Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny

Kaja Ciglic, Mariusz Jurczyk, Agnieszka Konkel,
Izabela Lewandowska-Wiśniewska,
Dariusz Mikołajczyk, Krzysztof Podwiński,
Leonid Rozenblum, Jarosław Sordyl, Marcin Spychała,
Yitzhak (Itzik) Vager, Robert Żelechowski
Redakcja: Dominik Skokowski
Współredakcja: Ziemowit Jóźwik

INSTYTUT KOŚCIUSZKI

Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny

Kaja Ciglic, Mariusz Jurczyk, Agnieszka Konkel,
Izabela Lewandowska-Wiśniewska, Dariusz Mikołajczyk,
Krzysztof Podwiński, Leonid Rozenblum,
Jarosław Sordyl, Marcin Spychała, Yitzhak (Itzik) Vager,
Robert Żelechowski
Redakcja: Dominik Skokowski
Współredakcja: Ziemowit Jóźwik

Instytut Kościuszki

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

Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny
Kaja Ciglic, Mariusz Jurczyk, Agnieszka Konkel, Izabela Lewandowska-Wiśniewska, Dariusz Mikołajczyk, Krzysztof Podwiński, Leonid Rozenblum, Jarosław Sordyl, Marcin Spychała, Yitzhak (Itzik) Vager, Robert Żelechowski

Redakcja: Dominik Skokowski
Współredakcja: Ziemowit Jóźwik

Ikony z the Noun Project: Electric Boiler by Alexander Panasovsky, Washing Machine by Focus, lamp by Drishya, Electricity by Nakul Dhaka, Computer by art shop, signal tower by Surya, database by Grant Fisher, Server by Grant Fisher, Monitor by unlimicon, Cloud by Kimmi Studio, Phone by Kimmi Studio, hub by Chameleon Design, meter by Eucalyp, Electricity Meter by Stepan Voevodin, Smart Home by artworkbean, Radiator by Michael Thompson, Radiator by Stepan Voevodin, plumbing by Stepan Voevodin, counter by Sergey Demushkin, counter by Stepan Voevodin, Gas by Stepan Voevodin, brick wall by Tom Tom, Key by Icon Depot

Instytut Kościuszki
ul. Feldmana 4/9-10
31-130 Kraków, Poland
e-mail: ik@ik.org.pl
+48 126329724
ww.ik.org.pl
ISBN: 978-83-63712-32-7

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.

Podsumowanie

Celem raportu *Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny* jest analiza najważniejszych aspektów związanych z zapewnieniem cyberbezpieczeństwa w kluczowym z punktu widzenia funkcjonowania państwa sektorze energetycznym. Poszczególne rozdziały prezentują zarówno wyzwania związane z budową systemu i rozwojem kultury cyberbezpieczeństwa infrastruktury krytycznej, jak i dobre praktyki. Grono autorów obejmujących swoim doświadczeniem sektor energetyczny, globalną branżę IT oraz sektor ubezpieczeniowy, a także szeroka perspektywa uwzględniająca czynniki prawno-administracyjne, technologiczne, organizacyjne i gospodarcze pozwala dokonać kompleksowej prezentacji zagadnienia.

Konieczne jest budowanie kultury cyberbezpieczeństwa sektora energetycznego w oparciu o holistyczne podejście, uwzględniające zarówno aspekty techniczne, operacyjne, jaki i strategiczne. Cyberatak na obiekty infrastruktury energetycznej może mieć katastrofalne skutki dla mienia, zdrowia i życia pracowników, środowiska, całej gospodarki, czy nawet funkcjonowania państwa, włączając funkcjonowanie administracji i potencjał obronny. Wyzwania cyberbezpieczeństwa w szczególny sposób dotykają przedsiębiorstwa przemysłowe, ponieważ muszą one chronić nie tylko swoją infrastrukturę IT ale również OT. Potwierdza to fakt, że aż 16% cyberataków nakierowanych jest na branżę energetyczną[1], czyniąc ją drugim najczęściej atakowanym sektorem po administracji publicznej .

Poszczególne rozdziały raportu prezentują wnioski dotyczące różnych aspektów cyberbezpieczeństwa sektora energetycznego. Poniżej przedstawiamy zestaw rekomendacji sporządzonych na podstawie niniejszego opracowania.

1 Symantec: Targeted Attacks Against the Energy Sector, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf.

Ramowe rekomendacje:

- Wiodące podmioty polskiego sektora energetycznego powinny realizować kompleksowe podejście do budowy kultury cyberbezpieczeństwa oparte na rozwoju wyspecjalizowanego zespołu odpowiedzialnego za obsługę incydentów komputerowych (CERT), systematycznych szkoleniach dla kadry zarządzającej i pracowniczej wszystkich szczebli nakierowanych na podnoszeniu ogólnego poziomu świadomości zagrożeń cybernetycznych w organizacji na poziomie operacyjnym (w tym ćwiczenia), realizacji okresowych audytów (np. SIM3, SUOPT, Audyt APT) oraz umiejętnym zarządzaniu ryzykiem cybernetycznym.

- Operatorzy usług kluczowych – w tym szczególnie podmioty sektora energetycznego powinny budować wyspecjalizowane zespoły reagowania na incydenty komputerowe CERT/CSIRT, w skład których wchodzić powinni eksperci w dziedzinie bezpieczeństwa z uwzględnieniem wielu obszarów specjalizacji np. informatyka śledcza, inżynieria wsteczna oraz bezpieczeństwo automatyki przemysłowej. Zespół ten powinien uczestniczyć w bieżącej wymianie informacji nie tylko wewnątrz organizacji, ale poprzez udział w stowarzyszeniach dedykowanych CERT-om, mieć zapewniony dostęp do aktualnej wiedzy oraz dzielić się własnymi doświadczeniami z innymi CERT-ami w kraju i za granicą, co przyczyni się do podniesienia kompetencji zespołu. Pod rozwagę poddane jest utworzenie energetycznego CERT-u sektorowego, czy forum wymiany informacji (np. brytyjski *Cyber Security Information Sharing Partnership*).

- Dyrektywa NIS powinna być traktowana jako zestaw wymogów minimalnych w obszarze poziomu bezpieczeństwa sieci i systemów informatycznych a nie jako ostateczny punkt odniesienia. Z uwagi zarówno na specyfikę krajową oraz zaprogramowany w niniejszym akcie mechanizm okresowego przeglądu i nowelizacji, podmioty sektora energetycznego powinny dokonywać wdrożenia postanowień aktu w odniesieniu przede wszystkim do własnej oceny ryzyka, podatności i krajobrazu zagrożeń, traktując przedmiotowe przepisy prawa unijnego wyłącznie jako minimum. Niezależnie od legislacyjnej kwalifikacji poszczególnych systemów, elementów infrastruktury technicznej i urządzeń jako komponentów realizacji usług kluczowych, operator w oparciu o własną wiedzę i doświadczenie powinien opracować co najmniej procedury postępowania w przypadku incydentu, zarządzania ciągłością działania, monitorowania, audytu i testowania oraz zadbać o zgodność z normami międzynarodowymi (np. ISO 27001).

- Podmioty sektora energetycznego, z uwagi na potencjalne katastrofalne skutki dla mienia, zdrowia i życia, powinny zbudować centra operacji bezpieczeństwa (SOC, Security Operations Center) w celu efektywnego przeciwdziałania cyberatakom. W związku z dynamiką ewolucji i wzrostem liczby oraz częstotliwości zagrożeń

dotykających podmioty przemysłowe, zalecanie jest tworzenie tzw. SOC nowej generacji, wykorzystujących zdobycze innowacyjnych technologii, m.in. sztucznej inteligencji, która umożliwia „wirtualną analizę" incydentów. SOC nowej generacji zakłada odejście od bazowania na alertach bezpieczeństwa (*alert-driven approach*) do modelu opartego na analizie predyktywnej (*predictive intelligence-driven approach to cybersecurity*) zagrożeń.

- Z uwagi na specyfikę sektora przemysłowego niezbędne są przeglądy okresowe systemów infrastruktury technicznej i urządzeń. Kluczowy jest monitoring bezpieczeństwa styku sieci organizacji z siecią Internet i ochrona cybernetyczna obszarów zarówno IT, jak i OT, w tym szczególnie systemów sterowania, których elementami są m.in.: SCADA, DCS, HMI, PLC, RTU, IED, SIS, sensory, przekaźniki. Istotność infrastruktury technicznej i urządzeń jako jednego z wielu elementów występujących w zapewnieniu bezpieczeństwa krajowego systemu energetycznego dobrze ilustruje problematyka bezpieczeństwa Systemów Inteligentnego Opomiarowania AMI.

- W związku z automatyzacją systemów przemysłowych i postępem ich integracji z teleinformatyką, niezbędne jest, aby ich ochrona przed atakami cybernetycznymi zapewniała ich integralność, poufność, dostępność oraz rozliczalność. Dodatkowo, oprócz zastosowania specjalistycznych narzędzi do monitorowania, inspekcji, filtrowania i badania anomalii ruchu w kanałach komunikacyjnych, sama architektura systemu zdalnego sterowania musi być odporna na znane techniki ataku i włamań na poziomie warstwy aplikacyjnej oraz sieciowej poprzez zastosowanie partycjonowania i segmentacji sieci z określeniem granic tejże separacji.

- Ze względu na transgraniczny charakter zagrożeń cybernetycznych, międzynarodowe sojusze i współpraca są kluczowe w celu zapewnienia bezpieczeństwa sieci i informacji. W związku z tym, dobrowolne ramy cyberbezpieczeństwa opracowane przez amerykański Narodowy Instytut Standaryzacji i Technologii (*National Institute for Standards and Technology*, NIST) mogą stanowić jeden z modeli dla tworzenia polityk UE w tym zakresie.

- Biorąc pod uwagę fakt, że ekosystem cyberbezpieczeństwa jest rozdrobniony i zdominowany przez małe i średnie przedsiębiorstwa (MŚP) oraz startupy, tworzenie hubów cyberbezpieczeństwa angażujących te podmioty mogłoby wymusić konsolidację rynku produktów i usług tego sektora, szczególnie w kontekście szans, jakie zamówienia publiczne i prywatne w Europie przynoszą europejskim dostawcom.

- Określone sektory lub infrastruktury krytyczne mogą mieć zaawansowane wymagania dotyczące cyberbezpieczeństwa, lecz rzadko są one zharmonizowane na poziomie unijnym, często zaś są specyficzne dla danego kraju. Należy dążyć do stworzenia pojedynczej instytucji bazującej na Europejskim Katalogu Standardów (*European*

Catalogue of Standards) i oferującej jasne wskazówki co do wymogów ICT w obszarze zamówień publicznych. Mając na uwadze rekomendacje powołanej przez Komisję Europejską grupy ekspertów ds. cyberbezpieczeństwa w sektorze energetycznym, jak również niejednolity poziom zaawansowania technologicznego państw członkowskich należy zastanowić się nad dostosowaniem do europejskich potrzeb grupy modeli C2M2.

- UE powinna stworzyć specjalną strategię cyberbezpieczeństwa dla sektora energetycznego, w której standaryzacja oraz mechanizmy ułatwiające wymianę informacji byłyby potraktowane priorytetowo. Należy dokonać oceny, czy potrzebne będzie powołanie osobnego organu odpowiedzialnego za koordynację implementacji takiej strategii, czy zadanie to będzie mogło zostać powierzone agencji ENISA.

Sztuczna inteligencja w służbie cyberbezpieczeństwu infrastruktury krytycznej – szanse i zagrożenia

Marcin Spychała, IBM

Wprowadzenie

Kiedy George Clooney i Nicole Kidman ratowali Nowy Jork (dla odmiany) przed wybuchem przenośnej głowicy jądrowej w filmie Peacemaker, mało kto zdawał sobie sprawę, że film został zainspirowany rzeczywistymi wydarzeniami. Zresztą większość osób wychowanych na filmach akcji z okresu post zimnej wojny mogło nabrać przekonania, że większość zagrożeń terrorystycznych związana jest z niewłaściwym zabezpieczeniem dostępu do infrastruktury krytycznej albo do broni jądrowej w republikach post radzieckich. Taka narracja oczywiście nie była przypadkowa – ale nie wynikała jedynie z faktu, że za produkcje większości dostępnych filmów odpowiedzialni byli Amerykanie.

Paradoksalnie 24 lata później pytanie „czy lepszym zabezpieczeniem infrastruktury krytycznej jest supernowoczesny komputer czy większa kłódka w szopie?" wcale nie jest nieuprawnione. Tempo rozwoju świata wymusza coraz większą automatyzację zadań wykonywanych dotychczas albo manualnie albo przez sterowniki analogowe. Z perspektywy optymalizacji procesu jest to trend, którego nie da się już zawrócić. Dla specjalisty do spraw bezpieczeństwa jest to jednak coraz większy problem i ciągły ból głowy poczynając od potrzeby zapewnienia interoperacyjności narzędzi, których wyprodukowanie niejednokrotnie dzielą dekady, do ciągłego śledzenia potencjalnych zagrożeń dla zainstalowanej infrastruktury, które są odkrywane każdego dnia. A to tylko przy założeniu, że taki proces śledzenia podatności jest w przedsiębiorstwie realizowany oraz, że podatność da się wykryć zdalnie, a nie przez odwiedzenie wszystkich jednostek organizacyjnych firmy.

Dla przykładu na konferencji Black Hat 2017 przedstawiciel firmy IOActive pokazał wyniki badań nad oprogramowaniem stacji do wykrywania promieniowania radioaktywnego. Odkrycia są równie szokujące, co proste do niewłaściwego wykorzystania. Dla przykładu – jedna z bramek do wykrywania promieniowania miała wprowadzonych kilka poziomów uprawnień. Badanie

kodu programu ujawniło jednak, że producent pozostawił również tylną furtkę dającą maksymalne uprawnienia. Konstrukcja kodu pokazuje, że było to działanie jak najbardziej celowe a konsekwencją wykorzystania takiego dostępu jest na przykład możliwość wyłączenia alarmu radiacyjnego, czyli głównej funkcjonalności całego mechanizmu.

```
// Lmi.Sam.Supervisor.Host
private const string BackDoor = "5147";
```

```
// Lmi.Sam.Supervisor.Host
public void ValidatePassword(string Password)
{
    ApplicationSettings applicationSettings = Program.Monitor.Settings;
    this.currentPasswordLevel = Host.Level.None;
    if (Password == applicationSettings.PasswordDecrypt(applicationSettings.Level1Password))
    {
        this.currentPasswordLevel = Host.Level.Level1;
    }
    if (Password == applicationSettings.PasswordDecrypt(applicationSettings.Level2Password))
    {
        this.currentPasswordLevel = Host.Level.Level2;
    }
    if (Password == "5147")
    {
        this.currentPasswordLevel = Host.Level.Level2;
    }
}
```

W tym momencie przez głowę specjalisty do spraw zabezpieczeń infrastruktury krytycznej przelatuje tornado emocji. Od ulgi związanej z faktem, że ktoś wykrył tę podatność, przez ciekawość, ile takich podatności jest nieznanych, przez niepewność związaną z pytaniem, czy w zarządzanej infrastrukturze są takie tylne furtki, aby w końcu zatrzymać się na uczuciu przytłoczenia związanego z koniecznością zapewnienia ciągłości bezpieczeństwa nie tylko dla infrastruktury jako całości, ale również dla każdego komponentu z osobna wiedząc, że jedna rzecz od 24 lat na pewno się nie zmieniła. W dalszym ciągu zorganizowane grupy przestępcze stają się bardziej aktywne w próbie uzyskania dużych partii cennych materiałów z przedsiębiorstw. Kontaktują się z personelem, badają słabe punkty systemu i możliwości kradzieży lub zakłócenia działalności na wielką skalę.

Czy sztuczna inteligencja może przyjść tu z pomocą? Gdzie już jest wykorzystywana a gdzie powinniśmy ją zacząć wykorzystywać w najbliższej przyszłości? Co ze skutkami działań systemów autonomicznych posiadających funkcje samouczące? Jakie korzyści a jakie zagrożenia niesie za sobą wykorzystanie sztucznej inteligencji nie tylko do wykrywania, ale również do zwalczania cyberataków? Nie bez znaczenia będzie też wyciągnięcie wniosków z istniejących już wdrożeń systemów bezpieczeństwa wspomaganych sztuczną inteligencją.

Przykłady zastosowań

Głównym celem badań nad sztuczną inteligencją jest stworzenie technologii pozwalającej komputerom i maszynom funkcjonować w inteligentny sposób. Całość wyzwań można rozbić na podkategorie w następujący sposób:

- Uczenie się
- Rozumienie języka naturalnego
- Wnioskowanie i rozwiązywanie problemów
- Planowanie
- Kreatywność

- Inteligencja społeczna
- Generyczna inteligencja
- Prezentowanie wiedzy
- Percepcja
- Motywacja i manipulacja

W niedalekiej przyszłości, gdy systemy sztucznej inteligencji staną się bardziej skuteczne, zaczniemy widzieć bardziej zautomatyzowane i coraz bardziej wyrafinowane ataki socjotechniczne. Wzrost liczby cyberataków wspieranych sztuczną inteligencją spowoduje eksplozję włamań do sieci, kradzieży danych osobowych i rozprzestrzeniania się inteligentnych wirusów komputerowych na skalę epidemii. Ironicznie, naszą najlepszą nadzieją, aby bronić się przed włamaniami wspieranymi funkcją sztucznej inteligencji, jest użycie sztucznej inteligencji. Prawdopodobnie jednak doprowadzi to do wyścigu zbrojeń, którego konsekwencje mogą być bardzo kłopotliwe w dłuższej perspektywie, zwłaszcza gdy aktorzy rządowi dołączą w większej skali do cyberataków na cele komercyjne.

Biorąc pod uwagę ilość zastosowań sztucznej inteligencji w codziennym życiu (Siri, Netflix, Nest, Alexa, chatboty, autonomiczne samochody itp.) oczekiwania wobec zastosowania sztucznej inteligencji do walki z cyberprzestępczością są uprawnione. Niektóre raporty szacują, że wielkość rynku sztucznej inteligencji i robotyki osiągnie 153 miliardy dolarów do 2020 roku. Rozwój tego obszaru w ostatnich latach jest fenomenem. Google przewiduje, że roboty osiągną poziom ludzkiej inteligencji do roku 2029 a analitycy z McKinsey&Company dowiedli, że prawie 50% amerykańskich i europejskich miejsc pracy może być całkowicie zautomatyzowanych.

Czy można przyjąć więc, że mamy do czynienia ze zmierzchem cyberprzestępczości i świtem zautomatyzowanej ochrony opartej na sztucznej inteligencji? Tylko druga teza ma poparcie w analizowanych faktach. W związku z faktem, że cyberzagrożenia robią się coraz bardziej zaawansowane i również wspierane przez sztuczną inteligencję, należy dobrze zrozumieć, co sztuczna inteligencja może zrobić, czego nie może i czego wręcz nie powinna robić, aby zminimalizować płaszczyznę potencjalnego ataku. Zwłaszcza, że zgodnie z tezą ortogonalności Bostroma dowolny system sztucznej inteligencji może charakteryzować się dowolną konfiguracją inteligencji i celów. Takie cele mogą zostać zdefiniowane na etapie projektu, przez włamania przestępców lub w późniejszym etapie przy użytkowaniu systemów. W konsekwencji, w zależności od tego czyje cele realizuje system sztucznej inteligencji (korporacji, socjopatów, dyktatorów, wojska, przemysłu, terrorystów itd.) możemy mieć do czynienia z konsekwencjami bezprecedensowymi w historii ludzkości.

Obecnie systemy automatyzujące prace analityków bezpieczeństwa czy automatycznie zabezpieczające infrastrukturę krytyczną bez udziału człowieka są już dostępne. W dalszej części analizie poddane zostaną możliwości w kontekście potencjalnych zastosowań.

Ochrona przed atakiem i przed błędami w oprogramowaniu

Oprogramowanie zarządzające komputerami, sterownikami i urządzeniami typu „smart" w infrastrukturze jest naturalnie podatne zarówno na błędy w kodzie, jak i błędy ludzkie, które mogą być wykorzystane przez przestępców. Potencjał konsekwencji jest praktycznie nieskończony i może dotyczyć bezpieczeństwa jednostki, regionu czy całego kraju. Środki ochrony muszą więc być przystosowane do wykrywania pojedynczego hakera, grupy przestępczej oraz coraz częściej oprogramowania samodzielnie wspieranego przez systemy sztucznej inteligencji z mechanizmami polimorficznymi lub zmieniać sposób zachowania w zależności od konieczności i dostępnych wektorów ataku. Rozwój systemów, które mogą wyszukiwać i naprawiać te błędy i luki w zabezpieczeniach, a także bronić przed atakami wyrósł z tej pilnej potrzeby, a wiele firm które pracują nad autonomicznymi systemami jest finansowana przez wojsko (DARPA) i przez uznane uniwersytety na całym świecie.

Najczęściej podawanym przykładem samodzielnego systemu zabezpieczającego jest rozwiązanie Mayhem tworzone w startupie ForAllSecure wspólnie z Uniwersytetem Carnegie Mellon – zwycięzca zawodów autonomicznych systemów bezpieczeństwa – Cyber Grand Challenge które odbyły się 4 Sierpnia 2016 r. w Las Vegas. Ich organizatorem jest amerykańska agencja zaawansowanych projektów obronnych DARPA podlegająca Pentagonowi. Autonomiczne programy miały bronić się przed włamaniami i próbować zaatakować przeciwników, wykorzystując wiedzę o lukach. DARPA wprowadziła jednak nowy element – serwery, na których uruchomiono e-hakerów, musiały cały czas normalnie funkcjonować. Analiza kodu, obrona i atak nie mogły znacząco spowolnić normalnej pracy. Jak się okazało, miało to znaczenie dla ostatecznej klasyfikacji.

Tego typu systemy, autonomicznie analizujące luki w oprogramowaniu i potrafiące je automatycznie zabezpieczać to bliska przyszłość każdego centrum cyberbezpieczeństwa. Na chwilę obecną jednak są jeszcze niedoskonałe, co pokazała późniejsza konferencja Def Con 2016, gdzie Mayhem jako pierwszy w historii autonomiczny „haker" przystąpił do zawodów typu Capture the Flag. Mimo, że ostatecznie finiszował na ostatnim miejscu, to w trakcie rozgrywki parokrotnie wyprzedzał zespoły ludzkie. W ostatecznej klasyfikacji, zabrakło mu jedynie 1,8% punktów żeby wyprzedzić zespół sklasyfikowany na przedostatnim miejscu. To pokazuje, jak niewielki postęp jest potrzebny, żeby wprowadzić autonomiczne systemy do użytku komercyjnego.

Inteligentne systemy wsparcia analityków bezpieczeństwa

Podczas gdy autonomiczne systemy bezpieczeństwa są jeszcze (niedaleką) przyszłością, większość specjalistów do spraw bezpieczeństwa prędzej czy później będzie miała do czynienia z kilkoma problemami obrazującymi prozę współczesnego przedsiębiorstwa w tak dynamicznie rozwijającym się technologicznie środowisku.

Po pierwsze, przedsiębiorstwom zaczynają doskwierać konsekwencje dotychczasowego braku praktyk typu *security by design*. Innymi słowy, większość systemów komercyjnych, a zwłaszcza systemów dziedzinowych, była pisana nie uwzględniając współczesnych zagrożeń cybernetycznych. Konsekwencją takich wieloletnich zaniedbań jest konieczność de facto monitorowania całości infrastruktury informatycznej, anomalii w zachowaniu użytkowników oraz korelowania informacji między systemami w celu identyfikacji zagrożeń dla infrastruktury i danych firmy. Wykrywać należy również takie niespodziewane tylne furtki jak we wspomnianych systemach do monitorowania radiacji, których zresztą producent odmówił załatania twierdząc, że systemy wykrywania radiacji są instalowane w bezpiecznych lokalizacjach. Pytaniem otwartym pozostaje, co się stanie, jeśli w systemach chroniących te lokalizacje również znajdą się tylne furtki lub błędy w algorytmach zabezpieczeń.

Team	Final Score
PPP	113555
b1oOp	98891
DEFKOR	97468
HITCON	93539
KaisHack GoN	91331
LC¢BC	84412
Eat Sleep Pwn Repeat	80859
binja	80812
pasten	78518
Shellphish	78044
9447	77722
Dragon Sector	75320
!SpamAndHex	73993
侍	73368
Mayhem	72047

Drugim wyzwaniem dla każdego działu bezpieczeństwa jest efektywne wykorzystanie całości wiedzy dostępnej w Internecie i w sieciach zanonimizowanych typu Tor czy I2P. Każdy analityk bez wątpienia chciałby działać proaktywnie i wykrywać luki w zabezpieczeniach zanim zagrożenie nadejdzie. Praktyka jednak pokazuje, że większość czasu specjaliści spędzają raczej na gaszeniu pożarów, niż na systematycznym przyswajaniu dostępnej wiedzy. Zresztą istniejąca, i wciąż rosnąca ilość dostępnej wiedzy jest nie do przyswojenia przez człowieka. Co więcej, jej realne wykorzystanie w momencie zagrożenia, pod presją czasu i odpowiedzialności, jest mocno ograniczone.

Trzecim problemem, który zaczyna być coraz bardziej widoczny jest powiększający się niedobór doświadczonych specjalistów do spraw bezpieczeństwa. Szacuje się, że na rynku brakuje około 1,5 miliona specjalistów i liczba ta się powiększa.

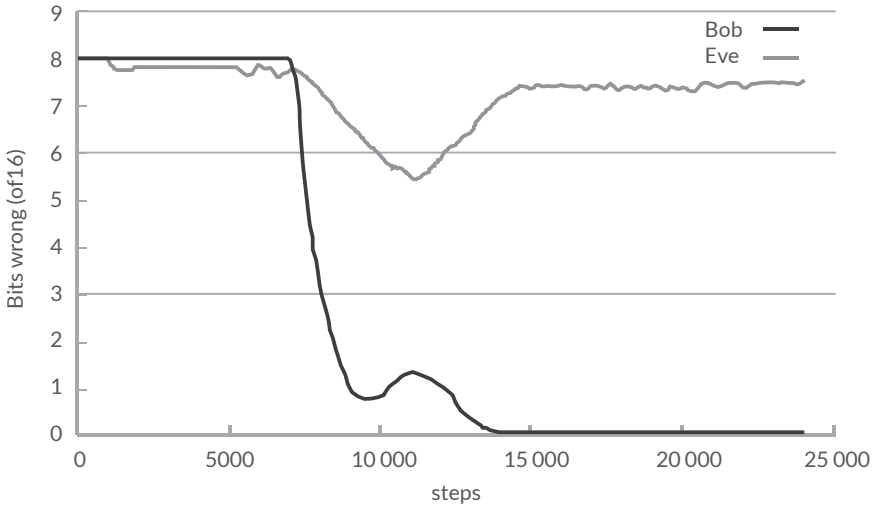
Odpowiedzią na wszystkie trzy problemy jest efektywne wykorzystanie dostępnych już na rynku systemów kognitywnych opracowanych (czyt. nauczonych) aby rozumiały zagadnienia z zakresu cyberbezpieczeństwa. Narzędzia kognitywne mają na celu wesprzeć analityków bezpieczeństwa w analizie zdarzeń i korelacji informacji z wewnątrz przedsiębiorstwa z wiedzą dostępną w sieci. Dzięki takiemu podejściu analityk, który zidentyfikuje podejrzane zachowania w infrastrukturze będzie automatycznie wsparty całą dostępną

w sieci wiedzą na temat tego konkretnego zagrożenia. Praktyka pokazuje, że współcześnie systemy kognitywne potrafią oszczędzić analitykom bezpieczeństwa i analitykom SOC do 50% czasu związanego z wyszukiwaniem i klasyfikowaniem informacji.

Ochrona prywatności i bezpieczna komunikacja

W przypadku każdej infrastruktury, ale w szczególności w przypadku infrastruktury krytycznej, zapewnienie bezpiecznej komunikacji pomiędzy komponentami systemu oraz zabezpieczenie danych wrażliwych staje się coraz większym wyzwaniem. Zwłaszcza w przypadku, gdy nadchodząca era komputerów kwantowych zaczyna poważnie zagrażać skuteczności części algorytmów szyfrowania.

Z tym większym zainteresowaniem świat obserwował jeden z najciekawszych eksperymentów przeprowadzonych prze badaczy z Google Brain, którzy oprogramowali dwie uczące się maszyny (a konkretnie dwie sieci neuronowe) Bob i Alice, aby same wymyśliły bezpieczny sposób komunikacji, oraz zlecili trzeciej maszynie (Eve) przechwycić i rozkodować przekaz. W skrócie, naukowcy z Google Brain odkryli, że odpowiednio oprogramowana sztuczna inteligencja, tworzy dziwnie *nieludzkie* schematy kryptograficzne i że lepiej radzi sobie z szyfrowaniem niż deszyfracją. Ostatecznie naukowcy stwierdzili, że Bob i Alice opracowały solidny protokół szyfrowania. Eve z drugiej strony po początkowych sukcesach nie potrafiła już odszyfrować komunikacji systemów, które nieustannie się uczyły i poprawiały swój algorytm. Oznacza to, że już dzisiaj roboty mogą ze sobą rozmawiać w sposób, którego ani inne roboty ani, co za tym idzie, ludzie, nie są w stanie zrozumieć i złamać.



Mimo, że na pierwszy rzut oka taka perspektywa może się wydawać niekomfortowa lub wręcz niebezpieczna, to niesie ze sobą kolosalne możliwości w zakresie zabezpieczania danych, a zwłaszcza w zakresie bezpiecznej pracy na danych zaszyfrowanych. Odkąd w 2009 roku Craig Gentry udowodnił, że pełne szyfrowanie homomorficzne jest możliwe w praktyce – badania nad tym obszarem przybliżają nas z każdym dniem do zastosowań komercyjnych. W skrócie – pełne szyfrowanie homomorficzne umożliwia dowolne działania na danych zaszyfrowanych. Dzięki zastosowaniu takiego szyfrowania oraz bezpiecznej komunikacji stworzonej przez samouczące się sieci neuronowe jesteśmy w stanie pracować na najważniejszych danych dla firmy nie tylko w szerszej skali, ale przede wszystkim bez strachu o to, że te dane wpadną w ręce przestępców lub konkurencji. Przez wielu szyfrowanie homomorficzne postrzegane jest jako Święty Graal kryptografii, a przez dostawców rozwiązań przetwarzania w chmurze wyczekiwana jest pełna komercjalizacja rozwiązań w oparciu o szyfrowanie homomorficzne.

Zabezpieczanie urządzeń IoT

Według Gartnera, do końca bieżącego roku konsumenci będą korzystać z ponad 8 miliardów podłączonych urządzeń. Te urządzenia IoT, takie jak inteligentne telewizory, tablety, smartfony, notebooki, urządzenia do noszenia, czujniki, termostaty, asystenci itd, sprawią, że nasze życie będzie bardziej efektywne, oszczędzające energię, bardziej komfortowe i mniej kosztowne. Jak pokazał przykład botnetu Mirai z 2016 roku – życie będzie również bardziej wygodne dla przestępców mogących wykorzystać niezabezpieczone (czyli większość) urządzeń IoT do swoich celów.

Rzeczywistość bezpieczeństwa IoT jest dość mizerna: wielu producentów inteligentnych urządzeń nie wie, jak zabezpieczyć urządzenia IOT przed cyberatakiem, a wielu to nie interesuje, bo koncentrują się na funkcjonalności. Przez to jednak ogromna liczba urządzeń IoT nie ma nawet infrastruktury wspierającej do uruchamiania rozwiązań zabezpieczających, a całkiem sporo również nie ma nawet mechanizmów aktualizacji.

Nie bez powodów Senat USA przyjął w sierpniu 2017 roku pierwszą legislację dotyczącą urządzeń IoT – The Internet of Things Cybersecurity Improvement Act. Prawo dotyczy wprawdzie urządzeń IoT używanych i kupowanych w ramach administracji rządowej, ale wprowadzone przez nie standardy będą prawdopodobnie podstawą do stworzenia standardów sektorowych. Tym bardziej przeraża fakt, że w 2017 roku potrzebne jest prawo, które wprowadza dla urządzeń cyfrowych:

a) możliwość aktualizacji;

b) zakazuje wpisywanych „na sztywno" haseł w kodzie;

c) nakazuje, aby urządzenia nie były podatne na znane podatności.

Ten ostatni wymóg jest zresztą trudny do wdrożenia, gdyż znając mechanizm zakupów w administracji udowodnienie, że urządzenie jest podatne, stanie się standardowym mechanizmem walki konkurencyjnej.

Z perspektywy infrastruktury krytycznej pojedynczy smartwatch czy telewizor wiszący w sali konferencyjnej nie jest może zagrożeniem krytycznym (chyba, że połączone są w sieć i wykorzystane do przeprowadzenia ataku typu DoS na infrastrukturę firmy), ale nawet takie pojedyncze urządzenia świetnie się sprawdzają w fazie rekonesansu poprzedzającej atak właściwy. Dzieje się tak ponieważ większość systemów bezpieczeństwa przedsiębiorstwa nie traktuje sprzętu IoT jako części infrastruktury informatycznej, którą należy zabezpieczać. W związku z tym nadają się one idealnie do wykorzystania nie tylko podczas rekonesansu, ale również (jeśli nie przede wszystkim) w atakach z wewnątrz firmy.

Zabezpieczenia przeciwko zagrożeniom wewnętrznym (*insider threat*)

Niezadowolony pracownik wynoszący w tajemnicy poufne informacje, niedbały kierownik klikający na link ze złośliwym oprogramowaniem, czy może przestępca uzyskujący dostęp do infrastruktury krytycznej za pomocą skradzionych poświadczeń: to wszystko dzieje się na co dzień i stanowi jedno z największych wyzwań cyberbezpieczeństwa w 2017 roku.

Alphabet, firma matka Google, złożyła ostatnio sprawę przeciwko byłemu inżynierowi Anthony'owi Levandowskiemu, który obecnie współpracuje z Uberem. Firma oskarżyła Levandowskiego o kopiowanie ponad 14 000 plików wewnętrznych i przekazanie ich bezpośrednio do swojego nowego pracodawcy.

Co jest zagrożeniem dla bezpieczeństwa spowodowanym przez wewnętrznych użytkowników? Prawdą jest, że typowe zagrożenia, takie jak ataki złośliwego oprogramowania, włamania do sieci, ataki typu „odmowa usługi" i *ransomware*, są znacznie częstsze niż ataki wewnętrzne. Takie przeświadczenie panuje przynajmniej w większości firm, dopóki nie przeprowadzona zostanie właściwa analiza. Podczas gdy wewnętrzne zagrożenia bezpieczeństwa cybernetycznego często są związane ze złośliwymi użytkownikami, w rzeczywistości zwykli pracownicy nieumyślnie powodują naruszenia i wycieki danych firmowych praktycznie codziennie

Utrata poświadczeń następuje z powodu *phishingu*, kradzieży lub nieświadomego wpuszczania złośliwego oprogramowania do systemu, gdy pracownik kliknie łącze w wiadomości e-mail lub przynosi zainfekowane urządzenie. Nie obejmuje to zwykłych błędów, takich jak wysyłanie poufnych plików na niewłaściwy adres. Wszystko to jest tylko małą listą sposobów, w jaki pracownicy mogą mniej lub bardziej nieświadomie narażać firmy zarówno na straty finansowe, jak i wizerunkowe.

Urządzenia IoT, a także zachowania pracowników na chwilę obecną wymykają się klasyfikacji jako zasoby wymagające monitorowania z uwagi na zagrożenia cybernetyczne. Na szczęście te niedociągnięcia można już zacząć adresować za pomocą sztucznej inteligencji i analityki, a także wykorzystywać matematykę i technologię rozpoznawania wzorów, aby poznać wzorce zachowań pracowników, przewidywać przyszłość i podejmować bardziej efektywne decyzje. Jest to trend, który sprawdził się już w różnych dziedzinach bezpieczeństwa i może poprawić skuteczność walki z zagrożeniami wewnętrznymi poprzez redukcję fałszywych alarmów i znalezienie przysłowiowej igły w stogu siana.

Kluczową technologią wydaje się tutaj być *User Behaviour Analytics* (UBA). Gartner definiuje UBA jako rozwiązania analizujące wzorce zachowań człowieka, a następnie stosujące algorytmy i analizę statystyczną w celu wykrycia znaczących anomalii z tych wzorców – anomalii, które wskazują potencjalne zagrożenia. Tym samym rozwiązania UBA nie tyle skupiają się na analizie informacji z systemów informatycznych co pozyskanych od ich użytkowników.

Systemy typu UBA docelowo mogą bardzo ułatwić również procesy audytu wewnętrznego. Zwłaszcza że nie muszą się przejmować potencjalnymi reperkusjami dla swojej kariery. Co więcej, takie systemy z definicji badają zachowania wszystkich pracowników, podwykonawców i pracowników czasowych mających dostęp do infrastruktury przedsiębiorstwa, a w sytuacji wykrycia niebezpieczeństwa mogą automatycznie zareagować w zaprogramowany sposób.

Zabezpieczanie przed włamaniami do systemów SCADA

Metody zabezpieczania systemów nadzorujących przebieg procesu technologicznego jest tematem na osobne opracowanie, zwłaszcza, że jest obciążone wszystkimi wadami struktur tworzonych przez lata. Właściwe zabezpieczenie infrastruktury będzie miało kluczowe znaczenie nie tylko w siedzibie przedsiębiorstwa, ale również (jeśli nie przede wszystkim) w ramach struktur, które znamy pod nazwą *smart cities*. Inteligentne miasta polegają na wzajemnie połączonych urządzeniach, aby usprawnić usługi miejskie w oparciu o dane uzyskiwane w czasie rzeczywistym. Systemy te łączą sprzęt, oprogramowanie i analizę geoprzestrzenną w celu polepszenia usług komunalnych i optymalizacji wykorzystania przestrzeni miejskiej. Wraz z rozwojem tych technologii, stawka ochrony cyfrowych fundamentów miasta będzie coraz wyższa. Tym bardziej, że inwestycje w inteligentną infrastrukturę wzrosły, ale wiele z innowacji jest wdrażanych bez solidnych testów, a cyberbezpieczeństwo jest często zaniedbywane. Miasta obecnie wykorzystujące system typu SCADA do kontroli i nadzoru nad swoją infrastrukturą są szczególnie podatne na częste ataki ze względu na słabe protokoły bezpieczeństwa. Choć systemy SCADA sterują procesami na dużą skalę i łączą zdecentralizowane obiekty, rzadko wykorzystują kryptografię na poziomie protokołu i uwierzytelniania.

W ramach europejskich projektów badawczych FP7-SEC-2011-1 Project 285647 i H2020-DS-2015-1 Project 700581 grupa inżynierów przedstawiła pełen zestaw ataków na

infrastrukturę opartą na protokole Modbus over TCP/IP. Dlatego też biorąc pod uwagę całą złożoność i historyczne obciążenie systemów SCADA i IASC lepszym pomysłem wydaje się być nie tyle stały i obciążający monitoring całości infrastruktury, co zwłaszcza w przypadku rozproszonego środowiska niesie również problemy związane z opóźnieniami w komunikacji, ale raczej zdefiniowanie standardów inteligentnego analizotora ruchu umożliwiającego zaadresowanie problemu nieprzystosowania systemów SCADA do łączenia się z Internetem. Skoro SCADA jednak jest połączona z Internetem, podstawowym celem takiego inteligentnego filtra jest ochrona przed atakami, które mogłyby doprowadzić do braku ciągłości działania.

Grupa naukowców z University of Michigan opracowała techniczną architekturę takiego samouczącego się systemu mającego na celu dopuszczanie do systemu wyłącznie zachowań o znanych parametrach, weryfikując pochodzenie ruchu płynącego przez system oraz przechwytując i buforując podejrzany ruch wykryty w systemie równolegle testując wykorzystanie przydzielonego pasma. Takie podejście może nie rozwiązuje problemów w sposób systemowy, ani nie zwalnia działu bezpieczeństwa od ciągłego monitoringu zagrożeń, ale umożliwia bezpieczne działanie systemu, gdzie bezpieczeństwo jest nadzorowane przez algorytmy samouczące.

Wsparcie procesu uwierzytelniania

Zarządzanie tożsamością i dostępem jest już obecnie jedną z kluczowych broni w arsenale bezpieczeństwa wielu organizacji w celu złagodzenia przypadków naruszania i wycieku danych oraz zaadresowania wyzwań wynikających z przyjęcia nowych trendów takich jak BYOD. Często za naruszenie danych odpowiada nie tyle system zarządzania tożsamością, ale wykorzystanie danych poświadczających tożsamość przez niewłaściwą osobę. Naturalnym kierunkiem migracji wydaje się być więc przejście od haseł biometrycznych do systemu sztucznej inteligencji dodatkowo weryfikującego tożsamość przy użyciu bodźców wizualnych i dźwiękowych. Zamiast więc uwierzytelniać dostęp w oparciu o wcześniej zdefiniowane i możliwe do wykradzenia dane jak identyfikator i hasło, maszyna może zidentyfikować osobę w oparciu o wskazówki wizualne i fonologiczne, nauczyć się, kiedy taki dostęp może być przydzielony i zachowywać się konsekwentnie w oparciu o zestaw wyuczonych wzorców zachowań użytkowników systemu. Taka sztuczna inteligencja posiada też potencjał w zapewnianiu inteligentnej i ścisłej kontroli dostępu. Dla przykładu – tylko dlatego że użytkownik poświadczył swoją tożsamość 10 minut temu, czy system nadal powinien uważać, że to ten sam użytkownik korzysta z dostępu? Systemy sztucznej inteligencji mogą tutaj zarządzać dostępem użytkownika w oparciu o parametry biometrii dynamicznej nawet jak przemieszcza się on po sieci czy terenie przedsiębiorstwa.

Legislacja i etyka stosowania sztucznej inteligencji

Istnieje silna i złożona relacja między etyką a prawem. Kodeksy etyczne są zagnieżdżone w ramach właściwych jurysdykcji prawa krajowego i międzynarodowego oraz znajdują odzwierciedlenie w ich przepisach. Chociaż prawo kraju w zasadzie zawiera pewne zasady etyczne, orzeczenia moralne często dotyczą kwestii, które wykraczają poza obręb prawa, w sferę życia prywatnego i osobistego włącznie.

Jednak, zwłaszcza gdy technologia szybko się rozwija, prawo może nie być w stanie dotrzymać tempa rozwojowi technologicznemu a wtedy organizacje branżowe, które rozważają etyczne aspekty takich technologii, muszą wymagać i wspierać powstawanie odpowiednich norm i zmian w prawie.

Trzeba zauważyć, że w niektórych aspektach prawa istnieją różnice między jurysdykcjami, a niektóre z tych różnic są bardzo istotne dla sztucznej inteligencji. Na przykład istnieją znaczne różnice między amerykańskim i europejskim prawem ochrony danych osobowych. Może to mieć duży wpływ na to, co można i czego nie można zrobić, np. z wykorzystaniem danych osobowych w ramach systemów sztucznej inteligencji oraz z tym, co może, a co nie może być zrobione, aby zaadresować etyczne obawy w tych różnych jurysdykcjach.

Istnieją już pewne wytyczne zarówno dla prawa amerykańskiego jak i dla prawa europejskiego. Europejskie wytyczne zawarte zarówno w dokumentach Parlamentu Europejskiego jaki i brytyjskiego komitetu House of Commons Science and Technology Committee są napisane w podobnej futurystycznej konwencji, gdzie stwierdzenia „science-fiction" występują w odniesieniu do współczesności.

Jednak oba te dokumenty zawierają więcej punktów wspólnych. Przede wszystkim oba jasno stwierdzają, że jest jeszcze za wcześnie, żeby przyjmować regulacje sektorowe narzucające ograniczenia na sztuczną inteligencję. Natomiast należy się bliżej przyjrzeć możliwym implikacjom wynikającym z odpowiedzialności za działanie sztucznej inteligencji. W tym miejscu należy przede wszystkim odpowiedzieć sobie na pytanie „kiedy trzeba będzie taką legislację wprowadzić?".

Większość długoterminowych prognoz dotyczących możliwości technicznych w przyszłości nie uwzględnia tempa przyszłego rozwoju, ponieważ wszelkie przewidywania w większości oparte są na intuicyjnej, liniowej wersji rozwoju. Badania pokazują jednak, że w przypadku technologii mamy do czynienia z postępem wykładniczym. Pokazując to na przykładzie – w XX wieku następowało stopniowe przyspieszenie do dzisiejszej szybkości postępu. Osiągnięcia ostatniego stulecia w związku z tym były równoważne około 20 latom postępu przy jego szybkości z 2000 r. Następnych 20 lat postępu od roku 2000 dokonano zaledwie w 14 lat a kolejne 20 lat dokona się już tylko w 7 przyjmując dzisiejsze tempo postępu. Wyrażając to w inny sposób, w XXI wieku będziemy świadkami nie stu lat postępu technologicznego, ale postępu rzędu 20

tys. lat (oczywiście w stosunku do dzisiejszej szybkości postępu) lub tysiąc razy większego niż ten osiągnięty w XX wieku. W związku z tym określenie ram legislacyjnych dla sztucznej inteligencji jest potrzebne praktycznie rzecz biorąc od zaraz.

Analizując projekt rezolucji parlamentu europejskiego z maja 2016 roku (2015/2103(INL)) w odniesieniu do podstawy odpowiedzialności, pkt 27 wniosku jest bardzo interesujący ponieważ stwierdza on że „przyszły akt legislacyjny powinien przewidywać stosowanie ścisłych odpowiedzialności co do zasady, wymagając jedynie dowodu że wystąpiła szkoda oraz związek przyczynowo skutkowy między szkodliwym zachowaniem robota a poniesioną szkodą." Byłby to zatem system ścisłej odpowiedzialności, który mógłby być oznaczony jako „odpowiedzialność zastępcza za robota". W takim przypadku podwójny ciężar udowodnienia odpowiedzialności spoczywałby na ofierze. Nawet jednak w tym szczególnym przypadku decyzja, gdzie leży ostateczna odpowiedzialność jest trudna.

W tym względzie ust. 28 wniosku stanowi jeden ze sposobów oceny odpowiedzialności każdej ze stron, uznając, że „zasadniczo po zidentyfikowaniu ostatecznie odpowiedzialnych stron ich odpowiedzialność byłaby proporcjonalna do rzeczywistego poziomu instrukcji przekazywanych robotowi a także do jego autonomii, tak aby im większa była zdolność uczenia się robota lub autonomia, to powinna być niższa odpowiedzialność innych stron, a im dłuższe wykształcenie robota, tym większa powinna być odpowiedzialność jego «nauczyciela»".

Należy upewnić się, że przyszły instrument jest dokładniejszy i prostszy w obsłudze, ponieważ jedną z potencjalnych obaw jest to, że sędziowie niewiele wiedzący na temat nowych technologii mogą mieć kłopoty ze zrozumieniem subtelności. Dlatego też, gdy warunki wywołujące dyrektywę 85/374 / EWG z dnia 25 lipca 1985 r. nie będą spełnione, ofiara może znaleźć inne odpowiedzialne strony. Warto rozpatrzyć kilka opcji:

1. Jeśli sztuczna inteligencja działa na zasadzie *open source*, osobą odpowiedzialną powinna być co do zasady ta, która zaprogramowała aplikację,

2. Jeśli sztuczna inteligencja powoduje uszkodzenia, które mogę być powiązane z jej projektem lub produkcją – na przykład błąd algorytmu powodujący szkodliwe działanie – projektant lub producent powinien ponosić odpowiedzialność.

3. Jeśli sztuczna inteligencja spowoduje szkody podczas procesu nauki, jej użytkownik lub właściciel powinien być odpowiedzialny. W tym kontekście rozwiązanie może się różnić w zależności od tego, czy użytkownik jest profesjonalistą i czy sam jest w takim przypadku ofiarą.

W tym samym projekcie rezolucji ustawodawca proponuje wprowadzenie etycznych ram dla projektowania, produkcji i wykorzystywania sztucznej inteligencji i robotów. Należy pamiętać,

że takie analizy i wytyczne już powstawały w przeszłości a pierwsze oficjalne europejskie etyczne i prawne rekomendacje dotyczące sztucznej inteligencji i robotyki zostały opublikowane w 2014 roku.

Oczywiście nie możemy na tym etapie mylić etyki w robotyce z etyką maszyn, która zobowiązywała by maszyny do przestrzegania zasad etycznych. Dzisiaj koncepcja etyki maszyny jest rozważaniem czysto teoretycznym, ponieważ nawet autonomiczne roboty nie są w stanie podejmować decyzji moralnych.

Rozważania te mają jedynie sens w przypadku legalnych i etycznych aspektów wykorzystania sztucznej inteligencji.

Niemniej jednak, światowi liderzy i szefowie bezpieczeństwa przedsiębiorstw powinni zapoznać się z najnowocześniejszymi zagadnieniami związanymi z bezpiecznym wykorzystaniem sztucznej inteligencji przy zapewnianiu cyberbezpieczeństwa. Uzbrojeni w tę wiedzę liderzy będą mogli świadomie zadecydować, jak dodanie sztucznej inteligencji do swojego produktu lub usługi pozwoli zapewnić pozytywne doświadczenia użytkowników przy jednoczesnym wyważeniu kosztów potencjalnych zagrożeń związanych z dodatkowym ryzykiem wycieku danych i innymi, opisanymi powyżej zagrożeniami. Zatrudnienie dedykowanego specjalisty do spraw sztucznej inteligencji może być naturalnym krokiem, ponieważ większość specjalistów do spraw bezpieczeństwa cybernetycznego nie jest przeszkolona (a co dopiero doświadczona) w zakresie przewidywania lub zapobiegania ataków wspieranych przez systemy inteligentne. Pozostaje mieć nadzieje, że obecnie trwające badania oraz prace legislacyjne pomogą włączyć sztuczną inteligencję w globalne i lokalne struktury zabezpieczeń z jak największym sukcesem.

Standaryzacja rozwiązań dotyczących cyberbezpieczeństwa w sektorze energetycznym – przegląd polityki UE

Agnieszka Konkel[1]

Wstęp

Atak na sieć energetyczną na Ukrainie w 2015 roku, w wyniku którego część Ukrainy została tymczasowo pozbawiona prądu, postrzega się jako przykład pierwszej, udanej próby ataku na system energetyczny. Równolegle podobne ataki na sieci energetyczne zanotowano w krajach bałtyckich[2]. W lipcu 2017 roku, irlandzka spółka energetyczna Electricity Support Board stała się obiektem ataku z użyciem spear phishingu. Atak był próbą przeniknięcia do system sterowania firmy i umożliwienie hakerom odcięcie części sieci elektroenergetycznej od zasilania[3]. Tylko w ostatnim czasie hakerzy włamali się do przynajmniej kilkunastu amerykańskich elektrowni, co wywołuje obawy, że ataki wymierzone były w luki w zabezpieczeniach sieci elektroenergetycznej[4]. Hakerom udało się uzyskać dostęp do sieci operacyjnych dając im możliwość realnego wstrzymania dopływu prądu w kilku amerykańskich firmach energetycznych i przynajmniej jednej w Turcji[5]. Te incydenty, zdarzające się coraz częściej, dobitnie wskazują na istniejące braki infrastruktur krytycznych oraz ich podatność na cyberataki, które nie są dłużej jedynie teoretycznym konceptem/pozostają w sferze teorii, ale są częścią naszej codzienności stwarzając „ogromne ryzyko dla urządzeń, których awaria może kosztować życie, wstrzymać produkcję czy wyrządzić szkody środowisku naturalnemu"[6]. Na domiar złego,

1 Poglądy i opinie autorki (występującej jako osoba prywatna) zawarte w niniejszym artykule nie muszą wyrażać lub reprezentować stanowiska rządów przedstawionych w publikacji.

2 Jewkes S., Vukmanovic O., Suspected Russia-backed hackers target Baltic energy networks, [online] http://www.reuters.com/article/us-baltics-cyber-insight-idUSKBN1871W5 http://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5

3 Dearden L. (2017), Hackers target Irish energy networks amid fears of further cyberattacks on UK's crucial infrastructure, [online] http://www.independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html

4 Riley M., Dlouhy J., Gruley B., Russians Are Suspects in Nuclear Site Hackings, Sources Say, [online] https://www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site

5 Greenberg A. (2017), Hackers gain 'switch-flipping' access to US power grid control systems, [online] https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

6 European Commission (2013), Commission Proposal for a Directive concerning measures to ensure a high common

powszechne wykorzystanie przemysłowych systemów sterowania, inteligentnych liczników oraz rozwiązań IoT (Internet rzeczy) zwiększyły płaszczyznę wystąpienia potencjalnego cyberataku, zwiększając podatność sektora energetycznego na olbrzymie szkody, czyniąc z niego istotny cel także działań motywowanych politycznie.

W obliczu niedawnych zakłóceń funkcjonowania krytycznej infrastruktury energetycznej, rodzi się potrzeba podjęcia dyskusji na temat krytyczności sektora energetycznego, bezpieczeństwa stosowanego oprogramowania i urządzeń, oraz uzależnienia UE od dostawców z państw trzecich. Dyskusja ta zostanie także wywołana w efekcie działań podjętych przez Komisję Europejską we wrześniu 2017 roku takich jak przedstawienie propozycji/wniosku rozporządzenia w sprawie ENISA (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji), Agencji UE ds. bezpieczeństwa cybernetycznego oraz certyfikatów bezpieczeństwa cybernetycznego systemów teleinformatycznych (Akt Cyberbezpieczeństwa)[7], oraz nową Strategię bezpieczeństwa cybernetycznego Unii Europejskiej: Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej[8]. Zarówno Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS[9]) oraz Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (rozporządzenie RODO), które wchodzą w życie w 2018, poświęcają wiele uwagi zagadnieniu bezpieczeństwa infrastruktury krytycznej, pobudzania rozwoju unijnego sektora cyberbezpieczeństwa i wzmacniania najsłabszych ogniw.

Zanim zagłębimy się w szczegóły dotyczące standaryzacji rozwiązań cyberbezpieczeństwa w sektorze energetycznym i związanych z tym działań politycznych, na początek przyjrzymy się cechom charakterystycznym tego sektora w odniesieniu do wzajemnych powiązań pomiędzy infrastrukturami, nierównym poziomem rozwoju innowacji w UE oraz uzależnieniem UE od rozwiązań pochodzących z państw trzecich. Najpierw jednak kilka słów o ograniczeniach. Ze względów praktycznych niniejszy artykuł nie jest w stanie w sposób kompleksowy dokonać przeglądu polityki dotyczącej wszystkich podsektorów przemysłu energetycznego. W związku z tym skupia się przede wszystkim na podsektorze wytwarzania energii elektrycznej, głównie w związku z wdrożeniem Dyrektywy NIS oraz pakietu Komisji Europejskiej „Czysta energia dla wszystkich Europejczyków"[10].

level of network and information security across the Union, [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048

7 European Commission (2017), Proposal for a regulation of the European Parliament and the Council on ENISA the „EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification („Cybersecurity Act"), [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505290611859&uri=COM:2017:477:FIN

8 European Commission (2017), Proposal for a regulation of the European Parliament and the Council on ENISA the „EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification („Cybersecurity Act"), [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505290611859&uri=COM:2017:477:FIN

9 Ibid.

10 European Commission (2016), Clean Energy for All Europeans – unlocking Europe's growth potential, [online] http://europa.eu/rapid/press-release_IP-16-4009_en.htm

Wzajemne powiązania oraz współzależności w sektorze energetycznym

Należy stwierdzić, że sektor energetyczny UE charakteryzują czynniki mające wpływ na rozwój skutecznej polityki bezpieczeństwa cybernetycznego dla tego sektora. Po pierwsze, chodzi o wzajemne powiązania oraz współzależność sieci energetycznych państw członkowskich, które mogą wywołać efekt domina w wielu krajach Unii w sytuacji, gdy sieć energetyczna stanie się celem cyberataku. Następnym czynnikiem jest niejednolity rozwój systemów energetycznych na terytorium UE, co może spowodować szereg szczególnych wyzwań w momencie pojęcia próby ujednolicenia rozwiązań zwiększających cyberbezpieczeństwo w UE[11]. Skutki wyżej wymienionych współzależności nie ograniczają się bynajmniej do jednego kraju, lecz obejmują swym zasięgiem całą Unię. Wraz ze wzrostem powiązań pomiędzy regionalnymi gospodarkami rośnie również ich podatność na wystąpienie awarii w dostawach energii na poziomie regionalnym i ponadpaństwowym, co może zagrozić stabilności całych regionów[12]. Oprócz współzależności występujących pomiędzy sektorami istnieją także współzależności, które można zaobserwować w wielu państwach członkowskich w obrębie tych samych sektorów. Tyczy się to na przykład sieci elektroenergetycznych wysokich napięć. Przegląd aktualnego Europejskiego programu ochrony infrastruktury krytycznej (ang. EPCIP) pokazał, iż kwestiom powiązań pomiędzy infrastrukturami krytycznymi w obrębie różnych sektorów oraz pomiędzy krajami UE poświęcono dalece niedostateczną uwagę[13].

Rysunek 1 poniżej obrazuje najważniejsze wzajemnie zależności pomiędzy różnymi infrastrukturami krytycznymi, z których wynika, że energetyka jest jedną z kluczowych infrastruktur. Uświadomienie sobie tych relacji ma kolosalne znaczenie w przypadku wystąpienia incydentu, który może mieć katastrofalne konsekwencje dla pozostałych infrastruktur czy państw członkowskich. Niestety ryzyko wywołujące efekt kaskadowy rzadko jest brane pod uwagę[14]. Przykładowo w Stanach Zjednoczonych, wszystkie 16 sektorów[15] amerykańskiej gospodarki przedstawionych poniżej i zaklasyfikowanych jako elementy krajowej infrastruktury krytycznej polegają na jednej sieci energetycznej[16].

11 European Parliament (2016), Cybersecurity strategy for the energy sector, [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

12 OSCE (2016), Protecting electricity networks from natural hazards, [online] http://www.osce.org/secretariat/242651?download

13 European Commission (2013), Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, [online] https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

14 ENISA (2017), op. cit.

15 Przemysł chemiczny; obiekty handlowe; łączność; krytyczne procesy wytwarzania; zapory wodne; obronne bazy przemysłowe; służby ratownicze; przemysł energetyczny; usługi finansowe; żywność i rolnictwo; obiekty rządowe; opieka zdrowotna i zdrowie publiczne; informatyka; reaktory jądrowe, materiały i odpady radioaktywne; transport; woda pitna i ścieki

16 Knake R. (2017), A Cyberattack on the U.S. Power Grid, [online] https://www.cfr.org/report/cyberattack-us-power-grid

Rysunek nr 1. 16 sektorów amerykańskiego przemysłu zdefiniowanych w Dyrektywie politycznej Prezydenta jako elementy infrastruktury krytycznej USA17. Źródło: IBM and Deloitte (2013), Breaking down the cybersecurity framework: closing critical IT security gaps.

Z drugiej strony, unijna dyrektywa NIS zalicza do grona sektorów o krytycznym znaczeniu przemysł energetyczny, transport, bankowość, infrastrukturę rynku finansowego, sektor opieki zdrowotnej, centra dostaw i dystrybucji wody pitnej oraz infrastrukturę cyfrową.

ENISA rozróżnia cztery typy takich współzależności:
- fizyczną – gdzie istnieje fizyczna zależność pomiędzy dwoma infrastrukturami;
- geograficzną – gdzie infrastruktury są od siebie zależne w sensie geograficznego położenia;
- cybernetyczną – gdzie stan infrastruktury jest uzależniony od informacji dostarczanej za pomocą infrastruktury informacyjnej lub komunikacyjnej;
- logiczną – gdzie występuje logiczna zależność pomiędzy dwoma infrastrukturami.

Niedawno pojawił się nowy, piąty typ współzależności – zależność społeczna. Odnosi się ona do wpływu ludzkiego zachowania, które często staje się irracjonalne w obliczu kryzysu (zbiorowa panika czy przeciążenie systemów łączności)[18].

Bazując na tych współzależnościach i wzajemnych powiązaniach, ENISA wskazuje potrzebę zdefiniowania podstawowych systemów ICS oraz SCADA (leżących u podstaw tych infrastruktur) biorąc pod uwagę ich interoperacyjność. Wzajemne powiązania i kompatybilność są czynnikami mającymi niezwykle istotne znaczenie. Dlatego też unikanie protokołów i technologii zamkniętych (własnościowych) a zamiast tego stosowanie protokołów i technologii kompatybilnych z innymi elementami staje się kluczowe[19]. Wyzwania natury technologicznej, przed jakimi stoi podsektor wytwarzania energii elektrycznej, zostaną omówione w dalszej

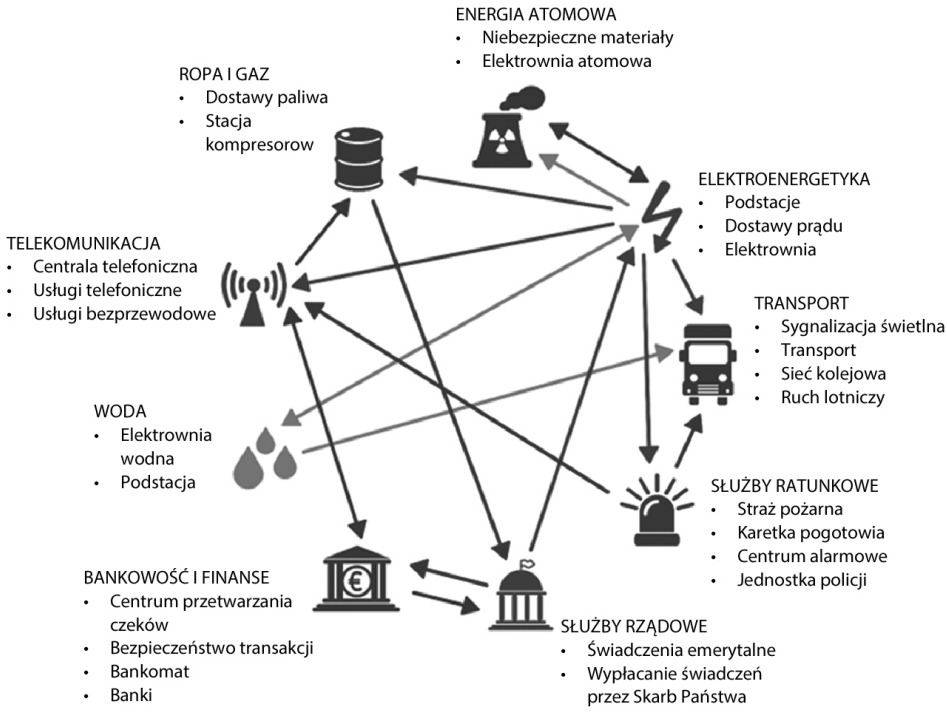
17 White House (2013), Presidential Policy Directive – Critical Infrastructure Security and Resilience, [online] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

18 Setola R., Theocharidou M. (2017), Modelling Dependencies Between Critical Infrastructures [w:] Managing the complexity of critical infrastructures, [online] https://link.springer.com/chapter/10.1007/978-3-319-51043-9_2/fulltext.html

19 ENISA (2017), op. cit.

części niniejszej publikacji. Teraz zajmiemy się naszkicowaniem problemu nierównego rozwoju państw członkowskich UE, spowodowanego zróżnicowanym stopniem przygotowania i zaszłościami historycznymi, a także różnym poziomem przygotowania do wdrożenia Dyrektywy NIS i rozporządzenia RODO.

Rysunek nr 2. Wzajemne zależności pomiędzy poszczególnymi infrastrukturami krytycznymi. Źródło: ENISA (2016), Communication network dependencies for ICS/SCADA Systems



Niejednolity rozwój krajów członkowskich UE – perspektywa kompleksowa

Niektóre kraje członkowskie UE, takie jak Holandia, Wielka Brytania czy Francja, są lepiej przygotowane do wdrożenia środków bezpieczeństwa cybernetycznego w sektorze energetycznym[20]. Aby wzmocnić najsłabsze ogniwa, należy jednak zapewnić równy poziom bezpieczeństwa cybernetycznego w całej UE. Mówiąc ogólnie, pewne państwa członkowskie, np. Niemcy, Francja, Austria, Estonia czy Republika Czeska, są w lepszej pozycji, by wdrożyć zapisy

20 Gurzu A. (2017), Hackers threaten smart power grids, Politico, [online] http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/

Dyrektywy NIS należycie i terminowo, częściowo dlatego, że kwestie cyberbezpieczeństwa już wcześniej zajmowały wysokie miejsce na liście politycznych priorytetów lub też były uregulowane prawnie[21].

Pozostałe państwa członkowskie, którym wcześniej brakowało świadomości, możliwości, czy woli politycznej, muszą uczynić z cyberbezpieczeństwa priorytet na szczeblu krajowym, aby na czas wdrożyć dyrektywę NIS. Przedłużający się proces negocjacji finalnego kształtu omawianego aktu prawnego ukazał rozbieżności w postrzeganiu kwestii cyberbezpieczeństwa. Warto zaznaczyć, że „trudności w osiągnięciu porozumienia w kwestii zasad regulujących cyberbezpieczeństwo infrastruktury krytycznej odzwierciedlają odmienne rozwiązania przyjęte przez państwa członkowskie UE. Niektóre kraje, np. Niemcy i Holandia, traktują cyberbezpieczeństwo w kategoriach bezpieczeństwa narodowego podczas gdy dla innych państw, takich jak Łotwa czy Dania, jest to problem obronności. Jeszcze inne kraje, w tym Finlandia i Włochy, postrzegają cyberbezpieczeństwo jako kwestię natury handlowej czy komunikacyjnej"[22]. Choć wiele rządów docenia wartość paneuropejskiego podejścia w tym zakresie, budzi ono obawy dotyczące zachowania suwerenności narodowej oraz wkraczania przez UE w wyłączne kompetencje państw członkowskich. Ponadto brak dostępu do twardych danych utrudnia porównanie potencjału państw członkowskich. Różnice pomiędzy krajami na obszarze UE mogłyby zostać zobrazowane na podstawie bardziej dogłębnej i solidniej oceny opierającej się na określonych kryteriach[23]. Inną kwestią jest czy pomimo niedostatecznych możliwości i różnych priorytetów, państwa członkowskie będą w stanie wdrożyć zapisy dyrektywy NIS w sposób jednolity, gdyż powodzenie tego przedsięwzięcia uzależnione jest od wdrożenia zapisów tego aktu prawnego przez wszystkie sektory wspomniane w Załączniku II dyrektywy NIS oraz wszystkie państwa członkowskie[24]. Może się to okazać kwestią dyskusyjną. Z tego też powodu, do nowej Strategii bezpieczeństwa cybernetycznego Unii Europejskiej[25], przedstawionej we wrześniu 2017 roku, został dołączony komunikat, którego celem jest wsparcie państw członkowskich w ich staraniach poprzez przedstawienie najlepszych praktyk związanych z wdrożeniem dyrektywy oraz wytycznych, jak dyrektywa powinna działać w praktyce[26].

Oprócz tego, jesienią 2017 roku zostaną opublikowane wytyczne wspierające zharmonizowane wdrożenie dyrektywy, które dotyczyć będą w szczególności operatorów usług kluczowych. Poza zróżnicowanym poziomem gotowości w obszarze

21 Tasheva I. (2017), European cybersecurity policy – Trends and prospects, [online] http://www.epc.eu/pub_details.php?cat_id=3&pub_id=7739

22 Ilves L., Evans T., Cilluffo F., Nadeau A., European Union and NATO Global Cybersecurity Challenges: A Way Forward PRISM Volume 6, No. 2, [online] http://cco.ndu.edu/Publications/PRISM/PRISM-Volume-6-no-2/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/

23 European Parliament (2016), Cybersecurity strategy for the energy sector, [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

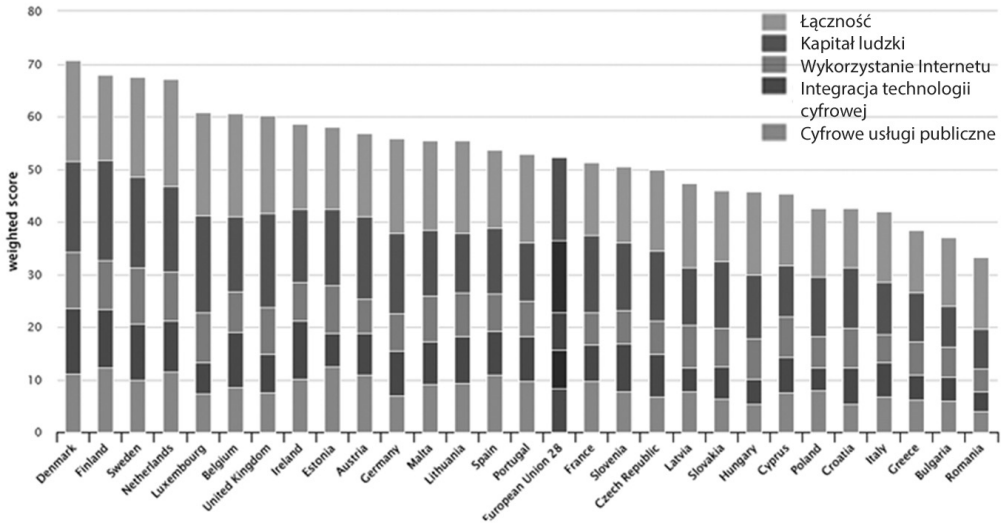
24 European Parliament (2016), ibidem

25 European Commission (2017), Joint communication to the European Parliament and the Council, op. cit.

26 European Commission (2017), Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, [online] https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-MAIN-PART-1.PDF

cyberbezpieczeństwa, dodatkowym źródłem rozbieżności jest poziom innowacyjności w krajach członkowskich. Na podstawie analizy indeksu DESI (ang. Digital Economy Society Index)[27], można stwierdzić, że Dania, Finlandia, Szwecja i Holandia należą do najbardziej zaawansowanych cyfrowo państw członkowskich UE. Zaraz za nimi są Luksemburg, Belgia, Wielka Brytania oraz Irlandia. Na przeciwległym końcu znajdują się kraje, które uplasowały się najniżej w rankingu DESI, czyli Rumunia, Bułgaria, Grecja i Włochy.

Rysunek nr 3. Digital Economy and Society Index 2017. Źródło: European Commission (2017), Digital Economy and Society Index



Niemniej najnowsza tablica innowacyjności ujawnia wzrost poziomu innowacyjności na obszarze UE. Szwecja zajmuje pierwsze miejsce w rankingu europejskich liderów innowacji. Za nią są Dania, Finlandia, Holandia, Wielka Brytania i Niemcy. Litwa, Malta, Wielka Brytania, Holandia i Austria są wśród najszybciej rozwijających się innowatorów. W kontekście globalnym, Unia Europejska dogania Kanadę i Stany Zjednoczone, choć Korea Południowa i Japonia nadal pozostają daleko z przodu. Z kolei Chiny zanotowały najszybszy wzrost spośród wszystkich międzynarodowych konkurentów[28].

W przypadku poziomu cyfryzacji systemów infrastruktury krytycznej, wpływ zaszłości historycznych jest jeszcze bardziej widoczny. Obraz poniżej przedstawia przegląd systemów ICS/SCADA mających połączenie z Internetem oraz wyraźne różnice pomiędzy„starymi" i „nowymi" państwami członkowskimi.

27 Indeks DESI podsumowuje około 30 wskaźników i śledzi ewolucję państw członkowskich oraz ich postępy w dziedzinie cyfryzacji w pięciu kategoriach: łączność, kapitał ludzki, wykorzystanie Internetu, integracja technologii cyfrowej oraz cyfrowe usługi publiczne.

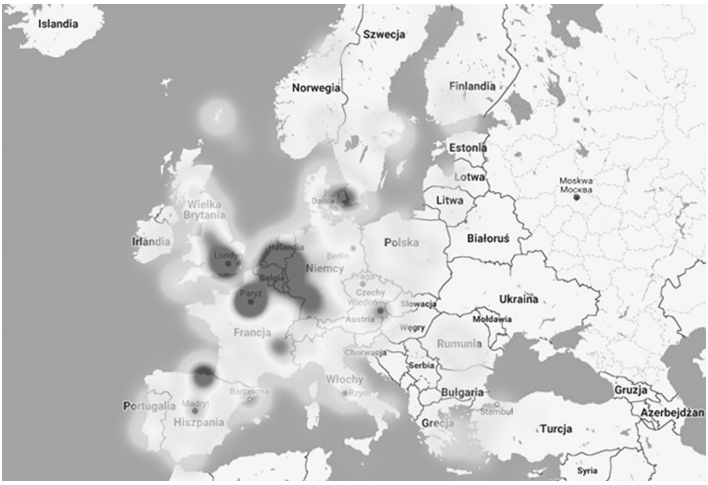
28 European Commission (2017), 2017 European Innovation Scoreboard, EU Member States' Innovation Performance, [online] http://ec.europa.eu/growth/industry/innovation/facts-figures/scoreboards_pl

Rysunek nr 4. Europejska Tablica Innowacyjności Wyniki państw członkowskich UE w dziedzinie innowacyjności. Źródło: European Commission (2017), 2017 European Innovation Scoreboard, EU Member States' Innovation Performance

Obserwując w szczególności inteligentne sieci energetyczne, widać wyraźne różnice pomiędzy państwami członkowskimi jeśli chodzi o ogólny poziom oraz tempo inwestycji. Ogólny, sprzyjający innowacjom klimat przekłada się na wysoki poziom cyfryzacji gospodarki i jej infrastruktur krytycznych. Istnieje jednak kilka czynników charakterystycznych dla poszczególnych krajów, które dodatkowo wyjaśniają różnice pomiędzy państwami członkowskimi.

Rysunek nr 5. Przegląd systemów ICS/SCADA połączonych z Internetem w UE. Źródło: ENISA (2016) Communication network dependencies for ICS/SCADA Systems

Rysunek nr 6. Mapa termiczna projektów dotyczących inteligentnych sieci 2017. Źródło: Joint Research Centre (2017), Smart grid projects heatmap: organisations and implementation sites

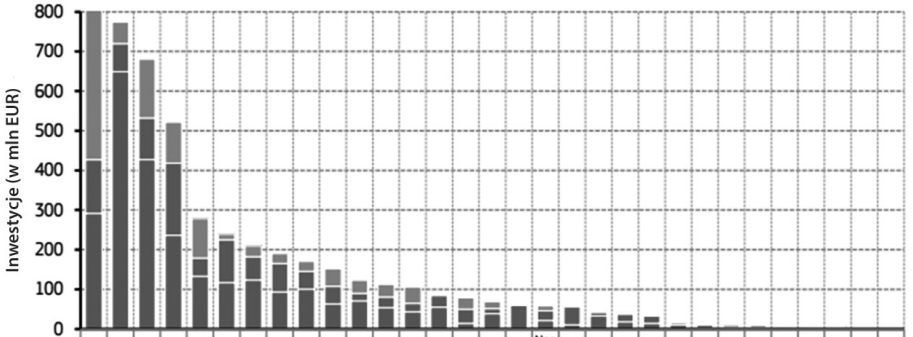


Sprzyjające warunki ogólnonarodowe i otoczenie regulacyjne, narodowe programy finansowania i skuteczna współpraca z sektorem prywatnym znacznie ułatwiają korzystanie z funduszy europejskich przez podmioty sektora prywatnego w obrębie państw członkowskich, co może przyśpieszyć inwestycje w inteligentne sieci. Jak pokazuje rysunek poniżej[29], niezależnie od różnic pomiędzy państwami członkowskimi, inwestycje sektora prywatnego stanowią główne źródło finansowania w większości państw UE. Widać to szczególnie wyraźnie w przypadku Wielkiej Brytanii, Francji, Niemczech i Hiszpanii, podczas gdy w państwach, które wstąpiły do UE po 2004 roku poziom inwestycji w tym obszarze jest znikomy.

Sektor energetyczny UE był i jest w dużej mierze kształtowany przez historię, a swoisty charakter systemów energetycznych państw UE ma swoje korzenie w konkretnym kontekście historycznym. Rządy państw UE pracowały nad ustanowieniem założeń koncepcyjnych/ramowych w celu zabezpieczenia własnych systemów energetycznych przed atakami z zewnątrz. Jednak z racji tego, że coraz częściej systemy te są ze sobą ściśle połączone, istnieje potrzeba podjęcia działań i koordynacji na szczeblu unijnym[30]. Niemniej jednak państwa członkowskie oraz operatorzy pozostają współodpowiedzialni za ochronę sieci energetycznych. Cechy sieci energetycznych takie jak krytyczność, transgraniczność oraz współzależność muszą zostać w pewnym stopniu zharmonizowane, aby zrekompensować ich nierówny poziom rozwoju w poszczególnych krajach UE. W tym celu można byłoby rozważyć wdrożenie zdefiniowanych na poziomie europejskim ram określających dojrzałość bezpieczeństwa cybernetycznego, opierających się na międzynarodowych standardach (np. ISO 27000). Takie ramy umożliwiłyby ocenę poziomu odporności sieci energetycznych na terytorium UE.

29 Gangale F., Vasilijevska J., Covrig C., Mengolini A., Fulli G., Smart grid projects outlook 2017, JRC science for policy report, [online] http://ses.jrc.ec.europa.eu/sites/ses.jrc.ec.europa.eu/files/u24/2017/sgp_outlook_2017-online.pdf
30 European Parliament (2016), op. cit.

Rysunek nr 7. Łączne inwestycje przypadające na kraj biorąc pod uwagę źródło finansowania. Źródło: Joint Research Centre (2017), Smart grid projects outlook 2017, JRC science for policy report

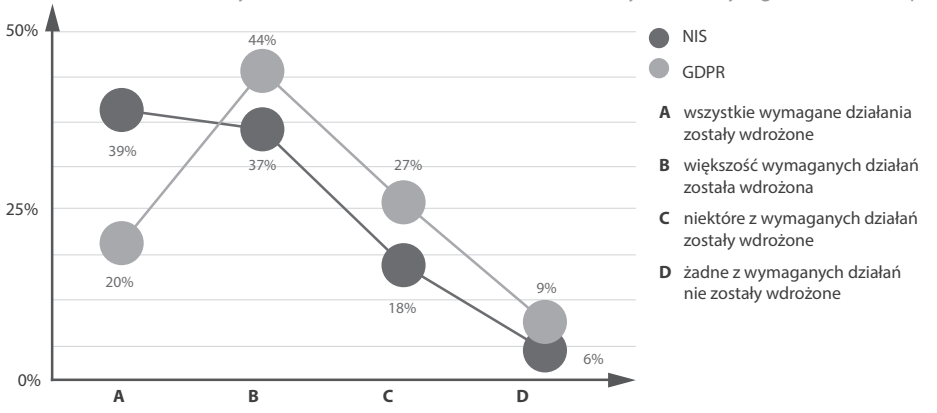


	DE	UK	FR	ES	DK	IT	NL	BE	SE	AT	CH	NO	FI	PT	EL	PL	LU	Non -EU	RO	CZ	SI	IE	HU	SK	LT	BG	LV	HR	CY	EE	MT
Razem	809	774	680	522	279	239	209	190	171	152	123	112	106	89	78	69	61	59	58	43	42	34	16	12	10	8	7.7	6.2	4.8	3.3	2.2
Krajowe	382	54	148	104	100	14	27	25	25	44	33	31	41	4.2	28	17	0.3	13	2.4	1.3	3.8	0.9		1			0.1		0.1	0.1	0
KC	136	71	105	182	46	108	58	71	45	45	19	27	22	30	36	14	0.5	24	45	9.7	20	19	5.8	8.8	6	5.7	3.4	3.3	3	2.1	1.6
Sekt. prywatny	291	649	428	236	133	117	124	94	101	63	71	54	43	55	14	38	60	21	10	32	18	14	10	2	4.1	2.3	4.1	2.9	1.7	1.1	0.6

Dyrektywa NIS i rozporządzenie RODO – zróżnicowany poziom gotowości

Zarówno dyrektywa NIS jak i rozporządzenie RODO tworzą harmonijne ramy dla rozpatrywania kwestii związanych z cyberbezpieczeństwem na obszarze UE. Mimo to, sposób wprowadzenia w życie rozporządzenie RODO może różnić się pomiędzy krajami członkowskimi, co wynika z różnic w gotowości, postępów w faktycznej implementacji dyrektyw unijnych w krajowym prawodastwie, czy odmiennych interpretacji[31]. Podobne rozbieżności w realizacji można zauważyć w odniesieniu do dyrektywy NIS.

Rysunek nr 8. Wykres porównujący poziom gotowości wdrożenia dyrektywy NIS i rozporządzenia RODO. Źródło: Fireye (2016), Mixed state of readiness for new cybersecurity regulations in Europe

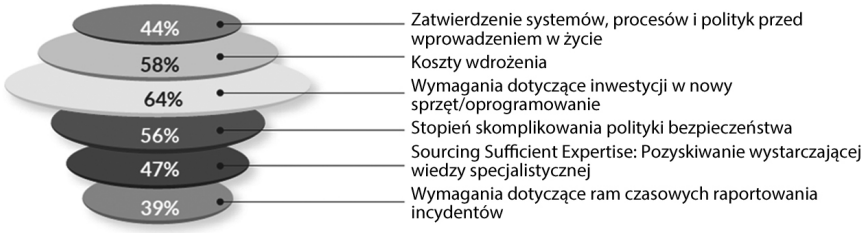


31 ENISA (2017), Gaps in NIS standardization. Recommendations for improving NIS in EU standardization policy, [online] https://www.enisa.europa.eu/publications/gaps-eu-standardisation.

Badanie przeprowadzone we francuskich, niemieckich i brytyjskich organizacjach pokazało mieszany stan gotowości do wdrożenia tych regulacji w UE. W 2016 roku większość firm nie była w pełni gotowa do wdrożenia zarówno dyrektywy NIS jak i rozporządzenia RODO. Niemieckie przedsiębiorstwa postrzegały się jako lepiej przygotowane do wdrożenia dyrektywy NIS niż firmy w innych krajach UE. 46% z nich było przekonanych, że wdrożyło wszystkie środki, w porównaniu do 36% firm we Francji i Wielkiej Brytanii. Z kolei 36% uważało, że wdrożyło większość wymagań. Pomimo, iż badanie nie uwzględniało krajów członkowskich, które wstąpiły do UE po 2004 roku, analiza nierównomiernego rozwoju, którą przedstawia wykres powyżej jeszcze wyraźniej podkreśla kontrast pomiędzy krajami jeśli chodzi o poziom gotowości.

Wyzwania, jakie mogą pojawić się w trakcie wdrażania zarówno dyrektywy NIS jak i rozporządzenia RODO dotyczą kilku istotnych czynników. Komisja Europejska oszacowała, iż całkowity koszt wdrożenia wymagań przedstawionych w dyrektywie NIS może sięgnąć 1–2 mld euro, przy czym małe i średnie przedsiębiorstwa musiałyby wyłożyć pomiędzy 2,5 tys. a 5 tys. euro. Kosz ten miałby pokryć nie tylko wydatki związane z nabyciem dodatkowego oprogramowania i sprzętu komputerowego (w opinii 64% respondentów), ale również usługi prawne i doradcze.

Rysunek nr 9. Najistotniejsze bariery utrudniające spełnienie wymagań nałożonych przez unijne inicjatywy w dziedzinie cyberbezpieczeństwa. Źródło: Fireye (2016), Mixed state of readiness for new cybersecurity regulations in Europe



Jedna trzecia z 260 uczestników ankiety przyznała, że jedynie częściowo rozumiała wpływ ram prawnych dyrektywy NIS i rozporządzenia RODO na obecne zapisy dotyczące ochrony i zabezpieczania danych. Pojawiły się również głosy, że wobec małego prawdopodobieństwa, że UE wskaże konkretne normy techniczne oraz programy certyfikacji, brak takich wytycznych może zwiększyć chaos na etapie oceny bieżących danych i statusu bezpieczeństwa oraz planowania aktualizacji[32].

Zauważono, że w przypadku kwestii dotyczących cyberbezpieczeństwa, prywatności i ochrony danych, normy europejskie i międzynarodowe oraz związane z nimi programy certyfikacji są

32 Fireye (2016), Mixed state of readiness for new cybersecurity regulations in Europe, [online] https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/rpt-mixed-state-of-readiness-for-new-cybersecurity-regulations-in-europe.pdf

niespójne w obrębie samej Unii i poza jej granicami Oprócz tego rozmaite sektory i kraje wprowadziły odrębne wymagania, które nie obejmują swym zasięgiem całej UE, a często wręcz ograniczają się do jednego kraju[33]. Warto jednak rozpatrzyć podejście brytyjskiego rządu do transpozycji dyrektywy NIS. Jak wiadomo dyrektywa ta nie narzuca wdrożenia standardów bezpieczeństwa cybernetycznego w sektorach ujętych w Załączniku nr 2 dyrektywy. Państwa członkowskie mają we własnym zakresie ustalić system kar za naruszenie zapisów przyjętych zgodnie z dyrektywą NIS. Biorąc pod uwagę fakty, iż utrata kluczowych usług teoretycznie może mieć duży wpływ zarówno na branżę jak i region, rząd brytyjski proponuje przyjęcie kar podobnych do tych przewidzianych w rozporządzeniu RODO zamiarem ujednolicenia podejścia do cyberbezpieczeństwa. W tym celu rząd brytyjski ustalił maksymalny pułap kary w wysokości 20 mln euro (18 mln funtów brytyjskich) lub równowartości 4% za brak wdrożenia odpowiednich i proporcjonalnych środków bezpieczeństwa zgodnych z ogólnymi zasadami zarządzania ryzykiem i łańcucha dostaw[34]. Choć na tym etapie byłoby trudno oceniać skuteczność tego rodzaju podejścia, które jest próbą zrekompensowania braku mechanizmów egzekwowania w dyrektywie NIS, nowa Strategia bezpieczeństwa cybernetycznego dla UE, przedstawiona we wrześniu 2017, będzie odnosić się do kwestii nierównej gotowości krajów członkowskich oraz wymiany dobrych praktyk, w zakresie wdrażania dyrektywy NIS.

Fragmentacja rynku cyberbezpieczeństwa i zależność od państw trzecich

Ogólnie rzecz ujmując, obecna fragmentacja rynku cyberbezpieczeństwa wynika poniekąd z faktu, iż cyberbezpieczeństwo – postrzegane jako część infrastruktury krytycznej oraz element ochrony krajowych zasobów – pozostaje w myśl traktatów unijnych obowiązkiem państw. Istnieje silny związek pomiędzy niezawisłością państwa a jego cyberbezpieczeństwem, zwłaszcza niektórych wrażliwych obszarach takich jak realizowanie przez państwo kluczowych funkcji, utrzymanie praworządności i porządku publicznego oraz ochrona bezpieczeństwa narodowego. Może to prowadzić do braku współpracy i dalszej fragmentacji rynku. Co więcej, geograficzne rozproszenie dostaw produktów zapewniających bezpieczeństwo systemów teleinformatycznych w UE ogranicza wybór bezpiecznych rozwiązań i hamuje konkurencję na poziomie krajowym, regionalnym i unijnym. Rozwój branży bezpieczeństwa cybernetycznego w UE jest napędzany głównie popytem krajowym, w szczególności generowanym przez sektor obronności. W rezultacie większość kontrahentów wykształciło w swoich strukturach oddziały zajmujące się cyberbezpieczeństwem, ale jest również miejsce dla MŚP i startup'ów, które mogą powstać na rynkach specjalistycznym i niszowych.

Unia Europejska jest w znacznym stopniu uzależniona od technologii spoza Europy, zarówno w obszarze cyberbezpieczeństwa i systemów teleinformatycznych. Wykorzystywanie

33 Cyberwatching.eu, Cybersecurity and privacy standards, [online] https://www.cyberwatching.eu/compliance/standards

34 GOV. UK (2017), Consultation on the Security of Network and Information Systems Directive, [online] https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

technologii pochodzących z państw trzecich w urządzeniach do zastosowań krytycznych staje się wyzwaniem, gdyż od tych dostawców nie wymaga się przestrzegania unijnych ram prawnych. Ponadto, nie istnieją żadne dowody na stosowanie takich samych wymogów jakościowych oraz nieistnienie wbudowanych tzw. tylnych drzwi (ang. backdoors)[35]. W Strategii cyberbezpieczeństwa UE 2013 przyznano, że „istnieje ryzyko, że Europa staje się nadmiernie uzależniona nie tylko od ICT pochodzących z zewnątrz, ale również od rozwiązań w zakresie bezpieczeństwa opracowanych poza jej granicami. Należy zagwarantować, aby elementy sprzętu i oprogramowania produkowane w UE oraz w państwach trzecich, które są stosowane w kluczowych usługach i w kluczowej infrastrukturze oraz w coraz większym stopniu w urządzeniach przenośnych, były wiarygodne i bezpieczne oraz aby gwarantowały ochronę danych osobowych"[36].

Aby skutecznie chronić łańcuch wartości, wszyscy uczestnicy rynku muszą przestrzegać tych samych reguł gry dotyczących cyberbezpieczeństwa oraz ochrony danych. Ryzyko ataków można zminimalizować jedynie poprzez zabezpieczenie całego łańcucha wartości. Oznacza to, że wszyscy aktywni gracze na jednolitym unijnym rynku, niezależnie od miejsce pochodzenia, muszą stosować się do wymagań dyrektywy NIS. Dotyczy to operatorów usług kluczowych, producentów sprzętu i oprogramowania komputerowego i usług społeczeństwa informacyjnego[37].

Systemy SCADA to tradycyjnie dedykowane systemy własnościowe, oddzielone od świata zewnętrznego. Od niedawna można zauważyć tendencję do korzystania w systemach SCADA z komercyjnego i ogólnodostępnego oprogramowania i sprzętu, co przyczynia się do zwiększenia ryzyka i zagrożenia w stopniu dotychczas niespotykanym[38]. Generalnie rzecz biorąc, łańcuchy dostaw dla niemal wszystkich przetargów publicznych mogą stać się celem cyberataku. Jeśli łańcuch dostaw nie przestrzega przejrzystego zestawu norm, staje się podatny na fragmentację i brak spójności w podejściu do spraw związanych z cyberbezpieczeństwem. Najsłabsze ogniwo w tym łańcuchu będzie szczególnie narażone na cyberatak[39].

Ostatnie badanie ujawnia, że 20% firm brytyjskich jest zaniepokojonych podatnościami, których źródłem są ich dostawcy. Około połowy respondentów (SMEs) było zobowiązanych do uzyskania standardu w dziedzinie cyberbezpieczeństwa, takiego jak ISO 27001 wdrożonego również przez ich klienta korporacyjnego w porównaniu do 28% w roku poprzednim, co

35 ECS (2016), European Cybersecurity Industry Proposal for a contractual public –private partnership, [online] http://www.ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

36 European Commission (2016), Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry, [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

37 European Commission (2016), Commissioner Oettinger receives the final report of the European Cybersecurity Industrial Leaders, [online] https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders

38 OSCE (2016), op. cit.

39 Atkins (2016), Cyber resilient infrastructure. Securing our critical national infrastructure and defence capabilities, [online] http://explore.atkinsglobal.com/cyber/Atkins_Cyber_Resilient_Infrastructure_Report.pdf

wyraźnie wskazuje na trend wzrostowy jeśli chodzi o wymogi narzucane na bezpieczeństwo informacji pochodzących od dostawców. Staje się oczywiste, że poprzez narzucanie małym i średnim dostawcom (SMEs) wymagań dotyczących cyberbezpieczeństwa, podmioty te mogą zminimalizować ogólne ryzyko i jednocześnie zwiększyć bezpieczeństwo informacji w całym łańcuch wartości[40].

Nakreśliwszy specyfikę sektora energetycznego, niniejsza analiza skupi się teraz na ogólnym krajobrazie politycznych w obszarze cyberbezpieczeństwa i energetyki, jak również na koncepcji jednolitego rynku cyfrowego.

Ogólny krajobraz polityczny UE

Na nakreślonym powyżej tle, warto w tym miejscu przestawić działania, jakie są planowane i podejmowane na szczeblu UE. Ramy czasowe powiązanych z nimi środków zostały zobrazowane poniżej (patrz Rysunek nr 9). W trakcie śródokresowego przeglądu realizacji strategii jednolitego rynku cyfrowego w maju 2017 roku, Komisja Europejska (KC) ogłosiła plany dotyczące gruntownej rewizji Strategii cyberbezpieczeństwa UE 2013, mandatu ENISA w celu zdefiniowania jej nowej roli w związku z wymogami wynikającymi z dyrektywy NIS oraz wprowadzenia europejskich ram certyfikacji i znakowania[41]. Ten „pakiet dotyczący bezpieczeństwa cybernetycznego" został opublikowany we wrześniu 2017 roku.

W dziedzinie energetyki, w listopadzie 2016 roku KE opublikowała zestaw środków w celu podtrzymania konkurencyjności europejskiego rynku energii w obliczu rozwoju sektora czystej energii i jego ogólnego wpływu na rynek. W ramach pakietu „Czysta energia dla wszystkich Europejczyków", KE zaproponowała opracowanie planów gotowości na wypadek zagrożeń dla sektora energetycznego[42] oraz utworzenie kodeksów sieci, między innymi dla zasad cyberbezpieczeństwa. KE przyznaje, iż w przypadku wystąpienia sytuacji kryzysowej, tj. złośliwego ataku, włączając atak cybernetyczny, kryzys taki ma często skutek transgraniczny. Państwa członkowskie mają jednakże tendencję do koncentrowania się na tym, co dzieje się na ich własnym podwórku, często ignorując kontekst międzynarodowy. Dlatego potrzebny jest instrument na szczeblu unijnym, by wyeliminować zauważalne niespójności w ich podejściach w tej kwestii[43].

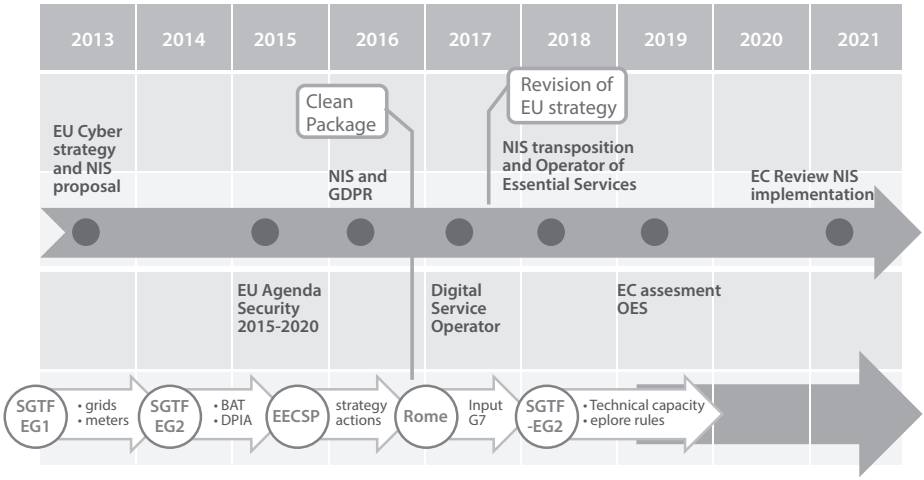
40 Ashford W. (2017), Enterprises are upping security demands on SME suppliers, [online] http://www.computerweekly.com/news/450423617/Enterprises-are-upping-security-demands-on-SME-suppliers

41 European Commission (2017), Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All, [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228

42 European Commission (2016), Proposal for a regulation on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, COM(2016) 862 final, [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0862

43 European Commission (2016), Proposal for a regulation on the internal market for electricity, COM(2016) 861 final/2, [online] http://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v9.pdf

Rysunek nr 9. Mapa cyberbezpieczeństwa UE oraz konkretne działania związane z sektorem energetycznym podejmowane na szczeblu UE. Źródło: Kollau (2017), Cybersecurity in the energy sector. IEA Digitalization and energy workshop. Digital Resilience



W komunikacie z lipca 2016, KE ogłosiła uruchomienie partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa (cPPP). W zamierzeniu cPPP ma poprawić skuteczności wdrożenia głównych celów programu „Horizon 2020" oraz dokonać rewizji Strategii cyberbezpieczeństwa UE 2013 oraz realizacji strategii Jednolitego rynku cyfrowego poprzez wspieranie innowacyjnych i niezawodnych rozwiązań w obszarach, gdzie UE ma przewagę konkurencyjną (np. energetyka). Jako cel szczegółowy związany z poprawą konkurencyjności, cPPP ma opracowywać rozwiązania prowadzące do wykorzystania technologii poprawiających bezpieczeństwo cybernetyczne w różnorakich infrastrukturach krytycznych. Oprócz tego cPPP ma za zadanie współpracować z państwami trzecimi w celu ujednolicenia podejść do kwestii cyberbezpieczeństwa, a w szczególności wspierać rozwój oraz wykorzystanie międzynarodowych standardów we wszystkich możliwych obszarach[44].

Wyżej wspomniane cPPP ma poparcie Europejskiego Stowarzyszenia ds. Cyberbezpieczeństwa (ang. European Cyber Security Organisation, ECSO), którego głównym celem jest wspieranie inicjatyw i projektów wzmacniających sektor cyberbezpieczeństwa, jego większą konkurencyjność i rozwój, oraz wdrażanie rozwiązań z obszaru cyberbezpieczeństwa dla etapów krytycznych zaufanych łańcuchów dostaw w sektorach, gdzie UE jest liderem. W zakresie swojego działania, ECSO będzie skupiać się na sieciach inteligentnych i przemysłowych systemach sterowania[45].

44 European Commission (2016), Annex Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union and the European Cyber Security Organization to the Commission decision on the signing of a contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organization, [online] https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp

45 European Cybersecurity Organization, [online] https://www.ecs-org.eu/about

W ostatnim czasie uruchomiono kilka inicjatyw sektorowych w celu wzmocnienia cyberbezpieczeństwa w kluczowych sektorach. W 2015 roku KE powołała specjalną grupę ekspercką, Energy Expert Cybersecurity Platform (EECSP), zajmującą się kwestiami cyberbezpieczeństwa w sektorze energetycznym[46]. Grupa ma na celu wspieranie procesu wdrażania dyrektywy NIS oraz ewaluację przyszłych potrzeb sektora dotyczących cyberbezpieczeństwa na terenie całej UE w odniesieniu do kwestii infrastrukturalnych, bezpieczeństwa dostaw, czy technologii sieci inteligentnych (ang. *smart grids*). Warto zauważyć, że prace w ramach grupy eksperckiej EECSP będzie prowadzić Dyrekcja Generalna ds. Energii (DG ENER) we współpracy z Sekretariatem Generalnym (SG), DG ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MŚP (DG GROW), Wspólnym Centrum Badawczym (JRC), DG ds. Migracji i Spraw Wewnętrznych (DG HOME), DG ds. Mobilności i Transportu (DG MOVE), DG ds. Sieci Komunikacyjnych, Treści i Technologii (DG CONNECT), DG ds. Sprawiedliwości i Konsumentów (DG JUST), co z jednej strony odzwierciedla złożoność badanego problemu, a z drugiej strony pokazuje, że KE wyciągnęła wnioski z przebiegu negocjacji w sprawie dyrektywy NIS i od samego początku chce podejść do problemu w sposób kompleksowy, angażując w to wiele sektorów. EECSP jest zwolennikiem kompleksowej strategii cyberbezpieczeństwa dla sektora energetycznego UE, co zwiększyłoby skuteczność implementacji dyrektywy NIS i stworzyło wielopoziomową płaszczyznę dialogu wspierającego synergię pomiędzy Strategią jednolitego rynku cyfrowego, Europejską agendą bezpieczeństwa i Unią energetyczną[47].

Działania przewidziane w dyrektywie mają na celu prowadzenie dalszych prac nad rozpoznaniem i wyznaczeniem europejskich infrastruktur krytycznych oraz ocenę potrzeb w zakresie poprawy ich ochrony[48], gdyż ewaluacja dotychczasowych osiągnięć pokazała ich częściowy sukces. Wspomniany akt prawny wezwał państwa członkowskie do określenia i wyznaczenia europejskich infrastruktur krytycznych. W efekcie zidentyfikowano mniej niż 20 europejskich infrastruktur krytycznych, a niektóre oczywiste infrastruktury obejmujące całą UE, takie jak główne sieci przesyłowe, wręcz pominięto. Dyrektywa, pomimo wyznaczonego celu dotyczącego rozwoju współpracy transgranicznej, zaangażowała państwa członkowskie do

46 Mandat grupy eksperckiej będzie ograniczony do dwóch lat, z możliwością prolongacji. Przewodnictwo i obsługę sekretariatu grupy eksperckiej zapewni DG ds. Energii. Grupa będzie liczyła maksymalnie 15 ekspertów. Aby skonkretyzować oczekiwane wyniki swoich prac, grupa ekspercka 1) dokona analizy istniejącego prawodawstwa, inicjatyw, projektów i strategii dotyczących cyberbezpieczeństwa związanych z całym sektorem energetycznym, aby dokładnie wskazać obszary, w których należy zastosować podejście sektorowe. EECSP zbada zależności pomiędzy różnymi instrumentami legislacyjnymi UE, np. dyrektywą NIS a rozporządzeniem RODO, sposoby usprawnienia stosownych obowiązków wpływających na sektor energetyczny oraz wskaże konkretne rozwiązania (pierwszy wynik prac); 2)opracuje krótko-, średnio- i długoterminową strategię opierając się na pierwszym wyniku prac, usprawni mechanizmy wdrażania nowej podstawy prawnej dyrektywy NIS i rozporządzenia RODO oraz dostarczy informacje dla przyjmowanych w przyszłości aktów prawnych (drugi wynik prac); 3) Trzeci wynik prac będzie uwzględniać regularne monitorowanie rozmaitych nieprawidłowości równolegle do wdrażania stosownych przepisów oraz ewolucji ryzyk, zagrożeń i podatności w sektorze energetycznym.

47 European Commission (2016), Energy Expert Cyber Security Platform (EECSP) Terms of Reference (EECSP) & Call for Experts (EESCP-Expert Group), [online] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=21275&no=1

48 Komisja Europejska (2008), 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, [online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

dwustronnej współpracy. Wydaje się, że podejście sektorowe okazało się być dla wielu krajów członkowskich sporym wyzwaniem, z racji tego, iż krytyczność infrastruktury nie jest kwestią wyłącznie sektorową, lecz uwzględniającą podejście systemowe i usługowe[49].

Jeśli chodzi o międzynarodowe aspekty polityki UE, rzeczone uzależnienie technologiczne UE od rozwiązań pochodzących z krajów trzecich oraz bezpieczeństwo łańcucha wartości wywołało dyskusję po obu stronach Atlantyku. W lutym 2017 roku, we wspólnym stanowisku, które zostało dopracowane w lipcu 2017 roku, Niemcy, Francja i Włochy wystosowały prośbę o zajęcie się problemem prowadzonych przez państwa spoza UE, głównie Chiny, strategicznych inwestycji istotnych z punktu widzenia całej Europy, które obejmują łańcuchy wartości, kluczowe technologie, produkcję oraz pochodzącą z Europy wiedzę praktyczną (know-how). We wspólnym stanowisku oświadczono, że obecne instrumenty unijne mogą nie gwarantować ochrony przed takimi działaniami, niezależnie od istnienia krajowych mechanizmów bezpieczeństwa i środków zapewniających porządek publiczny, i zwrócono się do KE z prośbą o podjęcie w tym względzie działań legislacyjnych[50]. To wspólne stanowisko spotkało się jednakże z ostrą reakcją pozostałych państw członkowskich na posiedzeniu Rady Europejskiej w 2017 roku, zarzucających mu możliwy protekcjonizm. Warto zaznaczyć, że 13 państw członkowskich wdrożyło u siebie pewne procedury kontroli bezpieczeństwa, jednak rodzi się pytanie czy podejście UE nie przełożyłoby się na ich wzmocnienie[51]. Wpływ akwizycji zagranicznych na kluczowe technologie, również w obszarze cyberbezpieczeństwa, stanowią główny aspekt ram kontrolnych bezpośrednich inwestycji zagranicznych w UE. Ramy te pozwalają skontrolować inwestycje dokonywane przez podmioty spoza UE pod kątem zapewnienia porządku publicznego i bezpieczeństwa[52]. Z kolei amerykański Kongres może rozważyć wprowadzenie regulacji wzmacniającej nadzór nad chińskimi inwestycjami w nowo powstające wrażliwe technologie, które są kluczowe dla amerykańskich interesów związanych z bezpieczeństwem narodowym[53]. Choć wyniki działań na szczeblu UE przyjdzie nam jeszcze ocenić, obawy te ukazują potencjalną wagę omawianego problemu.

Z racji tego, że przedmiotem niniejszego opracowania jest przegląd polityki UE pod kątem standaryzacji rozwiązań dotyczących cyberbezpieczeństwa w sektorze energii elektrycznej, baczną uwagę zwrócimy na niedawny wniosek KE w sprawie regulacji dotyczącej ENISA, „Agencji ds bezpieczeństwa cybernetycznego UE" oraz certyfikacji bezpieczeństwa cybernetycznego systemów teleinformatycznych (Akt Cyberbezpieczeństwa) w kontekście dyrektywy NIS oraz przepisów regulujących sektor energetyczny. Zgodnie z proponowanym rozporządzeniem, odnowiony mandat ENISY został wyznaczony i wzmocniony w obszarach, gdzie działalność agencji przyniosła wyraźną wartość

49 Komisja Europejska (2013), Dokument roboczy służb Komisji dotyczący nowego podejścia do europejskiego programu ochrony infrastruktury krytycznej: Zwiększenie ochrony europejskiej infrastruktury krytycznej, [online] https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

50 Hanke J. (2017), EU's Big 3 seek greater role for Brussels to stop Chinese takeovers, [online] http://www.politico.eu/article/eus-big-3-seek-greater-role-for-brussels-to-stop-chinese-takeovers/

51 EU Reporter Correspondent (2017), #Bruegel: Should the EU have the power to vet foreign #takeovers?, [online] https://www.eureporter.co/world/2017/09/04/bruegel-should-the-eu-have-the-power-to-vet-foreign-takeovers/

52 European Commission (2017), Joint communication to the European Parliament and the Council, op.cit.

53 Kania E. (2017), Beyond CFIUS: The Strategic Challenge of China's Rise in Artificial Intelligence, [online] https://www.lawfareblog.com/beyond-cfius-strategic-challenge-chinas-rise-artificial-intelligence

dodaną, szczególnie tyczy się to wdrażania dyrektywy NIS, rewizji Strategii bezpieczeństwa cybernetycznego UE, planowanej publikacji Planu bezpieczeństwa cybernetycznego UE na rzecz współpracy w przypadku kryzysu cybernetycznego, oraz wcześniej wspomnianej certyfikacji bezpieczeństwa systemów teleinformatycznych. W ramach ogłoszonych założeń, opublikowano wspólne podejście do programów oceny bezpieczeństwa TIK, które dostosowują poziom zabezpieczeń do ich wykorzystania (np. w infrastrukturach krytycznych). Program będzie miał charakter dobrowolny, tj. nie będzie nakładał na dostawców żadnych obowiązków, choć KE nie wyklucza możliwości podjęcia działań regulacyjnych bądź legislacyjnych na późniejszym etapie.[54]

Podsektor energii elektrycznej a dyrektywa NIS

Dyrektywa NIS stanowi pierwszy element prawodawstwa dotyczącego bezpieczeństwa cybernetycznego, które ma wymiar ogólnoeuropejski. We wstępnym wniosku, KE włączyła w zakres dyrektywy NIS ogólnie pojęty sektor energetyczny. W procesie międzyinstytucjonalnych negocjacji, wyodrębniono podsektory energii elektrycznej, ropy i gazu i przyporządkowano je do definicji określonych w innych odpowiednich sektorowych aktach prawnych UE lub opisach technicznych istotnych instrumentów unijnych. Oprócz tego dokonano oceny na temat tego, czy istniejące prawodawstwo sektorowe pokrywa się w jakiejś części z odpowiednimi zapisami dotyczącymi zarządzania ryzykiem i zgłaszaniem incydentów zawartymi w dyrektywie NIS.

Zgodnie z treścią Załącznika nr 2, rodzaje podmiotów ujętych w zakresie dyrektywy NIS obejmują przedsiębiorstwa energetyczne pełniące funkcję operatorów systemu dostaw, dystrybucyjnego i przesyłowego. Kwestią, na którą również zwrócono uwagę była standaryzacja. Artykuł 19 dyrektywy NIS zachęca państwa członkowskie do stosowania przyjętych w Europie i na świecie norm i specyfikacji odnoszących się do bezpieczeństwa sieci i systemów informatycznych, aby wspierać zbieżność działań związanych z wdrażaniem wymogów dotyczących bezpieczeństwa i zgłaszania incydentów przez operatorów usług kluczowych. Z kolei agencji ENISA powierzono zadanie opracowania porad i wytycznych dotyczących kwestii technicznych, jakie należy uwzględnić w tym temacie. Ponadto zadaniem grupy współpracy jest prowadzenie rozmów z przedstawicielami odpowiednich organizacji europejskich na temat norm i specyfikacji, o których mowa w artykule 19. Podczas gdy dyrektywa NIS nakreśla ogólne wytyczne to konkretne zasady dotyczące bezpieczeństwa cybernetycznego podsektora energii elektrycznej będą opracowane w ramach tzw. „kodeksu sieci" ujętego we wniosku KE w sprawie rozporządzenia dotyczącego wewnętrznego rynku energii elektrycznej z 2016 roku oraz wniosku w sprawie rozporządzenia dotyczącego gotowości na wypadek zagrożeń w sektorze energii elektrycznej[55].

W artykule 1 ust. 7 dyrektywy NIS uznano, iż tam, gdzie sektorowy akt prawny UE stawia operatorom usług kluczowych, wymóg zapewnienia bezpieczeństwo swoich sieci i systemów

54 European Commission (2017), Proposal for a regulation of the European Parliament and the Council on ENISA, op. cit.
55 European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council on risk preparedness …, op. cit.

Tabela nr 1. Prezentacja porównawcza sektora energetycznego w dyrektywie NIS. Źródło: opracowanie własne na podstawie dyrektywy NIS (propozycji i przyjętej wersji)

	Załącznik nr 2 Wstępna propozycja KE dotycząca dyrektywy NIS		Załącznik nr 2 Przyjęta dyrektywa NIS
Energetyka	Dostawcy energii elektrycznej i gazu	Elektryczność	Rodzaj podmiotu
			Przedsiębiorstwa energetyczne, zgodnie z definicją określoną w art. 2 ust. 35 Dyrektywy Parlamentu Europejskiego i Rady 2009/72/WE (1), które realizują dostawy, zgodnie z definicją określoną w art. 2 ust. 19 tejże dyrektywy
	Operatorzy systemu dystrybucji energii elektrycznej i/lub gazu ziemnego oraz sprzedawcy detaliczni obsługujący konsumentów finalnych		Operatorzy systemu dystrybucyjnego, zgodnie z definicją określoną w art. 2 ust. 6 dyrektywy 2009/72/WE
	Operatorzy systemu przesyłowego gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemu LNG		Operatorzy systemu przesyłowego, zgodnie z definicją określoną w art. 2 ust. 4 dyrektywy 2009/72/WE
	Operatorzy systemu przesyłowego energii elektrycznej	Ropa	Operatorzy rurociągów przesyłowych ropy naftowej
	Rurociągi przesyłowe ropy naftowej i magazynowanie ropy		Operatorzy instalacji służącej do produkcji, rafinacji i przetwarzania ropy naftowej; operatorzy systemu magazynowania i przesyłu
	Operatorzy rynku energii elektrycznej i gazu		Przedsiębiorstwa dostarczające ropę, zgodnie z definicją określoną w art. 2 ust. 8 Dyrektywy Parlamentu Europejskiego i Rady 2009/73/WE (2)
	Operatorzy instalacji służących do produkcji, rafinacji i przetwarzania ropy i gazu ziemnego	Gaz ziemny	Operatorzy systemu dystrybucyjnego, zgodnie z definicją określoną w art. 2 ust. 6 dyrektywy 2009/73/WE
			Operatorzy systemu przesyłowego, zgodnie z definicją określoną w art. 2 ust. 4 dyrektywy 2009/73/WE
			Operatorzy systemu magazynowania, zgodnie z definicją określoną w art. 2 ust. 10 dyrektywy 2009/73/WE
			Operatorzy systemu LNG, zgodnie z definicją określoną w art. 2 ust. 12 dyrektywy 2009/73/WE
			Przedsiębiorstwa gazowe, zgodnie z definicją określoną w art. 2 ust. 1 dyrektywy 2009/73/WE
			Operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego

informatycznych, stosuje się przepisy tego sektorowego aktu prawnego UE, pod warunkiem, że takie wymogi są przynajmniej równoważne pod względem skutku z obowiązkami określonymi w dyrektywie NIS. Z uwagi na to, że dyrektywa NIS określa jedynie ogólne obowiązki, rozporządzenia sektorowe umożliwiają wprowadzenie określonego rozwiązania definiującego konkretne warunki w celu skoordynowania działań państw członkowskich oraz zapewnienia odporności wzajemnie połączonych sieci elektroenergetycznych. Aby zapewnić bezpieczeństwo cybernetyczne sieci elektroenergetycznych, kodeks sieci powinien uwzględnić przynajmniej następujące cztery elementy: 1) metodologię identyfikacji operatorów usług

kluczowych dla sektora energetycznego, 2) program klasyfikacji ryzyka, 3) minimalne warunki wstępne gwarantujące, że zidentyfikowani operatorzy spełniają określone minimalne kryteria, oraz 4) ujednolicona procedura zgłaszania incydentów.

Z drugiej strony, rozporządzenie dotyczące gotowości na wypadek zagrożeń w sektorze energii elektrycznej wymusiłoby na państwach członkowskich opracowanie planów gotowości na wypadek zagrożeń, realizowanych w sytuacjach kryzysowych, wywołanych szkodliwymi działaniami takimi jak cyberataki. Uzupełnieniem tego rodzaju planów byłyby wytyczne/kodeks sieci dotyczący cyberbezpieczeństwa w sektorze energetycznym wynikające z dyrektywy NIS. Ponadto państwa członkowskie zostaną zobligowane do opracowania zasad ochrony własnych wrażliwych zasobów, zwłaszcza w sytuacji zmian dotyczących kontroli nad strukturą własnościową. Plany gotowości na wypadek wystąpienia zagrożenia zostaną wzmocnione planami dotyczącymi współpracy regionalnej, aby uwzględnić aspekty transgraniczne oraz powiązany charakter systemów elektroenergetycznych w UE. Mandat Grupy Koordynacyjnej ds. Energii Elektrycznej (Electricity Coordination Group) zostanie wzmocniony, aby grupa mogła nadzorować to, w jaki sposób kraje UE rozwiązują potencjalne kryzysy energetyczne, a także przyczyniać się do zacieśniania współpracy i zwiększania zaufania pomiędzy państwami członkowskimi[56]. Powyższe akty wykonawcze stanowią dopełnienie zarówno dyrektywy NIS, jaki i Dyrektywy w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, które ustanawiają wspólną procedurę identyfikacji europejskich infrastruktur krytycznych, skupiając się szerzej na sposobach wzmocnienia ogólnej odporności systemu energii elektrycznej jako całości oraz radzenia sobie z występującymi zagrożeniami[57].

Trzeba jednak pamiętać, iż samo podporządkowanie się standardom bezpieczeństwa cybernetycznego nie stanowi magicznego sposobu na eliminację wszystkich podatności infrastruktur krytycznych, głównie dlatego, że dyrektywa NIS nie wymusza wdrażania standardów. Niemniej ich wdrożenie może doprowadzić do postania mechanizmu kontrolnego, który przyczyni się do zwiększenia odporności. Wprowadzenie w życie norm dotyczących cyberbezpieczeństwa może zwiększyć popyt na bezpieczne produkty, usługi i praktyki, co z kolei może przełożyć się na wzrost konkurencyjności dostawców, którzy promują bezpieczne rozwiązania skrojone do potrzeb sektora. Wiele krajów wprowadziło programy certyfikacji, aby rozpowszechniać

56 Komisja Europejska (2016), Dokument roboczy służb Komisji, Ocena skutków oraz inne dokumenty towarzyszące: Wniosek Dyrektywa Parlamentu Europejskiego i Rady dotycząca wspólnych zasad rynku wewnętrznego energii elektrycznej (wersja przekształcona), Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie rynku energii elektrycznej (wersja przekształcona), Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Agencję ds. Współpracy Organów Regulacji Energetyki (wersja przekształcona), Wniosej Rozporządzenie Parlamentu Europejskiego i Rady w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej, [online] https://ec.europa.eu/energy/sites/ener/files/documents/mdi_impact_assessment_main_report_for_publication.pdf

57 European Commission (2016), Proposal for a regulation of the European Parliament and of the Council on the internal market…, op. cit.

kwestie dotyczące cyberbezpieczeństwa w branży. Stany Zjednoczone i Australia stymulują wdrażanie standardów poprzez stosowanie zachęt. Również Korea Południowa wprowadziła system zachęt, by zmobilizować branżę do wdrażania norm ISO/IEC 27001 oraz ISO/IEC15408[58].

A teraz zwrócimy uwagę na wyzwania natury ogólnej, związane ze standaryzacją rozwiązań w dziedzinie cyberbezpieczeństwa w sektorze energii elektrycznej.

Standaryzacja rozwiązań w dziedzinie cyberbezpieczeństwa w sektorze energii elektrycznej

Komunikacja wewnątrz sieci stanowi wyzwanie dla sieci elektroenergetycznych w ramach podsektora energii elektrycznej. Współczesne sieci inteligentne charakteryzują się 1) infrastrukturą komunikacyjną zarządzającą siecią oraz 2) elastycznością, która pozwala na integrację zdecentralizowanych komponentów sieci. Na cyberbezpieczeństwo sieci elektroenergetycznych wpływa wysoka podatność sieci elektroenergetycznych na poważne w skutkach cyberataki, przestrzeganie jedynie obowiązkowych norm, nierygorystyczne podejście do wdrażania dobrowolnych rekomendacji oraz zaniedbania w zakresie działań eliminujących podatności w sieci. Technologia jednocześnie usprawnia działanie sieci, jak i sprawia, że jest ona bardziej narażona na cyberataki. Wszechobecny Internet może potencjalnie zagrażać wszystkim elementom składowym inteligentnych sieci, co także stanowi wyzwanie dla ich fizycznego bezpieczeństwa. Z technologicznego punktu widzenia, cykl życia komponentów wchodzących w skład inteligentnych sieci jest dość długi. Nagłe wyłączenie i „załatanie" luki w systemie, który działa 24 godziny na dobę, 7 dni w tygodniu, może się okazać niemożliwe, co sprawia, że aktualizacje i usprawnienia systemu stanowią szczególne wyzwanie[59].

Ochrona technologii operacyjnej (OT) wykorzystywanej w infrastrukturach krytycznych nie ogranicza się jedynie do systemów SCADA. Niemal wszystkie przemysłowe systemy sterowania (ICS) stanowią hybrydę sieci informatycznych (IT) i SCADA. Obecne cyberataki to w większości wielowektorowe wrogie działania, które przenikają przez warstwę systemów IT, aby dotrzeć do infrastruktury kluczowej dla OT[60]. Koncepcje i narzędzia cyberbezpieczeństwa są na dobrej drodze do tego, by pojąć zawiłości i współzależności tych wielowektorowych ataków. Twierdzi się, że „dostawcy rozwiązują tylko te problemy, na których się znają", przy czym istnieje tylko garstka firm, które w pełni rozumieją działanie obu technologii, IT i OT. Większość dostawców w sektorze cyberbezpieczeństwa proponuje rozwiązania jedynie w zakresie systemów IT dysponując niewielką wiedzą na temat OT, którą muszą systematycznie nabywać[61].

58 KPMG (2016), Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection, [online] https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/Cyber-Security-Standards-Compliance-A-Vital-Measure-to-Critical-Infrastructure-Protection.pdf

59 European Cybersecurity Organization (2016), Industry proposal for contractual public private partnership, [online] http://www.ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

60 Dar A. (2017), Protecting Industrial Control Networks – It's Not Just About SCADA Security, [online] https://www.cyberbit.com/ot-security/protecting-industrial-control-networks-scada-security

61 Dar A. (2017), op. cit.

Mieszanka startych i nowych technologii stanowi wyzwanie, jeśli chodzi o rozwiązywanie problemów dotyczących cyberbezpieczeństwa w jednolity sposób. Koszty, jakie pociągają za sobą spuścizna technologiczna, gdzie Windows XP stanowi podstawowy system operacyjny OT w wielu infrastrukturach krytycznych, który dawno przestał już być wspierany przez Microsoft, oraz aktualizacja oprogramowania kluczowych urządzeń są ogromne. Dlatego właśnie te urządzenia stały się obiektem potencjalnych ataków[62]. Wiele systemów sterowania bazuje na jeszcze starszych wersjach systemów operacyjnych, mających 20 lat i więcej. Systemy te są już od dawna przestarzałe, a łaty i aktualizacje usuwające błędy czy usuwające luki nie są już dostępne[63]. Osiągnięcie porozumienia w kwestii tego, które standardy dotyczące cyberbezpieczeństwa należy zastosować jest trudne z uwagi na to, że inżynierowie IT i OT są przyzwyczajeni do różnych mechanizmów innowacji i obsługi technicznej. Jeśli chodzi o ramy czasowe, oczekuje się, że przemysłowe systemy sterowania będą służyć 25–125 lat, podczas gdy cykl życia większości produktów IT jest obliczony na 3–5 lat[64].

Wyzwania w obszarze interoperacyjności inteligentnych sieci odnoszą się do braku solidnych standardów dla nowych technologii i związaną z tym trudnością w łączeniu nowych i starych technologii[65]. W sektorze energetycznym normy mogą przyczyniać się do harmonizacji strategii zarządzania ryzykiem i ustanowienia wspólnych ram dotyczących kwestii bezpieczeństwa charakterystycznych dla tego sektora. Uważa się, że seria norm ISO 27000 związanych z zarządzaniem bezpieczeństwem informacji może zostać wykorzystana do tego właśnie celu. Dalsza współpraca pomiędzy graczami na rynku energii a organizacjami opracowującymi standardy może stanowić platformę dla osiągnięcia wspólnego zrozumienia i wprowadzenia w życie norm skrojonych do potrzeb sektora energetycznego[66]. Jak wskazano wyżej, brak interoperacyjności rozwiązań (norm technicznych) oraz ogólnoeuropejskiego mechanizmu certyfikacji hamuje rozwój jednolitego rynku cyberbezpieczeństwa. Certyfikacja przyczynia się do zwiększenia bezpieczeństwa produktów i usług. Jest to istotne z punktu widzenia systemów, takich jak sieci inteligentne czy przemysłowe systemy sterowania, które do działania wykorzystują technologie oraz wymagają wysokiego poziomu bezpieczeństwa[67]. We wrześniu 2017 roku, w ramach pakietu cyberbezpieczeństwa, KE zaproponowała stworzenie sieci europejskiego systemu certyfikacji, w którym kluczową rolę odgrywałaby ENISA. Proponowane rozwiązanie wprowadzałoby system certyfikacji obejmujący swym zasięgiem całą UE, który zawierałby

62 CISCO (2017), op. cit.

63 TrapX Original Research (2017), Industrial Control Systems Under Siege, [online] https://share.trapx.com/dl/aLo0ack8Kc

64 Weiss, J. (2010). Protecting Industrial Control Systems from Electronic Threats. New York, NY: Momentum Press [w:] Clark-Ginsberg A. and Slayton R., Innovation or Maintenance? The Creation and Evolution of Critical Infrastructure Cybersecurity Standards

65 OSCE (2016), op. cit.

66 ENISA (2016), Gaps in NIS standardization…, op. cit.

67 European Commission (2016), Commission signs agreement with cybersecurity industry to increase measures to address cyber threats, [online] https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats

zestaw reguł, wymogów technicznych, procedur i standardów. W celu zapewnienia spójności z podobnymi inicjatywami o charakterze międzynarodowym, rozwiązania proponowane w ramach systemu będą bazować w znacznej mierze na standardach międzynarodowych[68].

Wniosek KE w sprawie ENISA, „Europejskiej Agencji ds Bezpieczeństwa Cybernetycznego" oraz certyfikacji bezpieczeństwa cybernetycznego systemów teleinformatycznych (Akt Cyberbezpieczeństwa)

W ramach złożonego we wrześniu 2017 roku wniosku dotyczącego europejskich ram certyfikacji i oznakowania KE planowała, iż:

- „będzie badała ryzyko strategiczne/systemowe wynikające z incydentów cybernetycznych w wysoce współzależnych sektorach w obrębie granic państwowych i poza nimi;

- do końca 2016 r. opracuje plan działania prowadzący do sformułowania wniosku w sprawie ewentualnych europejskich ram certyfikacji bezpieczeństwa ICT, który to wniosek zostałby złożony przed końcem 2017 r., oraz przeprowadzi ocenę wykonalności i skutków europejskich ram oznakowania dotyczącego bezpieczeństwa charakteryzujących się niewielkim obciążeniem dla uczestniczących w nich podmiotów;

- przeanalizuje potrzebę zlikwidowania luk pod względem certyfikacji bezpieczeństwa ICT obecnych w istniejących mechanizmach certyfikacji/walidacji dotyczących określonych sektorów oraz w stosownych przypadkach wyeliminuje te luki;

- włączy, w stosownych przypadkach, certyfikację bezpieczeństwa produktów ICT do przyszłych unijnych wniosków prawodawczych;

- będzie pobudzała zaangażowanie administracji publicznej, aby ułatwić stosowanie certyfikacji i wspólnych specyfikacji przy udzielaniu zamówień publicznych oraz

- będzie monitorowała stosowanie odpowiednich wymogów w zakresie certyfikacji w udzielaniu zamówień publicznych i prywatnych oraz po trzech latach przedstawi sprawozdanie na temat stanu rynku"[69].

W rzeczywistości wspólny wniosek KE w sprawie ENISA, „Europejskiej Agencji ds Bezpieczeństwa Cybernetycznego" oraz certyfikacji bezpieczeństwa cybernetycznego systemów teleinformatycznych (Akt Cyberbezpieczeństwa) udziela ENISA stałego mandatu. Oprócz tego ENISA miałaby za zadanie aktywnie uczestniczyć w pracach nad polityką i politycznymi inicjatywami w różnych sektorach, w tym w energetyce. ENISA wspierałaby działania wzmacniające wewnętrzny rynek cyberbezpieczeństwa, m.in. opracowanie

68 European Commission (2017), The EU cybersecurity certification framework [online] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

69 European Commission (2016), Strengthening Europe's cyber resilience…, op. cit.

kryteriów normalizacji TIK oraz programów certyfikacji bezpieczeństwa cybernetycznego TIK. Rozporządzenie, o którym mowa, ustanawia europejskie ramy certyfikacji w dziedzinie cyberbezpieczeństwa dla produktów i usług TIK, tworzy programy certyfikacji zdolności operacyjnych oraz tworzy przyjazny system wdrażania programów dla konkretnych produktów i usług TIK. Ramy te zostaną przygotowane przez agencję ENISA we współpracy z nowo utworzoną europejską grupą ds. certyfikacji w dziedzinie cyberbezpieczeństwa (ang. European Cybersecurity Certification Group). Odwołanie się do tych ram będzie miało charakter fakultatywny, chyba że dorobek prawny UE stanowi inaczej. Aby przeciwdziałać fragmentacji oraz zapewnić harmonizację obecne narodowe programy certyfikacji produktów i usług TIK przestaną obowiązywać z datą uruchomienia europejskich ram certyfikacji w dziedzinie cyberbezpieczeństwa, które staną się nadrzędne w stosunku do programów na szczeblu krajowym. Wniosek ma na celu wsparcie procesu wdrażania dyrektywy NIS poprzez zaprezentowanie narzędzia zgodnego z wymogami dyrektywy NIS, które znajdują również odzwierciedlenie w proponowanych ramach certyfikacji.

ENISA już zajęła stanowisko w tej sprawie zachęcając KE do powołania organu koordynującego działania w obszarze standardów cyberbezpieczeństwa oraz ustalenia uproszczonego procesu klasyfikacji poziomu cyberbezpieczeństwa szybko rozwijających się produktów. Oprócz tego, ENISA dąży do tego, aby proces certyfikacji obejmował nie tylko produkty, ale też usługi i umiejętności. Agencja zachęca też KE do przeprowadzenia oceny tego, czy firmy powinny brać odpowiedzialność za konsekwencje nieujawnienia słabości zabezpieczeń, które narażają oprogramowanie na cyberataki.

Choć wyżej wymieniony wniosek nie odnosi się konkretnie do sektora energetycznego, to jednak odpowiada na potrzeby sektorowe wynikające z dyrektywy NIS, które zostaną dopracowane w przepisach dotyczących sektora energetycznego, tj. pakiecie „Czysta energia dla wszystkich Europejczyków".

Implikacje dla sektora energetycznego

Przepisy prawa dotyczące opracowania standardów bezpieczeństwa systemów energetycznych i ustanowienia rady certyfikacyjnej jest postrzegane jako niezbędny warunek realizacji efektywnej strategii cyberbezpieczeństwa dla sektora energetycznego w Europie. Kwestie wymagające uwagi w pierwszej kolejności, to powołanie centralnego organu ds. cyberbezpieczeństwa w sektorze energetycznym, obowiązkowe zgłaszanie incydentów związanych z naruszeniem bezpieczeństwa oraz przepisy narzucające obowiązkową wymianę informacji[70]. Podczas obrad okrągłego stołu na wysokim szczeblu, poprzedzających obecną dyskusję dotyczącą energetyki w Grupie G7, uznano, że unikalny charakter cyberbezpieczeństwa w sektorze energetycznym, wynikający z przemieszania najnowszych oraz startych technologii, uniemożliwia kopiowanie rozwiązań z innych sektorów. Wezwano również do podjęcia konkretnych działań w sprawie certyfikacji w sektorze energetycznym[71]. Z kolei podczas spotkania

70 European Parliament (2016), Cybersecurity strategy..., op. cit.

71 European Commission (2017), Roundtable meeting on cyber security in energy takes place in Rome, [online] https://

w Düsseldorfie w kwietniu 2017, liderzy cyfryzacji z krajów Grupy G20 wspierali i zachęcali do wykorzystania standardów technicznych, wytycznych i dobrych praktyk w oparciu o ocenę ryzyka, aby skutecznie radzić sobie z zagrożeniami. Stanowiłyby one część ogólnych wysiłków na rzecz poprawy bezpieczeństwa infrastruktury krytycznej wykorzystującej TIK[72].

Dokonawszy analizy istniejących luk w standaryzacji, ENISA stwierdza, iż jest praktycznie niemożliwe odseparowanie postanowień ogólnych dotyczących cyberbezpieczeństwa od szerokiej puli standardów w zakresie TIK, które w różnym stopniu zostały już wdrożone przez operatorów objętych dyrektywą NIS. Oprócz tego, ze względu na transgraniczny charakter bezpieczeństwa sieci i systemów informatycznych, standardy dotyczące cyberbezpieczeństwa nie mogą obowiązywać tylko w obrębie jednego regionu i być przyjęte jedynie na terenie UE. Z powodów komercyjnych, wiele usprawnień w dziedzinie bezpieczeństwa sieci i informacji zostanie wdrożonych przy użyciu oprogramowania oraz sprzętu pochodzącego z państw trzecich. Dlatego też ENISA rekomenduje, aby KE zgodnie z dyrektywą NIS i przy wsparciu państw członkowskich:

- „zastosowała otwarte standardy w kwestii wymiany informacji o zagrożeniach, bazujące na globalnie przyjętej platformie STIX/TAXII/CyBOX. Zostaną one sformułowane jako europejska norma (ang. European Norm, EN) definiująca składnię i semantykę danych, niezbędny protokół transferu oraz załączone wskazówki dotyczące jej implementacji

- rozbudowała zdolności analizy ryzyka i potencjał obronny, zdefiniowane w ramach obecnych standardów, aby umożliwić państwom członkowskim sprostanie zaleceniom NII i NIS, niezbędnym do minimalizowania zagrożeń na poziomie państwowym i regionalnym. Działania te powinny zostać podjęte w ramach rozbudowy przez EN zdolności opisanych uprzednio w ETSI TS 102 165-1, ETSI TR 103 305, ISO/IEC 15408 i w odpowiednich standardach serii ISO/IEC JTC1 2700x"[73].

Pomimo transgranicznej natury cyberataków, środki zaradcze są często podejmowane jedynie na poziomie państw członkowskich, które są nieświadome złożoności i istniejących współzależności pomiędzy systemami energetycznymi. Rozdrobnienie kwestii prawnych i politycznych dodatkowo komplikuje możliwą odpowiedź UE, a obecne przepisy dotyczące obszaru energetyki nie w pełni odpowiadają wyzwaniom w dziedzinie cyberbezpieczeństwa. W szczególności dotyczy to pewnych aspektów wymiany informacji. Zaobserwowano, że podmioty uczestniczące w inicjatywach bardzo często reprezentują sprzeczne interesy. Wiele przedsiębiorstw tego sektora przykłada więcej uwagi do bezpieczeństwa infrastruktury fizycznej niż do bezpieczeństwa sieci, systemów procesowych i danych[74].

---

ec.europa.eu/energy/en/news/roundtable-meeting-cyber-security-energy-takes-place-rome, [data dostępu: 20 lipca 2017]G20 DIGITAL ECONOMY MINISTERIAL DECLARATION Shaping Digitalisation for an Interconnected World

72 G20 (2017), G20 digital economy ministerial declaration. Shaping digitalization for an interconnected world, [online] https://www.de.digital/DIGITAL/Redaktion/EN/Downloads/g20-digital-economy-ministerial-declaration-english-version.pdf?__blob=publicationFile&v=3

73 ENISA (2016), Gaps in NIS standardization, op. cit.

74 ENISA (2017), Report on Cyber Security Information Sharing in the Energy Sector, [online] https://www.enisa.europa.

Jeśli chodzi o normy, standardy technologiczne skrojone do potrzeb sektora energetycznego są wykorzystywane jedynie do wspierania a nie egzekwowania wdrażania środków bezpieczeństwa. W praktyce wyegzekwowanie implementacji polityki i strategii dotyczących bezpieczeństwa sieci i systemów informatycznych przez wszystkie podmioty na rynku energetycznym będzie zadaniem dla organów regulacji energetyki. Na poziomie krajowym istnieją następujące organy regulacyjne: Agencja ds. Współpracy Organów Regulacji Energetyki (ang. Agency for the Cooperation of Energy Regulators, ACER) i Rada Europejskich Regulatorów Energii (ang. Council of European Energy Regulators, CEER). Zadaniem krajowych organów regulacyjnych (ang. National Regulatory Authorities, NRA) jest nadzorowanie i wprowadzanie w życie odpowiednich przepisów oraz zapewnianie ich przestrzegania przez wszystkie podmioty aktywne na rynku energetycznym. Niewłaściwe egzekwowanie tych standardów będzie miało negatywny wpływ na wdrażanie praktyk zarządzania ryzykiem w całym sektorze oraz na osiągnięcie porozumienia w kwestii specyficznych problemów sektora energetycznego[75].

Rekomendacje

1. Bazując na rekomendacjach grupy eksperckiej Energy Expert Cybersecurity Platform, EECSP oraz analizie Parlamentu Europejskiego[76], UE zyskałaby na **strategii cyberbezpieczeństwa dedykowanej sektorowi energetycznemu**, w której standaryzacja oraz mechanizmy ułatwiające wymianę informacji byłyby potraktowane priorytetowo. Należy dokonać oceny, czy potrzebne będzie powołanie osobnego organu odpowiedzialnego za koordynację implementacji takiej strategii, czy zadanie to będzie mogło zostać powierzone agencji ENISA.

2. Kluczowe znaczenie będzie miało prawidłowe, spójne i terminowe wdrożenie dyrektywy NIS, która wchodzi w życie w maju 2018 r. w całej UE. Lista operatorów usług kluczowych ma zostać zdefiniowana do listopada 2018 roku. Aby zapewnić jednakowe podejście, **identyfikacja operatorów usług kluczowych na szczeblu UE powinna zostać przeprowadzona w sposób ustrukturyzowany, kompletny i harmonijny** w celu rozwiązania problemu najsłabszych ogniw w systemie wzajemnie połączonych sieci elektroenergetycznych oraz infrastruktur krytycznych[77]. W związku z tym, grupa współpracy oraz Grupa Koordynacyjna ds. Energii Elektrycznej powinny działać wspólnie w celu zapewnienia minimalnego poziomu harmonizacji działań związanych z wypracowaniem wymogów dotyczących cyberbezpieczeństwa w sektorze energetycznym.

3. Dyrektywa NIS nie narzuca **wdrożenia standardów bezpieczeństwa cybernetycznego** w sektorach ujętych w Załączniku nr 2 dyrektywy. Rola ta zostanie powierzona krajowym regulatorom sektora energetycznego, a kraje członkowskie same ustalą zakres sankcji za nieprzestrzeganie zapisów dyrektywy. Przypadkiem wartym dalszej analizy jest podejście

eu/publications/information-sharing-in-the-energy-sector

75 ENISA (2016), Gaps in NIS standardization, op. cit

76 European Parliament, Cybersecurity strategy…, op. cit.

77 Energy Expert Cybersecurity Group (2017), Cybersecurity in the energy sector, op. cit.

rządu Wielkiej Brytanii, który proponuje w tym wypadku wprowadzenie kar podobnych do tych, postulowanych w rozporządzeniu RODO. Ponadto, należy wprowadzić obowiązek przeprowadzania oraz upubliczniania analiz ryzyka dla bezpieczeństwa przez operatorów sieci inteligentnych.

4. Wprowadzenie w życie określonych standardów technicznych oraz minimalnych wymagań dotyczących bezpieczeństwa może odegrać istotną rolę w harmonizacji wewnętrznego rynku energii elektrycznej, w szczególności w wyniku **zamówień publicznych i prywatnych lub przetargów**, które mogą przyspieszyć przyjmowanie europejskich standardów tam, gdzie jest to możliwe[78]. Określone sektory lub infrastruktury krytyczne mogą mieć wyśrubowane wymagania dot. cyberbezpieczeństwa, lecz rzadko są one zharmonizowane na poziomie unijnym, często zaś są specyficzne dla danego kraju. Według portalu cyberwatching.eu, należy dążyć do stworzenia pojedynczej instytucjo bazującej na Europejskim Katalogu Standardów (ang. European Catalogue of Standards) i oferującej jasne wskazówki co do wymogów TIK w obszarze zamówień publicznych[79].

5. Biorąc pod uwagę fakt, że ekosystem cyberbezpieczeństwa jest rozdrobniony i zdominowany przez MŚP oraz start-upy, tworzenie **hubów cyberbezpieczeństwa angażujących MŚP** mogłoby wymusić konsolidację rynku produktów i usług tego sektora, szczególnie w kontekście szans, jakie zamówienia publiczne i prywatne w Europie przynoszą europejskim dostawcom. Pomimo sprawności i elastyczności, MŚP często brakuje odpowiednich zasobów i specjalizacji na wszystkich wymaganych polach, aby skutecznie konkurować o duże zamówienia. Powołanie takich hubów mogłoby ułatwić tworzenie konsorcjów oraz wpłynąć na doraźną mobilizację MŚP.

6. W celu uzyskania kompleksowego wglądu w rynek cyberbezpieczeństwa oraz zrozumienia jego struktury, firmy dostarczające rozwiązań w dziedzinie cyberbezpieczeństwa dla sektora energetycznego skorzystałyby na **opracowaniu szczegółowej mapy ekosystemu cyberbezpieczeństwa**. Ogólnie rzecz ujmując, rynek cyberbezpieczeństwa jest geograficznie rozproszony, co do tej pory wpływało korzystnie na dominację małej grupy globalnych dostarczycieli usług z krajów trzecich. Dostawcy z UE są aktywne niemal wyłącznie lokalnie lub regionalnie. Pomimo siły i innowacyjności, europejskie firmy mają problemy z ekspansją na rynki zagraniczne. Opracowanie szczegółowej mapy firm aktywnych w sektorze energetycznym mogłoby przyczynić się do poprawy jakości tworzonych polityk ukierunkowanych na wsparcie tych firm[80]. Zarówno rozporządzenie RODO, jak i dyrektywa NIS, stanowią istotne czynniki stymulujące rozwój produktów i usług związanych z cyberbezpieczeństwem i skierowanych do operatorów infrastruktur krytycznych.

78 European Cybersecurity Organization (2016), European Cybersecurity Industry Proposal …, op. cit.

79 Cyberwatching.eu, Cybersecurity and privacy standards, [online] https://www.cyberwatching.eu/compliance/standards

80 European Commission (2016), Commission staff working document on cPPP and accompanying measures, [online] https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-cppp-and-accompanying-measures

7. Ze względu na nierówny rozwój innowacyjności, poziomu cyberbezpieczeństwa oraz sektorów energetyki wewnątrz UE, **huby innowacji cyfrowych** (ang. digital innovation hubs) mogą działać stymulująco na konsolidację jednego rynku cyfrowego, szczególnie, że 60% dużych przedsiębiorstw i ponad 90% MŚP nie nadążają za trendami w cyfrowej innowacji[81]. W związku z tym istotne może być nawiązanie ściślejszej współpracy między wspólnotami wiedzy i innowacji (ang. Knowledge and Innovation Communities, KIC) Europejskiego Instytutu Technologii, otwartymi hubami innowacji (testbets) oraz inicjatywą kontraktualnego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa.

8. Istnieje szereg **programów certyfikacji dla produktów TIK**. Problem w tym, że działają one jedynie w kilku państwach członkowskich i nie są szeroko promowane. Istnieją także problemy *stricte* sektorowe. Sektory przemysłowe nie posiadają wystarczających zabezpieczeń gwarantujących bezpieczeństwo komponentów TIK zintegrowanych z systemami[82]. Istnieją głosy opowiadające się za utworzeniem rady certyfikacyjnej odpowiedzialnej za koordynację certyfikacji sieci inteligentnych, nadzór nad stworzeniem wymogów dotyczących cyberbezpieczeństwa, regularny monitoring i przegląd wymogów i potrzeb, a także utrzymanie zgodności wymogów ze standardami unijnymi oraz międzynarodowymi[83].

9. W celu zwiększenia skuteczności systemu cyberbezpieczeństwa w sektorze energii elektrycznej, należy wzmocnić rolę cPPP. Inicjatywa cPPP może przyczynić się do powstania **spójnych ram bezpieczeństwa dla łańcucha dostaw** (części składowych i dostawców), zwłaszcza, że programy certyfikacji i testy penetracyjne nie stanowią skutecznych narzędzi do identyfikacji ukrytych funkcji i tzw. „tylnych drzwi". W nowej Strategii cyberbezpieczeństwa UE Komisja Europejska skupi uwagę na zapewnieniu bezpieczeństwa aplikacji kluczowych lub wysokiego ryzyka, a także na produktach i usługach z zakresu cyberbezpieczeństwa stosowanych szeroko zarówno w sektorze publicznym, jak i prywatnym (w tym w energetyce)[84]. Jest jednak bardzo istotne, aby zapewnić odpowiednie zrównoważenie sektorowe i geograficzne podmiotów wchodzących w skład ECSO (a co za tym idzie, cPPP), co aktualnie nie ma miejsca.

10. Zaproponowane przez Komisję Europejską utworzenie **Europejskiego Centrum Badań Naukowych i Kompetencji w Dziedzinie Bezpieczeństwa Cybernetycznego** (ang. European Cybersecurity Research and Competence Centre)[85], organu oddzielnego od ENISY, powinno

81 European Commission (2016), Pan-European network of digital innovation hubs (DIHs), [online] https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs

82 European Commission (2016), Commission staff working document. Contractual Public Private Partnership on Cybersecurity & Accompanying Measures, [online] https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/10102-2016-216-EN-F1-1-ANNEX-1.PDF

83 European Parliament (2015), Cybersecurity in the European Union and Beyond. Exploring the threats and policy responses, [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

84 European Commission (2017), Joint communication to the European Parliament and the Council, op. cit.

85 Stupp C. (2017), Ansip plans new EU cybersecurity centre, [online] https://www.euractiv.com/section/cybersecurity/news/ansip-plans-new-eu-cybersecurity-centre/

być traktowane z ostrożnością. Raport z oceny działalności agencji ENISA jasno wskazuje na rozdrobnienie instytucji unijnych zajmujących się cyberbezpieczeństwem oraz „istnienie wielu aktorów na poziomie UE aktywnych w dziedzinie cyberbezpieczeństwa włączając ENISA, CERT-EU oraz EC3 (Europol), co prowadzi do fragmentarycznego podejścia do cyberbezpieczeństwa wielu instytucji unijnych. (…) Podczas gdy mandaty tych organizacji są teoretycznie różne, w praktyce ich role nie są jasno zdefiniowane, co może prowadzić do dublowania kompetencji. (…) Wziąwszy to pod uwagę, ENISA z trudnością była w stanie znaleźć miejsce dla siebie, przy czym inne instytucje, a CERT-EU w szczególności, zajmowały się zadaniami z prawnego punktu widzenia podlegającymi kompetencjom ENISY"[86]. Przykład Stanów Zjednoczonych pokazuje, że zaangażowanie zbyt wielu instytucji bez jasnego podziału i koordynacji zadań może prowadzić do ogólnego spadku funkcjonalności systemu cyberbezpieczeństwa, nakładania się kompetencji, konfliktów interesów oraz braku przejrzystości. Z wyjątkiem sytuacji, gdzie zostanie zidentyfikowana konkretna potrzeba, UE powinna powstrzymać się od powoływania nowych agencji, skupiając się na wzmacnianiu mandatów instytucji już istniejących[87]. W tym kontekście przegląd mandatu ENISA da pewne pole do manewru w tym względzie.

11. Ze względu na transgraniczny charakter zagrożeń cybernetycznych, międzynarodowe sojusze i współpraca są kluczowe w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych. W związku z tym, dobrowolne ramy cyberbezpieczeństwa **Narodowego Instytutu Standaryzacji i Technologii** (ang. National Institute for Standards and Technology, NIST)[88] mogą stanowić jeden z modeli dla tworzenia polityk UE w tym zakresie. Z drugiej strony mogą pomóc europejskim interesariuszom w dopracowaniu nadchodzącej wersji ram NIST, aby ułatwić jej zastosowanie do europejskich potrzeb[89]. Do tej pory około 20 krajów wspólnie ze Stanami Zjednoczonymi podjęło wysiłek identyfikacji możliwości adaptacji ram NIST do swoich krajowych warunków[90]. Aby wzmocnić przepływ dobrych praktyk, należy dążyć do nawiązania bardziej regularnych relacji między grupą współpracy a NIST.

12. W świetle nierównego poziomu gotowości i odporności na cyberataki wśród różnych państw członkowskich, wydaje się być uzasadnione stworzenie długo postulowanych **europejskich ram dojrzałości dla sektora energetycznego**[91]. Biorąc pod uwagę wyłącznie sektor energii elektrycznej, ochrona sieci elektroenergetycznych stanowi wspólną odpowiedzialność państw członkowskich i operatorów Cechy sieci energetycznych takie jak krytyczność,

86 European Commission (2017), Study on the Evaluation of the European Union Agency for Network and Information Security, [online] https://ec.europa.eu/digital-single-market/en/news/final-report-evaluation-european-union-agency-network-and-information-security-enisa

87 European Parliament (2015), Cybersecurity in the European Union and Beyond, op. cit.

88 Zaktualizowana wersja projektu została przedłożona do przedstawienia uwag w lutym 2017 roku; konsultacje zakończyły się w kwietniu 2017 roku.

89 US Chamber of Commerce (2017), Transatlantic cybersecurity. Forging a united response to universal threat, [online] https://www.uschamber.com/TransatlanticCybersecurityReport

90 Wolff E., Lerner M., Miller P., Welling M. Hoff C., The global uptake of the NIST cybersecurity framework, Cyber Security Law & Practice – February 2016, [online] https://www.crowell.com/files/20160215-The-Global-Uptake-of-the-NIST-Cybersecurity-Framework-Wolff-Lerner-Miller-Welling-Hoff.pdf

91 European Cyber Security Organisation (2016), op. cit.

transgraniczność oraz współzależność muszą zostać w pewnym stopniu zharmonizowane, aby zrekompensować ich nierówny poziom rozwoju w poszczególnych krajach UE. W tym celu można byłoby rozważyć wdrożenie zdefiniowanych na poziomie europejskim ram określających dojrzałość bezpieczeństwa cybernetycznego, opierających się na międzynarodowych standardach (np. ISO 27000). Takie ramy umożliwiłyby ocenę poziomu odporności sieci energetycznych na terytorium UE[92]. Ponadto, ENISA mogłaby odegrać istotną rolę w opracowaniu **ram dojrzałości cyberbezpieczeństwa dla wszystkich sektorów wymienionych w Załączniku nr 2** do dyrektywy NIS w celu lepszego zrozumienia stopnia przygotowania sektorów, ich lepszej porównywalności i lepszego dopasowania polityk UE w tym zakresie.

13. Biorąc pod uwagę wyłącznie sektor elektroenergetyczny, amerykański **model dojrzałości cyberbezpieczeństwa podsektora energii elektrycznej** (ang. Electricity Subsector Cybersecurity Capability Maturity Model, ES-C2M2)[93], opracowany w ramach partnerstwa publiczno-prywatnego, mógłby zostać zaadaptowany do warunków europejskich.Rola ES-C2M2 polega na dostarczeniu mechanizmu pozwalającego organizacjom szacować, ustalać priorytety oraz poprawiać zdolności w zakresie cyberbezpieczeństwa. Model ten określa wytyczne dotyczące zarówno aspektów IT, jak i OT oraz środowisk, w jakich te zasoby funkcjonują. Mimo, iż nie ma on zastosowania regulacyjnego, stanowi narzędzie komplementujące istniejące zestawy programów cyberbezpieczeństwa. Z kolei, implementacja sektorowych standardów dla elektroenergetyki leży w gestii Północnoamerykańskiej Rady ds. Niezawodności w Elektroenergetyce (ang. North American Electric Reliability Corporation, NERC). Wprowadzono dotychczas obowiązkowy zestaw standardów odporności i bezpieczeństwa skierowany do użytkowników, operatorów i właścicieli sieci elektroenergetycznych[94].

14. Przyszły przegląd dyrektywy NIS (przewidziany w Artykule 23) mógłby stanowić przyczynek do objęcia dyrektywą odnawialnych źródeł energii. Zgodnie z unijną dyrektywą w sprawie odnawialnych źródeł energii[95] poziom energii z OZE musi osiągnąć 20% całkowitego zużycia energii w UE do 2020 roku, oraz 27% do 2030 roku. Poszczególne państwa członkowskie ustaliły krajowe cele w zakresie wykorzystania OZE do 2020 roku na poziomie wahającym się od 10% (Malta) do 49% (Szwecja). Podobnie jak w przypadku innych źródeł energii, OZE są w dużym stopniu zależne od przemysłowych systemów sterowania i są narażone na cyberataki, a ich udział w ogólnym „miksie" energetycznym stale rośnie.

92 Energy Expert Cybersecurity Report (2017), Cyber Security in the Energy Sector, op. cit.
93 Energy.Gov (2017), The Electricity Subsector Cybersecurity Capability Maturity Model, [online] https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity
94 North America Electric Reliability Corporation (2017), Standards, [online] http://www.nerc.com/pa/Stand/Pages/default.aspx
95 European Commission, Renewable energy. Moving towards a low carbon economy [online] https://ec.europa.eu/energy/en/topics/renewable-energy

Cyberbezpieczeństwo sektora energetycznego – Ramy cyberbezpieczeństwa NIST w kontekście działań Unii Europejskiej

Kaja Ciglic – Director, Government Cybersecurity Policy and Strategy, Microsoft

Ilość ataków[1] hakerskich ukierunkowanych na sektor energetyczny rośnie lawinowo. Ze względu na znaczący wpływ jaki ten sektor wywiera na inne infrastruktury krytyczne oraz ponadnarodowy charakter, energetyka jest wyjątkowo podatna na naruszenia bezpieczeństwa. Ataki nie są wyłącznie dziełem przestępców. Coraz częściej stoją za nimi obce państwa, które wykorzystują energetykę, a w szczególności sieci przesyłowo-rozdzielcze jako narzędzie nacisku w potyczkach w cyberprzestrzeni. Na politycznie motywowany charakter incydentu wskazała analiza działań, których celem w czerwcu 2017 roku były amerykańskie przedsiębiorstwa sektora energetycznego[2]. Powyższy incydent przyspieszył apel o podjęcie działań mających na celu rewizję amerykańskiej polityki cyberbezpieczeństwa w sektorze energetycznym[3].

Raport Zespołu Reagowania na Incydenty Komputerowe w obszarze Przemysłowych Systemów Sterujących ICS CERT)[4] ujawnia, że systemy energetyczne Stanów Zjednoczonych stanowią drugi co do popularności cel zgłaszanych ataków komputerowych. Jednakże, podobnie jak w wypadku innych branż, można przyjąć, że liczba zdarzeń zgłaszanych przez firmy energetyczne to tylko wierzchołek góry lodowej.

By zapewnić ochronę sobie, a biorąc pod uwagę krytyczne znaczenie tego sektora – także krajom, w których działają, przedsiębiorstwa energetyczne muszą przyjmować odpowiednie

1 National Institute of Standards and Technology (NIST), Cybersecurity framework [online] https://www.nist.gov/cyberframework.

2 Nakashima E. (2017), U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks, [online] https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.ed0175142e22.

3 Energy, Senat (2017), Cantwell: Cybersecurity is Energy Security. Senator Cantwell Continues Drumbeat on Energy Cybersecurity: Equates Energy Cybersecurity with Energy Security, [online] https://www.energy.senate.gov/public/index.cfm/democratic-news?ID=4A5A8A54-8213-429D-9365-3D68EA11AC92.

4 The Industrial Control Systems Cyber Emergency Response Team (2017), Year in review [online] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

podejście do obszaru bezpieczeństwa cybernetycznego umożliwiające im ograniczanie cyberzagrożeń. Filary tego podejścia powinny obejmować wypracowanie sprawnych i skutecznych strategii zarządzania ryzykiem, przyjmowanie dobrych praktyk w zakresie bezpieczeństwa cybernetycznego oraz wzajemną wymianę informacji o zagrożeniach, incydentach i przeciwdziałaniach[5].

Atak cybernetyczny na ukraiński system elektroenergetyczny, który miał miejsce 23 grudnia 2015 roku, jest uznawany za pierwszy znany skuteczny cyberatak na sieci elektryczne. Hakerom udało się skutecznie włamać do systemów komputerowych trzech ukraińskich przedsiębiorstw dystrybucyjnych i czasowo zakłócić dostawy energii elektrycznej do odbiorców.
Atak cybernetyczny był przemyślny i składał się z następujących etapów:

- wcześniejszego przełamania zabezpieczeń sieci zakładowych z wykorzystaniem wiadomości email typu „spear phishing" zawierających złośliwe oprogramowanie BlackEnergy;
- przejęcia kontroli nad systemem SCADA i zdalnego odłączania podstacji energetycznych;
- blokowania/niszczenia elementów infrastruktury;
- zniszczenia plików przechowywanych na serwerach i stacjach roboczych złośliwym oprogramowaniem KillDisk;
- ataku typu denial-of-service blokującego działanie centrum obsługi telefonicznej, pozbawiającego odbiorców energii aktualnych informacji o sytuacji.

W Unii Europejskiej na główne ramy prawne w obszarze cyberbezpieczeństwa składają się wchodzące w życie w maju 2018 roku dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych (NIS)[6] oraz ogólne rozporządzenie w sprawie ochrony danych osobowych (GDPR)[7]. Dyrektywa NIS nakłada na operatorów infrastruktury krytycznej obowiązek podjęcia odpowiednich działań mających na celu przeciwdziałanie zagrożeniom bezpieczeństwa oraz obowiązek zgłaszania incydentów naruszeń bezpieczeństwa właściwym organom krajowym. W odniesieniu do sektora energetyki zakresem obejmuje podsektory energii elektrycznej, ropy naftowej i gazu.

W Stanach Zjednoczonych elementem centralnym są Ramy Bezpieczeństwa Cybernetycznego[8] podlegające obecnie przeglądowi wprowadzone Dekretem Prezydenckim 13636, o którym mowa poniżej. Niniejszy rozdział jest poświęcony w szczególności wprowadzaniu efektywnych

5 ENISA (2016), *Report on cyber security information sharing in the energy sector*, [online]: https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector.
6 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, dostępne: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148.
7 Rozporządzenie PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
8 NIST, Cybersecurity Framework [online] : https://www.nist.gov/cyberframework.

strategii zarządzania ryzykiem poprzez wprowadzenie skutecznych zabezpieczeń minimalnych. Przedstawia także Ramy Bezpieczeństwa Cybernetycznego (zwane dalej Ramami) opracowane przez amerykański Krajowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology) jako dobrą praktykę, która mogłaby służyć Unii Europejskiej jako narzędzie wdrażania rozwiązań cyberbezpieczeństwa i ochrony danych osobowych oraz zostać przyjęta przez sektor energetyki w Polsce.

Istotność działań w skali międzynarodowej

Sieci energetyczne są ze sobą połączone, naruszenie ich bezpieczeństwa może wywrzeć efekt kaskadowy na inne sektory gospodarki. Problemy jednego operatora czy państwa członkowskiego nie są ograniczone wyłącznie do niego, ale mogą mieć skutki transgraniczne. W cyberbezpieczeństwie obowiązuje zasada najsłabszego ogniwa, czyli o odporności systemów wzajemnie połączonych decyduje ich najsłabszy element. Nie ma już czegoś takiego, jak zagrożenie wyłącznie krajowe. Dlatego też wykorzystanie dobrych praktyk międzynarodowych przyniesie korzyści wszystkim zaangażowanym interesariuszom. W uzasadnieniu dyrektywy NIS, Komisja Europejska wskazała, że „pomimo podjętych inicjatyw państwa członkowskie mają bardzo różne poziomy zdolności i gotowości, co prowadzi do fragmentacji podejścia w całej UE. Ze względu na fakt, iż systemy i sieci są wzajemnie połączone, ogólny poziom bezpieczeństwa sieci i informacji w UE jest obniżony przez państwa członkowskie nieposiadające odpowiedniego poziomu ochrony. (…) W rezultacie współpraca ma miejsce jedynie w przypadku będących w mniejszości państw członkowskich posiadających wysoki poziom zdolności.[9]"

Takim środkiem budowania zaufania mogą być zasady minimalnego bezpieczeństwa, o których mowa poniżej. Stosowanie globalnie komplementarnych zasad zapewnia, że odpowiednie siły i środki są przeznaczane na efektywne zarządzanie bezpieczeństwem i zagrożeniami a nie tylko na osiąganie zgodności prawnej. W wypadku dobrych praktyk, wykorzystywanie wypróbowanych i sprawdzających się metod daje państwom bardzo cenny punkt wyjścia i szybsze rezultaty, co pomaga w zwiększaniu poziomu bezpieczeństwa i stwarza możliwości uczenia się od siebie nawzajem i wymieniania wiedzą przez administracje publiczne wielu krajów. Rezultat powyższego ulega powieleniu w skali całego systemu, ponieważ również dostawcy zewnętrzni są w stanie przeznaczać stosowne siły i środki na zarządzanie bezpieczeństwem i zagrożeniami. Powoduje to, że organizacje dalej inwestują w innowacje w zakresie zabezpieczeń, ponieważ mają pewność, że stosowane polityki gwarantują wystarczający zakres swobody na tworzenie nowych technik, zdolności i architektur obronnych. Ostatecznie podejście to zapewnia, że organizacje w dalszym ciągu inwestują w zasoby, których skuteczność wzrasta dzięki sprzęganiu ich ponad granicami, utrzymując globalny ekosystem innowacji, produkcji i kooperacji, który nie tylko przyczynił się do zwiększenia w skali świata możliwości ekonomicznych, ale także spowodował spadek kosztów rozwoju i popularyzacji zaawansowanych technologii.

9 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148, *op.cit.*

Istotą działań podejmowanych na poziomie UE jest właśnie wyrównywanie różnic pomiędzy państwami członkowskimi celem wprowadzenia wspólnego, porównywalnego poziomu bezpieczeństwa sieci i informacji. Na poziomie międzynarodowym UE prowadzi działania zarówno w ramach kontaktów dwustronnych jak i wielostronnych. Podczas szczytu UE-USA w 2010 roku została powołana grupa robocza UE-USA ds. bezpieczeństwa cybernetycznego i cyberprzestępczości. W pracach grupy ekspertów powołanych przez Komisję Europejską celem przedstawienia propozycji przyszłych działań w obszarze cyberbezpieczeństwa sektora energetycznego uczestniczy również przedstawiciel NIST.

Na czym polegają zabezpieczenia minimalne?[10]

Minimalne wymagane zabezpieczenia to zbiór wyjściowych polityk, rezultatów, działań, praktyk i metod kontroli mających pomóc w zarządzaniu incydentami cybernetycznymi. Z założenia obejmują one szeroką gamę celów polityk zarządzania ryzykiem, takich jak ochrona przed atakami cybernetycznymi czy wykrywanie i reagowanie na incydenty. Mogą one także obejmować bardziej konkretne pożądane wyniki (np. znajomość zagrożeń organizacyjnych), działania czy praktyki z zakresu bezpieczeństwa (np. przeprowadzanie oceny ryzyk, dokumentowanie, weryfikację i upowszechnianie rezultatów; a także regularne uaktualnianie oceny), oraz mechanizmy kontroli bezpieczeństwa[11]. Określenie zabezpieczeń minimalnych jest szczególnie użyteczne przy zwiększaniu poziomu bezpieczeństwa cybernetycznego, ponieważ może obejmować szerokie gamy ryzyk, które typowo występują w bardzo różnych środowiskach. W większości zagrożenia, na które są narażone administracja publiczna i przedsiębiorstwa, są podobne, więc także i większość „minimów" – zasadniczych działań w obszarze zarządzania ryzykami oraz ich ograniczanie będzie podobna. Dotyczy to w jeszcze większym stopniu konkretnych branż, przedsiębiorstwa w nich działające na ogół są narażone na takie same zagrożenia.

Jednakże, mimo że minima bezpieczeństwa rozwiązują znaczącą część zagrożeń występujących w organizacjach, mogą także występować scenariusze zagrożeń specyficznych dla konkretnych funkcji biznesowych w ramach przedsiębiorstwa czy dla różnych sektorów. W związku z tym, minima bezpieczeństwa dotyczące wielu różnych branż mogą wymagać uzupełniania o wąskie zbiory wytycznych mających na celu ograniczanie zagrożeń dotyczących poszczególnych funkcji biznesowych czy konkretnych branż.

Zrewidowana w 2017 roku strategia cyberbezpieczeństwa Unii Europejskiej wskazuje, że sektory gospodarki musza sprostać właściwym dla danego sektora specyficznym wyzwaniom. Ogólne strategie cyberbezpieczeństwa wspierane powinny być zatem przez strategie sektorowe[12]. Na zasadność opracowania przeznaczonej dla sektora energetyki strategii wskazują

10 Microsoft: Aligning security baselines to protect critical infrastructure.

11 Mechanizmy kontroli bezpieczeństwa są rezultatem wdrożenia działań zabezpieczających.

12 Komisja Europejska (2017), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN, available at: https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe.

Jakie są skuteczne zabezpieczenia minimalne?

W ramach zabezpieczeń minimalnych na ogół stosuje się następujące dobre praktyki obejmujące:

- Wykorzystywanie zróżnicowanej wiedzy poprzez korzystanie z otwartego, opartego na współpracy i iteracyjnego procesu tworzenia polityki publicznej, angażującego różnorodnych interesariuszy;
- Ułatwianie podejmowania decyzji poprzez ujednolicenie rozumienia, czym jest zarządzanie ryzykiem, zarówno wewnątrz organizacji, jak i między różnymi organizacjami;
- Skuteczne zarządzanie ryzykiem poprzez zbiór spriorytetyzowanych praktyk minimalnych opartych na ryzyku;
- Umożliwianie innowacji poprzez dążenie do pożądanych rezultatów zabezpieczeń, a nie narzucanie wymaganych sposobów zabezpieczania;
- Przyśpieszanie postępów dzięki korzystaniu z dobrych praktyk;
- Wspieranie rozwoju gospodarczego realizowaniem korzyści płynących ze sprawnych zabezpieczeń.

rekomendacje grupy ekspertów powołanych przez Komisję Europejską celem przedstawienia propozycji przyszłych działań w obszarze cyberbezpieczeństwa sektora energetycznego[13]. Mając na uwadze nierównomierny poziom dojrzałości infrastruktury energetycznej w UE jak również jej krytyczny charakter rekomenduje się **również stworzenie europejskich ram dojrzałości** cybernetycznej jako przykład podając opracowany przez amerykański Departament Energii model ES – C2M2 (dla podsektora elektryczności) oraz ONG – C2M2 (dla podsektora gazu naturalnego i ropy) opisany bardziej szczegółowo poniżej. Zanim jednak będzie możliwe przedstawienie szczegółowego rozwiązania dla sektora energetycznego analiza skupi się na przedstawieniu ogólnych ram cyberbezpieczeństwa NIST.

Ramy bezpieczeństwa cybernetycznego NIST

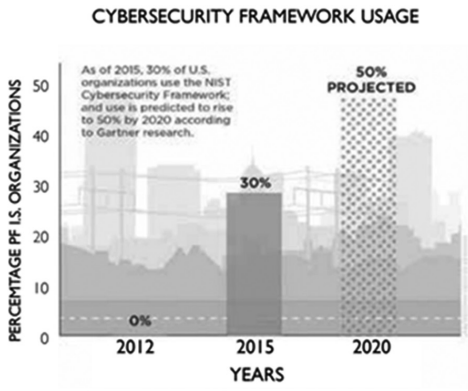
Jak już wspomniano powyżej, Ramy są **przykładem określenia minimów bezpieczeństwa**, których skuteczność została potwierdzona. Z badania przeprowadzonego wśród amerykańskich specjalistów IT i cyberbezpieczeństwa wynika, że Ramy postrzegane są jako rzeczywiście najlepsza praktyka, wymagana zarówno przez partnerów biznesowych jak i administrację federalną.

13 Energy Expert Cyber Security Platform (EECSP), Cyber Security in the Energy Sector, Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, [online] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf.

Rysunek nr 1. Motywacja do przyjęcia Ram. Źródło: Dimensional Research (2017), Trends in security framework adoption a survey of IT and security professionals [online]

Początkiem Ram NIST był Dekret Prezydencki (EO) numer 13636 w sprawie poprawy cyberbezpieczeństwa infrastruktury krytycznej[14] wydany 12 lutego 2014 roku. Jednocześnie zostało opublikowane rozporządzenie prezydenckie nr 21 – Bezpieczeństwo i odporność infrastruktury krytycznej. Obie inicjatywy zmierzają do zwiększenia odporności amerykańskiej infrastruktury krytycznej. Jednym z głównych elementów EO było stworzenie Ram Bezpieczeństwa Cybernetycznego przez NIST tak, aby wspomóc wysiłki dostawców i właścicieli infrastruktury krytycznej w redukcji i zarządzaniu ryzykiem cybernetycznym. Ramy dostarczają spójny zestaw standardów, metodologii, procedur i procesów do zarządzania cyberbezpieczeństwem. Będące wynikiem wspólnych wysiłków sektora publicznego i prywatnego. Ramy są owocem wytężonej pracy i przez cały czas są rozwijane i aktualizowane w ścisłej współpracy pomiędzy rządem i przemysłem. W styczniu 2017 roku zapoczątkowano proces rewizji Ram, który zakończyć ma się w 2018 roku przedstawieniem nowej, zaktualizowanej wersji. Podkreślić również należy, że rolą samych Ram nie jest nie jest jedynie rozwijanie standardów, ale przede wszystkim pełnienie roli facylitatora dyskusji zbliżającej ekspertów akademickich, sektora

Rysunek nr 2. Wykorzystanie ram NIST przez amerykańskie przedsiębiorstwa. Źródło: US Chamber of Commerce (2017), Transatlantic cybersecurity. Forging a united response to universal threats.



14 Whitehouse (2013), Executive Order – Improving Critical Infrastructure Cybersecurity [online] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

prywatnego oraz innych interesariuszy tak, aby osiągnąć porozumienie zainicjowane i wspierane przez przemysł. Co ważne, Stany Zjednoczone nie są jedynym krajem, który wdraża Ramy. Jak wskazano poniżej stosowany jest przez 30% przedsiębiorstw w Stanach Zjednoczonych, oczekuje się, że do roku 2020 ten odsetek wzrośnie do 50%[15].

Ponadto, obserwowany jest wzrost zainteresowania Ramami zarówno ze strony organizacji międzynarodowych, jak i rządów. W odniesieniu do kontekstu międzynarodowego dyskutuje się nad sposobami ujednolicenia strategii cyberbezpieczeństwa tak aby lepiej zwalczać zagrożenia transgraniczne, a także sprostać wymaganiom rozbieżnych, niespójnych polityk. Podkreśla się również potrzebę globalnej harmonizacji oraz ujednolicenia ram cyberbezpieczeństwa. W Unii Europejskiej w 2015 roku rząd Włoch przyjął nowe ramy bezpieczeństwa cybernetycznego oparte na NIST. Włochy dostosowały Ramy do specyfiki swojego sektora wytwarzania opartego na małych i średnich przedsiębiorstwach.[16]

Włoskie ramy cyberbezpieczeństwa

We Włoszech w 2015 roku we współpracy z sektorem prywatnym oraz akademickim przyjęto Framework Nazionale di Cyber Security. W dużej mierze wzorowany jest na Ramach NIST, które kładą nacisk na ochronę infrastruktury krytycznej, międzynarodową harmonizację, współpracę publiczno-prywatną oraz zdolność adaptacji. Jako uzasadnienie wyboru Ram NIST wskazano konieczność wprowadzenia harmonizacji rozwiązań cyberbezpieczeństwa na poziomie globalnym, a nie tylko na poziomie krajowym.

Źródło: Cyber inteligence and Information Security Centre (2015), Italian Cybersecurity Report. A national cybersecurity framework

Podobnie, od 2015 roku Australia zachęca swoich przedsiębiorców do wykorzystania Ram do oszacowania i ograniczenia zagrażających im ryzyk cybernetycznych lub do inwentaryzacji stosowanych przez nich praktyk zarządzania cyberryzykiem. Zdaniem rządu, zalety Ram to ich skalowalność i możliwość budowania odporności cybernetycznej przedsiębiorstw na jej podstawie w sposób proporcjonalny.[17] Ramy wykorzystywane są również przez organizacje w Wielkiej Brytanii, Kanadzie, Izraelu oraz Malezji[18], a więc w krajach o najwyższym poziomie przygotowania cybernetycznego. Przyjmowanie się na świecie Ram najprawdopodobniej będzie postępowało. Niedawno wydany Dekret Prezydencki (EO) na temat Bezpieczeństwa Cybernetycznego[19] nakłada obowiązek stosowania Ram Bezpieczeństwa Cybernetycznego przez wszystkie agendy rządu USA. Odnotować należy fakt, że niektóre rządy mogą odnosić się

15 US Chamber of Commerce (2017), Transatlantic Cybersecurity. Forging a united response to universal threats [online] https://www.uschamber.com/TransatlanticCybersecurityReport.

16 Cyber inteligence and Information Security Centre (2015), Italian Cybersecurity Report. A national cybersecurity framework [online] http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf.

17 ASIC (2015), Cyber resilience; Health check [online] http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.

18 NIST (2017), Cybersecurity Framework Workshop 2017 Summary. What we heard and next steps.

19 White House (2017), Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [online] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

jednak sceptycznie do międzynarodowej promocji Ram co stanowi formę zarówno politycznego jak i kulturowego oporu przed stosowaniem rozwiązań czysto amerykańskich. Te obawy zwiększyły się jeszcze po wprowadzenie nakazu stosowania Ram przez rząd federalny na mocy Dekretu Prezydenckiego 13800. Część rządów może być zatem bardziej skłonna do stosowania standardów organizacji międzynarodowych niż tych rozwijanych przez NIST[20]. Warto podkreślić, że Ramy już obejmują normy: CIS Critical Security Controls[21], Control Objectives for Information and Related Technology (COBIT)[22], ISA/IEC-62443 oraz ISO/IEC 27001:2013[23] i NIST SP 800-53 Rev.4[24].

Ramy Bezpieczeństwa Cybernetycznego NIST: Struktura

Ramy Bezpieczeństwa Cybernetycznego NIST oparto na istniejących normach, wytycznych oraz praktykach i zaprojektowano tak, by różne organizacje mogły je wykorzystywać do oceny swoich zagrożeń dla działalności, a następnie wdrażać je w sposób ekonomiczny. Składają się z trzech części:

1. **Szkielet ram:** Szkielet jest zbiorem działań i stosownych informacyjnych źródeł odniesienia, (czyli norm) podzielonych na pięć funkcji: Rozpoznanie, Ochrona, Wykrywanie, Reagowanie i Odbudowa. Szkielet wskazuje jak organizacje powinny podchodzić do swoich praktyk w obszarze bezpieczeństwa cybernetycznego w zakresie: 1) określania swoich najbardziej krytycznych zasobów, 2) wdrażania procedur ich ochrony, 3) uwzględniania zasobów niezbędnych do rozpoznawania potencjalnych naruszeń bezpieczeństwa, 4) utrzymywania procedur reagowania na naruszenia, oraz 5) tworzenia procedury umożliwiającej im odbudowanie się po ataku.

2. **Profil Ram:** Profil zapewnia metodę wspomagającą organizacje w zgrywaniu działań w zakresie bezpieczeństwa cybernetycznego z wymaganiami ich zasadniczej działalności, najlepszymi praktykami branżowymi, zakresem tolerancji ryzyka i zasobami oraz w jasnym wyartykułowaniu celów programu ochrony bezpieczeństwa cybernetycznego. Umożliwia także ustalenie pożądanych rezultatów ochrony cybernetycznej oraz luk występujących w aktualnych procedurach z tego obszaru.

20 NIST (2017), Cybersecurity Framework Workshop 2017 Summary. What we heard and next steps [online] https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf.
21 CIS Controls [online] https://www.cisecurity.org/critical-controls/.
22 ISACA (2017), http://www.isaca.org/cobit/pages/default.aspx.
23 ISO (2013) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements [online] http://www.iso.org/iso/catalogue_detail?csnumber=54534.
24 [online] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.

3. **Warstwy Wdrażania Ram:** opisują stopień zaawansowania stosowania w organizacji praktyk z obszaru bezpieczeństwa cybernetycznego. Rozróżnia się cztery poziomy klasyfikujące podejście do zarządzania ryzykiem ataków cybernetycznych, od poziomu „nieformalnego" do „adaptacyjnego"[25]:

Przyczyny szerokiego upowszechniania się Ram Bezpieczeństwa Cybernetycznego NIST

Istnieje szereg powodów, dla których Ramy Bezpieczeństwa Cybernetycznego NIST zyskały dużą popularność wśród profesjonalistów z dziedziny zarządzania ryzykami dla bezpieczeństwa cybernetycznego. Najważniejsze z nich to między innymi:

1. **Ramy tworzą wspólny język**. W wytycznych zarządzania ryzykiem konsekwentnie podkreśla się istotność komunikowania się w organizacjach, zarówno w poziomie, jak i w pionie. Jednakże bezpieczeństwo cybernetyczne jest zagadnieniem względnie nowym i „technicznym" dla wielu kierowników, dyrektorów i zarządów firm, więc z trudem im idą próby angażowania w temat całych organizacji. Do rozwiązania tego problemu niezbędne jest wprowadzenie wspólnego dla wszystkich osób i organizacji języka – wspólnego rozumienia, określania i używania różnych terminów i koncepcji.

   Ramy Bezpieczeństwa Cybernetycznego NIST zapewniają to poprzez wykorzystanie powszechnie zrozumiałych funkcji (tzn. rozpoznanie, ochronę, wykrywanie, reagowanie i odtwarzanie), a także rozlicznych kategorii i podkategorii. Pojedynczy dokument pokazujący powiązania pomiędzy zarówno konkretnymi, jak i ogólnymi wytycznymi jest zrozumiały dla specjalistów oraz kierownictwa – działa jak tłumacz między tymi grupami. Docelowo takie odwzorowanie umożliwi wszystkim zainteresowanym grupom prowadzenie opartego na konkretach i sensownego dialogu na temat usprawniania działania organizacji w ramach poszczególnych funkcji lub pomiędzy nimi.

2. **W Ramach zastosowano podejście oparte na ryzyk**. Organizacje stosujące podejście oparte na ryzyku wykorzystują wykonywane przez siebie oceny ryzyka do podejmowania decyzji o tym, jak podchodzić do ryzyk oraz inwestować w zabezpieczenia. W szczególności podejście oparte na ryzyku, takie jak zarysowane w Ramach Bezpieczeństwa Cybernetycznego NIST, uwzględnia występujący w organizacji krajobraz szczególnych podatności (np. jej wyrobów,

25 Warstwa 1 (nieformalnie): organizacja podchodzi do bezpieczeństwa cybernetycznego na zasadach doraźnych. Ma minimalną świadomość zagrożeń cybernetycznych dla organizacji. Warstwa 2 (ze świadomością ryzyka): organizacja ma politykę zarządzania ryzykiem dla bezpieczeństwa cybernetycznego i prowadzi aktualnie działania mające na celu opracowanie celów zarządzania tym ryzykiem i zrozumienie zagrożeń, jakie niesie ono dla organizacji. Warstwa 3 (powtarzalnie): organizacja działa zgodnie z formalnymi procedurami dotyczącymi bezpieczeństwa cybernetycznego, które regularnie aktualizuje, dysponuje dobrze przeszkolonym personelem i rozumie współzależności oraz otoczenie swoich partnerów biznesowych. Warstwa 4 (adaptacyjnie): dostosowuje swoje praktyki w obszarze bezpieczeństwa cybernetycznego na bieżąco w oparciu o zachodzące zdarzenia i wskaźniki predykcyjne tworzone na podstawie poprzednich i aktualnych działań w tym obszarze.

usług i środowiska działania), szczególnych zagrożeń (np. atakujący usiłujący uzyskać dostęp do środowiska organizacji lub zakłócić jego funkcjonowanie) oraz potencjalne konsekwencje skutecznego zaatakowania podatności przez napastników.

Zabezpieczenia minimalne oparte na ryzyku umożliwiają organizacjom wdrażanie podejścia do bezpieczeństwa opartego na ryzyku i podejmowanie decyzji inwestycyjnych najlepiej przystających do ich profili ryzyka i priorytetów gospodarczych. Różne sektory gospodarki i organizacje o różnych wielkościach mogą korzystać na innym inwestowaniu swoich zasobów ochronnych. W ten sposób minimum ochrony opartej na ryzyku daje organizacjom elastyczność w podejmowaniu decyzji o postępowaniu z ryzykami i zwiększaniu lub zmniejszaniu inwestycji w ochronę w sposób przystający do ich profilów ryzyka.

3. **Ramy są nastawione na wyniki**. Oprócz oparcia na ryzyku i priorytetyzacji, Ramy Bezpieczeństwa Cybernetycznego NIST są nastawione na wyniki – kładą nacisk na to, do osiągania czego powinny dążyć organizacje (np. „kontrolowania dostępu logicznego do zasobów krytycznych") a nie na to *jak* organizacje powinny realizować zabezpieczenia (np. „wykorzystywać uwierzytelnianie dwuskładnikowe"). Minima bezpieczeństwa oparte na wynikach są niezbędne do zapewnienia, że przedsiębiorstwa będą mogły korzystać z najbardziej aktualnych wyrobów, usług i zabezpieczeń. W miarę jak przyśpieszają innowacje w dziedzinie teleinformatyki a zagrażający jej błyskawicznie unowocześniają techniki i strategie atakowania, przedsiębiorstwa także muszą mieć możliwości błyskawicznego wzmacniania obrony. Podobnie, by organizacje zajmujące się rozwiązaniami teleinformatycznymi i zabezpieczającymi mogły rozwijać i dostarczać coraz bezpieczniejsze rozwiązania, muszą mieć możliwość prowadzenia działalności badawczo-rozwojowej, innowacyjnej. Błyskawiczny postęp techniczny dodatkowo przyczynia się do potrzeby oparcia minimów zabezpieczeń na wynikach i to w sposób uniwersalny dla wielu branż. Minima zabezpieczeń oparte na wynikach dają organizacjom elastyczność we wdrażaniu zaleceń lub wytycznych sposobami, które uzupełniają tak zróżnicowane architektury.

Wdrażanie Ram Bezpieczeństwa Cybernetycznego NIST w sektorze energetyki

W styczniu 2015 roku Departament Energetyki USA wydał wytyczne wdrożeniowe[26] mające wspomóc sektor energetyki w tworzeniu lub dostosowaniu istniejących w nim programów ochrony przed zagrożeniami cybernetycznymi do celów Ram. Przy opracowywaniu wytycznych Departament Energetyki współpracował z interesariuszami z sektora prywatnego. Waga przykładana przez Stany Zjednoczone do stworzenia podstaw bezpieczeństwa dla sektora energetyki oraz wsparcie i wytyczne wdrażania tych podstaw pokazują jaką wagę do tego sektora przykłada rząd. Grupa ekspertów powołana przez Komisję Europejską celem

26 Energy. gov. (2015), Energy sector cybersecurity. Framework Implementation Framework [online] https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

przedstawienia rekomendacji przyszłych działań w obszarze cyberbezpieczeństwa w energetyce wskazała na model mierzenia dojrzałości sieci energetycznej (ES-C2M2) oraz dojrzałości sektora ropy i gazu (ONG-C2M2) jako narzędzia z jednej strony porównywania stopnia przygotowania państw członkowskich z drugiej strony modelu analitycznego wspomagającego proces podejmowania decyzji. Zastosowanie powyższych modeli odpowiada na wyzwania związane z wprowadzeniem porównywalnych zasad minimalnych celem wyeliminowania tzw. najsłabszego ogniwa oraz wdrożeniem nowych technologii oraz wykorzystaniem outsourcingu. Innym wyzwaniem jest wspomniana współzależność infrastruktur i efekt kaskadowości incydentów bezpieczeństwa. Modele dojrzałości ES – C2M2 i ONG – C2M2 składają się z podstawowego modelu C2M2 jak również wytycznych skierowanych dla podsektora elektroenergetycznego i odpowiednio ropy i gazu.

Amerykańskie podejście do ewaluacji dojrzałości sektora energetyki znalazło swoje odbicie w pracach Komisji Europejskiej, która wezwała europejskie przedsiębiorstwa do przyjęcia podobnego modelu wskazując na jego wysoki potencjał oraz możliwość dopasowania do potrzeb europejskich (zestaw narzędzi C2M2)[27].

Cytowane wytyczne mają pomóc sektorowi energetycznemu w:

- określeniu poziomu ich aktualnej i docelowej ochrony bezpieczeństwa cybernetycznego;
- rozpoznaniu luk w istniejących programach zarządzania ryzykiem cybernetycznym sektora, z wykorzystaniem Ram jako wytycznych oraz rozpoznaniu obszarów, w których obecnie stosowane praktyki mogą przekraczać wymagania nakładane przez Ramy;
- rozpoznaniu istniejących w sektorze narzędzi, norm i wytycznych, które mogą wspomóc wdrażanie Ram;
- zachęceniu interesariuszom wewnętrznym i zewnętrznym przyjęcia adekwatnych podejść do zarządzania ryzykiem oraz stosowania Ram.

W rozdziale 2 Wytycznych przedstawiono podstawową terminologię stosowaną w Ramach oraz koncepcje ich stosowania, zaś rozdział 3 wskazuje przykładowe zasoby mogące wspierać stosowanie Ram. W rozdziale 4 przedstawiono w ogólny zarys podejścia do wdrażania Ram, zaś rozdział 5 przedstawia przykład podejścia do wprowadzania Ram, związanego z konkretnym narzędziem. Wybranym do tego narzędziem jest Model Dojrzałości Zdolności w Zakresie Bezpieczeństwa Cybernetycznego (C2M2)[28], który został opracowany specjalnie dla sektora energetycznego. Istnieją także jeszcze bardziej przydatne modele dla Podsektora Energii Elektrycznej C2M2 (ES-C2M2)[29] oraz Podsektora Gazu Naturalnego i Ropy (ONG-C2M2)[30]

27 EECSP (2017), Cyber security in the energy sector. Recommendations for the European Commission on European Strategic Framework and potential future legislative acts for the energy sector [online] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf.

28 Energy.gov, Cybersecurity Capability Maturity Model (C2M2), [online[http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity.

29 Energy.gov, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.

30 Energy.gov, Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2), https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity.

będące wersjami branżowymi obejmującymi podstawowy C2M2 oraz dodatkowe materiały źródłowe i wytyczne wdrożeniowe specjalnie dostosowane do branży elektrycznej oraz gazu i ropy.

Jak zaznaczono w Wytycznych, proces wdrażania realizowany jest w sposób ustrukturyzowany i przewiduje ustawiczność i powtarzalność, pozwalającą organizacjom na rozpoznawanie i priorytetyzację możliwości wprowadzania usprawnień, a także informowania o tym, czego dowiedziały się o zagrożeniach cybernetycznych. Struktura procesu wdrożenia opiera się na następujących etapach:

1. Ustalić priorytety i zakresy działań w obszarze zarządzania ryzykami dla bezpieczeństwa cybernetycznego;
2. Zrozumieć interesariuszy wewnętrznych: utworzyć firmowy zespół ds. zarządzania ryzykiem bezpieczeństwa cybernetycznego i zapewnić mu poparcie kierownictwa;
3. Określić aktualny stan firmy, co pomoże w zrozumieniu wymagań na zarządzanie ryzykiem i występujących luk;
4. Określić stan docelowy poprzez ustalenie celów;
5. Przeprowadzić ocenę ryzyka by zrozumieć jak przejść od stanu obecnego do stanu docelowego;
6. Opracować i wdrożyć procesy zarządzania ryzykiem oraz dostosować stan firmy i jej strategię stosownie do potrzeb.

W opublikowanym we wrześniu 2017 roku rozporządzeniu w sprawie rewizji mandatu Agencji ENISA oraz systemu certyfikacji ICT ustanawia się europejskie ramy certyfikacji dla produktów i usług ICT oraz przyznaje Agencji ENISA rolę koordynującą w tym aspekcie. Propozycja wspiera i uzupełnia wdrożenie dyrektywy NIS poprzez stworzenie narzędzia wskazującego zgodność z wymaganiami dyrektywy NIS w całej UE. Przy wypracowywaniu nowego systemu certyfikacji KE oraz ENISA dołożą szczególnych starań, aby obowiązki wynikające z dyrektywy NIS zostały uwzględnione w opracowywanym systemie certyfikacji[31].

31 European Commission (2017), Proposal for a regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification [online] https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

Rekomendacje:

1. Model NIST powinien być zostać uznany przez właściwe organy krajowe jako narzędzie wdrożenia wymagań dyrektywy NIS. Włoski przykład stanowi w tym aspekcie rozwiązanie modelowe.

2. Zgodnie z przedstawioną we wrześniu 2017 roku propozycją KE, agencji ENISA zostanie nadany status europejskiego centrum certyfikacyjnego zostanie również wzmocniona rola agencji ENISA we wdrażaniu postanowień dyrektywy NIS. ENISA pełniąc rolę facylitatora mogłaby wspomagać państwa członkowskie w łączeniu różnych grup interesariuszy wykorzystując model współpracy NIST.

3. Zaangażowanie interesariuszy UE w trwający proces przedefiniowania Ram mogłoby przyczynić się do europeizacji czy też umiędzynarodowienia Ram jak również wzmocnienia aspektu Ram w obszarze ochrony danych osobowych na podstawie wchodzącego w życie w maju 2018 roku rozporządzenia GDPR.

4. Mając na uwadze rekomendacje powołanej przez Komisje Europejska grupy ekspertów ds. cyberbezpieczeństwa w sektorze energetycznym, jak również niejednolity poziom zaawansowania technologicznego państw członkowskich zastanowić się należy nad dostosowaniem do europejskich potrzeb grupy modeli C2M2.

5. Zainaugurowany w 2011 roku dialog UE-USA na temat cyberbezpieczeństwa mógłby służyć wymianie doświadczeń na podstawie wdrożeń dyrektywy NIS i rozporządzenia GDPR. Mandat forum mógłby zostać poszerzony tak, aby uwzględniać udział Grupy Roboczej Artykułu 29, agencji ENISA i szerokiego spektrum interesariuszy[32].

32 US Chamber of Commerce (2017), op.cit.

Podejście kompleksowe do budowy kultury cyberbezpieczeństwa operatorów infrastruktury krytycznej – działania w zakresie Cyber Industry

Izabela Lewandowska-Wiśniewska, PZU

Wstęp

Rosnąca popularność Internetu rzeczy, wchodzenie w wiek produkcyjny pokolenia wychowanego w erze cyfryzacji, automatyzacja procesów, nowe technologie przemysłowe powoduję, że ryzyko związane z zagrożeniami cybernetycznymi nabiera coraz większego znaczenia w kontekście bezpiecznego funkcjonowania przedsiębiorstw. Dyrektywa NIS nakłada na państwa członkowskie UE obowiązek wdrożenia przepisów, które pozwolą na zapewnienie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych. Spełnienie narzuconych przepisami standardów wymaga po stronie polskich przedsiębiorstw oraz instytucji odpowiedzialnych za bezpieczeństwo przejścia procesu transformacji w celu dostosowania procedur i norm do unijnych wymogów.

W szczególnej sytuacji są przedsiębiorstwa przemysłowe, ponieważ muszą chronić nie tylko swoją infrastrukturę IT ale również własne systemy sterowania (ICS). Cyberatak na obiekty przemysłowe może mieć katastrofalne skutki dla mienia, zdrowia i życia pracowników oraz dla otoczenia. Cyberryzyka nabierają jeszcze większego znaczenia u operatorów infrastruktury krytycznej, gdyż zakłócenie ich działalności może zachwiać funkcjonowaniem całego państwa, spowodować katastrofy przemysłowe czy stanowić wstęp do działań zbrojnych o charakterze cybernetycznych lub kinetycznym. Duża ilość zakładów przemysłowych i ich znaczenie gospodarcze czyni ten obszar szczególnie podatnym na ataki terrorystyczne, w tym przeprowadzane w cyberprzestrzeni.

Nowoczesne spojrzenie firmy ubezpieczeniowej na obszar cyberbezpieczeństwa – przykład PZU i PZU Lab

Temat cyberbezpieczeństwa jest dla ubezpieczycieli szczególnie istotny ze względu na pojawiające się nowe technologie i związane z nimi zagrożenia. Grupa PZU jako lider, nie tylko rodzimego rynku ubezpieczeń, ale także jako największa grupa finansowa w naszej części Europy, wychodzi naprzeciw potrzebom i oczekiwaniom klientów, dostarczając im zarówno kompleksowych produktów ubezpieczeniowych jak i szeroko rozumianego wsparcia w zarządzaniu ryzykiem cybernetycznym. W tym celu Grupa PZU powołała właśnie PZU Lab – nową,

samodzielną spółkę – córkę działającą w ramach Grupy PZU. Dla nowoczesnego i odpowiedzialnego ubezpieczyciela wzrastająca świadomość zagrożeń cybernetycznych, stwarza szansę na zbudowanie z klientami profesjonalnego partnerstwa, które zakłada wsparcie ich w zapewnieniu bezpieczeństwa cybernetycznego. Celem jest minimalizacja ryzyka cybernetycznego, a w konsekwencji zmniejszenie potencjalnych strat z tym związanych. Stanowi to istotny element z punktu widzenia ubezpieczyciela i dostosowania zakresu ochrony w cyberpolisach. Firmy ubezpieczeniowe powinny umiejętnie zarządzać ryzykiem i dostarczać swoim klientom najlepszych rozwiązań, budując w ten sposób przewagi konkurencyjne.

W tym aspekcie Grupa PZU zapewnia klientowi kompleksową ofertę. Z jednej strony poprzez optymalizację rozwiązań cyberbezpieczeństwa, opartych również na działaniach komercyjnych (w ramach PZU Lab), a z drugiej poprzez zaproponowanie nowoczesnej cyberpolisy dopasowanej do firmy (w ramach działalności PZU).

Oferta PZU Lab skierowana do dużych klientów przemysłowych, zawiera kompleksowe rozwiązania skrojone „na miarę", w tym produkty i usługi komercyjne. Wśród nich są audyty, ocena ryzyka, optymalizacja procesów związanych z bezpieczeństwem i zarządzaniem ryzykiem, szkolenia, doradztwo oraz inne działania w zakresie kompleksowego podejścia do obszaru cyberbezpieczeństwa. Działania te są uzupełnieniem całościowego podejścia do cyberzagrożeń oraz ochrony ubezpieczeniowej jaką dają cyberpolisy.

Większość ubezpieczycieli obecnych na polskim rynku oferuje wyłącznie proste rozwiązania na wypadek wycieku danych, konieczności poniesienia kosztów PR po cyberataku lub obsługi kosztów zatrudnienia ekspertów. Zauważalny jest brak kompleksowego podejścia firm ubezpieczeniowych do problemu zagrożeń cybernetycznych, które oprócz zapewnienia ochrony ubezpieczeniowej, nie prowadzą działań mających na celu budowanie kultury cyberbezpieczeństwa.

Budowanie kultury cyberbezpieczeństwa

Całościowe podejście do ochrony infrastruktury krytycznej jest konieczne, poczynając od budowania wśród klientów świadomości w zakresie cyberbezpieczeństwa, poprzez szkolenia, profesjonalny personel, dostarczanie wiedzy dotyczącej podatności danego przedsiębiorstwa na cyberzagrożenia, dokonanie analizy propozycji zabezpieczeń i rozwiązań, narzędzi do monitorowania, a kończąc na dopasowaniu odpowiedniej ochrony infrastruktury krytycznej w postaci cyberpolisy.

Działania PZU oraz spółki PZU Lab w zakresie cyberbezpieczeństwa opierają się na 4 obszarach:
- Działalności wewnętrznej badawczo-rozwojowej,
- Działalności komercyjnej – usługi oferowane przez PZU Lab,
- Działalności związanej z produktem – cyberpolisą,
- Wspieraniu innowacyjnych rozwiązań – Fundusz Witelo.

Cyberatak może być prowadzony z dowolnego miejsca na kuli ziemskiej, a cyberprzestępcy żyją w poczuciu bezkarności. Zagrożenie obiektów infrastruktury krytycznej cyberatakami mającymi podłoże ideologiczne (terrorystyczne) lub polityczne jest bardzo realne. Przygotowanie i przeprowadzenie ataku cybernetycznego pociąga za sobą duży niższy koszt w stosunku do wydatków wynikających z użycia „tradycyjnych" metod działania, takich jak np. sabotaż. Dlatego też obiekty infrastruktury krytycznej i ich znaczenie gospodarcze czyni ten obszar szczególnie podatny na ataki terrorystyczne, w tym także cyberataki.

Działania wewnętrzne – badawczo-rozwojowe *Cyber Industry*

PZU Lab prowadzi szereg działań mających zapewnić kompleksowe podejście do cyberbezpieczeństwa. Wspólnie z uznanymi w Polsce partnerami zewnętrznymi oraz uczelniami technicznymi uczestniczy w pracach w zakresie globalnego podejścia do cyberbezpieczeństwa w infrastrukturze krytycznej. Działania prowadzone są w zakresie analizy ryzyka cyberzagrożeń przeznaczonej dla odbiorców przemysłowych, narzędzi do wspierania polskich przedsiębiorstw w zarządzaniu cyberryzykiem w systemach ICS, dedykowanych programów szkoleniowych. Rozwiązania oferowane w tym zakresie będą jednym z istotnych elementów, które przyczynią się do zwiększania poziomu bezpieczeństwa infrastruktury krytycznej. Niestety, jeszcze niewiele mówi się o bezpieczeństwie systemów sterowania instalacjami przemysłowymi, gdzie konsekwencje nieautoryzowanego dostępu (ataku) mogą być znacznie bardziej poważne niż to ma miejsce w przypadku utraty danych. Obecnie trwają prace nad narzędziem do wspierania polskich przedsiębiorstw w zarządzaniu cyberryzykiem i tym samym zwiększania poziomu bezpieczeństwa ich funkcjonowania. Elementy Cyber Industry to:

- Informatyczny, ekspercki system audytowy do badania podatności na cyberataki systemów sterowania i odporności organizacji dla celów ubezpieczenia,
- System do monitorowania ryzyka cybernetycznego – *Watchdog*,
- Szkolenia w zakresie bezpieczeństwa cybernetycznego.

Analiza ryzyka przeprowadzana przez ekspertów ubezpieczyciela powinna obejmować analizę na wszystkich trzech polach działalności ubezpieczanego przedsiębiorstwa mających związek z cyberbezpieczeństwem:

1. Działalność organizacyjna;

2. Działalność operacyjna;

3. Działalność techniczna

Zaprojektowane narzędzia audytowe będą stosowane przez inżynierów ryzyka nie tylko w celu dostarczenia informacji do podjęcia decyzji ubezpieczeniowej, ale również w celu określenia podatności i sposobu minimalizacji ryzyka, ale także do stałego nadzoru instalacji przemysłowej.

Narzędzie audytowe obejmuje swoim zakresem następujące obszary :

- Organizacja (procedury, ryzyka, itp.),
- Polityka bezpieczeństwa,
- Kontrola dostępu,
- Zarządzanie profilem/kontem,
- Audyt i zakres odpowiedzialności,
- Ochrona komunikacji,
- Zarządzanie konfiguracją,
- Zachowanie ciągłości,
- Reagowanie na incydent,
- Ochrona informacji,
- Monitorowanie i ochrona przed złośliwym oprogramowaniem,
- Personel,
- Fizyczne środki bezpieczeństwa,
- Planowanie działań w zakresie bezpieczeństwa,
- Urządzenia mobilne /przenośne/bezprzewodowe,
- Ocena i zarządzanie ryzykiem,
- Integralnośc systemu,
- Ochrona systemu,
- Szkolenia,
- Definiowanie wejść do IT,
- Definiowanie wejść do OT,
- Punkt styku obszaru IT i OT (zagrożenia, problemy),
- Konsekwencje ingerencji w IT, OT, wielkość strat.

Rozwiązania związane ze szkoleniami oraz działaniami prewencyjnymi zostaną uzupełnione poprzez stworzenie *watchdog*, który w sposób ciągły będzie monitorował stan instalacji przemysłowej. W przypadku stwierdzenia naruszenia bezpieczeństwa pozwoli na bezpieczne jej odstawienie/zatrzymanie. W efekcie zastosowanie tego narzędzia pozwoli na minimalizację wysokości szkody, monitoring bezpieczeństwa cybernetycznego infrastruktury przemysłowej przedsiębiorstwa w czasie rzeczywistym oraz wykrywanie naruszeń mogących zakłócić realizowane procesy.

Szkolenia w zakresie bezpieczeństwa cybernetycznego

Statystyki w zakresie cyberincydentów wskazują, że najsłabszym ogniwem systemów bezpieczeństwa jest człowiek. Jego rola w bezpiecznym prowadzeniu działalności przez przedsiębiorstwa ma decydujące znaczenie. Błąd ludzki jest przyczyną około 80% wszystkich incydentów związanych z cyberbezpieczeństwem. Wystąpienie cyberincydentu może w swoich skutkach doprowadzić do awarii krytycznych systemów ze względu bezpieczeństwa lub doprowadzić do całkowitego przerwania działalności, w tym zatrzymania procesów przemysłowych.

Nie ulega wątpliwości, że ten błąd może być bardzo kosztowny i potencjalnie przyczynić się zagrożenia życia. Aby budować kulturę bezpieczeństwa niezbędna jest wiedza pracowników – nie tylko tych odpowiedzialnych za cyberbezpieczeństwo, ale wszystkich i na różnych szczeblach organizacji, którzy powinni mieć świadomość niebezpieczeństw i tego w jaki sposób postępować w celu zachowania bezpieczeństwa. Pracownicy bezpośrednio zaangażowani w bezpieczeństwo cybernetyczne w dziedzinie technologii informacyjnych i komunikacyjnych muszą posiadać wysokie kwalifikacje oraz niezbędne umiejętności do efektywnego zarządzania cyberzagrożeniami oraz kompetencje w zakresie wykrywania, zapobiegania i postępowania z incydentami.

W celu umożliwienia ochrony operatorom infrastruktury krytycznej oraz ich dostawcom PZU Lab we współpracy z partnerem merytorycznym Fundacją Bezpieczna Cyberprzestrzeń opracowało specjalne programy szkoleniowe obejmujące wszystkie szczeble zarządzania w organizacji jak

- Top Management (zarząd, kadra dyrektorska),
- Menedżerowie (kadra zarządzająca średniego szczebla – IT, OT),
- Specjaliści, Eksperci (kadra operacyjna IT, OT),
- Stanowiska funkcyjne (pełnomocnik ds. bezpieczeństwa informacji, pełnomocnik infrastruktury krytycznej, radca prawny itp.),
- Pracownicy pozostali.

Ścieżki rozwojowe dla poszczególnych poziomów dzielone są na dwa obszary IT, OT, dla których opracowywane zostały dodatkowe zagadnienia tematyczne oraz przeprowadzane szkolenia. Każda grupa docelowa ma przewidziany program szkoleniowy dostosowany do poziomu organizacji, potrzeb wynikających z poziomu stanowiska oraz wymagań kompetencyjnych dla personelu.

Szkolenia prowadzone są w cyklach kilku szkoleń oraz zakończone egzaminem sprawdzającym. Każdy z uczestników szkolenia zapewniony ma dostęp wymiany wiedzy do Platformy *Cert Games CTF*.

Drugim elementem ścieżki budowania kompetencji personelu na poziomie operacyjnym są szkolenia w formie cyberćwiczeń typu CTF (*Capture The Flag*) – *CERT Games CTF*. Są one przeprowadzane w trybie *online* i składają się na szereg zadań o różnym poziomie trudności. W każdym zadaniu uczestnicy muszą rozwiązać innego rodzaju problem, dokonać analizy danych i kodu lub odszukać kluczową informację. W następstwie wypełnienia zadania, ćwiczący odpowiadają na pytania kontrolne lub znajdują ukryte flagi. Różne zadania wymagają posiadania innego zestawu umiejętności – analizy sieci, zbierania informacji, analizy danych/logów czy inżynierii wstecznej. W odróżnieniu do typowych gier *CTF* zadania w ramach *CERT Games CTF* są opracowywane tak, by imitowały prawdziwe wyzwania związane z obsługą incydentów komputerowych. Uczestnicy mają nieograniczony dostęp do platformy. Tematyka obejmuje takie kwestie jak między innymi: ochrona infrastruktury technicznej, rozporządzenie

o ochronie danych osobowych (RODO), zarządzanie ciągłością działania, analizę ryzyka, ataki na infrastrukturę przemysłową oraz wiele innych ważnych aspektów. Szkolenia mają wywołać zmianę zachowania, powinny stymulować indywidualne zaangażowania w pracę – odpowiedzialne i bezpieczne oraz przyczyniać się do budowy środowiska pracy, którego bezpieczeństwo jest nieodłącznym elementem. W ramach szkolenia personel otrzymuje wiedzę, dzięki której może uczestniczyć w ochronie przed zagrożeniami charakterystycznymi dla środowisk IT oraz środowisk przemysłowych. Pozwoli to na lepsze zarządzanie najbardziej podatnym elementem jakim jest człowiek.

Audyty komercyjne

W ramach swojej działalności PZU Lab we współpracy z partnerem merytorycznym Fundacją Bezpieczna Cyberprzestrzeń realizuje usługi doradcze związane z podnoszeniem poziomu cyberbezpieczeństwa przedsiębiorstw i innych organizacji w postaci audytów bezpieczeństwa informatycznego w zakresie

- stopnia dojrzałości działania zespołu bezpieczeństwa IT w obszarze zarządzania incydentami bezpieczeństwa – audyt typu „analiza luki",
- stopnia dojrzałości działania komórki SOC (*Security Operations Centre*) zgodnie z metodyką SUOPT,
- stopnia wdrożenia RODO w organizacji,
- bezpieczeństwa styku sieci z siecią Internet, mający na celu dostarczenie pełnej i rzetelnej informacji o rzeczywistym poziomie bezpieczeństwa badanych urządzeń oraz wskazanie słabych punktów w zabezpieczeniach i architekturze bezpieczeństwa infrastruktury.

Audyt SIM3 poziomu dojrzałości zarządzania incydentami w organizacji
Metodyka SIM3 (*Security Incident Management Maturity Model*) jest narzędziem służącym do analizy poziomu dojrzałości organizacji w zakresie zarządzania incydentami cyberbezpieczeństwa. Audyt ten w szczególności dotyczy zespołów CSIRT/CERT. Zastosowanie tej metodyki pozwala na obiektywne sprawdzenie czy struktury odpowiedzialne za zarządzanie incydentami działają zgodnie z najlepszymi standardami i praktykami.

SIM3 mierzy poziom dojrzałości działania organizacji w 4 obszarach zarządzania incydentami: Organizacja, Ludzie, Narzędzia i Procesy. W każdym z nich zdefiniowano od 7 do 17 szczegółowych parametrów pozwalających na ocenę wskazanych aspektów danego obszaru w skali od 0 do 4. Szczegółowe kryteria parametrów umożliwiają określenie stanu dojrzałości zarządzania incydentami. Wyniki audytu prezentowane są w postaci wykresu radarowego oraz szczegółowego raportu prezentującego ocenę wszystkich parametrów wraz z opisem zdiagnozowanej sytuacji i zestawem rekomendacji służących do podniesienia poziomu dojrzałości. Dzięki temu powstaje zarówno poglądowy, jak i szczegółowy obraz sytuacji, który może być wykorzystany na różnym poziomie zarządzania organizacją.

Dzięki przeprowadzeniu audytu zgodnego z metodyką SIM3 audytowany podmiot uzyskuje wiedzę dotyczącą luki, która dzieli poziom jego dojrzałość od stanu wymaganego przy staraniu się o uzyskanie certyfikacji w *Trusted Introducer*.

Audyt stopnia dojrzałości i analiza luki działania komórki SOC (Security Operations Centre) zgodnie z metodyką SUOPT

Metodyka SUOPT służy badaniu stopnia dojrzałości komórek SOC w organizacjach. Stanowi ona rozwinięcie najpopularniejszych metodyk badania stopnia dojrzałości organizacji lub ich funkcji. W specjalnym zastosowaniu dla SOC opiera się na doświadczeniach wyżej opisanej metodyki SIM3. Metodyka SUOPT pozwala na ocenę funkcjonowania SOC w następujących obszarach: Strategia (S), Usługi i ich jakości (U), Organizacja i jej zasoby (O), Procesy i procedury (P) oraz narzędzia i Technologii (T).

Audyt za pomocą metodyki SUOPT jest ważnym krokiem, który pozwala na identyfikację kierunków dalszych działań zwiększających poziom kompetencji i efektywności komórki SOC. PZU Lab wspiera klientów w całym tym procesie, zarówno poprzez opracowanie brakujących dokumentów (od strategicznych po operacyjne), jak i wsparcie przy kontynuacji budowy SOC, dostawę rozwiązań SOC, a w dalszym etapie – outsourcingu (części) usług SOC.

Audyt stopnia wdrożenia Rozporządzenia „RODO" w organizacji

Audyt stopnia wdrożenia Rozporządzenia „RODO" w organizacji składa się z kilku kroków:

1. Identyfikacja interesariuszy oraz stworzenie zespołu projektowego.
   W pierwszym kroku następuje selekcja odpowiednich osób spośród kadr organizacji, które dysponują odpowiednimi uprawnieniami decyzyjnymi i informacjami (najczęściej będzie to zarząd, najwyższe kierownictwo, ABI – jeśli jest powołany, dział prawny, dział *compliance*, dział IT, działy biznesowe – zapewniające organizacji dochody).

   Konieczne jest wyłonienie zespołu projektowego do sprawnego przeprowadzenia organizacji przez proces implementacji RODO. Aby działać skutecznie zespół projektowy musi składać się z przedstawicieli wszystkich działów, które uczestniczą w przetwarzaniu danych osobowych i mieć umocowanie w najwyższym kierownictwie.

2. Podział pracy na etapy i fazy:

   a) Określenie zasad projektowych;

   b) Audyt wstępny i *data mapping*;

   c) Identyfikacja wymogów RODO w odniesieniu do zakresu przetwarzania danych osobowych przez organizację;

d) Analiza stanu prawnego;

e) Określenie dalszych działań:
   - stworzenia koniecznych dokumentów;
   - przeprowadzenia koniecznych zmian;
   - czasu wymaganego na realizację powyższych prac.

3. Najważniejsze obszary do zbadania.
   W etapie tym powinny zostać przygotowane do wdrożenia rekomendacje, czyli odpowiednie dokumenty wymagane przez RODO. Jednocześnie należy zaprojektować zmiany w procesach biznesowych, komunikacji, czy modyfikacje w systemach IT. Stworzony zostanie raport zawierający informacje na temat zidentyfikowanej sytuacji oraz zestaw rekomendacji wdrożeniowych.

Audyt APT (advanced persistent threat)
Ze względu na charakterystykę ataku, audyt APT organizacji rozłożony jest w dłuższym czasie celem symulacji realnego ataku APT. Wyodrębniono następujące fazy, podczas których organizacja jest testowana.

- Faza rekonesansu

Przeprowadzenie rekonesansu w celu profilowania audytowanej organizacji oraz jej pracowników. W tym celu wykorzystywane są wszelkiego rodzaju dostępne źródła informacji, pozwalające zidentyfikować „punkty wejścia" do infrastruktury organizacji, zarówno techniczne, jak i dotyczące personelu.

- Faza uzyskania dostępu

Przeprowadzenie serii ukierunkowanych ataków na organizację wykorzystując w głównej mierze ataki socjotechniczne. Wszystkie scenariusze ataku uzgadniane są z organizacją i wymagają każdorazowej akceptacji. Wektory ataku dobierane są w oparciu o informacje pozyskane w trakcie fazy rekonesansu.

- Faza obecności i podwyższania uprawnień

W przypadku udanej próby uzyskania dostępu do infrastruktury organizacji przeprowadzany jest *black boxowy* test penetracyjny celem symulacji rozpoznawania przez adwersarza infrastruktury od wewnątrz, wykrycia podatności i możliwości zwiększenia uprawnień w testowanych systemach.

Audyt bezpieczeństwa styku sieci organizacji z siecią Internet
Audyt bezpieczeństwa styku sieci organizacji z siecią Internet składa się z poniższych działań.

1. Audyt architektury bezpieczeństwa infrastruktury styku z Internetem (topologii punktu styku).

2. Audyt konfiguracji i ustawień urządzeń (w tym pod względem niezawodności, spójności konfiguracji i reguł).

3. Przegląd dokumentacji dotyczącej architektury bezpieczeństwa.

4. Analiza rozkładu ruchu i architektura rozwiązania w poszczególnych lokalizacjach.

5. Analiza sieciowych rozwiązań BCP (w tym podejścia do redundancji).

6. Testy penetracyjne zewnętrzne.

7. Analiza ryzyka dla zidentyfikowanych podatności.

8. Raport z audytu.

Dalsze kroki to wspólnie opracowany program działań zwiększających świadomość pracowników organizacji.

Ochrona cybernetyczna w ICS

Kompleksowe podejście do budowania kultury bezpieczeństwa cybernetycznego oraz zapewnienie cyberbezpieczeństwa to również elementy ochrony cybernetycznej obszarów zarówno IT i OT, głównym elementem o którym mówimy w zakresie infrastruktury krytycznej są systemy sterowania których elementami są m.in.: SCADA, DCS, HMI, PLC, RTU, IED, SIS, sensory, przekaźniki. Pełnią one istotną rolę tam, gdzie procesy są zautomatyzowane, a urządzenia zdalnie sterowane i monitorowane.

Podstawowa ochrona cybernetyczna ICS może być realizowana przy pomocy:

- segmentacji i separacji sieci,
- ochrony granic,
- modelu stref i połączeń,
- strefy zdemilitaryzowanej,
- zapory sieciowej,
- obrony w głąb.

Wyjątkowej ostrożności wymaga postępowanie z danymi krytycznymi i ich ochroną szczególnie w dobie powszechności zagrożeń terrorystycznych. Wynika to z potencjalnie wysokich szkód finansowych, możliwą utratą zaufania partnerów biznesowych oraz reputacji firmy. PZU Lab w ramach prowadzonej działalności świadczy usługi doradcze w zakresie optymalizacji rozwiązań oraz właściwego ich doboru.

Cyberpolisy

Temat cyberzagrożeń jest dla firm ubezpieczeniowych szczególnie ważny, ze względu na pojawiające się nowe technologie, zagrożenia oraz konieczność oferowania klientom skrojonych na miarę ubezpieczeń, w tym cyberpolis. PZU jako wiodąca firma ubezpieczeniowa w Polsce pracuje nad wprowadzeniem na rynek dedykowanych ubezpieczeń, które będą chroniły firmy przed skutkami ataku cyberprzestępców na ich krytyczną infrastrukturę, w tym instalacje przemysłowe. Firmy ubezpieczeniowe obserwują zwiększone zainteresowanie ochroną ubezpieczeniową, która zrekompensuje ewentualne szkody związane z utratą i koniecznością odtworzenia danych wrażliwych przedsiębiorstwa lub klientów. Obserwowane zainteresowanie potencjalnych odbiorców tego rodzaju ochrona wskazuje na potrzebę intensywnego rozwoju firm ubezpieczeniowych w tym kierunku. Rozwój nowych technologii i Internetu powoduje powstanie wielu nowych cyberryzyk niezależnie od branż i wielkości firm, nieznanych jeszcze w niedalekiej przeszłości. Skala skutków cyberataku może być różna: od utraty danych i ich przestępczej sprzedaży np. konkurencji, naruszenia wizerunku przedsiębiorstwa do zniszczeń w mieniu (pożar, wybuch, itp.) oraz ofiar w ludziach. Dlatego warto spojrzeć na problematykę cyberbezpieczeństwa kompleksowo i rozważyć transfer ryzyka do firmy ubezpieczeniowej.

Podsumowanie

Podejście kompleksowe PZU i PZU Lab do budowania kultury cyberbezpieczeństwa w organizacjach obejmuje wiele aspektów jakimi są: szkolenia, audyty, wymagania proceduralne, ochrona techniczna, ochrona fizyczna, projekty rozwojowe oraz wspieranie innowacyjnych projektów. Ochrona ubezpieczeniowa, jak również rozwiązania techniczne w tym zakresie w systemach ICS oraz opracowane metodyki dotyczące postępowania z ryzykiem, będą jednym z istotnych elementów rozwiązań „przemysłu 4.0". Umożliwiają one redukcję ryzyka systemów ICS związanego z zagrożeniami cybernetycznymi. System diagnostyczny stanowi ostatnią warstwę umożliwiającą wykrycie cyberataków jeśli przejdą one przez wszystkie inne warstwy ochrony.

Rynek polis ubezpieczeniowych od skutków i następstw cyberataku może przynieść pożądany skutek w postaci zwiększenia odporności na cyberatak instalacji przemysłowych i wzrostu poziomu cyberbezpieczeństwa. Transfer ryzyka cybernetycznego do firm ubezpieczeniowych pozwoli na kompensację strat związanych ze skutecznym atakiem cybernetycznym.

Budowa CERT-u PSE oraz podejmowane działania na rzecz budowy CERT-u sektorowego – wymagania dla zapewnienia cyberbezpieczeństwa.

Jarosław Sordyl, PSE

Początki funkcjonowania CERT-ów w organizacjach

O konieczności pojawienia się w strukturach organizacji takich zespołów jak CERT/CSIRT, odpowiedzialnych za reagowanie na incydenty komputerowe, przekonaliśmy się już w latach 80. ubiegłego wieku, kiedy to atak „robaka"1stworzonego przez Roberta Tappmana Morrisa – studenta MIT, spowodował poważne zainfekowanie dużej liczby komputerów na uczelniach w USA oraz na świecie. Był to sygnał, że tylko dzięki stałej współpracy w zakresie bezpieczeństwa IT organizacje będą w stanie szybko reagować na zagrożenia oraz wyprzedzać pewne działania atakujące te systemy.

Pierwszy z CERT-ów został powołany przez Agencję DARPA (ang. Defense Advanced Research Project Agency), na Uniwersytecie Carnegie Mellon w Pittsburgu. Tego typu model potwierdził swoją efektywność i sprawność działania, dlatego już w latach 90. w Europie powstały podobne rozwiązania. Początkowo głównym zadaniem CERT-ów/CSIRT-ów było reagowanie na wszelkie zdarzenia w systemach teleinformatycznych, a później – biorąc pod uwagę konieczność edukacji użytkowników – do zadań wprowadzono również działania z obszaru prewencji i szkolenia w celu podnoszenia kompetencjii poszerzania wiedzy. Obecnie zespoły CERT/CSIRT wykształciły sprecyzowany obszar kompetencyjny związany z reagowaniem na incydenty z obszaru bezpieczeństwa IT, przeciwdziałaniem oraz rozwiązywaniem incydentów, a przy ustalaniu źródła incydentu rekomendowaniem rozwiązań podnoszących stopień skuteczności zabezpieczeń w organizacji. Od początku swoich działań zespoły CERT/CSIRT ewoluowały, m.in. za sprawą pojawiających się nowych rozwiązań, które miały bezpośredni wpływ na stopień skomplikowania infrastruktury IT. Sprzyjały one budowie rozległych sieci, skomplikowanych w obsłudze i zarządzaniu, oraz pojawieniu się na scenie cyberprzestępców

1 Robak komputerowy – samoreplikujący się program komputerowy, podobny w swoim działaniu do wirusa komputerowego, rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym. W odróżnieniu do wirusa komputerowego robak nie potrzebuje nosiciela, czyli zwykle jakiegoś pliku wykonywalnego.

– osób lub grup osób, których celem było m.in. prowadzenie działalności cyberprzestępczej przynoszącej zyski finansowe. Dzisiejszy zespół CERT może dostarczać wielu usług i wsparcia w zakresie zapewnienia i utrzymania bezpieczeństwa w środowisku IT w organizacji. Do listy zadań CERT-u mogą wchodzić również takie usługi jak informatyka śledcza – niezbędna do zabezpieczenia i analizy dowodów cyfrowych oraz wskazania np. czy faktycznie doszło do incydentu, czy też mamy do czynienia z błędem np. programowym. Do takich usług możemy również zaliczyć analizę wsteczną (ang. reverse engineering), zapewniającą wiedzę na temat sposobu funkcjonowania programów atakujących oraz sposobów obrony.

Budowa i funkcjonowanie CERT-u w PSE S.A.

W maju i czerwcu 2017 r., w związku z pojawieniem się w sieci poważnego zagrożenia związanego z serią ataków złośliwego oprogramowania, zespoły ds. bezpieczeństwa we wszystkich organizacjach państwowych i biznesowych zostały postawione w stan najwyższej gotowości. W tym okresie odnotowano wiele ataków oprogramowania ransomware[2], m.in. „WannaCry", wykorzystującego jedną z podatności w systemach Microsoft (lukę w systemie można było załatać już w marcu br., kiedy to Microsoft opublikował *patch*)[3] oraz „NotPetya", którego zadaniem było wykasowanie danych z zaatakowanych systemów. Wszystkie te ataki miały na celu nie tylko wyrządzenie szkody materialnej i fizycznej organizacjom, ale były także wymierzone w indywidualnych użytkowników systemu IT.

Kolejnym zidentyfikowanym w ostatnim czasie zagrożeniem dla systemów współpracujących bądź nadzorujących urządzenia przemysłowe, które zostało opisane w raporcie firmy ESET oraz DRAGOS[4], jest szkodliwe oprogramowanie (ang. malware[5])o nazwie „Industroyer" lub też „Crash Override". Oprogramowanie to jest modułowym programem, który pozwala na dostosowanie poszczególnych jego elementów do przeprowadzenia ataku na dowolny system przemysłowy sterowany za pośrednictwem komputera. Jak wynika ze wstępnych analiz oraz prób ustalenia powiązań pomiędzy użyciem tego programu a innymi atakami, które miały dotychczas miejsce, okazuje się, że mógł być on użyty w 2016 roku na Ukrainie, gdzie wyłączeniu uległa podstacja energetyczna, powodując wyłączenie energii elektrycznej w obwodzie kijowskim. Analiza opublikowanego raportu przynosi kilka wniosków:

- system atakujący jest zaawansowanym narzędziem, którego użycie może mieć krytyczny wpływ na infrastrukturę przemysłową każdego kraju;
- wykorzystanie złośliwego oprogramowania na Ukrainie pokazuje częściowo skuteczność oraz możliwości atakujących i należy je traktować z cała powagą;
- jeżeli ktokolwiek nie rozpoczął starań o budowę systemu zabezpieczeń, izolowania i monitorowania zasobów kluczowych w swojej organizacji, może zostać

2 Oprogramowanie ransomware – rodzaj szkodliwego oprogramowania używanego w przestępczości internetowej, najczęściej do wymuszania okup za skradzione dane.
3 Patch – poprawka lub uaktualnienie do programu, przeznaczona do usunięcia pewnych problemów, błędów
4 A. Keeve, *ESET discovers dangerous malware designed to disrupt industrial control systems*, (w:)www.eset.com [data dostępu: 26.07.2017 r.]
5 Malware – różnego rodzaju szkodliwe oprogramowanie próbujące zainfekować komputer lub urządzenie mobilne.

zaatakowany w chwili, kiedy najmniej się tego spodziewa, a skutki ataku mogą mieć dla niego bardzo poważne konsekwencje.

Najnowsze, jak i wcześniejsze ataki z wykorzystaniem złośliwego oprogramowania dowodziły destrukcyjnych zamiarów atakujących oraz pośrednio wskazywały na obce rządy i służby motywowane politycznie, jako siły stojące za ich organizacją.

Analizując obecną sytuację cyberbezpieczeństwa systemów teleinformatycznych, jak również systemów komputerowych współpracujących z systemami przemysłowymi, w PSE S.A. od dawna doceniano skalę potencjalnych zagrożeń dla bezpieczeństwa energetycznego Polski. Jedynym rozwiązaniem, jakie uznano za kompleksowe i odpowiadające poziomowi zagrożeń, było powołanie zespołu operacyjnego reagowania na incydenty w systemie IT – SOC[6] oraz zespołu reagowania na incydenty komputerowe – CERT[7]. Oba te zespoły są odpowiedzią na zagrożenia oraz stanowią centrum kompetencyjno-operacyjne, którego celem jest m.in:

- wykonywanie zadań zespołu reagowania na incydenty komputerowe (ang. Computer Emergency Response Team) – CERT PSE;
- prowadzenie laboratorium bezpieczeństwa teleinformatycznego;
- opiniowanie i weryfikacja nowych rozwiązań teleinformatycznych pod względem spełniania wymogów bezpieczeństwa;
- współpraca z departamentem teleinformatyki w zakresie wspólnego budowania odporności i reagowania na cyberzagrożenia;
- zarządzanie systemami bezpieczeństwa teleinformatycznego wspierającymi działalność SOC PSE;
- współpraca z Narodowym Centrum Cyberbezpieczeństwa (NCCyber) oraz innymi instytucjami krajowymi i międzynarodowymi w zakresie budowania odporności sektora elektroenergetycznego na zagrożenia płynące z cyberprzestrzeni.

Realizacja powyższych zadań jest wynikiem identyfikacji potrzeb organizacji, których celem jest zapewnienie dostępu do usług wzmacniających bezpieczeństwo, podnoszących odporność systemów na bieżące i zmieniające się zagrożenia modułowe czy też hybrydowe, a także zwiększających świadomość użytkowników końcowych na temat potencjalnych zagrożeń pochodzących z sieci.

Oprócz standardowej realizacji zadań, w wyniku analizy bieżących potrzeb dostępu do aktualnych informacji na temat podatności, zagrożeń oraz rozwiązań zabezpieczających systemy IT/OT, w CERT PSE zdecydowano się na podjęcie działań zmierzających do nawiązania szerokiej współpracy z CERT-ami w Europie. Konsekwencją tego było przystąpienie do organizacji „Trusted Introducer"[8] i rozpoczęcie procesu akredytacji, który zakończył się w czerwcu 2017 r. uzyskaniem statusu jednostki akredytowanej. Ponadto zwrócono uwagę

6 https://exatel.pl/cyberbezpieczenstwo/security-operations-center/.
7 http://cert.pse-online.pl/cert-4/.
8 https://www.trusted-introducer.org/.

na wartość dodaną współpracy z krajami spoza Europy, gdzie wykształciły się tak profesjonalne ośrodki jak ICS CERT US[9] – będący centrum kompetencyjno-operacyjnym w dziedzinie bezpieczeństwa rozwiązań przemysłowych w Stanach Zjednoczonych. Dodatkowym obszarem zainteresowania ze strony CERT-u PSE są stowarzyszenia i projekty, których celem jest promowanie współpracy zmierzającej do znacznego ograniczenia działalności cyberprzestępców oraz dzielenia się najlepszymi praktykami w obszarze bezpieczeństwa IT. Obecnie CERT PSE jest członkiem projektu założonego przez jednostkę EC3 Europolu pod nazwą „No More Ransom"[10].

Warto w tym miejscu przywołać Dyrektywę NIS[11] w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE, która zakłada budowę systemowego rozwiązania dla CERT-ów poprzez określenie ich kompetencji i podział m.in. na CERT-y krajowe oraz sektorowe, o czym mowa w artykule 9. przywołanego dokumentu. Oprócz formalnych podstaw, które dzięki tej dyrektywie zostały wyznaczone, na poziomie krajowym może dojść do właściwego umiejscowienia kompetencji w zakresie reprezentowania poszczególnych sektorów w gospodarce. Jednocześnie może to wpłynąć na „uproszczenie" kanałów przekazywania informacji, a przez to uzyskanie większej sprawności w zakresie jej wymiany. Biorąc pod uwagę powyższe regulacje oraz doświadczenia innych krajów dotyczące budowy sprawnego i funkcjonalnego systemu obiegu informacji oraz ujednolicania podejścia do cyberbezpieczeństwa, w CERT PSE podjęto decyzję o nawiązaniu współpracy dot. wymiany informacji oraz budowy wzajemnego systemu wymiany dobrych praktyk. Do tej współpracy zaproszono obecnie Kraft CERT – energetyczny CERT sektorowy z Norwegii, z którym podpisano umowę o współpracy. Nawiązano również kontakt z CERT-em austriackim, którego zakres kompetencji obejmuje sektor energetyczny. Nie bez znaczenia jest również współpraca z centrami zapewniającymi wymianę informacji oraz ich analizę. Tego typu współpraca w przypadku CERT PSE jest ukierunkowana na dostęp do bieżących informacji o rozwiązaniach, jakie stosują producenci oprogramowania, czy też sprzętu, który jest wykorzystywany w środowisku produkcyjnym. Tyczy się ona również dostępu do bieżących informacji dotyczących wysoko wyspecjalizowanego obszaru, jakim jest automatyka przemysłowa, a ich bezpośrednie wykorzystanie odbywa się poprzez dystrybucję wiedzy do właściwych jednostek w organizacji odpowiadających za bezpieczeństwo tego obszaru.

Bardzo ważnym elementem funkcjonowania każdego CERT-u, zwłaszcza umiejscowionego w jednorodnej organizacji, jest stworzenie odpowiedniego programu szkoleniowego i jego systematyczna realizacja, zapewniająca odpowiedni poziom kompetencji wśród wszystkich pracowników. Z doświadczenia CERT-u PSE wynika, iż tego typu działanie jest niezbędne, aby

9 https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

10 European Cybercrime Centre – EC3, jednostka działająca w ramach Europolu, została powołana w 2013 r. w celu zacieśnienia współpracy między europejskimi organami ścigania w walce z zagrożeniami w cyberprzestrzeni, tj. wyłudzeniami przez zorganizowane grupy przestępcze, pedofilią oraz atakami na infrastrukturę krytyczną i systemy informatyczne.

11 http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013AE1414.

każdy z pracowników był wyposażony w specjalistyczną wiedzę z zakresu specyfiki wykonywanych przez niego zadań. Oprócz standardowych szkoleń, w których każdy z pracowników obowiązkowo musi uczestniczyć, wdrożono system szkoleń/spotkań informacyjnych, których zadaniem jest dostarczenie wiedzy o aktualnych zagrożeniach oraz jak się przed nimi ustrzec. Przykładowo, podczas szkoleń zadbano o dostarczenie informacji o bezpiecznym sposobie korzystania z sieci bezprzewodowych podczas wakacji, będąc z dala od organizacji. Poprzez zwiększanie świadomości pracowników o zagrożeniach w sieci oraz edukowaniu ich w kwestii zasad bezpieczeństwa przechowywania swoich prywatnych danych, CERT zmniejsza również ryzyko ataku na organizację przez zainfekowane złośliwym oprogramowaniem urządzenie pracownika PSE S.A.

Wykorzystanie standardów w działalności CERT-u

Na realizację nałożonych na CERT zadań wynikających z dobrych praktyk, zaleceń, czy też wewnętrznych regulacji, składa się wiele elementów. Najważniejszym z nich jest odpowiednia kadra, a następnie dostępne narzędzia do pracy, systemy wspierające m.in. obsługę incydentów i reagowanie na bieżące zgłoszenia oraz dostęp do szeroko rozumianej informacji, w tym zaufanych kanałów współpracy. Nie bez znaczenia jest umiejscowienie CERT-u w organizacji w taki sposób, aby był jednostką niezależną od innych jednostek wewnętrznych tak, aby mógł swobodnie realizować swoje zadania i egzekwować realizację wymagań związanych z bezpieczeństwem teleinformatycznym. Kolejnym elementem jest odpowiedni system szkolenia dla zespołu CERT, który musi na bieżąco monitorować najnowsze „trendy" w obszarze cyberzagrożeń.

Wszystkie elementy składające się na organizację pracy oraz realizację usług, do jakich CERT jest zobligowany, można odnaleźć w wytycznych, czy też zaleceniach do wdrożenia w takim zespole. Jednym z takich dokumentów na poziomie europejskim jest publikacja organizacji ENISA – „Etapowe podejście do założenia zespołu CSIRT"[12]. W tym dokumencie opisano plany oraz wytyczne do zainicjowania takiego zespołu, jakim jest CERT/CSIRT oraz wyznaczenia obszarów jego funkcjonowania w organizacji. Znajdziemy w nim również informacje zalecające tryb postępowania od momentu powzięcia planu o ustanowieniu takiej komórki zarządzającej incydentami bezpieczeństwa do wdrożenia jej w operacyjne funkcjonowanie w organizacji. Oprócz ustanowienia samego CERT-u należy również zadbać o możliwość realizacji zadań, m.in. poprzez opracowanie stosownych procedur, np. na wypadek incydentu, a także organizację sposobu realizacji poszczególnych zadań, podział obowiązków, czy określenie celu. Powyższe kroki możemy zaplanować w oparciu o najlepsze praktyki dostarczane przez komitet ISO/IEC. Norma dotycząca zarządzania incydentami ISO/IEC 27035 „Zarządzanie incydentami w systemach teleinformatycznych"[13], pozwala na sprawne opracowanie planów działania na taką ewentualność. W budowie CERT PSE z uwagi na szczególne uwarunkowania operacyjne wykorzystuje się dodatkowo

12 https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-polish.
13 https://www.iso.org/standard/60803.html.

wiedzę z obszarów bezpieczeństwa automatyki przemysłowej, która jest dostarczana m.in. przez NIST (National Institute of Standards and Technology)[14]oraz ICS-CERT US. Mając na uwadze ostatnie ataki na infrastrukturę energetyczną na Ukrainie w 2015 i 2016 r., w środowisku, gdzie istnieje styk systemów IT z OT (automatyki przemysłowej), szczególnie należy zwracać uwagę na bieżące trendy w zabezpieczeniach i zagrożeniach. Akumulacja i wykorzystanie wiedzy, dostarczanej przez obie instytucje jest praktycznie obligatoryjna. Nie bez znaczenia dla całego systemu prac CERT-u są bieżące informacje na temat bezpieczeństwa, organizacji i rozwoju systemów zabezpieczających, pojawiających się nowych rozwiązań IT oraz systemów wspierających pracę CERT-u, która z dnia na dzień staje się coraz bardziej złożona i wymaga elastycznego podejścia w nadawaniu odpowiednich priorytetów.

E-CERT – konsolidacja bezpieczeństwa IT obszaru energetyki

Zespół CERT PSE funkcjonuje w bardzo specyficznym środowisku operatora sieci elektroenergetycznych, którego usługi są kluczowe dla całego państwa. Wiąże się z tym dodatkowo odpowiedzialność za sprawność i bezpieczeństwo funkcjonowania całego systemu, na który składają się również systemy IT oraz OT nadzorowane poprzez sieci IT. Dlatego CERT PSE podejmuje bieżące działania, których celem jest utrzymanie odpowiedniego poziomu bezpieczeństwa dla nadzorowanych systemów, na co składa się m.in. tworzenie szerokiej grupy współpracujących podmiotów z sektora energetycznego. W ramach tworzenia te grupy w marcu 2017 r. CERT PSE podpisał umowę o współpracy z CERT Energa. Współpraca między tymi dwoma CERT-ami ma na celu przekazywanie informacji o zagrożeniach i podatnościach, które mogą stanowić zagrożenie dla każdej z organizacji. Podpisana umowa przewiduje wymianę doświadczeń zespołów oraz utworzenie zaufanego kanału wymiany informacji, co w przypadku CERT-u jest jednym z kluczowych elementów odnoszących się do wiarygodności uzyskiwanych danych. Ta inicjatywa w krótkim okresie czasu pokazała, że był to krok we właściwym kierunku. Na bazie tych doświadczeń podjęto dalsze działania zmierzające do podpisania podobnych porozumień z pozostałymi operatorami, wytwórcami oraz dystrybutorami z sektora energetycznego.

Filarem każdej z umów jest wymiana informacji o zagrożeniach, podatnościach oraz dystrybucja informacji mogących mieć znaczenie dla bezpieczeństwa organizacji i wpływających bezpośrednio na wzrost jego poziomu. Do tego należy dodać zaufany system wymiany takich informacji oraz centrum kompetencyjno-zarządzające, przetwarzające i analizujące informacje o zagrożeniach oraz dystrybuujące je w sposób szybki i efektywny do właściwych organizacji w sektorze. Już teraz możemy wskazać, iż zaprojektowaliśmy funkcjonalne podwaliny E-CERT-u. Sprawdziły się one w działaniu w czasie ataku z wykorzystaniem oprogramowania typu ransomware: „WannaCry" i „Notpetya", czy też w związku z zagrożeniem, jakie dla systemów przemysłowych stanowią ataki z użyciem „Industroyer/Crash Override". Przekazanie informacji pomiędzy CERT-em PSE a partnerami z sektora następowało szybko

14 https://www.nist.gov/.

i efektywnie, bezpośrednio po otrzymaniu i potwierdzeniu tego typu informacji z innych zaufanych źródeł zewnętrznych. Dodatkowo należy podkreślić, iż zgromadzone dane zostały przekazane CERT-owi krajowemu – NCCyber oraz CERT-owi rządowemu w celu udostępnienia innym podmiotom, które mogłyby wykorzystać te informacje do podjęcia działań wyprzedzających, uniemożliwiających skuteczne zaatakowanie ich struktur IT. Wydaje się, że właśnie w taki sposób potwierdzono zasadność funkcjonowania jednego punktu kontaktowego dla całego sektora energetycznego, który skupia kanały informacyjne z poszczególnych organizacji. Pozwala to dodatkowo na ujednolicenie, zweryfikowanie i ocenę wiarygodności informacji, których źródła oraz pochodzenie mogą być różne. To z kolei jest ważnym elementem podejmowania dalszych działań w zakresie bezpieczeństwa. Postępowanie takie jest zalecane m.in. przez organizację NIST w jednym z opublikowanych poradników dot. przekazywania informacji o zagrożeniach. Podkreśla się w nim, iż wiarygodna informacja, przekazywana w sposób efektywny innym podmiotom, stanowi klucz do sukcesu w zwalczaniu różnego rodzaju zagrożeń[15].

Powstanie E-CERT-u będzie elementem realizacji strategicznych planów zwiększających bezpieczeństwo nie tylko sektora energetycznego, ale także całego państwa. Za umiejscowieniem takiej niezależnej, specjalistycznej i analitycznej komórki organizacyjnej odpowiedzialnej za bezpieczeństwo systemów sektora energetycznego w CERT PSE przemawia dodatkowo państwowy i pozabiznesowy charakter krajowego operatora sieci przesyłowej, a przez to brak „negatywnego" wpływu na współpracujące organizacje w sektorze. Taki model wprost przekłada się na niezależne i obiektywne funkcjonowanie komórki reagowania na incydenty komputerowe.

Podsumowanie

Powołanie tak ważnej dla bezpieczeństwa teleinformatycznego organizacji jednostki, jaką jest CERT, wymaga dogłębnej analizy bieżących potrzeb, stanu zagrożenia i ryzyka dla organizacji, a także możliwości utrzymania skuteczności działania takiej struktury. Nie bez znaczenia jest ogólne poparcie zarządu i kierownictwa organizacji dla takiego rozwiązania, gdyż wiąże się ono z wieloma zmianami na poziomie podejścia organizacji do zarządzania bezpieczeństwem i incydentami. Wszystkie obszary powiązane z taką jednostką muszą być poddane przeglądowi/audytowi. Należy ustanowić procedury i polityki bezpieczeństwa, aby CERT był w stanie podjąć realną i skuteczną działalność. Jak już wcześniej wspomniano, bardzo ważną kwestią jest umiejscowienie CERT-u w strukturze organizacji. Pozwala to na realne wpływanie na bezpieczeństwo, ciągłe jego podnoszenie do poziomu określonego polityką organizacji, a także sprawne działanie w przypadku wystąpienia incydentu. Pamiętać należy o odpowiednim doborze osób do zespołu, w skład którego powinni wchodzić eksperci w dziedzinie bezpieczeństwa z uwzględnieniem wielu obszarów specjalizacji np. informatyka śledcza, inżynieria wsteczna oraz bezpieczeństwo automatyki

15 NIST Special Publication 800-150 – Guide to Cyber Threat Information Sharing.

przemysłowej. Zespół ten powinien uczestniczyć w bieżącej wymianie informacji nie tylko wewnątrz organizacji, ale poprzez udział w stowarzyszeniach dedykowanych CERT-om, zapewnić sobie dostęp do aktualnej wiedzy oraz dzielić się własnymi doświadczeniami z innymi CERT-ami w kraju i za granicą, co przyczyni się do podniesienia kompetencji zespołu. Takie podejście realizuje CERT PSE, który ze względu na swoje umiejscowienie organizacyjne i sektorowe odgrywa szczególną rolę w tworzeniu systemu bezpieczeństwa Polski oraz podejmowaniu działań na wypadek wystąpienia incydentów.

Zmiana paradygmatu walki z rosnącym zagrożeniem cybernetycznym dla infrastruktury krytycznej

Yitzhak (Itzik) Vager – Verint
Leonid Rozenblum – Cyber Security, Israel Electric Co.

Rosnące zagrożenie cybernetyczne dla infrastruktury krytycznej

W ciągu ostatnich kilku lat infrastruktura krytyczna stała się głównym celem sprawców ataków cybernetycznych: od rządowych najemników, przez politycznych haktywistów i cyberprzestępców, po doskonale zorganizowane cybergangi uzbrojone w ransomware szukające łatwego zarobku w wirtualnym świecie. Bez względu na motywacje, sposoby działania i cele, mamy zatem do czynienia ze zjawiskiem, które zrewolucjonizowało środowisko bezpieczeństwa operatorów usług kluczowych dla funkcjonowania współczesnego społeczeństwa i gospodarki. Światowe Forum Ekonomiczne definiuje systemowe zagrożenie cybernetyczne [1] jako ryzyko zdarzenia cybernetycznego lub innego szkodliwego zdarzenia w elemencie ekosystemu infrastruktury krytycznej, powodującego znaczące opóźnienia, przerwy w dostawie, awarie, zaburzenia lub straty nie tylko w tym elemencie, lecz również w powiązanych (logicznie lub geograficznie) ekosystemach.

Nawet nie w pełni udany atak na infrastrukturę krytyczną może być druzgocący i spowodować ogromne straty pieniężne, środowiskowe i społeczne. Atak na ukraińską sieć energetyczną w latach 2015-2016, w wyniku którego dziesiątki tysięcy osób zostało pozbawionych prądu, doskonale zobrazował potencjalne skutki choćby „miejscowego" zdarzenia. Atak ten był skomplikowaną, dopracowaną w najmniejszych szczegółach operacją oraz pociągał za sobą konsekwencje również w świecie fizycznym. Podjęła go grupa wyjątkowo utalentowanych hakerów, którzy poświęcili wiele miesięcy planując swój napad: zaczęli od rozpoznania sieci energetycznych i danych ich operatorów, by na końcu przeprowadzić wyćwiczoną, skoordynowaną ofensywę. Według wielu analityków zdarzenie na Ukrainie było tylko próbą przed prawdziwym atakiem.

1 Światowe Forum Ekonomiczne – publikacja „Zrozumieć systemowe zagrożenia cybernetyczne".

W maju tego roku ransomware o nazwie *Wannacry* dało się we znaki brytyjskiej służbie zdrowia. Mimo że *Wannacry* nie był wymierzony konkretnie w infrastrukturę krytyczną, to zmusił 40 zainfekowanych szpitali do odwołania operacji i wizyt, przekierowania karetek, żądając okupu za przywrócenie dostępu do niezbędnych danych medycznych.

Dobrze zorganizowany cyberatak na wiele celów jednocześnie mógłby sparaliżować cały region lub nawet kraj. Hipotetyczny, jednoczesny atak na sieć energetyczną, telekomunikacyjną i transportową oraz infrastrukturę szpitalną skutecznie zaburzyłby – a może i całkowicie zatrzymał – możliwość reakcji ze strony napadniętego kraju. Skutki ataku byłyby odczuwane jeszcze przez całe lata lub dziesięciolecia. Obejmowałyby straty w ludziach i szkody finansowe, a także wpłynęłyby na gospodarkę, społeczeństwo i politykę.

W coraz bardziej złożonym świecie uniwersalne rozwiązania w kwestii cyberbezpieczeństwa nie sprostają wyzwaniom bezpieczeństwa współczesnej infrastruktury krytycznej. Cyberprzestępcy mają wiele czasu i duży wybór. Do zrealizowania swojego celu, muszą odnaleźć tylko jeden słaby punkt (podatność). Mogą na przykład skupić się na podatności zauważonej w konkretnym urządzeniu (DCS, PLC czy HMI) lub za pomocą ataku typu DDoS uderzyć w systemy dostępne przez sieć. W końcu – wykorzystując wiedzę o ICS, OT, dobrze udokumentowanych procesach i cyberbezpieczeństwie, mogą przypuścić skomplikowany, długotrwały atak o potencjalnie katastroficznych skutkach. Bezpieczeństwo infrastruktury krytycznej, takiej jak sieć energetyczna, paliwowa, gazociągowa czy transportowa, od dawna sprowadza się do „krycia się w cieniu" lub liczeniu na to, że tzw. szczelina powietrzna (o niej w dalszej części artykułu) powstrzyma intruzów. Lecz czas pokazał, że chowanie się nie pozwoli zminimalizować nadchodzących zagrożeń. Obrona w głąb (ang. *defense in depth*) od dawna jest uznawana za

Atak na Aramco w 2012 roku

Saudi Aramco to jeden z największych na świecie koncernów paliwowych.

Pierwszy etap cyberataku rozpoczął się w lipcu. Odbył się po cichu i obejmował:

- Włamanie do kilku firmowych komputerów Aramco,
- Zainstalowanie złośliwego oprogramowania,
- Automatyczne rozesłanie rzeczonego oprogramowania do wszystkich podłączonych do sieci informatycznej komputerów z systemem Windows.

Drugi etap cyberataku miał miejsce w sierpniu i został przeprowadzony błyskawicznie.

- W ciągu zaledwie kilku godzin oprogramowanie zniszczyło część lub całość danych na 35 tys. komputerów. Firma straciła możliwość zapłaty kontrahentom. Cysterny przyjeżdżające po paliwo odsyłane były z niczym. Znienacka możliwość obsługi 10% światowego rynku paliwowego przez tego potentata naftowego została zagrożona.
- Pięć miesięcy później, po wymianie sieci komputerowej na bezpieczniejszą i rozszerzeniu zespołu ds. cyberbezpieczeństwa, system Saudi Aramco ruszył na nowo.

najlepszą strategię ochrony infrastruktury krytycznej. Jest to całościowa metoda polegająca na łączeniu sieci informatycznych i ICS w warstwy, przedzielonymi dla ochrony i izolacji zaporami ogniowymi, diodami danych i innymi rozwiązaniami cybernetycznymi. Sieci, protokoły i punkty końcowe na każdej warstwie również są chronione. Całość składa się na potężną, wielowarstwową linię obrony.

O ile wprowadzenie modeli bezpieczeństwa IT pozwoliło znacznie złagodzić presję na sieci firmowe, o tyle nie miało to znacznego wpływu na sieci ICS. Powodem tego są różnice technologiczne (komputery stacjonarne i ethernet z jednej strony, a SCADA, PLCS, DCS, itd. z drugiej), a także znacząco różne priorytety. Cyberbezpieczeństwo w wymiarze IT co do zasady polega przede wszystkim na ochronie poufności danych, dopiero na następnym etapie odnosi się do ich integralności i dostępności. Natomiast ochrona infrastruktury krytycznej skupia się przede wszystkim na bezpieczeństwie i integralności.

Dlaczego zabezpieczanie infrastruktury krytycznej jest takie trudne?

Zadaniem kadry ds. bezpieczeństwa jest ochrona różnorodnych rodzajów organizacji oraz zakładów produkcyjnych – od fabryk przez rafinerie i platformy wiertnicze po elektrownie. Zakłady takie są zazwyczaj rozproszone w terenie i nierzadko znajdują się w nieprzystępnym otoczeniu. Liczba urządzeń podłączonych do sieci ICS i ich rodzajów stale się zwiększa – a każde urządzenie to potencjalna droga obejścia zabezpieczeń. Systemy kontroli muszą więc chronić firmę przed zagrożeniami zarówno od wewnątrz, jak i z zewnątrz. Muszą też być odizolowane

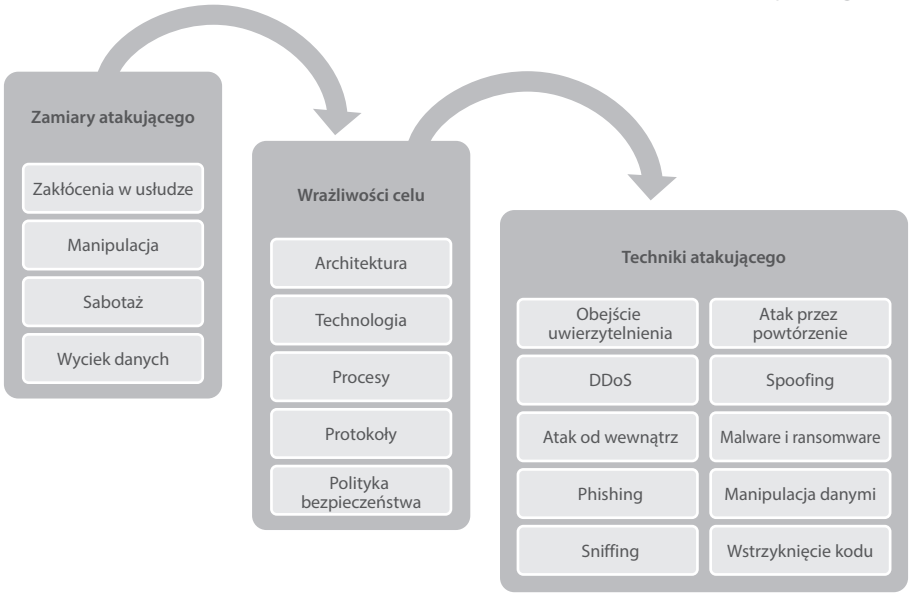
Metody ataku na infrastrukturę krytyczną

- Zainfekowanie programów ICS złośliwym oprogramowaniem.
- Blokowanie danych lub przekazywanie operatorowi systemu niepełnych bądź fałszywych informacji w celu ukrycia rozwoju sytuacji albo zmuszenia go do podjęcia niewłaściwych działań.
- Nieuprawnione zmiany w progach alarmowych bądź całkowite ich usunięcie.
- Ingerencja w działanie sprzętu w zakładzie, skutkujące zmianami w ustawieniach bezpieczeństwa.
- Blokowanie lub opóźnianie przepływu informacji przez sieci ICS, skutkujące zaburzeniami w pracy ICS.
- Nieuprawnione zmiany w poleceniach zaprogramowanych w miejscowych procesorach w celu przejęcia kontroli nad zależnościami typu master-slave pomiędzy terminalami nadrzędnymi (ang. MTU, master terminal unit) a terminalami rozprowadzającymi (ang. FTU, feeder terminal unit)
- Zmiana oprogramowania lub ustawień ICS.
- Przeciążanie kadry jednoczesnymi awariami w wielu systemach.

od innych sieci, a punkty dostępu należy chronić i stale monitorować. Środowiska operacyjne często wymagają zmodyfikowania sprzętu i interfejsu kontrolnego tak, aby były zgodne z normami przemysłowymi i najlepszymi praktykami. Z kolei centra operacji bezpieczeństwa (SOC) na bieżąco monitorują działalność systemów w celu wykrycia anomalii wskazujących na cyberatak. Dodatkowym wyzwaniem jest fakt, że wiele sprzętu informatycznego działa na dawno już nieaktualizowanych systemach operacyjnych – panele operatorskie oparte na Windows XP to nierzadki widok. Podsumowując, najważniejszym zagadnieniem jest bezpieczeństwo i integralność, tj. należy sprawić, żeby mechanizmy bezawaryjne faktycznie takie były a skutki awarii nie przenosiły się na inne elementy łańcucha i nie wywołały dalszych szkód.

Cele atakujących mogą być różne, od przerwania usługi, przez sabotaż, po wyciek danych. Potencjalne podatności można znaleźć w każdej warstwie, bądź to w fizycznej architekturze, bądź też w stosowanych procesach i politykach. Hakerzy mają do dyspozycji prawie niewyczerpany zestaw technik pozwalających im zrealizować swoje cele od ataków DDoS po subtelne manipulacje danymi i wszczepianie fragmentów kodu.

Schemat przebiegu ataku



Air gap – dominujące podejście

W niektórych firmach i branżach jako główną linię obrony wykorzystuje się tzw. „szczeliną powietrzną" (ang. *air gap*). Pomysł jest prosty – to tak jak podnieść most zwodzony w średniowiecznym zamku: jeśli nie ma logicznej ścieżki prowadzącej do chronionego obszaru, to żaden intruz się nie dostanie. Takie podejście bazujące na izolacji może wydawać się uzasadnione, ale w rzeczywistości ma wiele wad. Po pierwsze, szczelinę powietrzną można utrzymać

praktycznie tylko dopóty, dopóki nikt nie korzysta z chronionych danych ani nie ma zamiaru ich konfigurować czy korygować. Doświadczenie pokazuje zresztą, że do systemów wykorzystujących szczelinę powietrzną często można dostać się na wiele sposobów. Udowodniono już niestety, że może tutaj wystarczyć zwykły nośnik USB. Powszechnie uważa się, że niesławny robak komputerowy *Stuxnet*, który w roku 2009 zainfekował elektrownię jądrową w irańskim mieście Natanz, został wprowadzony przy pomocy pendrive'a.

Izolowanie sieci przemysłowych przestało już być skutecznym sposobem na bezpieczeństwo. Duży udział urządzeń mobilnych, infekcji kopii zapasowych i wyszukanych sposobów na wydobycie danych z izolowanych sieci w całkowitej liczbie ataków za pomocą złośliwego oprogramowania pokazuje, że nie da się uniknąć ryzyka zwyczajnie odłączając system od Internetu.

Holistyczny cyberfizyczny paradygmat bezpieczeństwa infrastruktury krytycznej

W związku z powyższym, konieczne jest usprawnienie niewystarczających już działań i inwestycji zabezpieczających infrastrukturę krytyczną. Szybka ewolucja metod ataku uzasadnia przyjęcie nowego podejścia. Wraz z rozwojem coraz inteligentniejszych i ściślej połączonych ze sobą sieci infrastruktury krytycznej pojawia się nagląca potrzeba przyjrzenia się ochronie tychże sieci zarówno od strony cybernetycznej, cyfrowej, jak i fizycznej, sektorowej. Najlepszych specjalistów, najlepsze platformy, procesy i umiejętności oraz najlepszą wiedzę pochodzące z obu tych wymiarów należy połączyć w jeden zespół, który wniesie zupełnie nowe podejście do ochrony infrastruktury krytycznej.

Israel Electric Corporation (IEC)

to największy w Izraelu dostawca energii elektrycznej. Przedsiębiorstwo buduje, konserwuje i obsługuje elektrownie i stacje elektroenergetyczne i zarządza sieciami przesyłowymi i sieciami dystrybucji. Instalacje elektryczne IEC odpowiadają za ok. 75% całkowitej zdolności do produkcji energii elektrycznej w kraju i okolicznych rejonach i zaopatrują w prąd ok. 12 mln ludzi. IEC stanowi więc pierwszorzędny cel dla cyberprzestępców z całego świata. W każdym miesiącu spółka doświadcza od 4 do 20 mln incydentów komputerowych.

W tym celu firma Verint Systems i Israel Electric Corporation powołały elitarny zespół ekspertów ds. cyberbezpieczeństwa infrastruktury krytycznej, łączący wyjątkowy repertuar umiejętności, doświadczenie w informatyce śledczej, analizie, przechowywaniu i wizualizacji danych masowych, wykrywaniu anomalii, ocenie ryzyka. Głównym celem zespołu jest określenie pierwotnej przyczyny nieprawidłowości operacyjnych i biznesowych, co stanowi fundamentalny krok do wykrycia zaawansowanych, długotrwałych ataków typu APT (ang. APT, *advanced persistent threat*).

Dobrym przykładem ukazującym konieczność przyjęcia nowego, holistycznego paradygmatu cyberbezpieczeństwa infrastruktury krytycznej jest sektor energetyczny. Produkcja energii elektrycznej i jej dystrybucja od elektrowni do odbiorców opierają się na złożonym systemie połączonych sieci. Obecnie zauważa się tendencję do cyfryzacji i zwiększania liczby wzajemnych połączeń w tychże sieciach (inteligentne sieci i liczniki, Internet rzeczy). Choć działania te poprawiają wydajność operacyjną i redukują koszty, powodują jednak równoczesny wzrost złożoności oraz tworzą kolejne wektory potencjalnych ataków cybernetycznych. IEC zbudowała sektorową wiedzę w dziedzinie cyberbezpieczeństwa w ciągu dziesięcioleci poświęconych opracowywaniu, integracji i wprowadzaniu metod, zasad, zaleceń oraz specyfikacji dotyczących obrony przed zagrożeniami cybernetycznymi na różnych etapach życia projektu. Ochrona sieci i łańcucha dostaw wchodzących w skład infrastruktury krytycznej (w wymiarze fizycznym, jak i logicznym) wymaga wiedzy zarówno w zakresie najlepszych praktyk cyberbezpieczeństwa oraz kompetencji do identyfikacji podatności w różnych częściach sektora energetycznego, takich jak: produkcja energii elektrycznej (energia termalna i odnawialna), przesył i dystrybucja, inteligentne liczniki, sieci i gospodarstwa domowe, wydajność energetyczna, czy Internet rzeczy.

Promowane przez Verint podejście SOC nowej generacji (Intelligence Security Operations Center, ISOC), pozwala organizacjom lepiej przygotować się na mnożące się cyberzagrożenia przez skrócenie czasu pomiędzy wykryciem zagrożenia a reakcją na nie dzięki wykorzystaniu narzędzi automatyzujących analizę incydentów. Zespolony SOC obejmujący IT i OT, pozwala operatorom sieci infrastruktury krytycznej poprawić widoczność bezpieczeństwa we wszystkich sieciach, scentralizować rozproszone umiejętności i ułatwić szybką, całościową odpowiedź na każde zidentyfikowane zagrożenie. Takie podejście zakłada, że włamanie do sieci już nastąpiło a działania powinny się skupić na odkryciu pełnego ciągu wydarzeń i punktów dostępu, informatyce śledczej sieci i punktów końcowych w ramach obszaru IT, jak i OT oraz przywróceniu sprawności i zaufania.

Zespół ma za zadanie wykryć, już na wczesnym etapie, każdy cyberatak zagrażający dużymi szkodami. Polega to na uruchomieniu i zarządzaniu procesami łagodzącymi efekty incydentu. Główny cel to zapobieganie efektowi domina i całkowitej utracie kontroli nad systemem. Dalszy cel to zbieranie dowodów do śledztwa.

Skala cyberataków jeszcze nigdy nie była tak duża jak obecnie. Każda firma, w której ochrona infrastruktury krytycznej nie jest choćby częściowo zautomatyzowana naraża się ryzyko wynikające z braku możliwości odparcia pojawiających się ataków. Zgodnie z danymi PWC, liczba wykrytych ataków w firmach sektora energetycznego zwiększyła się sześciokrotnie w ciągu zeszłego roku, co daje ponad 20 ataków dziennie na każdą firmę. Hakerzy mają do dyspozycji zasoby rozproszone w chmurze i superszybkie sieci. Kluczem do skutecznej ochrony jest zatem automatyzacja.

Według firmy analitycznej Gartner, „należy projektować inteligentne centra operacji bezpieczeństwa (SOC) – zbudować architekturę bezpieczeństwa dostosowującą się do okoliczności oraz w oparciu o decyzje poprzedzone zaawansowaną analizą[2]". Gartner zaleca, aby: „kierownicy ds. bezpieczeństwa tworzący lub rozbudowujący SOC, powinni: (a) wychodzić z założenia, że bezpieczeństwo zostało już naruszone; (b) zmodyfikować SOC tak, żeby zapewnić pełną widoczność; (c) postępować zgodnie z następującymi pięcioma zaleceniami dotyczącymi inteligentnych SOC":

1. Strategicznie i taktycznie wyszukiwać zagrożenia posiłkując się wieloma źródłami naraz.
2. Stosować zaawansowaną analizę w celu operacjonalizacji uzyskanej wiedzy.
3. Wprowadzać automatykę wszędzie, gdzie jest to możliwe.
4. Zbudować architekturę bezpieczeństwa dostosowującą się do okoliczności.
5. Aktywnie wyszukiwać zagrożenia i poddawać je analizie.

Inteligentny SOC Verint łączy wiele z powyższych cech i parametrów funkcjonalnych w jeden, zespolony ośrodek, korzystający m. in. z następujących zasobów i metod:

Źródła danych – zróżnicowane i kompleksowe źródła danych: pokrycie i widoczność w całej sieci, punkty końcowe oraz pliki, uzupełniane w miarę potrzeby automatycznymi raportami.

Metody wykrywania – bogaty zestaw wyspecjalizowanych czujników wykrywających zaawansowane zagrożenia, nawet już po pierwszym wtargnięciu (takie jak zarządzanie i kontrola, ruch poprzeczny, pułapki, czy dynamiczna analiza plików i emaili). System zbiera powiadomienia i selekcjonuje zagrożenia, co daje dokładne pokrycie i całościowy wgląd.

Metody badania zdarzeń – dynamiczna logika wykorzystująca maksimum możliwości zintegrowanej z nią platformy w celu automatyzacji badań za pomocą aktywnych kwerend śledczych i narzędzi dostarczanych na żądanie. Rezultatem są potwierdzone zdarzenia o dobrze widocznej historii ataku.

Ramy czasowe – ciągły monitoring i analiza.

Zdolności badawcze – zdolności i narzędzia badawcze są wbudowane w infrastrukturę i procesy operacyjne. Dostosowująca się architektura bezpieczeństwa pozwala na wykrywanie, badanie i reakcję za pomocą zintegrowanej sieci.

Podstawową zasadą tego nowego paradygmatu jest scalone, zespolone podejście do cyberbezpieczeństwa infrastruktury krytycznej, dotyczące zarówno obszaru IT, jak i OT oraz skupiające się na wykrywaniu, badaniu zdarzeń oraz reakcji na nie. Kluczowe szczegóły czy wątki często wydają się nieistotne, jeśli do dyspozycji mamy niespójny obraz sytuacji. Może to

2 Gartner, „Pięć cech centra bezpieczeństwa opartego na inteligentnych systemach", listopad 2015 r.

uniemożliwić ustalenie trwałości i częstości mało poważnych (zdawałoby się) zagrożeń, które są częścią szerszego kontekstu. Stworzenie zespolonego SOC pozwala analizować wątki i kojarzyć ze sobą zdarzenia w całej sieci, niezależnie od tego, gdzie te incydenty zostały początkowo rozpoznane oraz miejsca wejścia do systemu. Możliwość śledzenia i badania pełnego przebiegu ataku we wszystkich sieciach i technologiach umożliwia zespołom SOC sprawniej rozpoznawać ataki i łagodzić ich skutki, a także lepiej przygotować się na zagrożenia w przyszłości.

W oparciu o powyższe założenia, Verint i IEC powołały wspólny zespół ds. cyberbezpieczeństwa, którego zadaniem jest walka z rosnącymi zagrożeniami dotykającymi globalnej infrastruktury krytycznej. Zespół wprowadził zupełnie nowe podejście do ochrony infrastruktury krytycznej, od działania której zależy funkcjonowania społeczeństwa i nowoczesnej gospodarki. Korzysta on z dwudziestu lat doświadczenia sektorowego IEC związanego z produkcją, przesyłem i dystrybucją energii elektrycznej, by bronić kluczowych systemów przed nasilonymi cyberatakami. Zespół łączy również wiedzę IEC na temat OT z technologię Verint Systems i kapitałem wiedzy firmy w dziedziny cyberbezpieczeństwa (identyfikacja, analiza, informatyka śledcza, raportowanie, i analiza Big Data). Współpraca pomiędzy tymi dwoma podmiotami podkreśla, że nastąpiła drastyczna zmiana w podejściu do bezpieczeństwa infrastruktury krytycznej, polegająca na konieczności współdziałania ekspertów w wielu różnych dziedzinach w celu zabezpieczenia zarówno obszarów IT oraz OT w świecie, który z dnia na dzień staje się bardziej skomplikowany i ściślej połączony.

Zapewnienie ciągłości dostaw energii na potrzeby transportu kolejowego w Polsce. Ochrona cybernetyczna ze szczególnym uwzględnieniem systemów sterowania przemysłowego.

Dariusz Mikołajczyk, Robert Żelechowski,
PKP Energetyka

Charakterystyka i znaczenie PKP Energetyka S.A.

W Polskiej rzeczywistości gospodarczej spółka PKP Energetyka S.A. ma szczególne znaczenie ze względu na infrastrukturę, której jest właścicielem i operatorem. Jest ona bowiem istotna dla dwóch systemów infrastruktury sieciowej: energetycznej i kolejowej. Dwie podstawowe dziedziny funkcjonowania spółki dotyczą po pierwsze przetwarzania prądu zmiennego na prąd stały i dostarczania go do całej zelektryfikowanej sieci kolejowej w Polsce (ok. 12 tys. km linii kolejowych), a po drugie utrzymania elektrycznej sieci trakcyjnej w należytym stanie technicznym. W związku z powyższymi zadaniami spółka zarządza siecią tzw. podstacji trakcyjnych, które zapewniają dostawy energii elektrycznej do linii trakcyjnych oraz flotą ok. 100 specjalistycznych pociągów umożliwiających budowę oraz utrzymanie techniczne tejże sieci, której właścicielem jest PKP Polskie Linie Kolejowe S.A. (PKP PLK). PKP Energetyka S.A. jest również dystrybutorem energii elektrycznej. Pomimo niewielkiego udziału w krajowym rynku sprzedaży energii, jest w tym kontekście ważnym elementem systemu, z racji bycia jedynym podmiotem, który posiada sieć dystrybucji w całym kraju. Spółka została wyznaczona na operatora systemu dystrybucyjnego 25 lipca 2001 roku, z ponowną decyzją wydaną 14 marca 2008 roku na okres do 31 grudnia 2030 roku (Koncesja na dystrybucję energii elektrycznej z dnia 25 lipca 2001 r.). Istotnym obszarem działalności spółki jest również sprzedaż przewoźnikom kolejowym oleju napędowego do spalinowych pojazdów trakcyjnych. W rzeczywistości jest jedynym podmiotem na polskim rynku prowadzącym koncesjonowaną sprzedaż paliwa za pośrednictwem kolejowych stacji paliw.

Podobnie jak ma to miejsce w przypadku energetyki, transport kolejowy jest jednym z najważniejszych elementów systemu gospodarczego państwa. Należy również do najbardziej kosztownych w utrzymaniu, a jego prawidłowe funkcjonowanie uzależnione jest od bardzo rozbudowanej infrastruktury, obowiązkowo podlegającej stałej konserwacji i modernizacji. W przypadku Polski efekt ten potęgują dodatkowe nakłady inwestycyjne związane

z koniecznością całkowitej przebudowy części połączeń. Jeszcze kilka lat temu wydatki w latach 2014–2020 mające obejmować cały sektor szacowano na 35 mld złotych, z czego oczekiwana pula dofinansowania z Unii Europejskiej miała wynosić 25 mld złotych). Dziś mówi się już o 67 mld złotych. Całkowitą katastrofą byłaby konieczność zwrotu części dofinansowania europejskiego. O tym, że bywa to realnym zagrożeniem, można się było przekonać choćby w 2012 roku, kiedy Grupa PKP musiała zintensyfikować realizowane inwestycje w krajową infrastrukturę kolejową właśnie pod groźbą zwrotu części dotacji unijnych. Zgodnie z uchwałą Rady Ministrów z 15 września 2015 roku w sprawie ustanowienia „Krajowego programu kolejowego do 2023 roku" (RM-111-16515) mają zostać zrealizowane zadania związane z modernizacją, przebudową lub budową infrastruktury dystrybucji energii elektrycznej na potrzeby kolei. Te działania widoczne są dziś gołym okiem w postaci przeprowadzonych modernizacji torów kolejowych, taboru pasażerskiego, infrastruktury dworcowej, ale także towarzyszących im urządzeń elektroenergetycznych (program MUZA I – Modernizacja Urządzeń Zasilających, w którym uczestniczyła PKP Energetyka S.A.). Całość tych działań ma jednak przede wszystkim za zadanie stworzenie z systemu transportu kolejowego trzeciej alternatywy komunikacyjnej dla milionów obywateli naszego kraju oraz działających w nim podmiotów gospodarczych, obok infrastruktury drogowej i bardzo dynamicznie rozwijającego się systemu transportu lotniczego. Alternatywy wygodnej, szybkiej, nowoczesnej i przede wszystkim bezpiecznej.

Bezpieczeństwo energetyczne oraz elementy infrastruktury krytycznej w funkcjonowaniu PKP Energetyka S.A.

Kwestie dotyczące bezpieczeństwa energetycznego są w Polsce dyskutowane w zasadzie nieustanie. Zmieniają się co najwyżej poruszane aspekty. W ostatnim okresie dołączyły do tej dyskusji kwestie związane z wydolnością krajowego systemu produkcji, przesyłu i dystrybucji energii, a przyczyną tego stanu rzeczy było wprowadzenie w sierpniu 2015 roku stopni zasilania w energetyce, podyktowane ówczesną falą upałów zmniejszającą podaż i radykalnie zwiększającą popyt na energię. Czynnikiem dodatkowym jest fakt całkowitej integracji systemu dystrybucji spółki z systemem zasilania trakcyjnego PKP PLK. PKP Energetyka S.A. w swym Statucie wymienia trzy podstawowe obszary swej działalności. Są to sprawy związane z:

a) wytwarzaniem i zaopatrywaniem w energię elektryczną (wytwarzanie, przesył, dystrybucja, handel);

b) świadczeniem usług elektroenergetycznych (naprawa i konserwacja urządzeń; instalowanie maszyn, sprzętu i wyposażenia; roboty związane z budową linii telekomunikacyjnych i elektroenergetycznych; wykonywanie instalacji elektrycznych; inżynieria i doradztwo techniczne);

c) sprzedażą paliw (sprzedaż hurtowa paliw i produktów pochodnych; sprzedaż detaliczna paliw do pojazdów silnikowych na stacjach paliw; handel paliwami gazowymi w systemie sieciowym).

Z punktu widzenia bezpieczeństwa energetycznego naszego kraju istotne są punkty a) i c) Statutu. Jednakże z uwagi na dominację koncernu Polskie Górnictwo Naftowe i Gazownictwo (PGNiG) na rynku sprzedaży gazu w systemie sieciowym oraz posiadanie przez spółkę PKP Energetyka 18 stacji sprzedaży paliw kolejowych, punkt c) ma niewielkie znaczenie (jeśli nie liczyć zaopatrzenia lokomotyw spalinowych). Udział w rynku dystrybucji i handlu energią elektryczną także nie należy do znaczących. Liczy się dziś zatem głównie rozbudowana ogólnopolska sieć dystrybucyjna. Działalność opisana powyżej jest ściśle regulowana w ustawie z 10 kwietnia 1997 roku Prawo energetyczne (Dz. U. 1997 nr 54, poz. 348), gdzie w obszarze zapewnienia bezpieczeństwa energetycznego do działalności spółki odnoszą się zapisy art. 3, ust. 16, 16a i 16b definiujące najważniejsze pojęcia dotyczące tego zagadnienia:

- bezpieczeństwo energetyczne – stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska;
- bezpieczeństwo dostaw energii elektrycznej – zdolność systemu do zapewnienia bezpieczeństwa pracy sieci elektroenergetycznej oraz równoważenia dostaw energii elektrycznej z zapotrzebowaniem na tę energię;
- bezpieczeństwo pracy sieci elektroenergetycznej – nieprzerwana praca sieci elektroenergetycznej, a także spełnianie wymagań w zakresie parametrów jakościowych energii elektrycznej i standardów jakościowych obsługi odbiorców, w tym dopuszczalnych przerw w dostawach energii elektrycznej odbiorcom końcowym, w możliwych do przewidzenia warunkach pracy tej sieci" (Dz. U. 1997 nr 54, poz. 348: art. 3, ust. 16, 16a i 16b).

Inne zapisy Statutu dotyczą szeroko rozumianych prac remontowych, budowlanych, transportowych i innych, które de facto nie podlegają wprost regulacji ustawowej w zakresie bezpieczeństwa energetycznego i bezpieczeństwa transportu kolejowego. Niemniej są elementami współzależności między PKP Energetyka S.A. a podmiotami należącymi do Grupy PKP. Wspomnieć należy, iż granica majątku między PKP PLK a spółką PKP Energetyka jest wyznaczona bardzo dokładnie – jest nią punkt przyłączenia sieci trakcyjnych do sieci dystrybucyjnych. PKP Energetyka wypełnia zadania operatora systemu dystrybucyjnego (OSD) na majątku sieciowym nie obejmującym sieci trakcyjnej, która pozostaje integralną częścią drogi kolejowej i jest zarządzana przez PKP PLK. W tym miejscu należy wspomnieć także o pojęciu „zarządzania infrastrukturą kolejową", co obejmuje m.in. budowę i utrzymanie infrastruktury kolejowej w stanie zapewniającym bezpieczne prowadzenie ruchu kolejowego. Zadania te należą do spółki PKP PLK, przy czym w kwestiach związanych z utrzymywaniem sieci trakcyjnej i dostawą energii, niezmiernie istotnym podmiotem jest PKP Energetyka, bez której trudno sobie wyobrazić realizowanie tych zadań z racji dysponowania przez ten podmiot odpowiednią infrastrukturą techniczną. Powyższe skłania do konkluzji, że najistotniejszym elementem specyfiki spółki PKP Energetyka jest fakt, że jest ona prywatnym właścicielem ogólnopolskiej sieci dystrybucyjnej energii elektrycznej, zasilającej sieć trakcyjną na liniach kolejowych zarządzanych przez PKP PLK.

Drugim istotnym elementem związanym z bezpieczeństwem zarządzanej przez PKP Energetyka infrastruktury dystrybucyjnej energii elektrycznej jest pełnienie funkcji operatora obiektów infrastruktury krytycznej w rozumieniu ustawy z 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590, z późn. zm.). Zgodnie z definicją ustawową, przez infrastrukturę krytyczną (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). Ustawodawca wymienił systemy, które wchodzą w skład takiej infrastruktury i należą do nich systemy zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, teleinformatyczne, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, ratownicze, zapewniające ciągłość działania administracji publicznej oraz transportowe. Zakres działalności firmy PKP Energetyka plasuje zarządzaną przez nią infrastrukturę wśród systemów wskazanych przez ustawodawcę jako krytyczne dla możliwości normalnego funkcjonowania państwa. Dodatkowo jest ona wyrażona explicite przynajmniej w dwóch z wyszczególnionych w ustawie obszarach: zaopatrzeniu w energię elektryczną oraz transporcie. Spółka w 2015 roku uczestniczyła w pracach koordynowanych przez PKP S.A., których celem było stworzenie jednego wykazu obiektów stanowiących infrastrukturę krytyczną dla całej Grupy PKP. W wyniku procesów prywatyzacyjnych działania te nie zostały ukończone, ale powróciła do nich sama PKP Energetyka w 2016 roku. Efektem współpracy z Ministerstwem Infrastruktury i Budownictwa było wyselekcjonowanie obiektów administrowanych przez spółkę jako stanowiących elementy infrastruktury krytycznej. Ustalenia ta znalazły odzwierciedlenie w umieszczeniu ich w jednolitym wykazie obiektów, instalacji i urządzeń wchodzących w skład infrastruktury krytycznej prowadzonym przez Rządowe Centrum Bezpieczeństwa pod koniec 2016 roku. Tym samym spółka została włączona w system współdziałania, mający na celu realizację określonych zadań na rzecz bezpieczeństwa państwa.

System ochrony obiektów infrastruktury krytycznej powinien mieć zastosowanie do wszystkich typów zidentyfikowanych zagrożeń: naturalnych, intencjonalnych oraz technicznych, a także być przygotowany do możliwie szybkiego przywrócenia funkcji realizowanych przez dany obiekt. Ponadto powinna cechować go kompleksowość i elastyczność oraz, co nie mniej ważne, łatwość zastosowania i zrozumienia przez odpowiedzialnych za ich ochronę.

Działania podejmowane na rzecz zapewnienia bezpieczeństwa obiektów infrastruktury krytycznej zostały określone w „Narodowym Programie Ochrony Infrastruktury Krytycznej – Załącznik nr 1 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje". Mają na celu minimalizację ryzyka zakłócenia obiektów infrastruktury przez zmniejszenie prawdopodobieństwa wystąpienia zagrożenia, zmniejszanie podatności oraz minimalizowanie skutków wystąpienia zagrożenia. Na działania, które mają doprowadzić do takiego stanu, składają się:

- zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
- zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
- zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
- zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
- zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
- plany ciągłości działania i odtwarzania rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania.

Należy podkreślić, iż cała infrastruktura służąca do przetwarzania i dostaw energii elektrycznej na potrzeby sieci kolejowej w Polsce, którą zarządza PKP Energetyka S.A., jest sterowana zdalnie za pomocą systemów automatyki przemysłowej poprzez tzw. nastawnie centralne, którym przypisana jest terytorialnie odpowiednia liczb podstacji trakcyjnych. Wymienione wyżej zasady bezpieczeństwa, rekomendowane przy ochronie obiektów infrastruktury krytycznej, winny być stosowane przy ochronie całej infrastruktury na zasadzie dobrych praktyk. Dotyczy to w szczególności kwestii zapewnienia bezpieczeństwa systemom sterowania przemysłowego. Nabiera to szczególnego znaczenia w dobie bardzo dynamicznego rozwoju technologii sieciowych. W zasadzie nie mówimy już o sterowaniu przemysłowym w ujęciu klasycznym OT, tj. odseparowanym od systemów telekomunikacyjnych. Z racji minimalizacji kosztów ich obsługi dochodzi bowiem do coraz częstszego stosowania w jego obrębie różnych systemów łączności. Dlatego też systemy te określa się mianem systemów teleinformatycznych – ICT.

W dalszej części niniejszej publikacji skoncentrujemy się na opisie idealnych wymagań, jakie mają służyć zapewnieniu bezpieczeństwa systemów zdalnego sterowania zaopatrujących w energię elektryczną sieci kolejowe właśnie z punktu widzenia cyberbezpieczeństwa systemów ICT. Obydwa te czynniki, tj. stosowanie uniwersalnych rozwiązań i funkcjonowanie systemów zdalnego sterowania w strukturze ogólnodostępnej sieci Internet, wpływają na wzrost ryzyka zakłócenia ich działania. Może ono nastąpić w wyniku zwiększenia podatności

na zagrożenie w postaci dedykowanego sieciowego cyberataku z zewnątrz lub narażenia się na oddziaływanie negatywnych zjawisk sieciowych, takich jak rozprzestrzeniające się wirusy, robaki sieciowe czy ograniczenie dostępu do sieci. Systemy nadzorujące przebieg procesów technologicznych lub produkcyjnych (np. klasy SCADA lub DCS) działają na standardowych, popularnych platformach systemów Windows, Unix czy Linux. Dlatego cyberataki sieciowe wykorzystujące słabości systemów operacyjnych dotyczyć mogą również działających na nich systemów przemysłowych.

Bezpieczeństwo cybernetyczne w systemach sterowania przemysłowego – wymagania modelowe

Dziedzina taka jak bezpieczeństwo cybernetyczne systemów sterowania przemysłowego należy obecnie traktować jako nieodzowny proces, którego utrzymanie i stały rozwój jest niezbędny do prawidłowego funkcjonowania przedsiębiorstwa posiadającego sterowalną i zarządzaną infrastrukturę techniczną ICS będącą głównym segmentem obszaru automatyki OT.

Z uwagi na fundamentalne różnice pomiędzy systemami OT a systemami IT wymienione w poniższej tabeli, bezpieczeństwo automatyki przemysłowej traktowane było do niedawna bez należytej staranności. Ze względu na te różnice, zastosowanie wprost polityk bezpieczeństwa z obszaru IT w świecie OT okazywało się niemożliwe.

Różnice pomiędzy obszarami IT a OT

	Information Technology (IT)	Operational Technology (OT)
Cel	pozyskiwanie, przetwarzanie i analiza danych	sterowanie, kontrolowanie i zarządzanie procesem technologicznym
Architektura i komponenty	głównie stacje robocze użytkowników, serwery, aplikacje, dla których łatwo zaimplementować polityki bezpieczeństwa czy zastosować system szybkich aktualizacji	głównymi komponentami to automaty, sterowniki, przemysłowe przełączniki i ściśle dedykowane systemy zazwyczaj czasu rzeczywistego, dla których zastosowanie aktualizacji usuwających podatności jest bardzo graniczone
Interfejsy	graficzne GUI, przeglądarki WEB, terminale, klawiatura, myszka	czujniki, wyłączniki, sterowniki, siłowniki, wyświetlacze
Właściciel	IT i CIO	inżynierowie, technicy, operatorzy, dyspozytorzy, menadżerowie
Łączność	sieć oparta na protokole IP: LAN, korporacyjna, Internet,	sieci dedykowane, kontrolne, sterowanie prądowe, twarda skrętka, oparte na IP, protokoły automatyki: modbus, PLC, M-BUS, DNP3, etc.
Rola	wsparcie dla ludzi	sterowanie maszynami

Priorytety w ochronie teleinformatycznej infrastruktury OT, z uwagi na wyżej wymienione różnice względem infrastruktury IT, są również znacząco inne. Głównym elementem

chronionym w IT jest najcenniejsze aktywo, jakim są dane, w tym ich poufność, integralność i dostępność. W OT najcenniejszym elementem chronionym jest niezawodność i dostępność procesu technologicznego/przemysłowego, a w kolejnym etapie integralność i poufność.

Naturalne czynniki ewolucyjne w świecie automatyki, takie jak m.in. dążenie do optymalizacji procesów i kosztów lub wzrost wymagań funkcjonalnych, wymuszały zastosowanie rozwiązań zdalnej kontroli, współdzielenie dróg komunikacji oraz integrację z systemami analitycznymi czy biznesowymi. Dwa światy OT i IT zaczęły się wzajemnie przenikać, otwierając drogę do hermetycznego wcześniej świata OT dla nowych zagrożeń, jakie niesie ze sobą cyberprzestępczość i cyberterroryzm. Pomimo wcześniejszych, skutecznych ataków na systemy przemysłowe, powszechnie nazywane systemami SCADA, które odpowiedzialne są za nadzorowanie przebiegu procesów technologicznych w przedsiębiorstwach, przełomowym w zakresie uświadomienia użytkownikom systemów konsekwencji takich ataków był rok 2010. W lipcu tego roku wykryto nowego, groźnego wirusa o nazwie Stuxnet. Szczególnym celem działania wirusa było naruszenie procesu technologicznego związanego ze sterowaniem pracy wirówki odpowiedzialnej za wzbogacanie uranu w irańskich zakładach, co w skrajnym przypadku mogło doprowadzić nawet do jej wybuchu. Kolejne lata przyniosły mniej lub bardziej spektakularne ataki na infrastrukturę przemysłową w praktycznie każdym sektorze przemysłu na całym świecie. Ostatnie wyłączenia sieci energetycznej na Ukrainie czy w Turcji, czy też wstrzymanie na kilka dni produkcji w japońskiej fabryce Hondy wykazały, z jaką łatwością odpowiednio przygotowany i ukierunkowany atak może doprowadzić do bardzo poważnych konsekwencji w technologicznym funkcjonowaniu przedsiębiorstw. Ukierunkowane ataki cybernetyczne i przejęcie kontroli nad infrastrukturą krytyczną są już obecnie ujęte w „portfolio" praktycznie każdego arsenału wojskowego, jako jedna z opcji militarnych w przypadku konfliktu zbrojnego. Jedną z częstych przyczyn pozwalających na skuteczność tego typu ataków jest istnienie tzw. długu technologicznego w zakresie implementacji mechanizmów bezpieczeństwa w urządzeniach i systemach ICS w stosunku do zabezpieczeń w świecie IT. „Zacofanie technologiczne" powoduje, że ataki na infrastrukturę automatyki stały się obecnie stosunkowo łatwe dla cyberprzestępców oraz bardzo kuszące z uwagi na większe do osiągnięcia korzyści finansowe (w skutek szantażu) czy medialne.

Infrastruktura systemu OT w systemie elektroenergetyki PKP Energetyka, pomimo swojej niepowtarzalności w skali kraju, z uwagi na sterowanie urządzeniami prądu stałego, nie odbiega znacząco od innych systemów automatyki o podobnym charakterze dla prądu zmiennego. Ma charakter częściowo scentralizowany w zakresie fragmentu infrastruktury serwerowej i rozproszony dla ogólnie pojętych urządzeń telemechaniki znajdujących się na obiektach elektroenergetycznych. Sterowanie obiektami elektroenergetycznymi odbywa się z kilkunastu regionalnych centrów dyspozytorskich. Nadzór nad całościowym stanem infrastruktury odbywa się z jednego centralnego punktu monitoringu. Komunikacja w sieci zdalnego sterowania jest prowadzona za pomocą separowanego ruchu w dedykowanej infrastruktury sieciowej. Celem nadrzędnym w aspekcie bezpieczeństwa systemów OT

wykorzystywanych w PKP Energetyka jest zapewnienie ciągłości działania i dostępności ich sterowania. Cele te wspiera duplikacja łączy komunikacyjnych do obiektów elektroenergetycznych opartych o łącza IP VPN (podstawowe) i dedykowaną komunikację APN GSM (łącza redundantne). Bezpieczeństwo infrastruktury automatyki w PKP Energetyka wspierają również regulacje wewnętrzne w postaci procedur i instrukcji zgodnych z wymaganiami normy ISO/IEC 27001, określających zasady m.in. dla stacji roboczej operatora dystrybucyjnego czy stacji operatora telemetrii dokonującego zmian w oprogramowaniu liczników energii elektrycznej.

Rozwijane na świecie innowacyjne systemy i technologie umożliwiają transformację tradycyjnych sieci elektroenergetycznych w sieci inteligentne (tzw. smart grid). Taka przemiana niesie ze sobą niezaprzeczalne korzyści niezawodnościowe, poprawę bezpieczeństwa oraz stabilności i jakości zasilania. Przekłada się to bezpośrednio na wysoką jakość usług świadczonych na rzecz odbiorców. Przykładem takiej innowacji w świecie elektroenergetyki są systemy klasy FDIR (ang. *Fault Detection, Isolation and Restoration*), które na bieżąco analizują infrastrukturę elektroenergetyczną i automatycznie wykrywają uszkodzenia sieci, ograniczając ich zasięg do miejsca wystąpienia poprzez ominięcie uszkodzonego fragmentu infrastruktury.

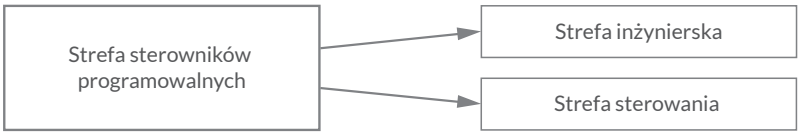
W celu osiągnięcia powyższych korzyści, PKP Energetyka podjęła decyzję o uruchomieniu projektu kompleksowej modernizacji systemu zdalnego sterowania, w tym niektórych elementów obszaru OT wraz z uruchomieniem pełnej funkcjonalności systemu ADMS (ang. *Advanced Distribution Management System*).

Projekt ten obejmie swoim zakresem również udoskonalenie mechanizmów cyberbezpieczeństwa automatyki przemysłowej w PKP Energetyka. Wytycznymi w zakresie doboru i zastosowania rozwiązań, dobrych praktyk czy kierunków budowy poszczególnych mechanizmów bezpieczeństwa tego systemu w PKP Energetyka będą normy i opracowania powstałe w tym zakresie:

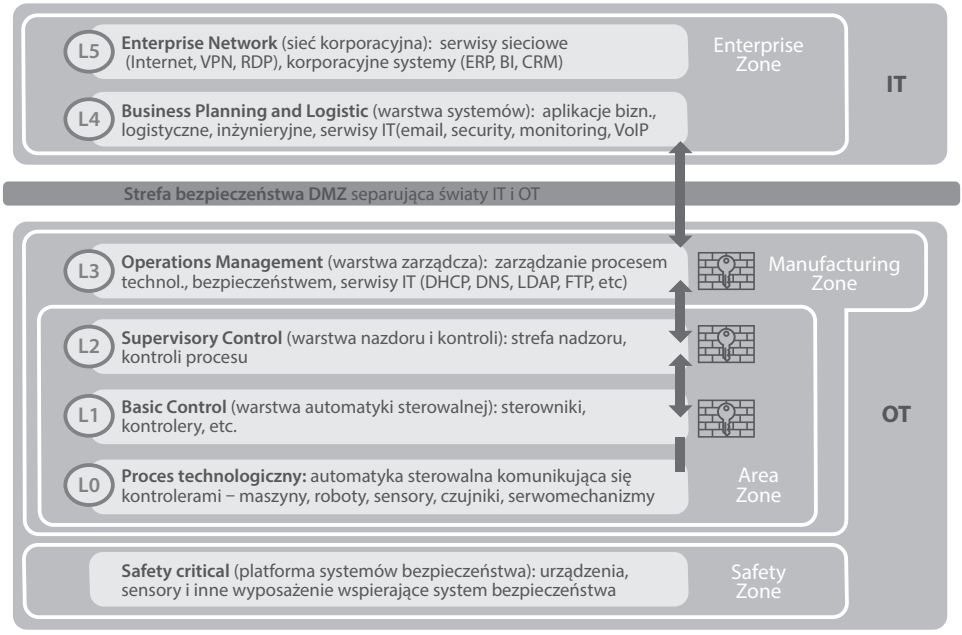
- Standard ISA 62443 (ISA99) – opracowany przez komitet *International Society of Automation on Security for industrial automation and Control System* (USA),
- NERC's CIP – *North American Electric Reliability Corporation – Critical Infrastructure Protection*,
- NIST SP 800-82 – *Guide to Industrial Control Systems (ICS) Security*,
- ENISA – wytyczne Europejskiej Agencji Bezpieczeństwa Sieci i Informacji,
- Norma IEC 62351 (od 1 do 11),
- Norma ISO/IEC 27002 – obejmująca wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

Głównymi założeniami architektury bezpieczeństwa systemów automatyki jest budowa tzw. stref z jasno określonymi granicami, z ograniczeniem komunikacji pomiędzy nimi do tzw. bezpiecznych kanałów komunikacyjnych. Strefy tworzą grupy urządzeń lub obiektów posiadających wspólne cechy i funkcjonalności, dla których można zastosować wspólną politykę ochrony.

Wzorcowa architektura bezpieczeństwa systemów automatyki oparta na strefowaniu i komunikacji



Kanały komunikacyjne obejmują każdą potencjalną metodę komunikacji między strefami. Tyczą się one zarówno wymiany danych za pomocą protokołów, sygnałów sterujących, kanałów serwisowych, jak również plików przenoszonych za pomocą dowolnych nośników czy bezpośrednich połączeń konsolowych. Dobierając technologię zabezpieczeń dla kanałów komunikacyjnych pomiędzy strefami, przy wsparciu wewnętrznych regulacji, polityk i instrukcji bezpieczeństwa, dokonane zostanie mapowanie infrastruktury OT w ujęciu poniższego modelu referencyjnego ISA99:



Główne założenia projektowe dla budowy architektury bezpieczeństwa systemów zdalnego sterowania powinny spełniać następujące wymagania:

- współistnienie dwóch izolowanych sieci LAN – dla środowiska biurowego IT oraz środowiska technologicznego TAN (ang. *Technology Area Network*),
- redundancję serwerów systemów zdalnego sterowania z możliwością pracy w jednym z trybów: *active-active* lub *hot standby*, aby zapewnić możliwie krótkie czasy odzyskiwania funkcjonalności serwerów,
- redundancja łączy sieciowych w połączeniu z wykorzystaniem protokołów routingu dynamicznego IP,
- budowa strefy DMZ dla punktu styku pomiędzy sieciami LAN/TAN oraz inspekcja ruchu sieciowego z użyciem urządzeń klasy NG Firewall,
- zabezpieczenie komunikacji pomiędzy wszystkimi elementami systemu oraz systemami zewnętrznymi z użyciem protokołów posiadających mechanizm wzajemnego uwierzytelniania
- użycie metod kryptograficznych dla uwierzytelniania elementów systemu
- zapewnienie wysokiej dostępności z wykorzystaniem terminali mobilnych,
- wirtualizację węzłów zdalnych telemechaniki,
- wdrożenie dla kanałów inżynierskich, połączeń serwisowych i kont wysoko uprzywilejowanych systemu klasy PAM (ang. *Privileged Access Manager)*,
- wdrożenie narzędzi analitycznych klasy NBAD (ang. *Network Behavior Anomaly Detection*)
- wdrożenie narzędzia korelacji zdarzeń i powiadamiania klasy SIEM

Docelowa architektura systemu zakładać powinna możliwość komunikacji i wymiany danych pomiędzy dwoma infrastrukturami IT oraz OT. Obydwa obszary (LAN i TAN) skomunikowane są wewnętrznie za pośrednictwem odpowiednio przygotowanej strefy buforowej DMZ. Strefa DMZ, z uwagi na swoje strategiczne znaczenie dla bezpieczeństwa automatyki, powinna być wyposażona w mechanizmy zabezpieczeń poddające każdy ruch komunikacyjny pomiędzy strefami (również szyfrowany) szczegółowej weryfikacji i inspekcji, sondowaniu przez IPS/IDS, filtrowaniu przez Firewall i ewentualnej analizie za pomocą środowisk SandBoxing. Każdy z elementów systemu posiadać winien zabezpieczenia kryptograficzne – zarówno w obszarze uwierzytelniania jak i komunikacji. Uwierzytelnianie urządzeń i użytkowników powinno odbywać się z użyciem certyfikatów oraz protokołów z mechanizmami wzajemnej autentykacji, a system zawierać powinien wewnętrzne Centrum Autoryzacji (CA) na potrzeby dostarczania certyfikatów.

Ważnym aspektem bezpieczeństwa powinny być mechanizmy weryfikacji i kontroli sesji użytkowników systemu, w szczególności kont inżynierskich i zdalnego dostępu serwisowego. Stosowane w tym przypadku narzędzia klasy PAM posiadają mechanizmy zarządzania kontami wysoko uprzywilejowanymi, nagrywania sesji (np. w celach dowodowych) i ograniczania możliwości komunikacji wyłącznie do określonych zasobów. Oparcie systemów serwerowych (a nawet stacji operatorskich) o wirtualizację pozwala na uzyskanie krótkiego czasu powrotu do funkcjonowania infrastruktury w przypadku wystąpienia awarii krytycznej powodującej

pełną niedostępność środowiska lub jej pojedynczego elementu. Dodatkowo dla zwiększenia dostępności zasobów powinno zakładać się nadmiarowość zarówno w obszarze urządzeń serwerowych jak i sieciowych w obszarze infrastruktury LAN, TAN oraz WAN. Dla zrównoważenia obciążenia i uzyskania płynnego dostępu do zasobów zakłada się zastosowanie klastrów wydajnościowych oraz mechanizmów priorytetyzacji ruchu. Na potrzeby diagnostyki oraz weryfikacji pracy sieci TAN dla wybranych użytkowników należy zapewnić dostęp zdalny, zabezpieczony zarówno z poziomu weryfikacji stacji roboczej, z której dokonywane jest połączenie, jak i użytkownika, który nawiązuje sesję, oraz politykami narzędzia PAM.

Głównym założeniem każdego systemu czasu rzeczywistego, jakim jest system zdalnego sterowania, powinien być brak przerw konserwacyjnych w przypadku jego rutynowej eksploatacji. Dostępność pracy systemu winna zostać określona na poziomie 99,9% w skali miesiąca (praca 7 dni w tygodniu przez 24 godziny na dobę), a budowa architektury systemu (w tym kopii zapasowych) pozwolić na zabezpieczenie danych w taki sposób, aby po awarii krytycznej można było odzyskać dane sprzed ostatnich 2 godzin. W celu uzyskania wysokiego współczynnika dostępności, zapewnione powinny być mechanizmy wczesnego wykrywania awarii (proaktywnego zarządzania wydajnością i pojemnością zasobów systemowych). Wykonywanie kopii zapasowych musi być dokonywane online, bez możliwości wyłączania całości systemu zdalnego sterowania. W przypadku awarii elementów architektury systemu lub konieczności przeprowadzenia konserwacji (aktualizacji), zastosowane mechanizmy redundancyjne muszą zapewnić nieprzerwaną pracę systemu w lokalizacji rezerwowej.

Niezmiernie istotne dla ochrony systemów zdalnego sterowania przed atakami cybernetycznymi jest wdrożenie rozwiązań zapewniających tym systemom spełnienie cech ich integralności, poufności, dostępności oraz rozliczalności.

Dla zapewnienia **integralności** informacji systemu zdalnego sterowania, dane przechowywane w logach i plikach dziennika zdarzeń chronione muszą być przed edycją lub usunięciem. System musi zawierać mechanizmy automatycznego powiadamiania o zdarzeniach zarejestrowanych poza zadanym zakresem tolerancji, takich jak próba użycia identyfikatora w celu wykonania nieuprawnionych czynności. W celu zapewnienia integralności, szczególnie wrażliwe lub istotne dane muszą być zabezpieczane przy użyciu metod kryptograficznych. Dla spełnienia wymagania **poufności**, które zakłada uniemożliwienie dostępu do danych lub ich ujawnienie nieuprawnionym osobom, procesom lub innym podmiotom, stosowany winien być system szyfrowania danych oraz kontroli dostępu. W systemie sterowania realizowana musi być pełna kontrola na każdym etapie dostępu do danych i funkcji wyłącznie dla uprawnionych użytkowników **(dostępność)**. Hasła podczas wpisywania muszą być zamaskowane i przechowywane w sposób zaszyfrowany. Stacje robocze korzystające z systemu również muszą być uwierzytelniane przy użyciu dodatkowych mechanizmów kryptograficznych, takich jak certyfikaty. Komunikacja stacji roboczych z systemem podlegać musi ochronie przy pomocy algorytmu

szyfrującego. Natomiast dla udostępnianych z systemu informacji z użyciem interfejsu użytkownika przez przeglądarkę internetową musi odbywać się wyłącznie z zastosowaniem protokołu połączenia szyfrowanego.

W celu spełnienia wymagania pełnej **rozliczalności dostępu**, mechanizmy zaimplementowane w systemie zdalnego sterowania muszą umożliwiać jednoznaczne przypisanie każdego działania w systemie do osoby fizycznej lub procesu oraz oznaczyć je tzw. stemplem czasowym.

Dla skutecznego zarządzania uprawnieniami w systemie muszą być zaimplementowane mechanizmy zarządzania tożsamością, odpowiedzialne za umożliwianie użytkownikom dostępu do usług informatycznych, danych lub innych zasobów systemu zdalnego sterowania za pomocą określonej metody uwierzytelniania. Mechanizmy zarządzania uprawnieniami powinny cechować się możliwością określenia poziomu dostępu do informacji zarówno w obszarze konkretnych ekranów, raportów, dokumentów, grup obiektów biznesowych, obiektów spełniających określone właściwości, obszarów geograficznych, funkcji systemu czy pojedynczych rekordów. Definiowanie uprawnień dostępu dla użytkowników powinno odbywać się za pomocą mechanizmu ról (profili) z przypisanymi im profilowanymi uprawnieniami. Mechanizmy jednoznacznej weryfikacji i potwierdzenia zadeklarowanej tożsamości użytkownika lub procesu powinny zapewniać prawidłowe uwierzytelnianie użytkowników w systemie. Dodatkowo, oprócz zastosowania specjalistycznych narzędzi do monitorowania, inspekcji, filtrowania i badania anomalii ruchu w kanałach komunikacyjnych, sama architektura systemu zdalnego sterowania musi być odporna na znane techniki ataku i włamań na poziomie warstwy aplikacyjnej oraz sieciowej poprzez zastosowanie partycjonowania i segmentacji sieci z określeniem granic tejże separacji.

Podsumowanie

W ostatnim czasie coraz więcej podmiotów posiadających systemy automatyki przemysłowej zdaje sobie sprawę z postępu integracji tych systemów z teleinformatyką. W coraz większym stopniu tracą one poczucie bezpieczeństwa związane z ich pierwotną, historyczną separacją, która dawała pewność ich niezakłóconego funkcjonowania. Podawane w mediach, a przytoczone w niniejszym artykule przykłady zdalnego zakłócenia ich funkcjonowania przez wyspecjalizowane grupy, boleśnie uwidoczniły, jak wiele kwestii bezpieczeństwa zostało w nich niezauważonych na etapie ich projektowania, unowocześniania lub codziennej eksploatacji. Ta, czasami nieświadoma, ignorancja naraża codziennie wiele podmiotów gospodarczych na realne straty finansowe, które nie są możliwe do realnego oszacowania. Większość podmiotów nie informuje o tego typu wydarzeniach związanych z zakłóceniem administrowanych przez nie systemów. Na szczęście świadomość w tym zakresie ulega stałemu zwiększeniu. Przyczyniają się do tego nie tylko realne incydenty odnotowywane przez operatorów systemów, ale także działania legislacyjne i organizacyjne prowadzone przez instytucje rządowe. Przedsiębiorcy prowadzą szeroko zakrojone działania mające na celu analizę zagrożeń oraz implementowanie rozwiązań, które w maksymalny sposób zabezpieczą ich przed atakami cybernetycznymi

nie tylko w przypadkach wymaganych przepisami prawa, jak choćby w przypadku administrowania obiektami infrastruktury krytycznej. W sektorze energetycznym działania te mają za zadanie zapewnić bezpieczeństwo dostaw energii elektrycznej do finalnych odbiorców oraz bezpieczeństwo pracy sieci elektroenergetycznej służącej do dystrybucji energii. Skutki zakłócenia pracy tych systemów mogą mieć ogromny wpływ na bieżące funkcjonowanie wszystkich gałęzi gospodarki, systemów produkcyjnych, komunikacyjnych oraz transportowych. Sektor energetyczny w naszym kraju prowadzi bardzo zaawansowane działania w tym zakresie. Istnieją już operatorzy posiadający własne CERT-y, a wielu jest w trakcie ich tworzenia. Specjaliści z tej dziedziny, opierając się na własnej wiedzy i doświadczeniu, znanych przypadkach ataków oraz założeniach opisanych w niniejszej publikacji, współpracują nad opracowaniem standardów bezpieczeństwa automatyki przemysłowej dla sektora energetycznego. Prace te koordynuje Rządowe Centrum Bezpieczeństwa i należy mieć nadzieję, iż w niedługim czasie przyniosą one wymierne rezultaty w postaci publikacji owych standardów. To bardzo dobry przykład współpracy pomiędzy biznesem a administracją rządową na rzecz wspólnego przeciwdziałania zagrożeniom płynącym z możliwych ataków cybernetycznych. Wartym podkreślenia jest przede wszystkim wzrost świadomości podmiotów gospodarczych o możliwych zagrożeniach, jakie pojawiają się lub mogą pojawić w tej dziedzinie. To absolutna podstawa do tego, by skutecznie zapewnić bezpieczeństwo systemom sterowania automatyki przemysłowej – systemom często zarządzającym kluczowymi procesami produkcyjnymi w przedsiębiorstwach.

Rola systemu AMI w zapewnieniu bezpieczeństwa energetycznego kraju w kontekście zagrożeń cybernetycznych

Krzysztof Podwiński, TAURON Dystrybucja S.A.,
Mariusz Jurczyk, TAURON Dystrybucja Pomiary sp. z o.o.

W okresie ostatnich dwóch dekad w związku ze stale wzrastającym trendem udziału technik informatycznych w przedsięwzięciach gospodarczych coraz mocniej zarysowuje się wzrost ryzyka związanego z występowaniem cyberzagrożeń. Początkowo były one pomijane lub marginalizowane. W najlepszym wypadku w systemach informatycznych wspierających działania biznesowe implementowane były proste mechanizmy ochrony przed tymi zagrożeniami. Jednak szybko przekonano się, że bezpieczeństwo systemu informatycznego musi stanowić podstawowy element jego funkcjonalności. Świadomość tych zagrożeń jest jeszcze większa, gdy ich skutki mogą przenieść się na inne systemy bądź infrastrukturę techniczną i urządzenia stwarzając widmo awarii masowych. Systemy Inteligentnego Opomiarowania AMI są dobrym przykładem do tego, aby wskazać istotność infrastruktury technicznej i urządzeń jako jednego z wielu elementów występujących w zapewnieniu bezpieczeństwa krajowego systemu energetycznego.

Systemy inteligentnego opomiarowania AMI

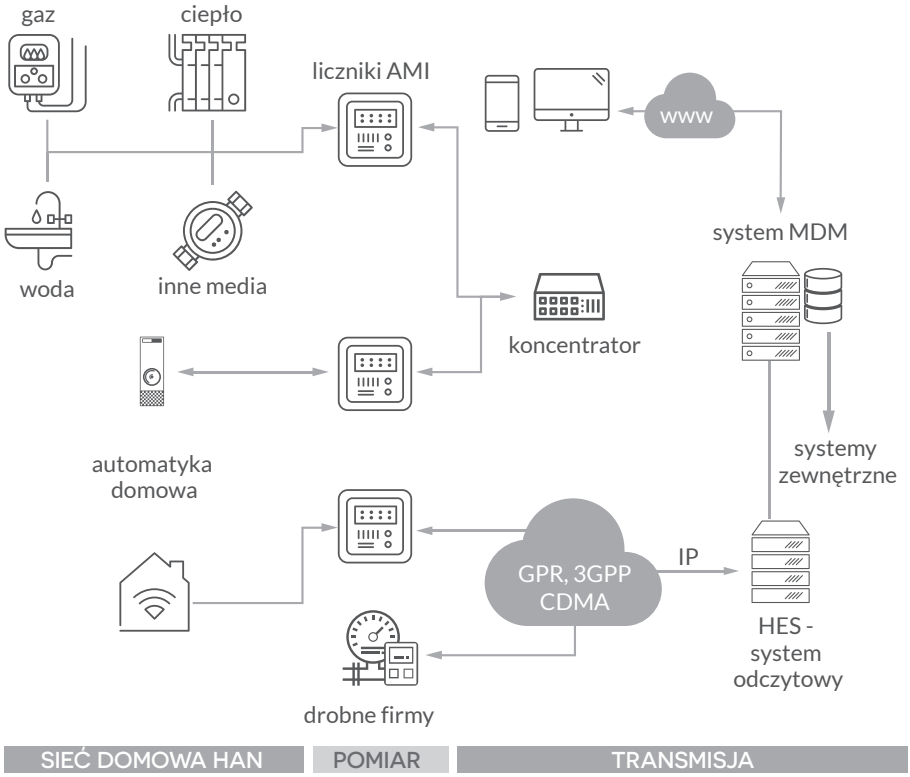
System inteligentnego opomiarowania AMI (ang. AMI = *Advanced Metering Infrastructure*) to kompletna infrastruktura obejmująca urządzenia pomiarowe (liczniki), urządzenia transmisyjne, aplikacje odczytowe, protokoły komunikacyjne oraz procesy organizacyjne, służąca do odczytywania, nadzoru i sterowania licznikami inteligentnymi (ang. *smart meters*). Rozwiązania AMI przynoszą szereg korzyści dla szerokiego grona interesariuszy. Wśród najważniejszych należy wymienić klientów końcowych, Operatora Sieci Dystrybucyjnej, sprzedawców energii. Korzyści dotyczą przede wszystkim oszczędności związanych z optymalizacją procesów biznesowych, ograniczeniem kosztów dostawy energii elektrycznej, wreszcie możliwością podejmowania świadomych decyzji związanych z ograniczeniem zużycia energii elektrycznej.

Licznik inteligentny umożliwia klientowi dostęp do danych pomiarowych z licznika poprzez bezpośredni odczyt danych dostępnych na wskazanym interfejsie komunikacyjnym licznika lub poprzez dedykowaną platformę lub aplikację mobilną (np. platformę TAURON eLicznik). Klient ma możliwość kontroli na bieżąco poziomu zużycia energii elektrycznej, ponadto aplikacje dostarczają podstawowe funkcjonalności w zakresie analiz konsumpcji energii.

Obowiązek instalacji inteligentnego opomiarowania AMI (ang. AMI – *Advanced Metering Infrastructure*) został przedstawiony w Dyrektywie Parlamentu Europejskiego i Rady Europejskiej nr 2009/72/WE z dnia 13 lipca 2009 r. dotyczącej wspólnych zasad rynku wewnętrznego energii elektrycznej. Zgodnie z tekstem Dyrektywy, w przypadku, gdy państwo członkowskie oceniło wdrożenie inteligentnych systemów pozytywnie, wyposaża w nie co najmniej 80 % klientów do 2020 r.

Architektura instalacji inteligentnego opomiarowania została przedstawiona na rys.1.

Rys.1 Architektura rozwiązania instalacji inteligentnego opomiarowania.



Instalacja inteligentnego opomiarowania składa się z liczników inteligentnych, medium transmisyjnego, systemu odczytowego HES (ang. HES — *HeadEnd System*). Licznik inteligentny realizuje pomiar mocy i energii elektrycznej, pomiar wartości sieciowych, rejestrację zdarzeń. Posiada ponadto możliwość realizacji funkcji przedpłatowej, strażnika mocy, zdalnego wstrzymania i wznowienia dostawy energii elektrycznej. Licznik AMI posiada interfejsy komunikacyjne, w kierunku do systemu odczytowego HES, jak również w kierunku do sieci domowej HAN (ang. HAN — *Home Area Network*).

Interfejs komunikacyjny stosowany w liczniku AMI w kierunku do sieci domowej HAN to najczęściej interfejs oparty o komunikację z wykorzystaniem protokołu M-Bus, wireless M-Bus, ZigBee, *Power Line Communication* (tzw. PLC-C band). Bardzo ważnym aspektem jest, aby dane pomiarowe wymieniane pomiędzy licznikiem AMI a siecią domową HAN były zabezpieczone, a komunikacja wykorzystywała techniki autentykacji i szyfrowania komunikacji. Należy pamiętać, że dane pomiarowe to informacja o zużyciu energii elektrycznej. Informacja ta powinna być chroniona przed dostępem osób niepowołanych.

Interfejs komunikacyjny stosowany w liczniku AMI w kierunku systemu odczytowego HES to najczęściej interfejs oparty o komunikację PLC (ang. PLC — *Power Line Communication*, tzw. PLC A-Band), BPL (ang. BPL — *BroadBand Power Line Communication*), GSM, RF (ang. RF — *Radio Frequency*).

W przypadku wykorzystywania komunikacji PLC lub BPL, komunikacja odbywa się po linii elektroenergetycznej niskiego napięcia, przy wykorzystaniu zdefiniowanych podnośnych częstotliwości. W tym modelu stosuje się urządzenia typu koncentrator do zarządzania grupą liczników. Koncentrator pośredniczy w zarządzaniu licznikami AMI, komunikuje system odczytowy HES z licznikami AMI. Jest instalowany na stacjach energetycznych SN/nN. Koncentrator dodatkowo rejestruje zdarzenia związane z jego pracą (nadzór urządzenia, zarządzanie systemem operacyjnym koncentratora, komunikacja do liczników i do systemu odczytowego, zarządzanie pamięcią, raportowanie alarmów, diagnostyka systemu operacyjnego). Istotnym jest, aby komunikacja od koncentratora do liczników AMI oraz od koncentratora do systemu odczytowego HES była szyfrowana oraz wykorzystywała narzędzia do autentykacji.

W przypadku wykorzystania sieci GSM, komunikacja odbywa się bezpośrednio pomiędzy licznikiem AMI a systemem odczytowym HES. Należy pamiętać, aby komunikacja ta była szyfrowana, a urządzenia podlegały mechanizmom autentykacji w systemie odczytowym HES.

System odczytowy HES stanowi centralną aplikację AMI, zarządzającą parkiem licznikowym AMI oraz koncentratorami.

TAURON Dystrybucja S.A. od ponad 10 lat wdraża systemy inteligentnego opomiarowania.

Największe projekty to rozwiązania oparte o komunikację PLC:

a) Instalacja w standardzie OSGP, łącznie 350 tys. liczników inteligentnych, zrealizowana w mieście Wrocław, pod nazwą AMIplus Smart City Wrocław,

b) Instalacja w standardzie DCSK, łącznie 21 tys. liczników inteligentnych, zrealizowana na Dolnym Śląsku (Oddział Opole, Oddział Legnica, Oddział Wałbrzych, Oddział Wrocław, Oddział Jelenia Góra),

c) Instalacja w standardzie IDIS, łącznie 15 tys. liczników inteligentnych, zrealizowana w Oddziale w Gliwicach

d) Instalacja w standardzie PRIME, łącznie 3 tys. liczników inteligentnych, zrealizowana w Oddziale w Tarnowie

TAURON Dystrybucja S.A. jako jedyna w Polsce, posiada zainstalowane na sieci inteligentne systemy, pracujące w różnych standardach komunikacji PLC, charakteryzujących się największą ilością wdrożeń w Europie, tj. PRIME, IDIS i OSGP. Pozwoliło to Spółce na zebranie doświadczeń w zakresie powyższych rozwiązań, w zakresie technicznym, funkcjonalnym jak również bezpieczeństwa poszczególnych rozwiązań.

Wdrożone systemy pozwoliły zmienić sposób pozyskiwania odczytów z liczników energii elektrycznej. Odczyty pozyskiwane są jako odczyt zdalny, bez konieczności udziału inkasenta. Zmienił się również sposób obsługi technicznej układów pomiarowych. Obecnie prace związane z obsługą techniczną układów pomiarowych wykonywane są również zdalnie, bez udziału służb monterskich. Pozwala to znacznie poprawić poziom obsługi klienta – obsługa odbywa się szybciej i sprawniej. Dla Spółki wdrożenie inteligentnego opomiarowania to oszczędność na kosztach obsługi lokalnej układów pomiarów.

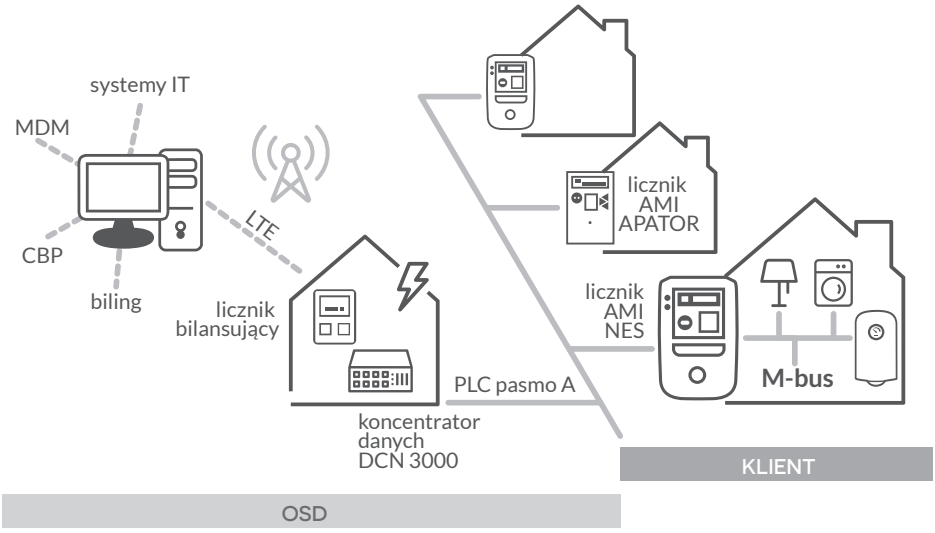
Równocześnie instalacje inteligentnego opomiarowania umożliwiają monitoring incydentów. Jest to realizowane za pomocą rejestracji zdarzeń (ang. *events*) przez licznik inteligentny jak również inne urządzenia tworzące infrastrukturę inteligentnego opomiarowania, np. koncentratory. Zdarzenia mogą mieć charakter zdarzeń spontanicznych i zdarzeń niespontanicznych. Zdarzenia spontaniczne to takie zdarzenia, które po wystąpieniu są przekazywane przez urządzenie do systemu odczytowego HES. Mają one najwyższy priorytet w komunikacji. Zdarzenia niespontaniczne to takie zdarzenia, które po wystąpieniu zapisywane są przez urządzenie w pamięci wewnętrznej i przekazywane do systemu odczytowego HES w trybie harmonogramu. **W kontekście cyberbezpieczeństwa, informacja o incydentach zarejestrowanych przez licznik inteligentny ma szczególne znaczenie. Stanowi ona bowiem dla operatora systemu odczytowego informację czy układ pomiarowy podlega próbom nieuprawnionej**

manipulacji oraz w jakim stanie pracy znajduje się układ pomiarowy. Wiedza ta pozwala na podejmowanie właściwych decyzji operacyjnych dla utrzymania systemu AMI w jak najbardziej optymalnych warunkach pracy.

Projekt AMIplus Smart City Wrocław

Największym wdrożeniem infrastruktury inteligentnego opomiarowania, gdzie spełniony jest warunek interoperacyjności liczników AMI, jest instalacja wykonana w mieście Wrocław – projekt AMIplus Smart City Wrocław. Jest to instalacja oparta o komunikację PLC w standardzie OSGP. Na sieci dystrybucyjnej zostały zainstalowane liczniki AMI dwóch producentów, NES oraz APATOR. Urządzenia potrafią komunikować się wzajemnie między sobą, a zastosowany standard OSGP spełnia wymóg interoperacyjności liczników AMI. Komunikacja pomiędzy urządzeniami jest szyfrowania kluczem 128 bitowym, dodatkowo uwierzytelnianie komunikacji realizowane jest przy pomocy kluczy. Ma to zasadnicze znaczenie, ponieważ chroni przed nieuprawnionym dostępem z zewnątrz do urządzeń jak również przed nieuprawnionym dostępem do danych pomiarowych. Na rys. 3 przedstawiono schemat rozwiązania AMIplus Smart City Wrocław.

Rys.3 Architektura rozwiązania AMIplus Smart City Wrocław



Komunikacja pomiędzy koncentratorem a systemem odczytowym HES oparta jest o sieć GSM pracującą w standardzie LTE. Ten kanał komunikacji jest również zabezpieczony, a komunikacja jest szyfrowana.

Dane pomiarowe z liczników AMI dostępne są dla klientów TAURON na platformie TAURON eLicznik. Platforma uruchamiana jest w trybie połączenia szyfrowanego, co zabezpiecza przed

nieuprawnionym dostępem do danych przez „przypadkowych" nasłuchujących. Platforma dostępna jest poprzez stronę internetową, jak również na urządzenia mobilne. Dodatkowo, TAURON Dystrybucja S.A. jako pierwszy OSD w Polsce w ramach instalacji AMIplus Smart City Wrocław udostępnił dla klienta dane pomiarowe w czasie rzeczywistym wprost z licznika energii elektrycznej wykorzystując interfejs wireless M-Bus zabudowany w liczniku. Usługa ta nosi nazwę HAN TAURON AMIplus. Aktywacja usługi następuję poprzez portal TAURON eLicznik. Po aktywacji usługi klient otrzymuje dedykowany numer do komunikacji oraz klucz uwierzytelniający.

Instalacja we Wrocławiu charakteryzuje się bardzo wysokimi współczynnikami odczytowymi, na poziomie 99,5%. Tak wysoki poziom stanowi również o bezpieczeństwie rozwiązania. Wysoki współczynnik odczytowy przedkłada się bowiem na dostępność do licznika. To umożliwia OSD na wprowadzanie nowych usług dla klientów, osiągnięcie celów w sposób bezpieczny dla wykonywanej działalności i świadczonych usług. Spółka ma zapewnioną możliwość zarządzania licznikami AMI oraz oferowania dodatkowych usług (np. przedpłata AMI) klientom z zachowaniem bezpieczeństwa procesów biznesowych.

Korzyści z wdrożenia rozwiązań inteligentnej infrastruktury pomiarowej

Wdrożenie rozwiązań AMI przynosi korzyści dla wielu interesariuszy, tj. Operator Systemu Dystrybucyjnego, Operator Systemu Przesyłowego, Klient, Sprzedawca. Dla Operatora Systemu Dystrybucyjnego system AMI to przede wszystkim skrócenie czasu pozyskiwania i przetwarzania odczytów z liczników energii elektrycznej. Dodatkowo system AMI dostarcza informacji o architekturze i topologii połączeń sieci dystrybucyjnej na nN. Informacja ta stanowi dodatkowe źródło danych dla zapewnienia bezpieczeństwa zarządzania i utrzymania systemu AMI, operator posiada bowiem wizualizację połączeń elektrycznych pomiędzy urządzeniami. Bezpośrednia komunikacja z licznikiem AMI to również ułatwienie procesu weryfikacji poprawności podłączeń układu pomiarowego, co ma istotne znaczenie przy coraz większym udziale i podłączaniu do sieci źródeł generacji rozproszonej. Informacje pomiarowe i zdarzeniowe pozyskane z liczników AMI umożliwiają wykonywanie szeregu analiz na poziomie aplikacji centralnej. Do najważniejszych zaliczyć można bilansowanie obwodów niskiego napięcia, co pozwala na ograniczenie nielegalnego poboru energii elektrycznej oraz ograniczenie strat handlowych. Te działania podnoszą bezpieczeństwo zarządzania siecią dystrybucyjną, operator dysponuje bowiem aktualną i wiarygodną informacją pomiarową i bilansową.

Odczyt liczników AMI kilka razy dziennie to również informacja dla operatora systemu dystrybucyjnego o wykorzystaniu sieci dystrybucyjnej, jaka moc jest pobierana w poszczególnych fragmentach sieci dystrybucyjnej. Ma to wpływ na decyzje związane z definiowaniem optymalnych punktów podziału sieci, weryfikację przyjętych współczynników jednoczesności. Licznik AMI umożliwia rejestrację napięć skutecznych, co umożliwia optymalizację poziomu napięć w sieci niskiego napięcia.

System AMI umożliwia Operatowi prowadzenie czynności obsługi układów pomiarowych bez konieczności wyjazdów związanych z eksploatacją układów pomiarowych (kontrole, zmiana taryfy, odczyty). Poza oszczędnościami na działalności operacyjnej, Operator prowadzi obsługę Klienta szybciej i skuteczniej w porównaniu do obsługi zwykłych liczników indukcyjnych i statycznych.

Poszczególne korzyści, zebrane jako całość, mają wpływ na zapewnienie bezpieczeństwa systemu elektroenergetycznego. To bezpieczeństwo należy rozumieć jako posiadanie poprawnej informacji pomiarowej, obrazującej stan pracy sieci dystrybucyjnej. Poprawna informacja pomiarowa pozwala podejmować działania po stronie operatora systemu, adekwatne do danej sytuacji. Należy jednak pamiętać, iż obsługa zdalna musi być realizowana z zachowaniem odpowiedniego poziomu wymaganych zabezpieczeń i ochrony systemu AMI. Dobre praktyki wskazują iż Operator Systemu Dystrybucyjnego powinien posiadać i stosować polityki bezpieczeństwa dla wdrożonych rozwiązań infrastruktury inteligentnego opomiarowania.

Bezpieczeństwo infrastruktury AMI na przykładzie wdrożenia AMIplus Smart City Wrocław

Obecnie budowane systemy AMI są zbiorem rozproszonej infrastruktury technicznej, aplikacji i technologii informatycznej oraz kanałów komunikacji funkcjonujących na warstwie sieciowej systemu dystrybucji energii elektrycznej. Pierwotną funkcjonalnością może jeszcze nie systemów AMI, ale systemów zdalnego odczytu pomiarów z liczników było pozyskanie w sposób zdalny danych o zużyciu energii elektrycznej u odbiorcy oraz przesłanie tych danych do baz danych OSD. Dynamiczny rozwój technik informatycznych oraz rozwój w obszarze technik transmisji danych z liczników spowodował, że oprócz aspektów związanych z pozyskaniem danych o zużyciu energii powstał obszar skupiający w sobie również szereg możliwości występujących na płaszczyźnie interakcji z klientem poprzez wykorzystanie dodatkowych funkcjonalności liczników inteligentnych AMI oraz funkcjonalności agregowanych w systemach AMI.

Pojawienie się w tym obszarze sieciowym OSD rozwiązań technicznych wspieranych przez techniki informatyczne oraz zdalną komunikację spowodowało konieczność przemodelowania podejścia do bezpieczeństwa systemów dystrybucji energii elektrycznej, z uwzględnieniem roli inteligentnych liczników AMI oraz systemów odczytowych AMI. Ważnym elementem z punktu widzenia bezpieczeństwa jest nie tylko bezpieczeństwo samych danych pomiarowych znajdujących się w liczniku czy w systemie i ich transmisja oraz przetwarzanie, ale również bezpieczeństwo techniczne i fizyczne urządzeń, co bezpośrednio przekłada się na bezpieczeństwo systemów Operatora Systemu Dystrybucyjnego i sieci dystrybucyjnej energii elektrycznej oraz bezpieczeństwo dostaw energii dla samego odbiorcy. Z punktu widzenia systemu odczytowego AMI ważne jest zapewnienie optymalnego poziomu bezpieczeństwa i warunków pracy systemu AMI, na takim poziomie, aby w sposób właściwy móc realizować zakładane funkcjonalności oraz otrzymywać korzyści z wdrożonego systemu, uzyskując oczekiwaną wydajność systemu.

Głównymi czynnikami rzutującymi na właściwy poziom bezpieczeństwa systemu jest zachowanie poufności, integralności i dostępności informacji; dodatkowo muszą być brane pod uwagę także inne czynniki takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, będące w bezpośrednim związku z aspektem działalności biznesowej OSD. W celu zapewnienia właściwego wysokiego poziomu bezpieczeństwa systemu AMI niezbędne jest zdefiniowanie spójnych, precyzyjnych reguł i procedur, według których należy już we wczesnej fazie zaprojektować mechanizmy, na bazie których budowane jest bezpieczeństwo. Na tak przygotowanym fundamencie, należy je następnie zbudować i zaimplementować oraz w całym cyklu użytkowania w sposób programowy eksploatować. Ważne jest, aby w tych działaniach opierać się na modelach bezpieczeństwa.

W ramach modelu przyjętego we wdrożeniu realizowanym przez TAURON Dystrybucja – AMIplus Smart City Wrocław znajduje się szereg elementów określających, które zasoby i w jaki sposób mają być chronione, zawierających sposoby bezpiecznego przetwarzania danych i udostępniania zasobów, wskazujących niezbędne kompetencje, środki organizacyjne i techniczne do tego potrzebne, a także ustanawiających obowiązki i odpowiedzialności.

Architektura systemu AMIplus zawiera dwa podstawowe modele implementacji technicznej dla których kryterium jest rodzaj wykorzystywanej przez licznik komunikacji. W pierwszym przypadku podstawowy model komunikacji pomiędzy licznikiem a koncentratorem danych odbywa się z wykorzystaniem technologii PLC a następnie w dalszej części poprzez sieć komórkową operatora telefonii komórkowej do serwerów Systemu AMI.

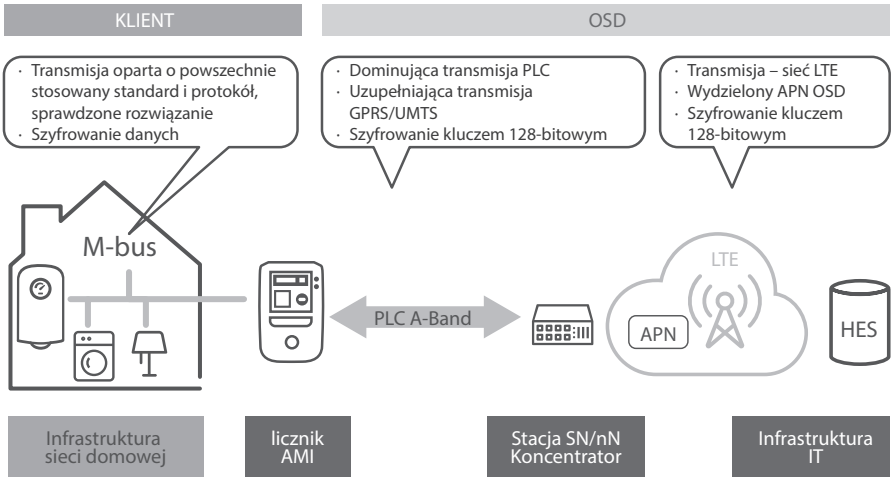
W drugim przypadku alternatywnym sposobem komunikowania się liczników AMI z systemem odczytowym HES jest transmisja poprzez sieć komórkową GSM operatora telefonii komórkowej. Liczniki AMI komunikujące się z w technologii GPRS, w warstwie sieci wykorzystują protokół IP, a w warstwie transportowej protokół TCP.

Funkcjonalności systemu zarówno w modelu z komunikacją PLC jak GPRS zapewniają realizację wszystkich usług systemu AMI w sposób tożsamy. Użycie oprócz podstawowego modelu komunikacji PLC drugiego rozwiązania czyli GPRS wymusza rozciągnięcie adaptację i przemodelowanie mechanizmów zapewniających bezpieczeństwo występujących dla sieci PLC na architekturę rozwiązania GPRS. Dodatkowym czynnikiem wpływającym na kształt modelu bezpieczeństwa jest zastosowanie na sieci jednofazowych i trójfazowych liczników energii elektrycznej pochodzących od dwóch producentów w technologii komunikacyjnej PLC i jednego producenta w technologii GPRS.

Na rysunku 5 została przedstawiona w sposób schematyczny architektura bezpieczeństwa systemu AMI zdekomponowana na płaszczyźnie implementacji technicznej. Zostały wyróżnione wszystkie komponenty techniczne oraz media komunikacyjne, przedstawiono podział na strefy – obszary aktywności klienta oraz OSD. W obu strefach znajdują się elementy

fizyczne oraz logiczne systemu AMI, dla których zostały opracowane polityki bezpieczeństwa. Urządzenia oraz komunikacja w obszarze bezpieczeństwa zostały zaprojektowane z uwzględnieniem wymagań cyberbezpieczeństwa sieci *smart metering*. Wszystkie zestawione tory komunikacyjne i urządzenia w obszarze klienta oraz OSD stanowią łańcuch bezpieczeństwa – komunikacja na każdym odcinku jest szyfrowana oraz uwierzytelniania. Zastosowane rozwiązanie w standardzie OSGP umożliwia ponadto wymianę kluczy bezpieczeństwa poszczególnych urządzeń.

Rys.5 Architektura bezpieczeństwa systemu AMI



Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 (Dyrektywa NIS) określa, że do dnia 8 listopada 2018 roku należy zdefiniować operatorów usług kluczowych. Do chwili obecnej nie jest ostatecznie wyartykułowane stanowisko operatorów systemów dystrybucyjnych w zakresie, czy jest uzasadnione i wymagane, aby włączać systemy AMI do usług kluczowych sektora energetycznego. Niezależnie od toczących się dyskusji w tym zakresie, TAURON Dystrybucja poczynił starania w tym kierunku, implementując w systemie AMIplus te zasady, które stanowią zapisy Dyrektywy w zakresie podstawowych wymagań dotyczących bezpieczeństwa. Uwzględniając wymagania Dyrektywy, TAURON Dystrybucja buduje wysoki bezpieczeństwa systemu AMI odpowiednio do istniejącego ryzyka uwzględniając następujące elementy:

- bezpieczeństwo systemów i obiektów;
- postępowanie w przypadku incydentu;
- zarządzanie ciągłością działania;
- monitorowanie, audyt i testowanie;
- zgodność z normami międzynarodowymi.

Możliwe cyberzagrożenia dla rozwiązań klasy AMI

Dokładna znajomość architektury systemu oraz zasady funkcjonowania jego elementów przy dostatecznym poziomie wiedzy technicznej jest elementem, który w zależności od użytych intencji może stać się czynnikiem skutecznie chroniącym bezpieczeństwo systemu bądź też skrajnym zagrożeniem dla jego bezpieczeństwa.

Jednym z głównych elementów funkcjonalnych systemów AMI wpływających na bezpieczeństwo krajowego systemu energetycznego jest możliwość zdalnego załączenia lub wyłączenia zasilania każdego odbiorcy posiadającego licznik AMI. Wyłączenie lub załączenie pojedynczego odbiorcy oczywiście nie jest w stanie w żaden sposób zakłócić bezpieczeństwa systemu energetycznego kraju, ale wykonując taką operację w jednym czasie na dużej ilości liczników taki wpływ niewątpliwie występuje. Jako element ochrony krajowego systemu energetycznego można wskazać również rozwiązania wykorzystujące usługę DSR (ang. *Demand Side Response*), zwiększające stabilność pracy krajowego systemu energetycznego, dla których podstawą działania są dane pomiarowe pozyskiwane z liczników AMI. Zakłócenie pracy licznika, komunikacji z systemem odczytowym lub samego systemu odczytowego może w sposób istotny zaburzyć realizację wspomnianych wyżej funkcjonalności i w sposób oczywisty przełoży się na bezpieczeństwo krajowego systemu.energetycznego.

Funkcjonowanie systemu AMI jest ściśle związane z technologią teleinformatyczną, która w powiązaniu z architekturą systemu rodzi względnie dużą płaszczyznę występowania podatności na czynniki zewnętrzne, jak również na zmiany, jakie dokonują się w otoczeniu systemu, naturalnie wymuszając budowę odpowiednio do występującego ryzyka – cyberbezpieczeństwa systemu AMI. Zagrożeniami mogą być zarówno możliwe usterki techniczne, błędy ludzkie, ale również zamierzone wrogie działania prowadzone w cyberprzestrzeni. **Z kilku powodów to właśnie ten ostatni rodzaj zagrożeń, mimo iż rzadki, jest brany pod uwagę jako zagrożenie realne z uwagi na doniosłość skutków, które może za sobą pociągnąć. Przedstawiając problem cyberbezpieczeństwa należy zdać sobie sprawę, że zakłócenie funkcjonowania pracy systemu AMI lub doprowadzenie do jego zatrzymania oraz zniszczenie danych mogą być efektem dokonania ataku na jego infrastrukturę.** Działania w cyberprzestrzeni cechują między innymi relatywnie niskie koszty przygotowania i przeprowadzenia ataku przy jednoczesnym dużym potencjale zadanych strat stronie zaatakowanej. Dodatkowo niewątpliwym atutem skłaniającym potencjalnych sprawców do takiego działania jest trudność wykrycia, udowodnienia winy i ukarania.

Nie wykluczając możliwości wystąpienia potencjalnych zagrożeń wynikających z zamierzonych działań destrukcyjnych związanych z wykorzystaniem technologii informatycznych, kluczowe pozostaje zapewnianie ochrony przed błędami, awariami technicznymi, błędami ludzkimi a także zagrożeniami o charakterze naturalnym. Bezpieczeństwo fizyczne urządzeń jest elementem często niedoszacowanym pod względem występującego ryzyka związanego z bezpieczeństwem systemów. Charakter tego zagrożenia jest

zgoła inny aniżeli zagrożeń z obszaru cyberbezpieczeństwa, ale w konsekwencji słabe zabezpieczenie fizyczne może stać się czynnikiem inicjalnym zagrożeń z obszaru cyberbezpieczeństwa lub komunikacji.

Wdrożenie systemu AMI w TAURON Dystrybucja S.A. zrealizowane zostało zgodnie z koncepcją *privacy by design*, z zachowaniem 7 podstawowych zasad:

- Podejście proaktywne zakładające przede wszystkim prewencję zdarzeń mogących naruszyć bezpieczeństwo;
- Bezpieczeństwo jest domyślnym stanem, który gwarantuje poszanowanie prywatności odbiorcom;
- Prywatność z założenia jest zintegrowana z podstawową usługą Systemu AMI już od momentu projektowania;
- Pełna funkcjonalność jest zapewniona poprzez dążenie do uwzględnienia prawnie uzasadnionych interesów i celów, w sposób zapewniający korzyści po obydwu stronach;
- System zapewniający prywatność na całej drodze komunikacji i wszystkich biorących w niej udział danych;
- Konstrukcja i zasady systemu są transparentne;
- Dobro odbiorcy jest w centrum zainteresowania i nie podlega kompromisom.

System, który z punktu widzenia cyberbezpieczeństwa jest bezpieczny, to nie tylko taki, który posiada rozbudowane mechanizmy ochrony teleinformatycznej, lecz także taki, który posiada zespół zdefiniowanych środków organizacyjnych i technicznych służących do odtworzenia systemu oraz uzyskania pełnej sprawności i wydajności technicznej po wystąpieniu awarii. W przypadku wystąpienia okoliczności, w wyniku których konieczne jest odtworzenie systemu lub jego naprawa, niezbędnym jest posiadanie przetestowanych na ten czas procedur awaryjnych które z założenia pozwolą na utrzymanie ciągłości działania systemu lub ograniczą skutki awarii. Procedury awaryjne mogą ograniczać wydajność systemu jak również ilość informacji przetwarzanych przez system jednak z zachowaniem podstawowych funkcjonalności systemu.

W ramach systemu AMI, analizując zakres możliwych zdarzeń, należy brać pod uwagę między innymi poniższe przypadki:

- Awaria pojedynczego węzła komunikacyjnego;
- Awaria pojedynczego serwera uczestniczącego w połączeniu;
- Awaria pojedynczego serwera uczestniczącego w realizacji usługi systemu HES;
- Awaria klastra VPN -load balancera systemu VPN;
- Awaria klastra serwerów usługowych systemu HES;
- Odtwarzanie zawartości serwerów/systemów na wypadek całkowitej utraty danych na nośnikach dyskowych – odtworzenie z systemu kopii zapasowych.

System AMI jest tak zbudowany i skonfigurowany, aby awaria pojedynczego elementu infrastruktury technicznej systemu nie powodowała zatrzymania całego systemu, może jedynie powodować spadek wydajności lub częściową utratę funkcjonalności.

Opisane przypadki nie zamykają wszystkich możliwych sytuacji, jakie są związane z wystąpieniem awarii systemu AMI, stanowią jednak źródło wiedzy i podstawę do analizy w związku z tworzeniem planów reakcji i odtwarzania. Kluczowym staje się określenie założeń do utworzenia redundantnego obszaru, na którym można w sposób systemowy odbudować usługi i funkcjonalności systemu, których awaria dotknęła. Przy tej okazji należy również wspomnieć o konieczności przeanalizowania parametrów SLA (*Service Level Agreement*) umów z kontrahentami, którzy udostępniają usługi sprzętowe, aplikacyjne i wsparcia, na których bazuje system AMI. Wartość parametrów SLA jest czynnnikiem w sposób bardzo ścisły powiązanym z czasem odtwarzania lub naprawy systemu lub czasem niezbędnym do odbudowy zakładanej wydajności systemu, co z kolei przekłada się na wymiar ekonomiczny zarówno po stronie kosztów – lepsze parametry SLA umów pociągają za sobą ich większe koszty, ale z drugiej strony stanowią pewną gwarancję i podstawę do założenia minimalizacji strat związanych z wystąpieniem awarii.

Audyt systemu AMI

Proces budowy w pełni funkcjonalnego a także bezpiecznego systemu nie kończy się wcale wraz z zakończeniem etapu wdrożenia, wręcz przeciwnie – zamknięcie etapu wdrożenia pokazuje jak problem cyberbezpieczeństwa był widziany oczami inżynierów konstruktorów i specjalistów budujących system. Należy zauważyć, że jest to grupa osób posiadająca bardzo dużą wiedzę oraz wysokie kompetencje i kwalifikacje w obszarze swojego działania, znająca doskonale rozwiązania branżowe i regionalne występujące w ramach wdrażanych rozwiązań. Oczywiste jest zatem przypuszczenie, że produkt będący wytworem ich wysiłku, z jednej strony spełnia wszystkie wymagania funkcjonalne i użytkowe stawiane na etapie projektowania systemu, a z drugiej stanowi produkt najwyższej jakości w sensie technicznym.

Niemniej jednak, zmienność warunków towarzysząca wdrożeniu skłania ku temu, aby dokonać weryfikacji i sprawdzenia skuteczności zaprojektowanych i wdrożonych rozwiązań. Oczywiście podstawą oceny w momencie zakończenia wdrożenia są testy odbiorowe potwierdzające spełnienie wymagań postawionych na etapie projektowania i budowy systemu, ale nie rzadko bywa tak, że wyartykułowane wymagania nie pokrywają wszystkich występujących podatności systemu, mowa oczywiście o podatnościach, które nie zostały zidentyfikowane i odkryte na etapie tworzenia projektu i systemu. Skutecznym narzędziem adekwatnym do zakresu, w jakim chcemy dokonać weryfikacji systemu pod kątem bezpieczeństwa i odkrycia jego podatności potencjalnie rzutujących na nie jest audyt bezpieczeństwa. Z założeń, jakie należy przyjąć przy działaniach związanych z przygotowaniem audytu jest w głównej mierze udzielenie sobie odpowiedzi na pytanie czy ten moment jest właściwy na przeprowadzenie audytu. Pytanie z pozoru banalne, ale bardzo istotne, gdyż audyt należy przeprowadzić na wdrożonym i stabilnym systemie, bo tylko wówczas będzie można uzyskać miarodajną i precyzyjną odpowiedź na temat obszarów i rozmiarów, na których dane podatności występują oraz jakie są ich rodzaje. Przy planowaniu audytu bezpieczeństwa systemu warto posiłkować się mapą ryzyka systemu w celu zidentyfikowania i określenia obszarów największego oddziaływania skutków zmaterializowanych ryzyk na system, a tym samym na obszar biznesowy, który jest przez niego wspierany.

Przeprowadzenie samego audytu nie rozwiązuje jeszcze żadnej kwestii związanej z bezpieczeństwem, stanowi jednak pole informacji do przeprowadzenia dalszych działań, które finalnie mają podnieść poziom bezpieczeństwa. Najbardziej korzystnym, wydajnym oraz skutecznym sposobem na odniesienie się do zidentyfikowanych luk bezpieczeństwa jest w pierwszym etapie skupienie się na najprostszych do wyeliminowania podatnościach o wysokim ryzyku. W dalszej kolejności, gdy te zostaną złagodzone, wówczas należy się skupić na pozostałych, bardziej złożonych. W każdym przypadku należy oceniać je poprzez przyłożenie na mapę ryzyka. Klasyfikacja podatności poprzez dokonanie ich miary na mapie ryzyka daje zsyntetyzowaną informację na temat krytyczności danych zasobów, na których odkryta podatność występuje. Kolejnym elementem, który powinien być w sposób precyzyjny przedstawiony po audycie jest zbiór środków przeciwdziałających wystąpieniu awarii. Może to być zestaw precyzyjnie dobranych i dedykowanych środków technicznych, ale też często występujące zalecenie wprowadzenia zmian na poziomie operacyjnym niezwiązanym z techniką.

Niezmiernie ważną rzeczą jest wypracowanie, w oparciu o posiadaną wiedzę poaudytową, procedur funkcjonowania systemu w czasie trwania i po usunięciu awarii, jak również sposobów identyfikacji wczesnych symptomów awarii, które nie od razu są widoczne i dają zauważalne skutki. W zakresie rekomendacji po przeprowadzonym audycie należy skupić się na dwóch fragmentach, które będą wymagały dalszego działania, a mianowicie na fragmencie opisującym zestaw środków przeciwdziałających wystąpieniu awarii oraz na fragmencie dotyczącym procedur przywrócenia funkcjonalności systemu po awarii. Jeżeli w przypadku określonej podatności środki przeciwdziałające wystąpieniu awarii w stu procentach eliminują ryzyko bądź czynniki powodujące wystąpienie tego ryzyka, wówczas oczywiście nie ma konieczności definiowania procedur przywrócenia funkcjonalności systemu po awarii powstałej z powodu wystąpienia tej podatności.

Operacyjnym narzędziem do utrzymania właściwego poziomu funkcjonowania systemu AMI również na polu cyberbezpieczeństwa jest przegląd okresowy systemu. O ile audyt z reguły jest wykonywany przez zespól niezależnych ekspertów to przeglądy okresowe powinny być realizowane przez zespół osób prowadzących eksploatację systemu. Podstawowa różnica pomiędzy audytem a przeglądem okresowym polega na określeniu elementów które będą badane oraz na przyjętej metodyce tego działania. Audyt jest formą spontaniczną wynikającą bezpośrednio z postawy samego audytora, która jest pochodną jego wiedzy i doświadczenia, przegląd okresowy zaś jest formą sprowadzoną do wcześniej zdefiniowanej procedury w ramach której dokonuje się tego badania. Rola badających w przeglądzie okresowym sprowadza się do przeprowadzenia danej procedury. Dodatkowym elementem różnicującym audyt od przeglądu okresowego jest precedensowośc audytu tzn. w wyniku audytu spodziewamy się odkrycia nowych podatności, natomiast przegląd okresowy sprawdza jedynie funkcjonowanie już zaimplementowanych mechanizmów, które powstały na bazie wcześniej odkrytych podatności.

Zarówno w ramach audytu jak i przeglądu okresowego możemy definiować obszary które będziemy poddawać badaniu. Takie wycinkowe podejście warunkuje bezpośrednio kompetencje i kwalifikacje osób prowadzących te działania.

Wnioski

System AMI stanowi bardzo ważny element w obszarze bezpieczeństwa energetycznego kraju. Rola systemu AMI w prowadzeniu ruchu sieci dystrybucyjnej oraz dostaw energii do klientów i jej rozliczenia jest bardzo istotna. Informacja pomiarowa pozyskiwana z urządzeń infrastruktury AMI wpływa bezpośrednio na procesy biznesowe i działania operacyjne operatora systemu dystrybucyjnego, w obszarze obsługi klienta, rozliczeń, sterowania odbiorami, wprowadzania programów klasy DSR. Bezpieczeństwo systemu AMI bardzo mocno zależy od tego, w jaki sposób zabezpieczone zostały poszczególne warstwy komunikacji Sieć domowa HAN – licznik AMI, Licznik AMI – koncentrator, koncentrator – system odczytowy HES) oraz w jaki sposób zostały zabezpieczone pojedyncze urządzenia. **Projektując system AMI, należy zwrócić uwagę na opracowanie, wdrożenie i stosowanie polityk bezpieczeństwa. Polityki powinny obejmować cały zakres i obszar stosowania infrastruktury AMI. Polityka powinna również określać zachowania i reakcje wskutek zdarzeń możliwych do wystąpienia w pracy systemu. System AMI, poprzez możliwość zdalnego odłączenia licznika energii elektrycznej, ma wpływ na pracę systemu elektroenergetycznego, na jego równowagę pracy. Ten obszar funkcjonalny systemu AMI musi być objęty specjalnym nadzorem oraz regułami.**

Bezpieczeństwo systemu AMI to również procedury i polityki w obszarze utrzymania w warstwie IT. Redundancja zasobów, procedury odtwarzania, szybkość reakcji służb serwisowych jak również czas reakcji dostawcy rozwiązania mają bardzo istotny wpływ na bezpieczeństwo realizacji procesów biznesowych OSD.

Bardzo ważny element systemu AMI to komunikacja, stanowiąca podstawę dostępu do informacji pomiarowej oraz do urządzenia. Należy zatem stosować rozwiązania charakteryzujące się wysokim stopniem odporności na zakłócenia przewodzone i zakłócenia radiowe. Obszar ten powinien też być objęty monitoringiem sygnalizującym stany pracy poprawnej i niepoprawnej.

System AMI to również narzędzie i infrastruktura umożliwiająca wprowadzanie programów związanych z ograniczeniem poboru mocy przez klientów. W Europie są stosowane programy DSR, które w określonych warunkach pracy systemu elektroenergetycznego przywołują klientów do podjęcia działań dla ograniczenia poboru mocy. System AMI pośredniczy tutaj w przekazaniu informacji pomiędzy operatorem a klientem. Po stronie klienta obsługę tego typu komend DSR przejmują rozwiązania sieci domowej HAN, sterującej elektryczną infrastrukturą domową. Dla systemu elektroenergetycznego programy DSR stanowią zwiększenie bezpieczeństwa i poprawę stabilności, w szczególności w zakresie zabezpieczenia przed *blackoutami*.

Autorzy

Kaja Ciglic

Jako członek zespołu *Government Security Policy and Strategy Team w Microsoft*, Kaja Ciglic jest odpowiedzialna za wprowadzanie strategicznych zmian, zarówno w firmie jak i poza nią, mających na celu rozwój cyberbezpieczeństwa. Kaja, wykorzystując swoje doświadczenie, mierzy się z wyzwaniami związanymi z szeroko pojętą obroną infrastruktury krytycznej, wliczając w to zarządzanie ryzykiem strategicznym i operacyjnym, wymianę informacji, reagowanie na incydenty oraz bezpieczeństwo i integralność oprogramowania.

Przed dołączeniem do Miscrosoft, Kaja Ciglic prowadziła sekcję technologiczną w APCO Worldwide w Seattle, gdzie zarządzała oddziałem ds. relacji publicznych i komunikacji. Wcześniej obejmowała pozycje dyrektora biura APCO Worldwide w Brukseli. Była odpowiedzialna zapaneuropejskie kampanie skierowane na wyzwania regulacyjne i antytrustowe.

Mariusz Jurczyk

Doradca Zarządu, TAURON Dystrybucja Pomiary sp. z o.o.

Absolwent Wydziału Elektrycznego Politechniki Częstochowskiej (specjalność elektroenergetyka). Mariusz Jurczyk rozpoczął pracę zawodową w roku 2000 w Zakładzie Energetycznym Częstochowa S.A. od projektowania sieci energetycznych, następnie kilka lat pracował w pionie obrotu energią elektryczną (rynek bilansujący, kontrakty bilateralne, giełda energii, prognozowanie).

Od roku 2004 w ENION S.A., a następnie od roku 2009 jako Kierownik Wydziału Pomiarów w TAURON Dystrybucja Oddział w Częstochowie zajmował się pomiarami (wdrożenie i rozwój systemu zarządzania pomiarami Operatora Pomiarów). W roku 2013 objął stanowisko Kierownika Projektu AMI w TAURON Dystrybucja S.A. Obecnie pracuje na stanowisku Doradca Zarządu ds. Inteligentnej Infrastruktury Pomiarowej w TAURON Dystrybucja Pomiary sp. z o.o.

W 2007 r. Mariusz Jurczyk otrzymał nagrodę na konferencji European Electricity Market, za najlepszy referat dla doktorantów. Uczestniczył w wielu konferencjach branżowych.
Jest członkiem Zespołu PTPiREE dot. Smart Metering, Cyberbezpieczeństwo AMI, Polskiego Komitetu Normalizacyjnego – KT 304 ds. Aspekty Techniczne Dostaw Energii Elektrycznej oraz Grupy Roboczej ds. inteligentnych sieci energetycznych przy Głównym Urzędzie Miar. Aktywnie uczestniczy w krajowych pracach nad Smart Meteringiem oraz cybersecurity AMI organizowanych m.in. przez Urząd Regulacji Energetyki oraz PTPiREE.

Agnieszka Konkel

Radca Ministra w Ministerstwie Cyfryzacji RP

Pani Agnieszka Konkel pracowała w Parlamencie Europejskim w latach 2012–2015 w Sekretariacie Komitetu Ochrony Rynku Wewnętrznego i Konsumentów, gdzie była współodpowiedzialna za negocjacje dyrektywy NIS oraz ogólnych zapisów strategii jednolitego rynku cyfrowego. Wcześniej kierowała polską prezydencją w Radzie UE, pracując dla Stałego Przedstawicielstwa Rzeczypospolitej Polskiej przy Unii Europejskiej. W Fundacji Rozwoju Społeczeństwa Informacyjnego, pani Agnieszka uczestniczyła w odnoszącym duże sukcesy Programie Rozwoju Bibliotek, realizowanym w partnerstwie z Fundacją Billa i Melindy Gatesów. Obecnie, pani Agnieszka piastuje stanowisko Radcy Ministra w Ministerstwie Cyfryzacji RP.

Izabela Lewandowska-Wiśniewska

Koordynator, PZU Lab

Absolwentka Wydziału Inżynierii Chemicznej i Procesowej, Politechniki Warszawskiej, Specjalizacja: Inżynieria Chemiczna i Procesowa. Absolwentka studiów podyplomowych „Bezpieczeństwo procesów przemysłowych" – Politechniki Łódzkiej, Studiów podyplomowych, „Bezpieczeństwo i ochrona człowieka w środowisku pracy" – CIOP, Autoryzacja techniczna – UDT w zakresie bezpieczeństwa procesowego, Wdrożeniowiec, Pełnomocnik, Trener i Audytor systemów zarządzania związanych z szeroko pojętym bezpieczeństwem, środowiskiem, jakością, CSR, PSM, IWAY, EMAS, OHSAS, AQAP, zarządzania ryzykiem i cyberbezpieczeństwem. Specjalista zarządzania projektami w zakresie bezpieczeństwa technicznego PSM, cyberbezpieczeństwa, rozwiązań systemowych dla klientów biznesowych oraz projektów innowacyjnych, w zakresie Infrastruktury Krytycznej, ZZR i ZDR, analiz dotyczących zarządzania ryzykiem (Hazop, FMEA, LOPA, PHA, ATEX), ciągłości działania. Expert Bezpieczeństwa i BHP z wieloletnim doświadczeniem w zakresie działań prewencyjnych i rozwiązań systemowych dotyczących bezpieczeństwa w wielu sektorach min, w sektorze przemysłowym, logistycznym, wojskowym. W PZU Lab między innymi koordynuje projekt „Cyber Industry". Obecnie Koordynator – Starszy Inżynier Ryzyka PZU Lab.

Dariusz Mikołajczyk

Dyrektor Biura Bezpieczeństwa, PKP Energetyka S.A.

Absolwent Wydziału Prawa i Administracji UAM w Poznaniu oraz studiów doktoranckich na Wydziale Prawa i Administracji UW. Certyfikowany przez służby bezpieczeństwa państwa administrator bezpieczeństwa teleinformatycznego oraz w IRCA audytor wiodący normy ISO/IEC 27001 System Zarządzania Bezpieczeństwem Informacji. Od 2000 r. zajmuje się szeroko rozumianym bezpieczeństwem. Odpowiadał za ochronę informacji niejawnych, danych osobowych oraz informacji stanowiących tajemnicę przedsiębiorstwa w tym za ich ochronę w systemach teleinformatycznych. W latach 2006 – 2009 odpowiedzialny m.in. za bezpieczeństwo fizyczne, teleinformatyczne oraz informacyjne w Holdingu UNIPETROL w Republice Czeskiej. Obecnie Dyrektor Biura Bezpieczeństwa PKP Energetyka S.A. odpowiedzialny min. za bezpieczeństwo teleinformatyczne.

Krzysztof Podwiński

Zastępca Kierownika Projekt AMI, Kierownik Zespołu Bezpieczeństwa AMI, TAURON Dystrybucja S.A.

Absolwent Akademii Ekonomicznej we Wrocławiu (specjalność Informatyka i Ekonometria) oraz Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości. Krzysztof Podwiński rozpoczął pracę zawodową w roku 1986 w Zakładzie Energetycznym Wałbrzych S.A., w obszarze telekomunikacji i łączności.

Od roku 2004 w ENERGIA PRO S.A., jako Specjalista ds. telekomunikacji, zajmował się zagadnieniami łączności radiowej, eksploatacją urządzeń radiokomunikacyjnych, bezpieczeństwem rozwiązań. W roku 2013 objął stanowisko Starszego Specjalisty w Biurze Planowania i Rozwoju Teleinformatyki TAURON Dystrybucja S.A. Obecnie pracuje na stanowisku Kierownik Zespołu Bezpieczeństwa AMI w Projekcie AMI TAURON Dystrybucja S.A.

W latach 1997–2003 brał czynny udział w realizacji dużego projektu pn. „Budowa radiowej sieci łączności dyspozytorskiej DIGICOM7" oraz systemu telekomunikacyjnego HiPath.

Jest członkiem Zespołu PTPiREE dotyczącym Cyberbezpieczeństwa rozwiązań Smart Grid, w tym również rozwiązań AMI.

Jarosław Sordyl

Zastępca Dyrektora ds. Cyberbezpieczeństwa, CERT PSE, Departament Bezpieczeństwa, PSE

Wieloletni konsultant w zakresie bezpieczeństwa systemów teleinformatycznych, ekspert Informatyki Śledczej oraz eDiscovery, Lead Auditor Systemów Zarzadzania Bezpieczeństwem Informacji – ISO/IEC 27001, a także Certified Lead Penetration Tester. Wykładowca współpracujący na co dzień z instytucjami szkoleniowymi, akademickimi oraz jednostkami naukowymi w zakresie tematów związanych z bezpieczeństwem IT. Do 2014 roku członek Zarządu Europou, przedstawiciel Polski na forum Szefów Krajowych

Jednostek Europolu, członek grup roboczych Zarządu Europolu ds. IT i korporacyjnych. Produkt Menadżer oraz trener systemów informacyjnych Europolu. Były Szef Krajowej Jednostki Europolu w Biurze Międzynarodowej Współpracy Komendy Głównej Policji. Od ponad 18 lat zajmuje się problematyką bezpieczeństwa IT i cyberprzestępczości, m.in. w ramach międzynarodowej współpracy organów ścigania. Posiada wiele certyfikatów związanych z bezpieczeństwem teleinformatycznym m.in.: CISSO, CDFE, CPTE, CDRE, ISO 27001 – Lead Auditor, ISO 27002 – Lead Implementer, CLPT – Certified Lead Penetration Tester, ISO 37001 Lead Implementer. Równocześnie posiadacz certyfikacji – MCP: Microsoft Certified Profession. Członek stowarzyszeń specjalistów organów ścigania "Computer Forensics – IACIS" oraz członek HTCIA – High Technology Crime Investigation Association. Ukończył Akademię Interpolu – IP Crime Investigators.

Marcin Spychała

Architekt Cyberbezpieczeństwa, Polska & Kraje Bałtyckie, IBM

Marcin Spychała jest doświadczonym ekspertem ds. cyberbezpieczeństwa, pracującym dla IBM Security Practice. Przez ostatnie lata był odpowiedzialny za projektowanie rozwiązań z zakresu bezpieczeństwa teleinformatycznego. W swojej pracy łączy praktyczną wiedzę na temat hackingu z dobrym rozpoznaniem realnych zagrożeń dotykających klientów IBM.

Interesuje się inżynierią społeczną, której zasady często demonstruje podczas wystąpień na konferencjach i pokazach hakerskich. Marcin posiada również znaczącą wiedzę na temat regulacji prawnych w zakresie ochrony danych osobowych i oraz legislacji dotyczącej cyberbezpieczeństwa w krajach UE.

Yitzhak (Itzik) Vager

Wiceprezes ds. Zarządzania Produktem i Rozwoju Biznesu,
Verint Cyber Security Solutions

Yitzhak (Itzik) Vager jest wiceprezesem departamentu ds. Zarządzania Produktem i Rozwoju Biznesu w Verint Cyber Security Solutions. Przez ostatnie 18 lat w firmie, Itzik wykorzystywał swoją wiedzę z zakresu cyberbezpieczeństwa, technologii sieciowych oraz Big Data na różnych, wyższych stanowiskach związanych z biznesem i technologiami. Przed dołączeniem do Verint, przez 11 lat odbywał służbę w Korpusie Wywiadu Armii Izraelskiej, gdzie obejmował szereg pozycji związanych z inżynierią oraz dowództwem. Do jego obowiązków należało zarządzanie wielkimi, nowoczesnymi, multi-dyscyplinarnymi projetkami.

Itzik posiada dyplom inżyniera *cum laude* z Technion Institute of Technology.

Leonid Rozenblum

Architekt Systemów Cyberbezpieczeństwa, Israel Electric Co.

Leonid Rozenblum jest Architektem Systemów Cyberbezpieczeństwa w Israeli Electric Co. (IEC). Przez ostatnie 17 lat w firmie, wykorzystując swoją ekspertyzę z zakresu planowania i monitorowania infrastruktury cyberbezpieczeństwa oraz szacowania cyber--ryzyka w kontekście IT i OT, Leonid przewodził projektom związanym z cyberbezpieczeństwem.

Leonid jest absolwentem Kazan Aviation Institute, gdzie zdobył tytuł magistra cum laudez inżynierii radiowo-elektornicznej.

Robert Żelechowski

Naczelnik Wydziału Bezpieczeństwa Teleinformatycznego

Biuro Bezpieczeństwa, PKP Energetyka S.A.

Absolwent informatycznych studiów inżynierskich i magisterskich Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych w Warszawie na kierunku robotyka i systemy wieloagentowe. W PKP Energetyka pracuje od 2001 roku kreując i rozwijając od podstaw infrastrukturę teleinformatyczną. Zbudował struktury organizacyjne IT tworząc Biuro Informatyki. Stanowisko dyrektora biura IT obejmował do roku 2015. Obecnie w Grupie PKP Energetyka kieruje nowoutworzoną komórką ds. bezpieczeństwa teleinformatycznego. Odpowiada m.in. za kreowanie standardów bezpieczeństwa IT i automatyki przemysłowej na poziomie organizacyjnym oraz technicznym, rozwój i utrzymanie infrastruktury bezpieczeństwa oraz budowę zespołu reagowania na incydenty.

Partnerzy publikacji

IBM

Jedyny koncern informatyczny na świecie o ponad 100-letniej tradycji, obecny w Polsce od ponad 25 lat. Obecnie na świecie zatrudnia 380 tys. osób w ponad 170 krajach, zajmujących się głównie usługami doradczymi i informatycznymi oraz tworzeniem oprogramowania. W ubiegłym roku IBM zarejestrował ponad 8 tysięcy nowych rozwiązań patentowych i od 24 lat jest światowym liderem w tej dziedzinie. Bazując na projektach wykorzystujących zaawansowaną analitykę biznesową i pierwsze systemy poznawcze, m.in. IBM Watson, IBM powołał pierwszy na rynku dział usług biznesowych, koncentrujący się na wdrażaniu rozwiązań kognitywnych.

Microsoft

Jest wiodącym dostawcą platformy technologicznej i usług zwiększających produktywność. W myśl strategii „Cloud First. Mobile First", Microsoft tworzy rozwiązania wykorzystujące potencjał mobilności i chmury obliczeniowej, które pozwalają każdemu użytkownikowi i organizacji działać sprawniej i osiągać więcej. Microsoft Corporation powstał w 1975 roku w USA, a polski oddział firmy istnieje od 1992 r. W swoich filiach na całym świecie Microsoft zatrudnia blisko 110 tys. specjalistów z różnych dziedzin, w tym około 500 osób w Polsce.

PKP Energetyka

PKP Energetyka S.A. to jeden z czołowych dostawców energii elektrycznej i usług elektroenergetycznych w Polsce. Właścicielem PKP Energetyka jest fundusz CVC Capital Partners.
Spółka prowadzi działalność w zakresie sprzedaży i dystrybucji energii elektrycznej, usług elektroenergetycznych, sprzedaży paliw płynnych dla pojazdów szynowych oraz budowy i modernizacji infrastruktury najwyższych napięć. PKP Energetyka S.A. posiada własną sieć dystrybucyjną energii elektrycznej na terenie całej Polski. PKP Energetyka S.A. zatrudnia obecnie ponad 5 800 osób. Od stycznia 2016 r. spółka jest oficjalnym członkiem UN Global Compact.

Polskie Sieci Elektroenergetyczne

Jesteśmy operatorem elektroenergetycznego systemu przesyłowego w Polsce. Naszym celem jest zapewnienie niezawodnej pracy sieci przesyłowej i dostaw energii elektrycznej do wszystkich regionów kraju. Świadczymy usługi w oparciu o zasady TPA – równego dostępu do infrastruktury sieciowej oraz z poszanowaniem środowiska naturalnego.
Jesteśmy właścicielem ponad 14 000 km linii oraz 106 stacji elektroenergetycznych najwyższych napięć. Odpowiadamy za utrzymanie, eksploatację i rozwój systemu przesyłowego, co ma bezpośredni wpływ na bezpieczeństwo energetyczne Polski. Należymy do Europejskiej Sieci Operatorów Systemów Przesyłowych Energii Elektrycznej ENTSO-E – stowarzyszenia zrzeszającego 43 operatorów systemów przesyłowych z 36 krajów.

Więcej na: www.pse.pl

PZU

Jest największą grupą finansową w Polsce oraz Europie Środkowo-Wschodniej. Tradycje PZU sięgają 1803 roku, kiedy powstało pierwsze na ziemiach polskich towarzystwo ubezpieczeniowe. Obecnie PZU prowadzi działalność w zakresie ubezpieczeń, zdrowia, inwestycji, bankowości i finansów zapewniając kompleksową ochronę oraz dostarczając najwyższej jakości usług we wszystkich najważniejszych dziedzinach życia prywatnego, publicznego i gospodarczego.

TAURON Polska Energia SA

Jest spółką holdingową w grupie kapitałowej, która zajmuje się wydobyciem węgla, wytwarzaniem, dystrybucją i sprzedażą energii. Grupa TAURON obejmuje swoim działaniem 18 proc. powierzchni kraju i jest jednym z największych podmiotów gospodarczych w Polsce, w tym największym dystrybutorem oraz drugim sprzedawcą i wytwórcą energii elektrycznej. W skład Grupy TAURON wchodzą m.in. TAURON Wytwarzanie, TAURON Dystrybucja, TAURON Sprzedaż, TAURON Obsługa Klienta, TAURON Wydobycie, TAURON Ekoenergia oraz TAURON Ciepło. Od 2010 roku akcje TAURON Polska Energia SA notowane są na Giełdzie Papierów Wartościowych w Warszawie m.in. w indeksach WIG20 i WIG30. Spółka wchodzi w skład indeksu spółek odpowiedzialnych społecznie – RESPECT Index.

Verint

Światowy lider rozwiązań Actionable Intelligence®, redefiniuje sposób, w jaki organizacje walczą z cyberzagrożeniami. Verint Threat Protection System (TPS) firmy Verint to rozwiązanie przeznaczone dla centrów SOC, które zostało przygotowane w celu przyśpieszenia analizy potencjalnych incydentów poprzez automatyzację procesu analizy.

www.verint.com/cyber.

O WYDAWCY

Instytut Kościuszki — think tank kreujący nowe idee dla Polski i Europy – jest niezależnym, pozarządowym instytutem naukowo-badawczym o charakterze non-profit, założonym w 2000 r. Instytut Kościuszki opierając się na pogłębionej, interdyscyplinarnej analizie, propaguje rozwiązania w postaci rekomendacji programowych i ekspertyz, których odbiorcami są instytucje unijne, rządowe i samorządowe, polscy i europejscy politycy i decydenci, a także media, przedsiębiorcy oraz pasjonaci niezależnej myśli i otwartej debaty.

www.ik.org.pl

Partnerzy:

ISBN: 978-83-63712-32-7

INSTYTUT KOŚCIUSZKI