu podmiotowi w miejscu i czasie;
- awaria, czyli stan niesprawności systemu uniemożliwiający jego normalne użytkowanie;
- niezawodność, czyli własność stwierdzająca prawdopodobieństwo, że awaria nie wystąpi;
- zagrożenie, czyli stan obniżonego bezpieczeństwa;
- ryzyko, czyli prawdopodobieństwo, że zagrożenie przekształci się w awarię;
- podatność, czyli wysokie ryzyko zmiany zagrożenia w awarię;
- zabezpieczenie, czyli obniżanie ryzyka zmaterializowania zagrożenia (awarii);
- redundancja/nadmiarowość, czyli utrzymywanie aktualnej kopii danego systemu;
- kopia/archiwum, czyli utrzymywanie wyłączonej kopii danego systemu;
- odtwarzanie, czyli przywracanie stanu systemu sprzed awarii.

Przedstawione powyżej zagadnienia wskazują obszary wiedzy, które dotyczą ochrony produkcyjnych systemów komputerowych. Bazując na nich definiowane są potrzeby i możliwości ich zaspokojenia w zakresie tej ochrony i na wyższym poziomie abstrakcji znajdą się:

- systemy identyfikacji/autoryzacji/uwierzytelniania;
- systemy monitorowania/logowania/reagowania;
- systemy przeciwwirusowe/antymalware/antyspamowe;
- systemy ochrony sieciowej/firewalle;
- systemy wykrywania włamań/ataków penetracyjnych;
- procedury prowadzenia backupu/archiwizacji/kopii bezpieczeństwa;
- procedury przywracania systemu/odtwarzania danych;
- systemy i procedury zarządzania konfiguracją/zmianą/incydentem;
- itp.

Podsumowanie

Przedstawiona w niniejszym rozdziale analiza programu studiów wyższych wykonana została na bazie publikowanych do niedawna standardów, sukcesywnie wypieranych przez efekty kształcenia. Analiza ta porusza zagadnienia związane z edukacją w zakresie ochrony systemu sieci teleinformatyczne należącego do IK.

Programy kształcenia, które bazują tylko na standardach Ministerstwa Nauki i Szkolnictwa wyższego i związane są z kierunkami informatycznymi w swoim zakresie nie obejmują zagadnień ściśle związanych z ochroną IK, aczkolwiek jak najbardziej obejmują większość zagadnień związanych z ochroną informacji oraz systemów produkcyjnych. Wśród programów kształcenia są przynajmniej trzy kierunki studiów, które traktują o ochronie IK, ale żaden z nich nie specjalizuje się w ochronie systemu sieci teleinformatyczne w zakresie elementów takich jak instalacje, czy usługi.

Aby kształcenie na kierunku informatyka dawało przygotowanie z zakresu ochrony systemu sieci teleinformatyczne należy za podstawę przyjąć zakres zagadnień wymienionych we wcześniejszej części rozdziału, a dotyczących ochrony informacji i systemów produkcyjnych. Zdecydowanie jednak należałoby wprowadzić wykład mający na celu przedstawienie cech charakterystycznych dziedziny ochrony IK, aby przekazać wiedzę i przećwiczyć umiejętności, które pozwolą odpowiedzieć na pytania:

- co chronić (jaką informację) i dlaczego;
- co monitorować i dlaczego;
- co powinno być niezawodne i dlaczego;
- co archiwizować i dlaczego;
- itp.

Zatem, to co należałoby wprowadzić jeszcze, to umiejętność odpowiedzi na pytanie „co" oraz „dlaczego", gdyż „jak to robić" w dużej mierze jest już realizowane.

Ponowna analiza programu studiów, ale wykonana nie wcześniej niż za rok, powinna bazować już nie na standardach nauczania, ale bezpośrednio na opisach efektów kształcenia opracowanych przez poszczególne uczelnie.

Czynniki wpływające na bezpieczeństwo i rekomendacje

Opracowane przez Zespół Instytutu Kościuszki
w oparciu o poszczególne rozdziały

Poniżej zaprezentowane zostaną najważniejsze czynniki wpływające na ogólne bezpieczeństwo IK (oparte o kluczowe wnioski z części pierwszej raportu) oraz na bezpieczeństwo teleinformatyczne IK (wnioski z części drugiej). Czynniki odwołujące się do bezpieczeństwa IK zaprezentowane zostaną jako elementy ogólnego procesu, który ma doprowadzić do osiągnięcia założonego celu (bezpieczeństwa IK jako całości). Natomiast czynniki wpływające na bezpieczeństwo teleinformatyczne IK przedstawione zostaną za pomocą Diagramu Ishikawy, który pomaga nie tylko pogrupować poszczególne elementy, ale także odkryć nieujawnione uprzednio związki pomiędzy poszczególnymi przyczynami stanowiąc swoistą mapę rozpatrywanego zagadnienia.

Zdiagnozowane i zaprezentowane czynniki zarówno dotyczące bezpieczeństwa IK, jak i bezpieczeństwa teleinformatycznego IK należy czytać jako szanse i słabości wpływające na wskazane cele związane z bezpieczeństwem.

Podobny podział zastosowany został w odniesieniu do rekomendacji. Pierwsza grupa odnosi się do kwestii ogólnosystemowych, druga do problemów bardziej szczegółowych związanych z aspektem teleinformatycznym. Niezależnie od podziału, oba zestawy należy traktować komplementarnie.

Czynniki determinujące efektywne zapewnianie bezpieczeństwa IK

1. Wyznaczanie kierunków rozwoju IK, zarządzanie wiedzą oraz działania edukacyjno – uświadamiające
   1.1. kampania edukacyjna w zakresie zagrożeń i konieczności podejmowania działań związanych z bezpieczeństwem;
   1.2. specjalistyczna edukacja na poziomie akademickim;
   1.3. promowanie wiedzy o mechanizmach prawnych, np. o zamówieniach publicznych.

2. Budowanie efektywnej współpracy prywatno – publicznej:
   2.1. tworzenie systemu motywującego do efektywnej współpracy i zwiększania bezpieczeństwa;
   2.2. tworzenie sektorowych forów wymiany informacji z RCB jako instytucją „łącznikową";
   2.3. organizacja pracy forów.

3. Właściwa identyfikacja IK
   3.1. wiarygodne informacje warunkujące poprawność identyfikacji;
   3.2. rozważenie zaangażowania w identyfikacje IK podmiotów ze szczebli lokalnych;

4. Finansowanie działań związanych z zapewnianiem bezpieczeństwa.
   4.1. wsparcie finansowe dla właścicieli i operatorów IK w ponoszeniu kosztów budowy, utrzymania i ochrony IK (na przykład z funduszu celowego);
   4.2. promowanie unijnych źródeł finansowania.

Rekomendacje i postulaty

1. Rekomenduje się rozważenie możliwości uzupełnienia definicji IK w taki sposób, by nie pozostawiała wątpliwości, że obejmuje ona również infrastrukturę wirtualną (informacyjną), np. zbiory informacji z baz danych.

2. RCB powinno dążyć do postulowanej w NPOIK rezygnacji z kryteriów sektorowych, a tym samym zbliżyć się do podejścia „z dołu do góry" przy identyfikacji IK.

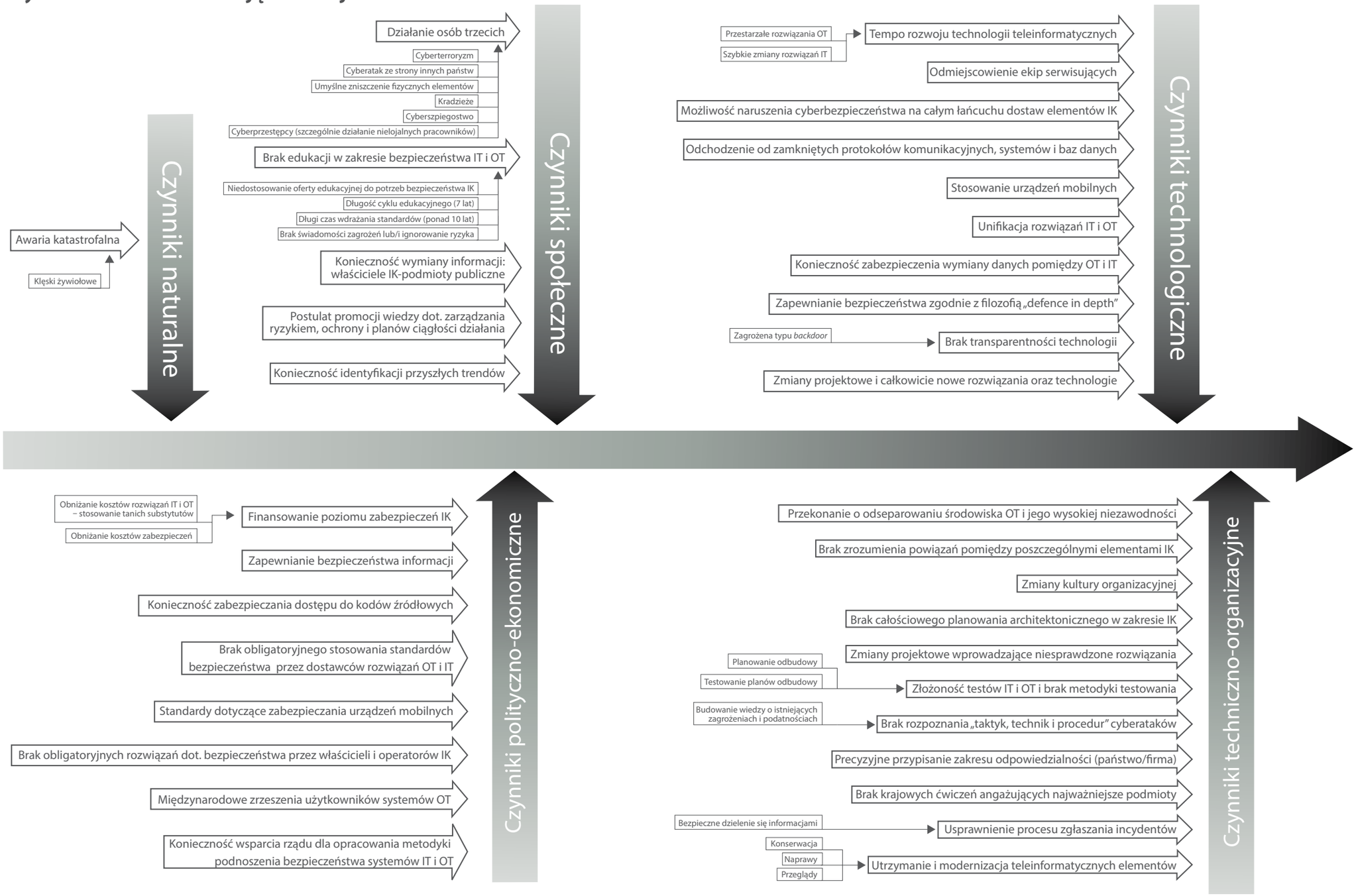
3. Państwo powinno stworzyć system bodźców (finansowych i niefinansowych)[1] zachęcających do podejmowania współpracy prywatno-publicznej, rzetelnego zapewniania bezpieczeństwa i działań samoregulacyjnych.

4. Sektorowe fora współpracy należy wzorować na najlepszych praktykach związanych z organizacją prac[2]. Podstawą winno stać się odejście od „klasycznego" hierarchicznego zarządzania na rzecz elastycznych i „sieciowych" rozwiązań.

5. Państwo powinno wspierać finansowo właścicieli IK w ponoszeniu kosztów budowy, utrzymania i ochrony IK (na przykład z funduszu celowego).

1 wstępna propozycja przedstawiona została w tekście.
2 patrz rozdział czwarty

Czynniki OT i IT determinujące funkcjonowanie IK



Rekomendacje i postulaty

1. Państwo powinno rozważyć nałożenie wymagań regulacyjnych i kontrolnych na dostawców rozwiązań OT i IT dla IK dotyczących spełnienia niezbędnego poziomu bezpieczeństwa (m.in. dostęp poprzez *escrow* do kodów).

2. Światowe standardy bezpieczeństwa systemów przemysłowych powinny zostać adaptowane do warunków polskich. Przykładowymi podmiotami jakie mogłyby tego dokonać to Polski Komitet Normalizacyjny, organizacje branżowe.

3. Rekomenduje się zapoczątkowanie dyskusji na temat regulacji wprowadzających wymogi stosowania przez właścicieli i operatorów IK określonych standardów IT w OT. Potencjalne regulacje powinny iść w parze z systemem bodźców motywujących (patrz rekomendacja 3 do części pierwszej).

4. Państwo powinno rozważyć finansowanie właścicielom i operatorom IK przeglądów bezpieczeństwa wybranych elementów systemów IT i OT oraz szkoleń w zakresie zarządzania ryzykiem IK, ochrony i planów ciągłości działania IK.

5. Zarówno państwo jak i podmioty branżowe oraz sami zainteresowani powinni wspierać i wdrażać działania związane ze zwiększeniem świadomości i edukacji w zakresie bezpieczeństwa IT i OT.

6. Rząd (za pomocą odpowiednich podmiotów) powinien prowadzić stałą identyfikację przyszłych trendów i przewidywanie zmian w dynamicznym otoczeniu (Foresight).

7. Powinno istnieć wsparcie działań na rzecz zrozumienia przez właścicieli i operatorów IK powiązań pomiędzy poszczególnymi elementami IK. W szczególności powinno dotyczyć to stosowania całościowego spojrzenia na aspekty zabezpieczania systemów teleinformatycznych.

8. Rekomenduje się tworzenie katalogu cyberzagrożeń. W tym kontekście postuluje się budowę krajowego centrum kompetencji w dziedzinie wiedzy o zagrożeniach o podatnościach, czyli polskiego podmiotu dysponującej wiedzą i narzędziami testującymi na światowym poziomie.

9. RCB powinno nieustannie wzmacniać i budować efektywne mechanizmy dzielenia się poufną informacja dotyczącą bezpieczeństwa IK pomiędzy operatorami IK w taki sposób, aby zachować bezpieczeństwo przekazywanych informacji.

10. Programy kształcenia związane z kierunkami informatycznymi obejmują zagadnienia związane z ochroną informacji oraz systemów produkcyjnych, lecz nie odnoszą się ściśle do tematyki infrastruktury krytycznej. Należy wprowadzić elementy edukacyjne mające na celu przedstawienie cech charakterystycznych dziedziny ochrony IK, aby przekazać wiedzę i przećwiczyć umiejętności. Powinno stać się to przedmiotem odpowiednich działań tak na poziomie uczelni wyższych jak i na poziomie samych właścicieli i operatorów IK.

11. Państwo powinno wspierać finansowo działania związane z badaniami i rozwojem w zakresie tworzenia między innymi krajowych narzędzi informatycznych zwiększających m.in. efektywność wykrywania, przeciwdziałania i neutralizacji skutków cyberzagrożeń. Np. w ramach NCBiR. W konsultacji z podmiotami prywatnymi stworzony winien zostać Narodowy Plan Rozwoju i Badań w zakresie cyberbezpieczeństwa zawierający na przykład: główne cele, priorytety oraz „mapę drogową" działań.

Aneks

Podkategoria	Odnośniki Informacyjne
ID.AM-1: Urządzenia i systemy w organizacji są zinwentaryzowane	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
ID.AM-2: Platformy oprogramowania i aplikacji w obrębie organizacji są zinwentaryzowane	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
ID.AM-3: Komunikacja w organizacji oraz przepływy danych są znane i opisane	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
ID.AM-4: Zewnętrzne systemy informacyjne są skatalogowane	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
ID.AM-5: Zasoby (np. sprzęt, urządzenia, dane i oprogramowanie) są ocenione na podstawie ich klasyfikacji, krytyczności i wartości biznesowej	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
ID.AM-6: Role w organizacji bezpieczeństwa i odpowiedzialności dla wszystkich pracowników i osób stron trzecich (np. dostawców, klientów, partnerów) są ustalone	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
ID.BE-1: Rola organizacji w łańcuchu dostaw jest zidentyfikowana i ogłoszona	· **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: Miejsce organizacji w infrastrukturze krytycznej i w jej sektorze przemysłu jest zidentyfikowane i ogłoszone	· **COBIT 5** APO02.06, APO03.01 · **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorytety dla misji organizacji, celów i działalności są ustalone i ogłoszone	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Zależności i funkcje krytyczne w zakresie świadczonych usług krytycznych są określone	· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Wymagania gotowości wspierania świadczonych sług krytycznych są określone	· **COBIT 5** DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
ID.GV-1: Polityka bezpieczeństwa informacji została określona	· **COBIT 5** APO01.03, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all families
ID.GV-2: Role w bezpieczeństwie informacji oraz odpowiedzialności są skoordynowane i dostosowane do zadań pracowników i partnerów zewnętrznych	· **COBIT 5** APO13.12 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 · **NIST SP 800-53 Rev. 4** PM-1, PS-7
ID.GV-3: Wymogi prawne i regulacyjne w zakresie cyberbezpieczeństwa, w tym zachowania prywatności i swobód obywatelskich, są rozumiane i zarządzane	· **COBIT 5** MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1 · **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
ID.GV-4: Procesy zarządzania i procesy zarządzania ryzykiem definiują ryzyka ceberbezpieczeństwa.	· **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **NIST SP 800-53 Rev. 4** PM-9, PM-11
ID.RA-1: Podatności aktywów są zidentyfikowane i udokumentowane.	· **CCS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Informacja o zagrożniu i podatności jest przekazywana z forum wymiany informacji i ze źródeł	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
ID.RA-3: Zagrożenia, zarówno wewnętrzne jak i zewnętrzne, są zidentyfikowane i udokumentowane	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potencjalne skutki biznesowe i ich prawdopodobieństwa są zidentyfikowane	· **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
ID.RA-5: Zagrożenia, podatności, ich prawdopodobieństwo i skutki są podstawą do określenia ryzyka	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

ID.RA-6: Ryzyka są identyfikowane i zhierarchizowane	· **COBIT 5** APO12.05, APO13.02
	· **NIST SP 800-53 Rev. 4** PM-4, PM-9
ID.RM-1: Procesy zarządzania ryzykiem są ustalone, zarządzane i uzgodnione przez zainteresowane strony organizacji	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
	· **ISA 62443-2-1:2009** 4.3.4.2
	· **NIST SP 800-53 Rev. 4** PM-9
ID.RM-2: Organizacyjna tolerancja ryzyka jest określona i jednoznacznie opisana	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.3.2.6.5
	· **NIST SP 800-53 Rev. 4** PM-9
ID.RM-3: Nastawienie organizacji do tolerancji ryzyka jest uzależnione od jej roli w infrastrukurze krytycznej i sektorowego podejścia do analizy ryzyka	· **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PR.AC-1: Tożsamości i poświadczenia dla autoryzowanych urządzeń i użytkowników są zarządzane.	· **CCS CSC** 16
	· **COBIT 5** DSS05.04, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.3.5.1
	· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
	· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
	· **NIST SP 800-53 Rev. 4** AC-2, IA Family
PR.AC-2: Fizyczny dostęp do aktywów jest zarządzany i chroniony	· **COBIT 5** DSS01.04, DSS05.05
	· **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8
	· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
	· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: Zdalny dostęp jest zarządzany	· **COBIT 5** APO13.01, DSS01.04, DSS05.03
	· **ISA 62443-2-1:2009** 4.3.3.6.6
	· **ISA 62443-3-3:2013** SR 1.13, SR 2.6
	· **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC17, AC-19, AC-20
PR.AC-4: Uprawnienia dostępu są zarządzane, spełniają zasady najmniejszych uprawnień i rozdzielania obowiązków	· **CCS CSC** 12, 15
	· **ISA 62443-2-1:2009** 4.3.3.7.3
	· **ISA 62443-3-3:2013** SR 2.1
	· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
	· **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
PR.AC-5: Integralność sieci jest zabezpieczona, stosuje się segregację sieci w odpowiednich przypadkach	· **ISA 62443-2-1:2009** 4.3.3.4
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.8
	· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, SC-7
PR.AT-1: Wszyscy użytkownicy są poinformowani i przeszkoleni	· **CCS CSC** 9
	· **COBIT 5** APO07.03, BAI05.07
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.7.2.2
	· **NIST SP 800-53 Rev. 4** AT-2, PM-13
PR.AT-2: Uprzywilejowani użytkownicy rozumieją role i obowiązki	· **CCS CSC** 9
	· **COBIT 5** APO07.02, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13

PR.AT-3: Zainteresowane strony trzecie (np. dostawcy, klienci, partnerzy) rozumieją role i obowiązki	· **CCS CSC** 9
	· **COBIT 5** APO07.03, APO10.04, APO10.05
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	· **NIST SP 800-53 Rev. 4** PS-7, SA-9
PR.AT-4: Kadra kierownicza j rozumie role i obowiązki	· **CCS CSC** 9
	· **COBIT 5** APO07.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.AT-5: Pracownicy ochrony fizycznej oraz informatycy odpowiedzialni za bezpieczeństwo rozumieją role i obowiązki	· **CCS CSC** 9
	· **COBIT 5** APO07.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.DS-1: Przechowywane dane są zabezpieczone	· **CCS CSC** 17
	· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06
	· **ISA 62443-3-3:2013** SR 3.4, SR 4.1
	· **ISO/IEC 27001:2013** A.8.2.3
	· **NIST SP 800-53 Rev. 4** SC-28
PR.DS-2: Przesyłane dane są zabezpieczone	· **CCS CSC** 17
	· **COBIT 5** APO01.06, DSS06.06
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** SC-8
PR.DS-3: Aktywa są formalnie zarządzane podczas usuwania, przesyłania i udostępniania	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1
	· **ISA 62443-3-3:2013** SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
	· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
PR.DS-4: Odpowiednia zdolność do zapewnienia dostępności jest utrzymywana	· **COBIT 5** APO13.01
	· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
	· **ISO/IEC 27001:2013** A.12.3.1
	· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
PR.DS-5: Zabezpieczenia przed wyciekami danych są wdrożone	· **CCS CSC** 17
	· **COBIT 5** APO01.06
	· **ISA 62443-3-3:2013** SR 5.2
	· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Mechanizmy sprawdzania integralności są wykorzystywane do sprawdzenia oprogramowania, oprogramowania sprzętowego oraz integralności informacji	· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8
	· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** SI-7

PR.DS-7: Środowisko(a) rozwoju i testowania są oddzielone od środowiska produkcyjnego	· **COBIT 5** BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2
PR.IP-1: Konfiguracja bazowa systemów informatycznych/systemów kontroli przemysłowej jest stworzona i utrzymywana	· **CCS CSC** 3, 10 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: System Development Life Cycle do zarządzania systemami jest wdrożony	· **COBIT 5** APO13.01 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
PR.IP-3: Zmiana konfiguracji kontroli procesów jest wdrożona i utrzymywana	· **COBIT 5** BAI06.01, BAI01.06 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
PR.IP-4: Kopie zapasowe danych są prowadzone, utrzymywane i testowane okresowo	· **COBIT 5** APO13.01 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
PR.IP-5: Zasady i przepisy dotyczące fizycznego środowiska pracy dla aktywów organizacyjnych są spełnione	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Dane są niszczone zgodnie z polityką	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6
PR.IP-7: Procesy ochrony są stale udoskonalane	· **COBIT 5** APO11.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Skuteczność technologii ochrony jest współdzielona z odpowiednimi stronami	· **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
PR.IP-9: Plany reagowania (Incident Response and Business Continuity) oraz plany odbudowy (Incident Recovery and Disaster Recovery) są wdrożone i zarządzane	· **COBIT 5** DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 · **NIST SP 800-53 Rev. 4** CP-2, IR-8

PR.IP-10: Plany reagowania i odbudowy są testowane	· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
PR.IP-11: Cyberbezpieczeństwo jest spełnione w praktykach zarządzania zasobami ludzkimi (np. odbieranie uprawnień, sprawdzanie pracowników)	· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS Family
PR.IP-12: Plan zarządzania podatnościami jest opracowany i wdrożony	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
PR.MA-1: Konserwacja i naprawa aktywów organizacyjnych wykonywane są we właściwym czasie przy użyciu zatwierdzonych i kontrolowanych narzędzi	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
PR.MA-2: Zdalna konserwacja aktywów organizacyjnych jest zatwierdzona, wymaga zalogowania i wykonywana jest w sposób, który zapobiega nieautoryzowanemu dostępowi	· **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4
PR.PT-1: Zapisy audytów/logów są określone, udokumentowane, wdrożone i przeglądane zgodnie z polityką	· **CCS CSC** 14 · **COBIT 5** APO11.04 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family
PR.PT-2: Nośniki wymienne są chronione, a ich zastosowanie jest ograniczone zgodnie z polityką	· **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
PR.PT-3: Dostęp do systemów i aktywów jest kontrolowany, włączając w to zasadę najmniejszej funkcjonalności	· **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
PR.PT-4: Sieci łączności i kontroli są chronione	· **CCS CSC** 7 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DE.AE-1: Bazowe operacje sieciowe i oczekiwane przepływy danych do użytkowników i systemów zostały okreslone i są zarządzane.	· **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4

DE.AE-2: Wykryte zdarzenia są analizowane, aby zrozumieć cele i metody ataku	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
DE.AE-3: Dane ze zdarzeń są łączone i korelowane z wielu źródeł i czujników	· **ISA 62443-3-3:2013** SR 6.1 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Wpływ zdarzeń jest określany	· **COBIT 5** APO12.06 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
DE.AE-5: Progi alarmowe dla incydentów są ustalone	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.2.3.10 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
DE.CM-1: Sieć jest monitorowana w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa	· **CCS CSC** 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: Środowisko fizyczne jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa	· **ISA 62443-2-1:2009** 4.3.3.3.8 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
DE.CM-3: Aktywność personelu jest monitorowana w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa	· **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Szkodliwy kod jest wykrywalny	· **CCS CSC** 5 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3
DE.CM-5: Nieautoryzowany kod mobilny jest wykrywalny	· **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1 · **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
DE.CM-6: Aktywność zewnętrznego usługodawcy jest monitorowana w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa	· **COBIT 5** APO07.06 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitorowanie nieautoryzowanych osób, połączeń, urządzeń i oprogramowania jest wykonywane	· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Skany podatności są wykonywane	· **COBIT 5** BAI03.10 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5
DE.DP-1: Role i odpowiedzialności w zakresie wykrywania są dobrze zdefiniowane, aby zapewnić rozliczalność	· **CCS CSC** 5 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14

DE.DP-2: Działania wykrywania są zgodne z wszystkimi obowiązującymi wymaganiami	· **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
DE.DP-3: Procesy wykrywania są testowane	· **COBIT 5** APO13.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
DE.DP-4: Informacje o wykrytych zdarzeniach są przekazywane do odpowiednich stron	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Procesy wykrywania są stale udoskonalane	· **COBIT 5** APO11.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RS.RP-1: Plan reakcji jest wykonywany podczas zdarzenia lub po	· **COBIT 5** BAI01.10 · **CCS CSC** 18 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
RS.CO-1: Pracownicy znają swoje role i kolejność czynności, gdy odpowiedź jest konieczna	· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
RS.CO-2: Zdarzenia są zgłaszane zgodne z ustalonymi kryteriami	· **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
RS.CO-3: Informacje są udostępniane zgodnie z planami reagowania	· **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Koordynacja z zainteresowanymi stronami następuje zgodne z planami reagowania	· **ISA 62443-2-1:2009** 4.3.4.5.5 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.CO-5: Dobrowolna wymiana informacji następuje z podmiotami zewnętrznymi w celu osiągnięcia szerszej świadomości sytuacyjnej cyberbezpieczeństwa	· **NIST SP 800-53 Rev. 4** PM-15, SI-5
RS.AN-1: Powiadomienia z systemów wykrywania są badane	· **COBIT 5** DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: Skutki incydentu są zrozumiałe	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
	· **ISO/IEC 27001:2013** A.16.1.7
RS.AN-3: Działania śledcze są wykonywane	· **NIST SP 800-53 Rev. 4** AU-7, IR-4
	· **ISA 62443-2-1:2009** 4.3.4.5.6
RS.AN-4: Incydenty są klasyfikowane zgodnie z planami reagowania	· **ISO/IEC 27001:2013** A.16.1.4
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	· **ISA 62443-2-1:2009** 4.3.4.5.6
	· **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4
	· **ISO/IEC 27001:2013** A.16.1.5
RS.MI-1: Incydenty są obsługiwane	· **NIST SP 800-53 Rev. 4** IR-4
	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10
	· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5
RS.MI-2: Incydenty są minimalizowane	· **NIST SP 800-53 Rev. 4** IR-4
RS.MI-3: Nowo zidentyfikowane podatności są ograniczane lub udokumentowane jako zaakceptowane ryzyka	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	· **COBIT 5** BAI01.13
	· **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4
RS.IM-1: Plany reagowania wykorzystują nabyte doświadczenia	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.IM-2: Strategie reagowania są aktualizowane	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	· **CCS CSC** 8
	· **COBIT 5** DSS02.05, DSS03.04
RC.RP-1: Plan naprawczy jest wykonywany podczas zdarzenia lub po	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	· **COBIT 5** BAI05.07
RC.IM-1: Plany odbudowy wykorzystują nabyte doświadczenia	· **ISA 62443-2-1** 4.4.3.4
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	· **COBIT 5** BAI07.08
RC.IM-2: Strategie odbudowy są aktualizowane	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.CO-1: Działania public relations są zarządzane	· **COBIT 5** EDM03.02
RC.CO-2: Reputacja po zdarzeniu jest naprawiana	· **COBIT 5** MEA03.02
RC.CO-3: Działania odbudowy są przekazywane do wewnętrznych interesariuszy i zespołów wykonawczych i zarządczych	· **NIST SP 800-53 Rev. 4** CP-2, IR-4

Skróty

APC – (ang. *Advanced Process Control*) zaawansowany proces kontroli
CAPEC – (ang. *Common Attack Pattern Enumeration and Classification*) lista i klasyfikacja wzorów ataków
CDB – (ang. *Configuration Data Base*) ogólno producenckie bazy konfiguracji
CII – (ang. Critical Information Infrastructure) teleinformatyczna infrastruktura krytyczna.
CIP – (ang. *Critical Infrastructure Protection*) ochrona infrastruktury krytycznej
COCOM – (ang. *Coordinating Committee for Multilateral Export Controls*) Komitet Koordynacyjny Wielostronnej Kontroli Eksportu skupiający 17 krajów (USA, Japonię, Australię i kraje zachodnioeuropejskie)
CRM – (ang. *Customer Relationship Management*) zarządzanie relacjami z klientami
CSSWG – (ang. *Control Systems Security Working Group*) grupa robocza ICS-CERT-u do współpracy z przedstawicielami instytucji federalnych
CVE – (ang. *Common Vulnerabilities and Exposures*) powszechne wrażliwości i zagrożenia
DCS – (ang. *Distributed Control System*) rozproszony system sterowania
DDoS – (ang. *Distributed Denial of Service*) atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania
DHS – (ang. *Department of Homeland Security*) Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych
DLP – (ang. *Data Leak Prevention*) ochrona przed wyciekami informacji
DMS – (ang. *Distribution Management System*) system zarządzania siecią dystrybucyjną
DNS – (ang. *Domain Name Service*) system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych
eCSIRT.net – (ang. *The European Computer Security Incident Response Team Network*) sieć Europejskiego Zespółu ds. Bezpieczeństwa Komputerowego i Reagowania na Incydenty
EIK – europejska infrastruktura krytyczna
EIS – (ang. *Executive Information System*) system informowania kierownictwa
EMS – (ang. *Energy Management System*) system zarządzania w sektorze energetycznym
ENISA – (ang. *European Union Agency for Network and Information Security*) Europejska Agencja Bezpieczeństwa Sieci i Informacji
EPOIK – Europejski Program Ochrony Infrastruktury Krytycznej
ERP – (ang. *Enterprise Resource Planning*) planowanie zasobów przedsiębiorstwa

HIDS – (ang. *Host Intrusion Detection System*) systemy wykrywania i zapobiegania włamaniom w jednym, ochranianym systemie operacyjnym
HLR – (ang. *Home Location Register*) rejestr abonentów macierzystych
HRM – (ang. *Human Resource Management*) zarządzanie zasobami ludzkimi
ICS – (ang. *Industrial Control Systems*) oprogramowanie będące częścią systemów OT
ICS-CERT – (ang. *Industrial Control Systems-CERT*) zespół ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego
ICSJWG – (ang. *Industrial Control Systems Joint Working Group*) grupa robocza ICS-CERT-u do współpracy z sektorem prywatnym
ICT – (ang. *Information and Communications Technology*) rozwiązania teleinformatyczne
IEC – (ang. *International Electrotechnical Commission*) Międzynarodowa Komisja Elektrotechniczna
IK – infrastruktura krytyczna
IR – (ang. *Incydent Response*) reagowanie na incydenty
ISA – (ang. *Instruments, Systems and Automation Society*) Stowarzyszenie ds. Oprzyrządowania, Systemów oraz Automatyzacji
IT – (ang. *Information Technology*) systemy informatyczne
KPOIK – Krajowy Plan Ochrony Infrastruktury Krytycznej
LIMS – (ang. *Laboratory Information System*) system komunikacji z laboratorium
MDM – (ang. *Mobile Device Management*) zarządzenie urządzeniami mobilnymi
MES – (ang. *Manufacturing Execution System*) system realizacji produkcji
MNiSW – Ministerstwo Nauki i Szkolnictwa Wyższego
MRP – (ang. *Manufacturing Resource Planning*) planowanie zasobów produkcyjnych
NERC – (ang. *North American Electrical Reliability Corporation*) Północno-Amerykańska Korporacja Niezawodności Elektrycznej
NIDS – (ang. *Network Intrusion Detection System*) systemy wykrywania i zapobiegania włamaniom dla wszystkich systemów w segmencie sieci
NIST – (ang. *National Institute of Standard and Technology*) Narodowy Instytut Standaryzacji i Technologii
NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej
OT – (ang. *Operational Technology*) systemy sterowania przemysłowego
PCS – (ang. *Process Control System*) system kontroli procesu
PLC – (ang. *Programmable Logic Controller*) system sterowania maszynami
PPP – partnerstwo publiczno-prywatne
Pzp – prawo zamówień publicznych
QoS – (ang. *Quality-of-Service*) całość charakterystyk usługi telekomunikacyjnej stanowiących podstawę do wypełnienia i zaspokajanych potrzeb użytkownika
SABSA – (ang. *Sherwood Applied Business Security Architecture*) metodyką wykorzystywaną do opracowania architektury bezpieczeństwa, w szczególności dla administracji publicznej
SCADA – (ang. *Supervisory Control and Data Acquisition*) system nadzorujący przebieg procesu technologicznego lub produkcyjnego
SCM – (ang. *Supply Chain Management*) zarządzanie łańcuchem dostaw
SPOF – (ang. *Single Point of Failure*) pojedyncze punkty awarii
SQL – (ang. *Structured Query Language*) strukturalny język zapytań używany do tworzenia, modyfikowania baz danych oraz do umieszczania i pobierania danych z baz danych

SZB – system zarządzania bezpieczeństwem
TCP – (ang. *Transmission Control Protocol*) połączeniowy, niezawodny, strumieniowy protokół komunikacyjny wykorzystywany do przesyłania danych pomiędzy procesami uruchomionymi na różnych maszynach
TCP/IP – (ang. *Transmision Control Protocol/Internet Protocol*) protokół transmisji danych
TIK – teleinformatyczna infrastruktura krytyczna
TOR – (ang. the Onion Router) wirtualna sieć komputerowa implementująca zapewniająca użytkownikom prawie anonimowy dostęp do zasobów Internetu.
VoIP – (ang. *Voice over IP*) technika umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP, popularnie nazywana „telefonią internetową"
WPOIK – Wojewódzki Plan Ochrony Infrastruktury Krytycznej
WPP – współpraca publiczno-prywatna

Autorzy

dr Grzegorz Abgarowicz

pracownik Rządowego Centrum Bezpieczeństwa i wykładowca Instytutu Politologii Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. W pracy zawodowej zajmuje się problematyką planowania cywilnego i zarządzania ryzykiem. Autor publikacji dotyczących bezpieczeństwa powszechnego, ochrony ludności i zarządzania kryzysowego.

prof. WAT, dr hab. inż. Ryszard Antkiewicz

pracownik Instytutu Systemów Informatycznych Wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie i jednocześnie członek Zespołu Badawczego Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Konfliktowych i Kryzysowych. Jego naukowe zainteresowania obejmują modelowanie i ocenę efektywności oraz bezpieczeństwa systemów informatycznych, modelowanie procesów walki, wspomaganie decyzji w procesie dowodzenia i zarządzania kryzysowego.

mgr inż. Piotr Ciepiela

menedżer w dziale Doradztwa Technologicznego, EY. Współtwórca i lider doradztwa z zakresu bezpieczeństwa infrastruktury krytycznej i systemów automatyki przemysłowej na region Europy Środkowej (23 kraje). Prowadził liczne projekty na terenie Stanów Zjednoczonych, Europy oraz obszaru Bliskiego Wschodu. Uczestniczy w tworzeniu międzynarodowych standardów dotyczących Cyberbezpieczeństwa i Bezpieczeństwa systemów przemysłowych (m.in. ISA oraz NIST). Jako jeden z pierwszych na świecie otrzymał certyfikat Global Industrial Cyber Security Professional przyznawany przez GIAC, a jako pierwszy w Polsce Certified SCADA Security Architect przyznawany przez IACRB. Uczestniczył w prestiżowym szkoleniu Control Systems Cyber Security Advanced Training zatwierdzonym przez U.S. Department of Homeland Security. Autor artykułów dotyczących systemów przemysłowych publikowanych m.in. w Harvard Business Review. Posiada certyfikaty z obszaru zarządzania bezpieczeństwem (CISM, CISA, CISSP, ISO27001), architektury korporacyjnej i architektury bezpieczeństwa (TOGAF, SABSA CF), zarządzania projektami (PRINCE2 Practitioner), zarządzania IT (ITIL Service Manager). Posiada poświadczenia bezpieczeństwa dostępu do informacji oznaczonych klauzulą „NATO SECRET" oraz „SECRET UE".

mgr inż. Michał Dyk

absolwent Wydziału Cybernetyki WAT. Od 2013 r. członek Zespołu Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Kryzysowych i Konfliktowych. Jego zainteresowania naukowe obejmują głównie sieci sensorowe, internet rzeczy oraz symulację komputerową. W trakcie zdobywania tytułu naukowego doktora.

dr Dominika Dziwisz

absolwentka stosunków międzynarodowych oraz zarządzania i marketingu na Uniwersytecie Jagiellońskim. W obrębie jej zainteresowań badawczych znajdują się formy współczesnego terroryzmu, w tym przede wszystkim te związane z rozwojem nowoczesnych technologii, bezpieczeństwo cybernetyczne oraz polityka bezpieczeństwa USA.

Zbigniew Fałek

absolwent Wydziału Zarządzania i Wydziału Matematyki Uniwersytetu Łódzkiego. Ukończył również The Strategic Leadership Academy (Executive Development Program Management II) prowadzoną przez HBSP&CIMI.
Od 1994 r. w branży energetycznej. W latach 2006-2009 był Prezesem Zarządu ZEŁ-T S.A. (Obecnie PGE Dystrybucja S.A.). Następnie Dyrektor Inwestycyjny w RE-Invest Sp. z o.o. Od 2009 r. zajmuje się działalnością doradczą. Autor kilkunastu publikacji z zakresu zarządzania przedsiębiorstwem.

Piotr Gajek

prawnik kancelarii WKB, członek zespołu rozwiązywania sporów. Współpracuje z zespołami pomocy publicznej i prawa ochronny konkurencji. Absolwent Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz Wydziału Prawa Europejskiej Wyższej Szkoły Prawa i Administracji w Warszawie. Stypendysta programu Leonardo da Vinci. W trakcie studiów odbył kilkumiesięczny staż w dziale Prawa Europejskiego i Konkurencji w kancelarii w Brukseli.
W ramach odbytego stażu w Wydziale ds. Pomocy publicznej Dyrekcji Generalnej ds. Konkurencji (DG COMP) Komisji Europejskiej przygotowywał projekty ocen skarg dotyczących udzielenia pomocy publicznej. Posiada kilkuletnie doświadczenie w zakresie Funduszy Europejskich. Brał udział w przygotowaniu opinii prawnych dla przedsiębiorców i podmiotów publicznych, oceniając ryzyko otrzymania bądź udzielenia przez nich pomocy publicznej w wyniku zawieranych transakcji.

mjr dr inż. Rafał Kasprzyk

pracownik naukowo-dydaktyczny Wydziału Cybernetyki WAT oraz członek Zespołu Badawczego Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Konfliktowych i Kryzysowych. Główny obszar jego zainteresowań dotyczy modelowania, symulacji i analizy systemów sieciowych z wykorzystaniem modeli i metod badań operacyjnych, a w szczególności teorii grafów i sieci oraz wybranych elementów sztucznej inteligencji. Kierownik projektów realizowanych przez studentów i doktorantów wielokrotnie wyróżnianych na międzynarodowych targach wynalazczości.

Włodzimierz Kotłowski

ekspert bezpieczeństwa ICT. Tematyką ochrony systemów ICT zajmuje się od 15 lat. Brał udział w wielu projektach ICT w Polsce jak i w krajach UE jako osoba odpowiedzialna za bezpieczeństwo teleinformatyczne. Absolwent WAT, studiował na kierunku fizyka techniczna. Długoletni pracownik naukowy w Instytucie Fizyki Technicznej Wojskowej Akademii Technicznej. Obecnie członek zarządu firmy Matic Sp. z o.o.

Mirosław Maj

od 2010 r. jest założycielem i prezesem Fundacji Bezpieczna Cyberprzestrzeń oraz wiceprezesem spółki ComCERT SA. Wcześniej związany kierował zespołem CERT Polska. Współpracuje z Rządowym Centrum Bezpieczeństwa w dziedzinie ochrony infrastruktury krytycznej. Prowadzi wykłady z bezpieczeństwa teleinformatycznego na UJ, PJWSTK i SGH.

W 2012 i 2013 r. koordynował pierwsze w Polsce ćwiczenia z ochrony w cyberprzestrzeni – Cyber-EXE Polska. Uczestniczył w budowaniu nowych CERTów w Polsce i zagranicą. Koordynował NATO-owski projekt CLOSER, dzięki któremu powstały CERT-y w Gruzji, Mołdawii, Armenii i Azerbejdżanie. Współorganizuje współpracę CERTów europejskich w ramach inicjatywy Trusted Introducer i TERENA TF-CSIRT. Blisko współpracuje z europejską agencją ENISA, będąc członkiem tematycznych grup roboczych i współautorem wielu opracowań wydawanych przez Agencję.

prof. WAT, dr hab. inż. Andrzej Najgebauer

kierownik Zespołu Badawczego Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Konfliktowych i Kryzysowych w Wojskowej Akademii Technicznej. Specjalista w obszarze komputerowej symulacji sytuacji kryzysowych i konfliktowych oraz w obszarze modelowania i projektowania informatycznych systemów wspomagania decyzji., modelowania i projektowania systemów bezpieczeństwa. Kierował i kieruje kilkunastoma projektami krajowymi i międzynarodowymi w zakresie informatyki w systemach bezpieczeństwa. Brał udział w opracowaniu ekspertyz w ramach przeglądu obronnego państwa i występował w zespole naukowo-przemysłowym przy Radzie Uzbrojenia SZ RP. Reprezentuje Polskę w panelu NATO Science and Technology Organization – NATO Modelling and Simulation Group od 2001 r., W latach 2002-2006 kierował zespołem, reprezentującym 10 państw NATO w projekcie MSG-026 pod nazwą „M&S Tool for Early Warning Identification of Terrorist Activities".

dr inż. Dariusz Pierzchała płk rez.

absolwent Wydziału Cybernetyki WAT oraz uczestnik kursów: NATO NAF (AT2-AT4), PRINCE2, Rationale RUP, SAS Master Class and ESRI ArcGIS. Obecnie adiunkt na Wydziale Cybernetyki, polski przedstawiciel w NATO Modelling and Simulation Group oraz sekretarz Polskiego Towarzystwa Symulacji Komputerowej. Zajmuje się dydaktyką oraz badaniami w dziedzinie komputerowej heterogenicznej symulacji rozproszonej (integracja systemów, zagadnienia sterowania dyskretno-zdarzeniowego) oraz wspomaganiem decyzji w sytuacjach konfliktowych i kryzysowych z wykorzystaniem metod prognostycznych, symulacyjnych i badań operacyjnych.

dr Aleksander Poniewierski

partner w dziale Doradztwa Technologicznego, EY; Lider Grupy Doradztwa Informatycznego w Europie Środkowej i Południowo-Wschodniej. Absolwent Uniwersytetu Śląskiego, doktor Nauk Ekonomicznych Uniwersytetu Ekonomicznego w Poznaniu. Uczestnik wielu prestiżowych programów organizowanych przez Harvard Business School oraz Carnegie Mellon University. Specjalizuje się we wdrażaniu systemów zarządzania IT, podnoszeniem efektywności systemów informatycznych stosowanych w biznesie oraz ryzykach związanych z ich użytkowaniem, jak również w zagadnieniach bezpieczeństwa cyberprzestrzeni i infrastruktury krytycznej. Doradzał czołowym spółkom w zakresie bezpieczeństwa IT, zarządzania IT, strategii IT oraz transformacji IT. Szczególnym obszarem zainteresowania Aleksandra jest tematyka cyberbezpieczeństwa oraz infrastruktury krytycznej.
Posiada następujące certyfikaty CISM przyznawany przez stowarzyszenie ISACA, CISA Certyfikowany Menedżer Projektów APM, CFE, PRINCE 2 Practicioner, ITIL Foundation (IT Infrastructure Library), ISSP (International Systems Security Profesional), CERT Certified Computer Security Incident Handler, SABSA Chartered Foundation (SCF) Certificate.

Maciej Pyznar

główny specjalista w Wydziale Ochrony Infrastruktury Krytycznej Rządowego Centrum Bezpieczeństwa. Absolwent Wydziału Nawigacji i Uzbrojenia Okrętowego Akademii Marynarki Wojennej oraz Studium Bezpieczeństwa Narodowego Uniwersytetu Warszawskiego. W RCB pracuje od jego utworzenia, gdzie zajmuje się działaniami planistycznymi i programowymi w zakresie ochrony infrastruktury krytycznej.

dr inż. Mirosław Ryba

dyrektor w dziale Doradztwa Technologicznego, EY. Kieruje globalnym centrum usług doradczych w zakresie Operational Technology (EY Global OT Advisory Services Center). W ciągu 15 lat swojej kariery zawodowej, zyskał ogromne doświadczenie w dziedzinie IT i OT zarządzając licznymi projektami, zarówno dla instytucji rządowych jak i dla największych przedsiębiorstw w Europie, Afryce, na Bliskim Wschodzie i w Ameryce Północnej. Specjalizując się w tematyce związanej z zarządzaniem architekturą i bezpieczeństwem systemów kontroli przemysłowej (ICS), w 2011 r. otrzymał akredytację Departamentu Bezpieczeństwa Krajowego Stanów Zjednoczonych (U.S. Department of Homeland Security) do uczestnictwa w zaawansowanym szkoleniu Control Systems Cyber Security Advanced Training prowadzonym przez Idaho National Laboratory w Idaho Falls, USA. Jest aktywnym członkiem ISA (International Society of Automation) i był zaangażowany w opracowanie standardu ISA-62443-3-3 poświęconego bezpieczeństwu w automatyce przemysłowej i systemach sterowania. Posiada liczne certyfikaty, m.in.: CSSA, SABSA, CISA, CISM i CISSP.

dr Krzysztof Rzecki

adiunkt w Instytucie Teleinformatyki Politechniki Krakowskiej. Był wieloletnim kierownikiem działu oprogramowania CCNS SA, kontraktorem w zakresie protokołów sieciowych dla Siemens AG oraz Nokia-Siemens-Networks. Obecnie wykonuje prace naukowo-badawcze na zlecenie biznesu z zakresu context-awareness (Orange / TP SA) oraz wirtualizacji i technologii mobilnych (VSoft SA). Jest ekspertem współpracującym z CTT PK z zakresu nowych technologii.

Joanna Świątkowska

politolog, przygotowuje rozprawę doktorską poświęconą współczesnej walce informacyjnej. Ekspert Instytutu Kościuszki do spraw cyberbezpieczeństwa.
Jest pomysłodawcą i liderem projektu Cel: Cyberbezpieczeństwo, który realizuje od 2011 r. Była inicjatorem, koordynatorem i uczestnikiem wielu krajowych i międzynarodowych projektów poświęconych bezpieczeństwu ze szczególnym uwzględnieniem problematyki bezpieczeństwa teleinformatycznego.
Brała udział w pracach Strategicznego Forum Bezpieczeństwa poświęconych cyberbezpieczeństwu organizowanym przez Biuro Bezpieczeństwa Narodowego, była uczestnikiem panelu ekspertów organizowanym przez Najwyższą Izbę Kontroli w związku z kontrolą dotyczącą realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Polski. Jest także uczestnikiem międzynarodowego dialogu Sino-European Cyber Dialogue.

prof. WAT, dr hab. inż. Zbigniew Tarapata ppłk rez.

absolwent Wydziału Cybernetyki WAT (1995), profesor nadzwyczajny WAT, od 2012 r. Dyrektor Instytutu Systemów Informatycznych Wydziału Cybernetyki WAT. Zajmuje się dydaktyką oraz badaniami naukowymi w obszarze analizy algorytmów (złożoność, dokładność, efektywność), modeli i metod teorii grafów i sieci (drogi ekstremalne, podobieństwo grafów i sieci, sieci semantyczne, sieci złożone, problemy transportowe) oraz wspomaganiem decyzji w sytuacjach konfliktowych i kryzysowych z wykorzystaniem modeli i metod badań operacyjnych oraz elementów sztucznej inteligencji.

współzałożyciel i partner w kancelarii WKB. Kieruje zespołem prawa własności intelektualnej i mediów oraz ściśle współpracuje z zespołem fuzji i przejęć. Absolwentka Wydział Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu. Jako stypendystka Fundacji Sorosa ukończyła studia podyplomowe z zakresu międzynarodowego prawa gospodarczego na Uniwersytecie Środkowoeuropejskim w Budapeszcie (LLM).

Doradza klientom we wszelkich kwestiach związanych z prawem autorskim, własności przemysłowej, prawem konsumenckim, czynami nieuczciwej konkurencji, ochroną danych osobowych, domen internetowych, prawem prasowym oraz ochroną dóbr osobistych. Prowadzi sprawy związane z marketingiem produktów sensytywnych oraz grami hazardowymi. W powyższym zakresie, oprócz bieżącego doradztwa, reprezentuje klientów w postępowaniach sądowych i polubownych. Od lat prowadzi również transakcje nabycia spółek na rynku prywatnym.

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym – think tank – o charakterze non profit, założonym w 2000 r.

W prace Instytutu zaangażowani są naukowcy, pracownicy polskiej i europejskiej administracji oraz praktycy działalności publicznej i społeczno-gospodarczej. Instytut tworzy ekspertyzy i rekomendacje programowe dla europejskich i polskich instytucji publicznych.

Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski, jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Opracowania Instytutu były i są podstawą zarówno ważnych reform legislacyjnych, jak i merytorycznym wsparciem dla bieżącej działalności osób podejmujących strategiczne decyzje.

Od 2011 r. Instytut Kościuszki realizuje projekt *Cel: cyberbezpieczeństwo*, który jest odpowiedzią na potrzebę podejmowania działań mających na celu zapewnienie bezpiecznego funkcjonowania w cyberprzestrzeni państwa, podmiotów komercyjnych i obywateli.

By umożliwić skuteczną ochronę przed cyberzagrożeniami należy przede wszystkim zdiagnozować niebezpieczeństwa płynące z przeniesienia znacznej części działań publicznych i prywatnych do cyberprzestrzeni. Kolejnym krokiem jest przygotowywanie we współpracy ze specjalistami branży IT, ekspertami ds. bezpieczeństwa i przedstawicielami podmiotów zajmujących się walką z cyberzagrożeniami, zestawu rekomendacji stanowiących wskazówki dla decydentów i prowadzących do podniesienia poziomu cyberbezpieczeństwa.

Tak przygotowany fundament jest punktem wyjścia do podejmowania kolejnych działań projektu – identyfikacji szans jakie daje cyberprzestrzeń i wykorzystywania jej pełnego potencjału.

RZĄDOWE CENTRUM BEZPIECZEŃSTWA

Rozwiązywanie sytuacji kryzysowych, z jakimi mamy do czynienia we współczesnym świecie, wymaga zaangażowania i współpracy wielu różnych służb i instytucji administracji publicznej, działających często wg różnych wewnętrznych procedur. Zatem kluczową sprawą jest odpowiednie skoordynowanie ich pracy. To jedno z głównych zadań Rządowego Centrum Bezpieczeństwa (RCB).

RCB jest instytucją realizującą zadania z zakresu zarządzania kryzysowego na poziomie rządowym. Misją Centrum jest przygotowanie administracji, tak aby w sytuacjach kryzysowych jak najlepiej służyła społeczeństwu i poprzez skoordynowane działania była w stanie zapewnić skuteczną pomoc obywatelom.

Do zadań Rządowego Centrum Bezpieczeństwa należy analiza zagrożeń, w oparciu o dane uzyskiwane zarówno z instytucji polskiej administracji publicznej, jak i od partnerów międzynarodowych. Centrum koordynuje także przepływ informacji o zagrożeniach.

RCB zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, Rządowego Zespołu Zarządzania Kryzysowego i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego. Pełni również funkcję krajowego centrum zarządzania kryzysowego.

Rządowe Centrum Bezpieczeństwa odgrywa główną rolę w budowie systemu ochrony infrastruktury krytycznej (IK) w Polsce. Dyrektor Centrum, we współpracy z ministrami i kierownikami właściwych urzędów centralnych, sporządza wykaz IK oraz europejskiej IK, a także tworzy Narodowy Program Ochrony Infrastruktury Krytycznej.

RCB realizuje także zadania planistyczne i programowe m.in. opracowuje Krajowy Plan Zarządzania Kryzysowego, organizuje i prowadzi szkolenia oraz współpracuje z NATO i Unią Europejską.

Rządowe Centrum Bezpieczeństwa rozpoczęło działalność 2 sierpnia 2008 roku. Powstało na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (art. 10) i rozporządzenia Prezesa Rady Ministrów z dnia 10 lipca 2008r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa.

Jest państwową jednostką budżetową podległą Prezesowi Rady Ministrów.

O firmie EY

EY jest światowym liderem rynku usług profesjonalnych obejmujących usługi audytorskie, doradztwo podatkowe, doradztwo biznesowe i doradztwo transakcyjne. Nasza wiedza oraz świadczone przez nas najwyższej jakości usługi przyczyniają się do budowy zaufania na rynkach kapitałowych i w gospodarkach całego świata. W szeregach EY rozwijają się utalentowani liderzy zarządzający zgranymi zespołami, których celem jest spełnianie obietnic składanych przez markę EY. W ten sposób przyczyniamy się do budowy sprawniej funkcjonującego świata. Robimy to dla naszych klientów, społeczności, w których żyjemy i dla nas samych.

Więcej informacji: www.ey.com/pl

O kancelarii WKB

Od 2004 roku kancelaria WKB świadczy kompleksowe usługi prawne z zakresu prawa gospodarczego. Ponad sześćdziesięcioosobowy zespół prawników WKB wprowadza nowatorskie rozwiązania prawne aby nadążyć za dynamicznie zmieniającymi się warunkami rynkowymi.

WKB świadczy specjalistyczne doradztwo m.in. w dziedzinie prawa energetycznego, prawa zamówień publicznych, prawa konkurencji, prawa korporacyjnego, prawa własności intelektualnej, prawa nieruchomości oraz ochrony środowiska. Doświadczenie kancelarii obejmuje prowadzenie projektów prywatyzacyjnych oraz transakcji na rynku fuzji i przejęć. Ponadto WKB posiada doświadczony zespół prawników procesualistów.

Z roku na rok WKB powiększa liczbę zespołowych i indywidualnych rekomendacji w Chambers Global, Chambers Europe, Legal 500, PLC Which Lawyer? i Who's Who Legal. Prawnicy kancelarii WKB są wysoko oceniani przez branżowe rankingi publikowane na łamach ogólnopolskich opiniotwórczych dzienników, takich jak Rzeczpospolita.

Więcej informacji: www.wkb.com.pl.

O firmie MATIC

Matic jest profesjonalną firmą wyspecjalizowaną w świadczeniu usług i dostaw rozwiązań w zakresie informatyki, łączności, analizy i przetwarzania danych, ochrony infrastruktury krytycznej, w tym cyber - bezpieczeństwa oraz obronności. Nasza oferta kierowana jest do podmiotów administracji publicznej oraz instytucji odpowiadających za bezpieczeństwo państwa. W toku ponad 20 lat naszej działalności zrealizowaliśmy z sukcesem wiele projektów pozwalających na wykorzystanie najnowocześniejszych technologii dla realizacji praktycznych celów zmierzających do poprawy bezpieczeństwa. Firma cieszy się wieloletnim zaufaniem Klientów prywatnych i instytucjonalnych.

Głównym celem firmy jest świadczenie wysokiej jakości usług z zakresu kompleksowej obsługi informatycznej i obronności. Firma przeprowadziła certyfikację usług, serwisu, produkcji i projektowania systemów zgodnie z normą ISO 9001:2001. W 2013 uzyskaliśmy również certyfikat ISO w zakresie spełniania standardów sysatemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO 27001:2007. Do realizacji projektów w zakresie obronności posiada koncesję wydaną przez Ministra Spraw Wewnętrznych na wytwarzanie oraz obrót wyrobów o przeznaczeniu wojskowym lub policyjnym.

Kompetencje zespołu ogniskują się na technologiach informacyjnych z uwzględnieniem zagadnień dotyczących kompleksowych wdrożeń i integracji systemów informatycznych, zaawansowanej analizie i przetwarzaniu danych, ochronie kryptograficznej, zarządzania operacyjnego, rozpoznania oraz łączności taktycznej i operacyjnej.

Więcej informacji: www.matic.com.pl.

Systemy teleinformatyczne w coraz większym stopniu warunkują funkcjonowanie najważniejszych obiektów, instalacji, urządzeń oraz usług, zidentyfikowanych i wyznaczonych jako infrastruktura krytyczna państwa (obejmująca m.in. systemy zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, transportowe i komunikacyjne). Z uwagi na ich fundamentalną rolę z punktu widzenia bezpieczeństwa całego państwa konieczne jest zapewnianie ich prawidłowego funkcjonowania. Pomimo olbrzymiej wagi problemu, w Polsce brakowało kompleksowej analizy problematyki cyberbezpieczeństwa infrastruktury krytycznej. Niniejszy Raport wypełnia tę lukę.

Głównym celem raportu jest dostarczenie podmiotom zaangażowanym w ochronę infrastruktury krytycznej rekomendacji przyczyniających się do zwiększenia poziomu jej bezpieczeństwa.

cel: cyberbezpieczeństwo

Raport powstał w ramach realizowanego przez Instytut Kościuszki projektu *Cel: Cyberbezpieczeństwo*

Partnerzy Raportu

WKB Wierciński Kwieciński Baehr

matic IT & Defence Systems

Współpraca w przygotowaniu Raportu

Fundacja bezpieczna cyberprzestrzeń

Politechnika Krakowska im. Tadeusza Kościuszki

BBN

Przedstawiciele Biura Bezpieczeństwa Narodowego uczestniczyli w pracach nad raportem wyłącznie w roli obserwatorów. Zgłoszone przez nich uwagi autorzy poszczególnych części opracowania wprowadzali w zakresie wynikającym z ich własnych decyzji, a całość opracowania nie jest oficjalnym stanowiskiem BBN.

ISBN: 978-83-63712-15-0

Instytut Kościuszki