Marek Pawlik*
Ewa Niewiadomska-Szynkiewicz**

Rola centrów wymiany i analizy informacji w budowaniu odporności kluczowych sektorów polskiej gospodarki

Streszczenie

W ostatnich latach obserwuje się lawinowy wzrost zagrożeń z cyberprzestrzeni zarówno systemów informacyjnych (systemów IT), jak i cyfrowych systemów eksploatacyjnych (systemów OT) wykorzystujących technologie informacyjne i komunikacyjne (technologie ICT). Jednocześnie rośnie ilość gromadzonych, przetwarzanych i udostępnianych cyfrowych danych. Dostępność tych danych istotnie wpływa na rozwój gospodarczy kraju, wspiera funkcjonowanie administracji państwa, podnosi poziom obronności, ochrony zdrowia, edukacji. W tej sytuacji podstawowego znaczenia nabiera budowanie świadomości ryzyk i nabywanie umiejętności zabezpieczania sieci, systemów i cyfrowych usług przed cyberzagrożeniami. Ważną rolę w tym zakresie odgrywają nowego typu struktury, tzw. centra wymiany i analizy informacji (ISAC). Współautorzy na podstawie zapisów prawa i własnych doświadczeń związanych z funkcjonowaniem ISAC-Kolej i ISAC-GIG przedstawiają ekosystem dookoła ISAC, zadania tych struktur oraz stojące przed nimi wyzwania.

Słowa kluczowe: cyberbezpieczeństwo, operatorzy usług kluczowych, centra wymiany i analizy informacji, ISAC

* Dr hab. inż. Marek Pawlik, prof. Instytutu Kolejnictwa, zastępca dyrektora ds. interoperacyjności kolei, Instytut Kolejnictwa w Warszawie, e-mail: mpawlik@ikolej.pl, ORCID: 0000-0003-3357-7706.

** Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz, kierownik Zespołu Złożonych Systemów, Instytut Automatyki i Informatyki Stosowanej, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska, doradca dyrektora w Głównym Instytucie Górnictwa (GIG), zastępca przewodniczącego ISAC-GIG, e-mail: ewa.szynkiewicz@pw.edu.pl, ORCID: 0000-0003-4782-3816.

Wprowadzenie

Technologie ICT, czyli technologie informacyjne i komunikacyjne (ang. Information and Communication Technologies), są obecne w wielu obszarach gospodarki, chociaż znaczna część społeczeństwa może nie zdawać sobie z tego sprawy. Dla wielu obywateli jest oczywiste, że cyfrowe usługi funkcjonują w sektorze finansowym, administracji centralnej i lokalnej państwa, a od czasu pandemii umożliwiają pracę i naukę zdalną. Prawdopodobnie niewiele osób zdaje sobie sprawę jak ważną rolę odgrywają technologie ICT we wspieraniu i realizacji usług transportowych, dostarczaniu wody pitnej, zapewnianiu i rozliczaniu energii elektrycznej czy w ochronie zdrowia. Obecnie bezpieczeństwo państw i ich obywateli w znacznym stopniu zależy od dostępności i kompetencji personelu oraz systemów i narzędzi programistycznych, które chronią kluczowe usługi cyfrowe we wszystkich warstwach systemów ICT, od warstwy fizycznej po warstwę aplikacji. Niestety, nawet wśród pracowników zajmujących się technologiami informacyjnymi obserwuje się stosunkowo niski poziom wiedzy na temat warstw systemów ICT oraz świadomości, w jaki sposób warstwy te ze sobą współpracują. Budowanie i utrzymywanie systemów zabezpieczeń przed cyberzagrożeniami, które mogą atakować na różnych poziomach wymiany i przetwarzania danych w systemach ICT, wymaga wiedzy i stałego podnoszenia kompetencji pracowników ważnych dla bezpieczeństwa państwa podmiotów. Braki lub luki w zabezpieczeniach przyczyniają się do łatwego rozprzestrzeniania się zagrożeń. Atakowane są kolejne instytucje i organizacje w poszczególnych branżach, pokonywane są bariery organizacyjne, cyberataków dotykają również jednostki z innych obszarów działalności. Atak na system egzaminowania kierowców może np. spowodować wstrzymanie pracy grupy placówek medycznych. Przyczyna może być oczywista, np. wykorzystywanie wspólnego centrum przetwarzania danych. Może być też trudna do wykrycia, np. atak w jednej z warstw wymiany danych przekazywanych siecią światłowodową. Wspomaganie podmiotów korzystających z rozwiązań cyfrowych do identyfikacji zagrożeń, budowania umiejętności cyfrowych pracowników, wdrażania i utrzymywania zabezpieczeń to zadania centrów wymiany i analiz informacji (ISAC), których działalności jest poświęcony niniejszy artykuł.

Lista podmiotów zobowiązanych do identyfikowania zagrożeń i przeciwdziałania zagrożeniom oraz raportowania incydentów bezpieczeństwa

W 2016 roku Parlament Europejski przyjął dyrektywę na rzecz wspólnego wysokiego bezpieczeństwa sieci i systemów[1]. Angielskie określenie sieci i systemów (network and information systems) jest wykorzystywane do szybkiego i niebudzącego wątpliwości identyfikowania tej dyrektywy jako dyrektywy NIS. Do polskiego porządku prawnego została ona wprowadzona w 2018 roku ustawą o krajowym systemie cyberbezpieczeństwa[2], identyfikowaną jako ustawa KSC. Zarówno dyrektywa NIS, jak i ustawa KSC wybierają grupy podmiotów, spośród których właściwe władze krajowe wskazują tzw. operatorów usług kluczowych. Podmioty te są zobowiązane do identyfikowania cyfrowych zagrożeń, zabezpieczania się przed nimi i raportowania incydentów. Sektor integrujący podmioty odpowiedzialne za pozyskiwanie i dostarczanie energii, w tym energii elektrycznej, podzielono na aż siedem podsektorów. Podsektory oraz odpowiadające im zakresy działań przedstawiono w tabeli 1. Za kluczowe uznano również usługi transportowe. W sektorze transportu wyróżniono cztery podsektory odpowiadające czterem rodzajom transportu, tj.: lotniczy, kolejowy, wodny i drogowy. Podmioty, z których są wskazywani operatorzy usług kluczowych w transporcie, zestawiono w tabeli 2.

Tabela 1. Operatorzy usług kluczowych w sektorze „energia"

Sektor	Podsektor	Rodzaje podmiotów/rodzaje działalności
Energia	wydobywanie kopalin	wydobywanie: gazu ziemnego, ropy naftowej, węgla brunatnego, węgla kamiennego oraz pozostałych kopalin
	energia elektryczna	wytwarzanie energii elektrycznej, przesyłanie energii elektrycznej, dystrybucja energii elektrycznej, obrót energią elektryczną, przetwarzanie albo magazynowanie energii elektrycznej, świadczenie usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną
	ciepło	wytwarzanie ciepła, obrót ciepłem, przesyłanie ciepła, dystrybucja ciepła

1 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE 2016, L 194/1.

2 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.

Sektor	Podsektor	Rodzaje podmiotów/rodzaje działalności
	ropa naftowa	wytwarzanie paliw ciekłych, przesyłanie ropy naftowej, przesyłanie paliw ciekłych siecią rurociągów, magazynowanie ropy naftowej, w tym bezzbiornikowego podziemnego magazynowania ropy naftowej, przeładunek ropy naftowej, magazynowanie paliw ciekłych, bezzbiornikowe podziemne magazynowanie paliw ciekłych, przeładunek paliw ciekłych, obrót paliwami ciekłymi, obrót paliwami ciekłymi z zagranicą, wytwarzanie paliw syntetycznych
	gaz	wytwarzanie paliw gazowych, przesyłanie paliw gazowych, obrót gazem ziemnym z zagranicą, obrót paliwami gazowymi, operator systemu przesyłowego gazowego, operator systemu dystrybucyjnego gazowego, operator systemu magazynowania paliw gazowych, operator systemu skraplania gazu ziemnego
	dostawy usług w sektorze energii	dostawy systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenie usług na rzecz sektora energii
	jednostki nadzorowane i podległe	jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane, jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane.

Źródło: Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa...

Tabela 2. Operatorzy usług kluczowych w sektorze „transport"

Sektor	Podsektor	Rodzaje podmiotów/rodzaje działalności
Transport	lotniczy	przewoźnik lotniczy, zarządzający lotniskiem, przedsiębiorca wykonujący określone usługi i/lub zadania związane z kontrolą bezpieczeństwa przewoźników lotniczych oraz innych użytkowników statków powietrznych, instytucja zapewniająca służby żeglugi powietrznej
	kolejowy	zarządcy infrastruktury kolejowej (z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, prywatnej i wąskotorowej), przewoźnicy kolejowi
	wodny	armatorzy w transporcie morskim pasażerów i towarów, armatorzy w żegludze śródlądowej, podmioty zarządzające portami i przystaniami morskimi, podmioty zarządzające obiektami portowymi, podmioty prowadzące na terenie portów działalność wspomagającą transport morski, służby kontroli ruchu statków (VTS)
	drogowy	zarządcy dróg, podmioty realizujące usługi ITS

Źródło: Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa...

Tabela 3. Operatorzy usług kluczowych w obszarze finansów, zdrowia, wody i infrastruktury cyfrowej

Sektor	Rodzaje podmiotów/rodzaje działalności
Bankowość i infrastruktura rynków finansowych	instytucje kredytowe, banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, spółdzielcze kasy oszczędnościowo-kredytowe, podmioty prowadzące rynek regulowany, CCP – osoby prawne działające w obrocie na rynku finansowym będące nabywcą dla sprzedawcy i sprzedawcą dla nabywcy, podmioty zależne krajowego depozytu uczestniczące w obsłudze depozytu papierów wartościowych
Ochrona zdrowia	podmioty lecznicze, jednostki właściwe w zakresie systemów informacyjnych ochrony zdrowia, Narodowy Fundusz Zdrowia, działy farmacji szpitalnej, apteki szpitalne, hurtownie farmaceutyczne, podmioty wprowadzające do obrotu produkty lecznicze, importerzy produktów leczniczych/substancji czynnych, wytwórcy produktów leczniczych/substancji czynnych, importerzy równolegli, dystrybutorzy substancji czynnych, ogólnodostępne apteki
Zaopatrzenie w wodę pitną	przedsiębiorstwa wodociągowo-kanalizacyjne
Infrastruktura cyfrowa	podmioty świadczące usługi DNS, podmioty prowadzące punkty wymiany ruchu internetowego (IXP), podmioty zarządzające rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD)

Źródło: Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa...

Ustawa o krajowym systemie cyberbezpieczeństwa zgodnie z dyrektywą NIS wskazuje także podmioty, które odgrywają rolę operatorów usług kluczowych w czterech kolejnych sektorach. Są to instytucje oferujące usługi bankowe i finansowe, ochrony zdrowia, zapewnienia wody pitnej i infrastruktury cyfrowej. Podobnie jak dla sektorów energii i transportu podano rodzaje podmiotów oraz działalności, które upoważniają właściwy organ krajowy do wskazywania, decyzjami administracyjnymi, podmiotów będących operatorami usług kluczowych i tym samym zobowiązanych do realizacji związanych z tym zadań.

Rozszerzona lista podmiotów zobowiązanych do identyfikowania zagrożeń i przeciwdziałania zagrożeniom oraz raportowania incydentów bezpieczeństwa

Wskazane w tabelach 1–3 podmioty nie wyczerpują katalogu instytucji i przedsiębiorstw, których działalność jest kluczowa dla funkcjonowania państwa i jego obywateli, których wszelkie zakłócenia w ich pracy mogą skutkować

bardzo poważnymi konsekwencjami. Intensywne ataki, z jakimi mają obecnie do czynienia państwa demokratyczne, w tym państwa członkowskie Unii Europejskiej, spowodowały, że w grudniu 2022 roku Parlament Europejski przyjął dyrektywę NIS-2[3]. Powiększa ona katalog podmiotów o operatorów systemów chłodniczych oraz operatorów instalacji wodorowych jako nowego rodzaju paliwa. Uwzględnia także przedsiębiorstwa zbierające, odprowadzające i oczyszczające ścieki. Dodatkowo do listy podmiotów obsługujących cyfrową infrastrukturę dołączono dostawców usług chmurowych, centra przetwarzania danych, sieci dostarczania treści, usługi zaufania, publiczne i publicznie dostępne usługi łączności elektronicznej oraz podmioty oferujące usługi ICT pomiędzy różnymi przedsiębiorstwami. Uwzględniono także instytucje administracji publicznej gromadzące i przetwarzające dane wrażliwe oraz operatorów naziemnej infrastruktury związanej z przestrzenią kosmiczną.

Oprócz sektorów kluczowych dyrektywa NIS-2 definiuje także sektory ważne z punktu widzenia cyberbezpieczeństwa. Zaliczono do nich usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcję, wytwarzanie i dystrybucję chemikaliów, produkcję, przetwarzanie i dystrybucję żywności, produkcję wyrobów medycznych, komputerów, wyrobów elektronicznych i optycznych, urządzeń elektrycznych, maszyn i urządzeń, pojazdów i pozostałego sprzętu transportowego, a także dostawców usług cyfrowych, w tym dostawców internetowych platform handlowych, wyszukiwarek internetowych, platform usług sieci społecznościowych oraz podmioty zaangażowane w badania naukowe.

Dyrektywa NIS-2 diametralnie zmieniła sytuację przedsiębiorstw działających w poszczególnych sektorach. Dotychczas status operatorów usług kluczowych był nadawany przedsiębiorstwom decyzją administracyjną właściwych władz krajowych. Po wejściu w życie dyrektywy NIS-2 status taki, zgodnie z zapisami dyrektywy, z mocy prawa uzyskają podmioty publiczne i prywatne działające w sektorach kluczowych i/lub sektorach ważnych, które kwalifikują się jako średnie przedsiębiorstwa zgodnie z zaleceniem 2003/361/WE[4] lub większe oraz świadczą usługi i/lub prowadzą działalność na terenie Unii

3 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Tekst mający znaczenie dla EOG), Dz. Urz. UE 2022, L 333/80.

4 Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji przedsiębiorstw mikro, małych i średnich (notyfikowane jako dokument nr C(2003) 1422), ibidem 2003, L 124.

Europejskiej. Podsumowując, wszystkie podmioty działające w sektorach kluczowych i sektorach ważnych, z wyłączeniem tych, które zatrudniają mniej niż 50 osób i mają obroty roczne i/lub roczną sumę bilansową nieprzekraczającą 10 mln euro, z mocy prawa będą zobowiązane do realizacji zadań przeciwdziałających cyberzagrożeniom. W ten sposób wiele podmiotów stanie się z mocy prawa operatorami usług kluczowych. Będą one zobowiązane nie tylko do wykrywania zagrożeń, kształtowania kompetencji pracowników w zakresie cyberbezpieczeństwa oraz wdrażania i utrzymywania zabezpieczeń, ale także do samodzielnego identyfikowania świadczonych przez siebie usług kluczowych, które dotychczas były wskazywane w decyzjach administracyjnych. Rozsądne podejmowanie decyzji w tym zakresie wymaga nie tylko przeglądu wszystkich cyfrowych rozwiązań oraz zapewnianych przez nie usług, lecz także określania możliwych konsekwencji różnego rodzaju cyberataków na te usługi.

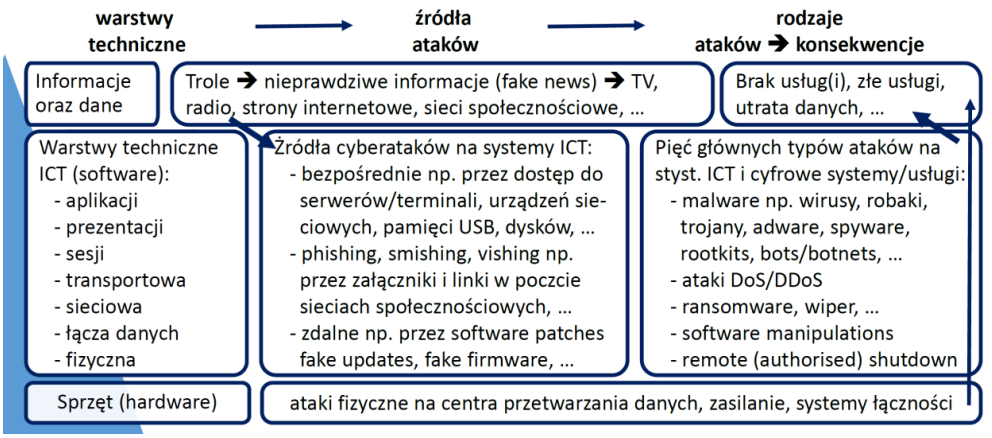
Centra wymiany i analizy informacji działające w Polsce

Zgodnie z wymaganiami dyrektywy NIS polska ustawa o krajowym systemie cyberbezpieczeństwa definiuje zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego (ang. Computer Security Incident Response Teams – CSIRT). W Polsce działają trzy CSIRT-y: CSIRT GOV, CSIRT MON oraz CSIRT NASK. Ustawa zawiera także wiele zapisów na temat tzw. sektorowych zespołów cyberbezpieczeństwa, przy czym nie ma w niej wytycznych dotyczących struktur typu CERT, takich jak SOC i NOC oraz struktur typu ISAC. Zespoły CERT (ang.Computer Emergency Response Team) zajmują się reagowaniem na incydenty komputerowe, obserwacją i analizą określonych aplikacji, usług cyfrowych, a także części cyfrowej infrastruktury, SOC (ang. Security Operations Centers) to centrum monitorowania bezpieczeństwa aplikacji i usług, a NOC (ang. Network Operations Centers) to centrum monitorowania bezpieczeństwa sieci. Zespoły takie jako CERT-y pracują w trybie 24/7 i zatrudniają wyspecjalizowany personel. Zupełnie inną funkcję pełnią ISAC (ang. Information Sharing and Analysis Centre). Centra wymiany i analizy informacji są tworzone w celu wymiany wiedzy i doświadczeń na temat incydentów cyberbezpieczeństwa w różnych sektorach gospodarki. Ich historia sięga lat 90. ubiegłego wieku. Idea zrodziła się w Stanach Zjednoczonych Ameryki w związku z raportem tzw. Prezydenckiej Komisji ds. Zabezpieczenia Infrastruktury Krytycznej (ang. President's Commission on Critical Infrastructure Protection – PCCIP). W raporcie tym wskazano internet i cyfrowe

systemy komunikacyjne jako najpoważniejsze zagrożenie dla infrastruktury krytycznej państwa. Pierwsze ISAC powstały po atakach terrorystycznych w Stanach Zjednoczonych i od tamtego czasu tworzone są kolejne w różnych częściach świata. Centra są miejscem wymiany informacji i doświadczeń na temat cyberbezpieczeństwa pomiędzy publicznymi i prywatnymi podmiotami funkcjonującymi w tym samym obszarze gospodarki lub powiązanych obszarach. Funkcję taką w sektorze usług bankowych i finansowych pełni Komisja Nadzoru Finansowego (KNF). W obszarze transportu kolejowego od grudnia 2020 roku – ISAC-Kolej, a w sektorze wydobywczo-energetycznym utworzony w 2022 roku ISAC-GIG. Autorzy artykułu uczestniczą w pracach ISAC-Kolej i ISAC-GIG. Podstawą ich działalności jest dobrowolna współpraca podmiotów różnej wielkości i o różnym charakterze, których łączy wykorzystywanie cyfrowych rozwiązań w tym samym lub współpracujących sektorach/podsektorach/obszarach działalności. Część z nich to duże przedsiębiorstwa dysponujące własnymi zasobami obejmującymi infrastrukturę i kompetentną kadrę, zapewniającymi wykrywanie cyberzagrożeń i im przeciwdziałanie. Pozostali członkowie to niewielkie podmioty, które nie mają takich zasobów. Cel jest wspólny – budowanie wiedzy i umiejętności w zakresie ochrony sieci, systemów i usług u wszystkich partnerów, bez względu na ich wielkość i zakres działania. Incydenty bezpieczeństwa i ataki dotykają wszystkich, szybko się rozprzestrzeniają, przenikają między różnymi podmiotami w branży, a nawet pomiędzy branżami.

Misja i zadania ISAC

Obecnie ISAC wspierają podmioty, które już zostały uznane za operatorów usług kluczowych oraz podmioty, które mimo że nie mają formalnie nadanego takiego statusu, zdają sobie sprawę z przynajmniej części cyfrowych zagrożeń i podejmują działania na rzecz cyberbezpieczeństwa. Budują niezbędne kompetencje i przygotowują się do spełnienia przyszłych wymagań formalnych. Mając świadomość cyberzagrożeń i wynikających z nich konsekwencji, dobrowolnie wprowadzają kolejne zabezpieczenia. Należy pamiętać, że skuteczna ochrona przed cyberzagrożeniami wymaga identyfikacji potencjalnych incydentów bezpieczeństwa i ataków oraz informacji na temat wykorzystywanych systemów ICT i ich otoczenia. Powiązania między cyberzagrożeniami oraz systemami ICT i ich otoczeniem przedstawia rysunek 1.



Źródło: Opracowanie własne.

Rys. 1. Środowisko cyberataków i ataków długoterminowych (typu APT)

Systemy infrastruktury krytycznej działają tylko wtedy, kiedy jest dostępna właściwa infrastruktura taka, jak: centra przetwarzania danych (CPD), infrastruktura energetyczna zapewniająca ich zasilanie i telekomunikacyjna zapewniająca łączność pozwalającą na wymianę danych pomiędzy geograficznie rozproszonymi na dużych obszarach cyfrowymi urządzeniami. Znaczenie infrastruktury krytycznej pokazują obserwowane w ostatnich latach zmasowane ataki. Widać to doskonale na przykładzie objętej wojną Ukrainy – to ataki na elektrownie, sieci przesyłowe czy maszty telekomunikacyjne. Zabezpieczanie tej infrastruktury i odtwarzanie jej po zniszczeniach to zadania dla wojska oraz służb energetycznych i telekomunikacyjnych. Z punktu widzenia ISAC infrastruktura taka ma po prostu być dostępna.

Z drugiej strony obserwuje się intensyfikację działań, których celem jest dezinformacja. Tak zwane farmy trolli tworzą i rozpowszechniają na szeroką skalę całkowicie nieprawdziwe lub zmanipulowane informacje oraz przekłamane dane, tzw. fake newsy, starając się w ten sposób budować fałszywy, sprzyjający określonym państwom lub grupom interesu przekaz medialny. Działania ISAC nie koncentrują się na wymianie i udostępnianiu informacji. Organizacje te zajmują się tym, co jest pomiędzy warstwą infrastruktury krytycznej, warstwą udostępniania i wymiany informacji oraz danych, w której stosowane są systemy cyfrowe wykorzystujące technologie ICT. Celem są działania, których rezultatem jest podnoszenie świadomości o potencjalnych zagrożeniach oraz wzmacnianie zabezpieczeń przed cyberzagrożeniami we wspieranych przez nie podmiotach.

Pojedynczy haktywiści[5], skrypt krakerzy[6] i hakerzy, a także coraz częściej i w coraz większej skali grupy hakerskie sponsorowane przez struktury mafijne, wojskowe czy państwowe atakują systemy ICT oraz cyfrowe usługi i urządzenia. Zazwyczaj wykorzystują do tego celu:

– **nieuprawniony bezpośredni dostęp** do serwerów i/lub terminali systemów ICT, urządzeń sieciowych w szczególności tych z niezabezpieczonymi spam portami. Podłączają do nie swoich komputerów, drukarek i innych urządzeń sieciowych zainfekowane pamięci USB czy zainfekowane dyski zewnętrzne. Wykorzystują inne systemy i urządzenia pozwalające na bezpośrednie przekazywanie złośliwego kodu, np. przez urządzenia korzystające z technologii bezprzewodowych takich jak WiFi czy bluetooth;

– **socjotechniki**, w tym fałszywe strony www, wiadomości e-mail z zainfekowanymi załącznikami lub linkami do specjalnie spreparowanych stron podszywających się pod strony popularnych serwisów, banków czy usługodawców (tzw. phishing). Wiadomości wymieniane między urządzeniami mobilnymi w formie SMS, MMS oraz w komunikatorach, z linkami do specjalnie tworzonych fałszywych stron www wprowadzających w błąd i/lub infekujących urządzenia nieostrożnych użytkowników (tzw. smishing). Głosowe namawianie na instalowanie aplikacji udostępniających atakującym zdalny dostęp do urządzeń (tzw. vishing);

– **nieuprawniony lub szkodliwie wykorzystywany zdalny dostęp** do systemów, wirtualnych serwerów, wirtualnych sieci prywatnych, kopii zapasowych systemów i danych oraz urządzeń przez instalowanie cyfrowych łat ze złośliwym kodem (tzw. fakepatches), fałszywe uaktualnienia (tzw. fakeupdaates), oprogramowanie sprzętowe podszywające się pod prawdziwy firmware (tzw. fakefirmware), które swoim działaniem może szpiegować użytkowników, blokować systemy i usługi lub nawet fizycznie niszczyć urządzenia.

Ataki na systemy ICT oraz cyfrowe usługi i urządzenia powodują materializację cyfrowych ryzyk opisanych na zlecenie Komisji Europejskiej przez ekspertów do spraw cyberbezpieczeństwa. Opis tych grup zawiera m.in.

5 Haktywiści – osoby, które używają komputerów i sieci do promowania celów społecznych i politycznych, zwłaszcza wolności słowa, praw człowieka i dostępu do informacji.

6 Skrypt krakerzy – osoby, które używają programów i skryptów napisanych przez innych bez dogłębnej znajomości zasad ich działania, jedynie po to, żeby uzyskać nieuprawniony dostęp do komputerowych kont użytkowników lub plików albo przeprowadzać ataki na systemy komputerowe.

„Transport cybersecurity toolkit”[7]. Zdefiniowano w nim cztery główne typy zagrożeń, tj.:

– **złośliwe oprogramowanie** obejmujące wirusy, robaki, trojany, adware, spyware, keyloggers, rootkits, bots & botnets itd., łącznie określane jako malware;

– generowanie **lawiny zapytań do systemów, stron www, cyfrowych usług** w wersji prostej (**ataki DoS**) i w wersji rozproszonej, tj. wykorzystującej wiele źródeł zapytań (np. z wykorzystaniem tożsamości uzyskanych poprzez phishing) **ataki DDoS** skutkujące blokowaniem lub zniszczeniem zaatakowanych usług cyfrowych;

– **nieuprawniony dostęp i kradzież danych** przez eksport danych lub ich szyfrowanie w celu wymuszenia korzyści majątkowych dzięki okupom (tzw. ransomware) lub **usuwanie danych** z wykorzystaniem tzw. wiperów. W tym drugim przypadku celem atakującego jest zazwyczaj zniszczenie systemu teleinformatycznego, np. w związku z działaniami zbrojnymi;

– **manipulacje oprogramowaniem** polegające na pozyskaniu ekspertów od dostawców systemów bądź wielomiesięcznym podsłuchiwaniu i analizowaniu działania systemów (tzw. ataki APT) w celu wytworzenia i wprowadzenia do systemu własnych urządzeń lub użytkowników, którzy mając złośliwe zamiary i wydając groźne polecenia, będą traktowani przez system jako w pełni uprawnieni użytkownicy. Takie ataki są trudne do realizacji, ale prowadzą do spektakularnych „zwycięstw” atakujących, np. katastrof.

Wojna za wschodnią granicą Polski pokazała, że do głównych zagrożeń dodać należy jeszcze **wyłączenie systemu lub urządzenia na odległość** [ang. remote (authorised) shutdown – RaS], które to działanie nie jest rozpoznane przez wyłączającego jako nieuprawnione. W wyniku prac prowadzonych w Instytucie Kolejnictwa wskazano kilka takich przypadków. Dotyczyły one m.in. skradzionych w Ukrainie i wywiezionych na wschód maszyn rolniczych czy linii automatycznego butelkowania win krymskich, która została wyłączona na odległość przez europejskiego producenta linii. W tym kontekście nowego znaczenia nabiera pytanie o to, kto jest producentem systemów, względnie kto i w jakim kraju przygotował i wgrał firmware.

7 *Transport cybersecurity toolkit*, European Union, 2020, https://www.fecc.org/wp-content/uploads/2020/12/DG-MOVE-Transport-Cybersecurity-Toolkit-FINAL.pdf [dostęp: 5.12.2022].

Polskie ISAC i zakres ich działania

W Polsce struktury typu ISAC nie pracują w trybie 24/7. Ich zadaniem jest wspomaganie już ustanowionych i przyszłych operatorów usług kluczowych. Działania koncentrują się na wymianie informacji pomiędzy podmiotami. Wymianą informacji, kompetencji i dobrych praktyk jest zainteresowanych wiele jednostek. Znacznie gorzej wygląda sprawa finansowania działalności ISAC. Ewentualny rozdział kosztów na podmioty jest poważnym wyzwaniem. Można wprawdzie założyć, że działania ISAC będą finansowane ze źródeł zewnętrznych, ale ich pozyskanie wymaga czasu i, niestety, dodatkowych środków. Dlatego członkowie ISAC-Kolej podjęli decyzję, że każdy podmiot przystępujący do ISAC, począwszy od założycieli, w pełni pokrywa koszty swojego zaangażowania we wspólne prace. Obecnie w podobnej formule funkcjonuje ISAC-GIG. W efekcie oba centra korzystają z wymiany informacji drogą elektroniczną i spotkań on-line. ISAC-Kolej nie ma ambicji przekształcić się w przyszłości w strukturę typu CERT, niezależnie od tego, że w wielu publikacjach wskazuje się przekształcenie struktur typu ISAC w struktury typu CERT jako naturalną konsekwencję rozwoju zabezpieczeń przed cyberzagrożeniami na poziomie branż czy sektorów. W transporcie kolejowym struktury typu CERT już działają, współpracują z branżowym centrum ISAC, i wydaje się niemal pewne, że będą się rozwijać równolegle do ISAC-Kolej. ISAC-GIG nie wyklucza budowy sektorowego SOC. Takie struktury funkcjonują u niektórych partnerów, ale mają one zasięg lokalny.

Jak ISAC wspierają swoich członków

ISAC-Kolej nie tworzy samodzielnie dużych opracowań o stanie cyberbezpieczeństwa sektora transportu. Dzieli się informacjami zarówno pozyskanymi z opracowań zewnętrznych, jak i z raportów przygotowanych przez swoich członków. Przykładem w obszarze transportu kolejowego mogą być przeznaczone dla kolei raporty Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[8] opracowane we współpracy z Agencją UE ds. Kolei (ERA), które nie

8 *Railway Cybersecurity, security measures in the Railway Transport Sector*, European Union Agency for Cybersecurity ENISA, November 2020, https://cyberpolicy.nask.pl/wp-content/uploads/2021/01/ENISA-Report-Railway-Cybersecurity.pdf [dostep: 25.01.2023]; *Railway Cybersecurity. Good practices in cyber risk management*, European Union Agency for

są dostępne w języku polskim, a były szczegółowo omawiane i dyskutowane na forum ISAC-Kolej. Podobnie były dyskutowane dokumenty normatywne dotyczące cyberbezpieczeństwa w transporcie kolejowym, np. specyfikacja techniczna CENELEC TS 50701[9] czy tom standardów kolejowych Centralnego Portu Komunikacyjnego (CPK) dotyczący spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa[10]. Omawiane i dyskutowane były także dokumenty prawne. W efekcie zostały zgłoszone uwagi zarówno do projektu dyrektywy NIS-2, jak i do specyfikacji TS 50701.

Na potrzeby podmiotów kolejowych podczas prac ISAC-Kolej zostały przyjęte wytyczne dotyczące cyberbezpieczeństwa pracowników tych podmiotów. Wytyczne zostały udostępnione nie tylko członkom ISAC, lecz także wszystkim zainteresowanym poprzez druk w „Problemach Kolejnictwa"[11] oraz „Magazynie Kultury Bezpieczeństwa"[12] wydawanym przez Urząd Transportu Kolejowego. Co istotniejsze, członkowie ISAC-Kolej drogą elektroniczną regularnie otrzymują:

– codzienne raporty CSIRT GOV dotyczące złośliwego ruchu sieciowego (rekomendacje dotyczące blokowania konkretnych IP);

– tygodniowe raporty CSIRT GOV zawierające informacje na temat wykrytych podatności w produktach IT (rekomendacje dotyczące aktualizacji systemów i oprogramowania);

– tygodniowy „Biuletyn Informacyjny" SOC PKP Informatyka dotyczący cyberbezpieczeństwa w transporcie kolejowym.

W przypadkach wykrycia zagrożeń:

– informacje o nowych kampaniach phishingowych;

– informacje o zarejestrowaniu domen, które mogą być wykorzystane do ataków phishingowych (rekomendacje blokowania złośliwych domen na

Cybersecurity ENISA, November 2021, https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management [dostęp: 25.01.2023]; *Zoning and conduits for railways*, European Union Agency for Cybersecurity ENISA and European Rail ISAC, February 2022, https://www.enisa.europa.eu/publications/zoning-and-conduits-for--railways [dostęp: 25.01.2023].

9 CENELEC Technical Specification TS 50701, Railway applications – Cybersecurity, 2021.

10 *Standardy techniczne. Szczegółowe warunki techniczne dla budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego. Wytyczne projektowania*, *t. 18*, *Wymagania w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa*, wersja 1.3.0, Warszawa 2021.

11 M. Pawlik, *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*, „Problemy Kolejnictwa" 2021, z. 191.

12 Idem, *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych* [w:] *Magazyn kultury bezpieczeństwa*, Warszawa 2021, s. 45–53.

urządzeniach brzegowych, stosowania odpowiednich filtrów antyspamowych, czujności przy wysyłaniu/odbieraniu wiadomości przesyłanych drogą elektroniczną przez pracowników);

– informacje o wykryciu podatności zero-day, możliwości ich wykorzystania oraz IoC (rekomendacje – różne, w zależności od typu podatności);

– informacje o kampaniach phishingowych dystrybuujących złośliwe oprogramowanie oraz IoC złośliwej kampanii (rekomendacje – wdrożenie stosownych reguł na urządzeniach filtrujących pocztę elektroniczną),

a w razie stwierdzenia – informacje o atakach DDoS, w tym o możliwych atakach na strony internetowe i serwisy (rekomendacje – ochrona antyDDoS, monitorowanie infrastruktury, przygotowanie się na ograniczenia ruchu przy eskalacji), oraz w razie konieczności – przydatne informacje, np. dotyczące certyfikacji produktów IT na terenie Rosji, działalności grup APT, Killnet itp.

Budowie ISAC-GIG przyświecała potrzeba wymiany wiedzy, doświadczeń oraz dobrych praktyk w zakresie stosowania zabezpieczeń systemów teleinformatycznych, a także współdziałania w obsłudze incydentów dotyczących cyberbezpieczeństwa w sektorach wydobywczym i energetycznym. W skład ISAC-GIG wchodzą główni przedstawiciele zakładów wydobywczych, w tym podziemne zakłady górnicze węgla kamiennego i miedzi, dostawcy energii, firmy wspierające górnictwo oraz jednostki naukowe, tj. instytuty badawcze oraz uczelnie wyższe. Do głównych zadań ISAC-GIG należy:

– umożliwienie aktywnego uczestnictwa podmiotom z sektora wydobywczego i energetycznego w krajowym systemie cyberbezpieczeństwa oraz dostępu do aktualnych informacji dotyczących bezpieczeństwa;

– wymiana doświadczeń, budowanie świadomości cyfrowej oraz rozwój kompetencji w dziedzinie cyberbezpieczeństwa (szkolenia, warsztaty, działania proaktywne);

– wymiana informacji na temat rodzajów stosowanych zabezpieczeń oraz struktur cyberbezpieczeństwa w organizacjach członkowskich ISAC-GIG;

– wsparcie w zakresie cyberbezpieczeństwa zaangażowanych podmiotów zgodnie z wymogami ustawy o krajowym systemie cyberbezpieczeństwa;

– wsparcie technologiczne w zakresie ciągłości działania systemów IT/OT/IoT;

– wypracowanie wytycznych dotyczących stosowania rozwiązań do ochrony przed zagrożeniami z sieci;

– określanie wymagań dotyczących certyfikacji cyberbezpieczeństwa produktów i usług w sektorach wydobywczym i energetycznym.

Do wymiany informacji na temat wskaźników zagrożeń i złośliwego oprogramowania w ISAC-GIG jest wykorzystywana platforma MISP (Malware Information Sharing Platform & Threat Sharing). Korzysta z niej wiele organizacji na świecie, a jej celem jest wspieranie prac na rzecz przeciwdziałania ukierunkowanym atakom oraz ich wczesnej detekcji. Na stronie domowej ISAC-GIG (https://isac.gig.eu) dostępne są informacje o bieżącej aktywności centrum i działaniach partnerów na rzecz cyberbezpieczeństwa. Będą na niej również udostępniane zbiorcze raporty roczne na temat cyberbezpieczeństwa w sektorze wydobywczo-energetycznym.

W ramach swojej dotychczasowej działalności ISAC-GIG i wchodzące w jego skład jednostki organizują regularne cyberpoligony, które dzięki rywalizacji zespołów bezpieczeństwa poszczególnych partnerów sprawdzają swoją wiedzę i umiejętności w zakresie reagowania na incydenty i zwalczania cyberataków. Organizowane są również warsztaty na konferencjach branżowych oraz seminaria, których celem jest podnoszenie poziomu świadomości cyberzagrożeń dotykających sektor oraz przekazywanie wiedzy o trendach i najnowszych rozwiązaniach w wykrywaniu cyberataków i ograniczaniu ich skutków. Prelegentami są naukowcy oraz przedstawiciele firm ICT. ISAC-GIG był inicjatorem oraz współorganizatorem utworzenia na Politechnice Śląskiej studiów podyplomowych z dziedziny cyberbezpieczeństwa systemów przemysłowych. W planach jest organizacja regularnych szkoleń z cyberbezpieczeństwa dla pracowników sektora.

Współpraca członków ISAC-GIG z środowiskiem naukowym zaowocowała pozyskaniem finansowania na projekt badawczy, którego celem jest opracowanie i wytworzenie nowych systemów typu SOAR wyposażonych w autorskie narzędzia sprzętowo-programowe do wykrywania anomalii w sieciach IT/OT/IoT, w tym wykorzystujące metody sztucznej inteligencji. Planuje się, że w przyszłości mogłyby one wspierać sektorowy SOC. Podmioty członkowskie ISAC-GIG planują w przyszłości dalsze wnioskowanie do krajowych i międzynarodowych jednostek finansujących badania o fundusze na prace związane z wytwarzaniem innowacyjnych rozwiązań w dziedzinie cyberbezpieczeństwa.

Podsumowanie

To początek drogi. Polskie ISAC to młode organizmy, które dopiero się kształtują i ciągle poszukują najlepszej drogi dla siebie. Stoi przed nimi wiele wyzwań, w tym taka organizacja współpracy z podmiotami dostarczającymi technologie

cyfrowe, żeby nie zostały naruszone równe zasady konkurencji pomiędzy dostawcami sprzętu i oprogramowania. Tego typu firmy nie są wprost zapraszane do udziału w pracach ISAC. Formuła współpracy musi być pilnie wypracowana.

Konieczna jest również intensyfikacja współpracy między partnerami centrów, budowanie wzajemnego zaufania i przekonania, że działając razem, można osiągnąć znacznie więcej. Z czasem mogą pojawić się potrzeby inwestycji, np. w sprzęt i oprogramowanie do tworzenia platform szkoleniowych, ale o tym będą już indywidualnie decydować poszczególne centra. Następnym krokiem będzie z pewnością większe otwarcie na otoczenie, nie tylko w ramach reprezentowanego sektora, ale też na lokalną społeczność, przedsiębiorców i instytucje administracji państwa. Z pewnością wskazane jest również zawarcie porozumień pomiędzy centrami zarówno krajowymi, jak i międzynarodowymi. Taka współpraca, szczególnie z bardziej już dojrzałymi organizacjami zagranicznymi, pozwoli na szybsze reagowanie w celu powstrzymania ataku, a wręcz zapobiegania jego wystąpieniu.

Bibliografia

Pawlik M., *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*, „Problemy Kolejnictwa" 2021, z. 191.

Pawlik M., *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych* [w:] *Magazyn kultury bezpieczeństwa*, Warszawa 2021.

Railway Cybersecurity. Good practices in cyber risk management, European Union Agency for Cybersecurity ENISA, November 2021, https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management [dostęp: 25.01.2023].

Railway Cybersecurity, security measures in the Railway Transport Sector, European Union Agency for Cybersecurity ENISA, November 2020, https://cyberpolicy.nask.pl/wp-content/uploads/2021/01/ENISA-Report-Railway-Cybersecurity.pdf [dostep: 25.01.2023].

Standardy techniczne. Szczegółowe warunki techniczne dla budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego – wytyczne projektowania, t. 18, *Wymagania w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa*, wersja 1.3.0, Warszawa 2021.

Transport cybersecurity toolkit, European Union 2020, https://www.fecc.org/wp-content/uploads/2020/12/DG-MOVE-Transport-Cybersecurity-Toolkit-FINAL.pdf [dostęp: 5.12.2022].

Zoning and conduits for railways, European Union Agency for Cybersecurity ENISA and European Rail ISAC, February 2022, https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways [dostęp: 25.01.2023].

The role of the Information Sharing and Analysis Centers' n building the resilience of the key sectors of the Polish economy

Abstract

As the threats from cyberspace to IT systems (information technology) and digital OT systems (operational technologies) using ICT technologies (information and communication technologies) grow exponentially, while at the same time the scale of the use of digital data collecting, processing and sharing for the needs of many national economy areas and to support functioning of the state in terms of, for example, defence, health care, education or citizen services, building awareness of the risks and skills to secure networks, systems and digital services against cyber threats becomes crucial. A new type of structures called ISACs (Information Sharing and Analysis Centres) play an important role in this respect. The co-authors, based on the provisions of the law and their own experience in ISAC-Kolej and ISAC-GIG centers, present the ecosystem around ISAC centers, their tasks and challenges.

Key words: cybersecurity, key service operators, ISACs Information Sharing and Analysis Centers