Przegląd Bezpieczeństwa Wewnętrznego

2025, nr 32, s. 97–117

 https://doi.org/10.4467/20801335PBW.25.005.22171

ARTYKUŁ

Cyberbezpieczeństwo w sektorze energetyki morskiej i okołomorskiej Rzeczypospolitej Polskiej

Cybersecurity in the offshore and coastal energy sector of the Republic of Poland

DAVID CYBULSKI

Autor niezależny

https://orcid.org/0009-0003-9195-4407

Abstrakt Celem artykułu jest omówienie poziomu cyberbezpieczeństwa polskiej energetyki morskiej i okołomorskiej w kontekście planowanych strategicznych projektów energetycznych. Autor przedstawił wybrane cyberataki na elementy sektora energetycznego innych państw, a także omówił, m.in. na podstawie *Polityki energetycznej Polski do 2040 r.*, planowane przez Polskę działania związane z infrastrukturą energetyczną w rejonie Morza Bałtyckiego. Wskazał zagrożenia dla polskiego sektora energetyki morskiej i okołomorskiej, do których należy działalność grup APT i grup sponsorowanych przez państwo, rywali biznesowych, haktywistów. Przedstawił stosowane sposoby ochrony tej infrastruktury oraz propozycje zabezpieczenia planowanych inwestycji przed atakami teleinformatycznymi.

Słowa kluczowe cyberbezpieczeństwo, cyberataki, grupy APT, energetyka, sektor energetyczny

Abstract

The purpose of the article is to discuss the level of cybersecurity of Poland's offshore and coastal energy sector in the context of planned strategic energy projects. The author presented selected cyberattacks on elements of other states' energy sector, he also discussed, among other things, on the basis of *Energy Policy of Poland until 2040*, Poland's planned activities related to energy infrastructure in the Baltic Sea region. He identified threats to Poland's offshore and coastal energy sector, which include: the activities of APT groups and state-sponsored groups, business rivals and hacktivists. He presented the methods used to protect this infrastructure as well as proposals for securing planned investments against ICT attacks.

Keywords

cybersecurity, cyberattacks, APT groups, energetics, energy sector

Wprowadzenie

W związku ze stale rosnącą digitalizacją w społeczeństwie niezbędny jest ciągły rozwój posiadanych mocy wytwarzania energii elektrycznej. Decydenci, świadomi konieczności modernizacji istniejącej infrastruktury energetycznej państwa, dostosowania się do regulacji unijnych[1] oraz spodziewanego wzrostu zapotrzebowania państwa na energię elektryczną, podjęli działania mające określić długofalowe cele strategiczne i projekty dla sektora energetycznego. Stworzono plan rozwoju energetyki państwa polskiego w postaci *Polityki energetycznej Polski do 2040 r.* (dalej: PEP2040).

Działania ofensywne na Morzu Bałtyckim, wymierzone np. w gazociągi Nord Stream 1 i Nord Stream 2[2], kabel telekomunikacyjny C-Lion 1 czy połączenie elektroenergetyczne EstLink 2, ukazują, jak w obecnych czasach jest zagrożone bezpieczeństwo infrastruktury energetycznej[3]. Dążenie do rozwoju narodowych projektów energetycznych na północy Polski oraz w jej wyłącznej strefie ekonomicznej zwiększa stopień informatyzacji zasobów sektora energetycznego. Potęguje

[1] *Polityka energetyczna Polski do 2040 r.*, Ministerstwo Klimatu i Środowiska, Warszawa 2021, s. 3–4.

[2] W. Lorenz, S. Zaręba, *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2*, Polski Instytut Spraw Międzynarodowych, 29 IX 2022 r., https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [dostęp: 16 VII 2025].

[3] K. Buchholz, *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025 r., https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [dostęp: 16 VII 2025].

możliwości oddziaływania przeciwnika na infrastrukturę teleinformatyczną polskiej energetyki. W związku z tym konieczna jest weryfikacja stanu cyberbezpieczeństwa w rozwijającym się polskim sektorze energetyki morskiej i okołomorskiej, jak również odpowiedź na pytanie, w jakim stopniu jest on odporny na zagrożenia.

Jednym ze sposobów prowadzenia polityki wywierania wpływu przez przestępców, w tym terrorystów, oraz podmioty prawa międzynarodowego (państwa) stało się ich oddziaływanie w sposób pośredni lub bezpośredni na sektor energetyczny drugiej strony, będący tzw. celem o wysokiej wartości (ang. *high-value target*). Atak, w tym teleinformatyczny, który doprowadzi do zaprzestania produkcji i dystrybucji określonego zapotrzebowania energetycznego, może spowodować czasową lub trwałą niezdolność do funkcjonowania państwa. W celu mitygacji ryzyka polski ustawodawca zdecydował się, na podstawie art. 3 pkt. 2 lit. a *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, na zaliczenie systemów zaopatrzenia w energię, surowce energetyczne i paliwa do infrastruktury krytycznej (IK). Ustawa o zarządzaniu kryzysowym nakłada na operatorów IK określone obowiązki mające zapewnić jej właściwe zabezpieczenie. Ponadto na podstawie *Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[4] operatorzy IK zostali zobligowani do zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w ramach swoich podmiotów, tak aby zminimalizować ryzyko wystąpienia incydentu bezpieczeństwa teleinformatycznego.

Celem artykułu jest omówienie poziomu bezpieczeństwa teleinformatycznego sektora energetyki morskiej i okołomorskiej RP w kontekście planowanych strategicznych projektów energetycznych. Przedstawiono w nim wybrane cyberataki na elementy sektora energetycznego innych państw, a także omówiono, m.in. na podstawie PEP2040, planowane przez Polskę działania związane z infrastrukturą energetyczną w rejonie Morza Bałtyckiego. Wskazano zagrożenia dla polskiego sektora energetyki morskiej i okołomorskiej, do których należy działalność grup APT[5] i grup sponsorowanych przez państwo, rywali biznesowych, haktywistów. Przedstawiono również stosowane sposoby ochrony tej infrastruktury oraz propozycje zabezpieczenia planowanych inwestycji przed atakami teleinformatycznymi.

---

[4] Procedowana jest nowelizacja tej ustawy. Zob. *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, nr UC32, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [dostęp: 16 VII 2025].

[5] Grupa APT (ang. *advanced persistent threat*) – rodzaj zaawansowanej grupy cyberprzestępczej, składającej się z wykwalifikowanych specjalistów od cyberbezpieczeństwa oraz teleinformatyki, którzy są w stanie zrealizować zaawansowane ataki teleinformatyczne na określone podmioty.

Przykłady cyberataków wymierzonych w sektor energetyczny

Infrastruktura energetyczna państw przez dwie pierwsze dekady XXI w. padła ofiarą wielu skutecznych ataków ukierunkowanych m.in. na systemy i sieci teleinformatyczne. Pierwszym z powszechnie znanych działań cyberofensywnych tego typu był atak na infrastrukturę teleinformatyczną ośrodka wzbogacania uranu w miejscowości Natanz w Iranie, dokonany w 2010 r. za pomocą oprogramowania Stuxnet. Zadaniami tej placówki są produkcja energii elektrycznej oraz realizacja strategicznych interesów Iranu dotyczących pozyskania zdolności odstraszania atomowego. Operację pod kryptonimem „Olimpic Games" przeprowadziły we współpracy m.in. Stany Zjednoczone Ameryki oraz Państwo Izrael[6]. Zdecydowano się na cyberatak, gdyż dokonanie ataku i sabotażu drogą kinetyczną nie było możliwe. Opracowano potencjalnie słabe punkty infrastruktury teleinformatycznej placówki, które skutecznie zaatakowane uniemożliwiłyby lub znacznie utrudniły kontynuowanie procesu wzbogacania uranu w Natanz. Za najbardziej destrukcyjną metodę zaszkodzenia irańskiej strategii atomowej uznano zniszczenie wirówek do wzbogacania uranu[7]. W związku z tym, że ośrodek nie miał bezpośredniego dostępu do sieci Internet, atakujący postanowili zainfekować wewnętrzne systemy teleinformatyczne placówki przez podłączenie przenośnej pamięci USB ze złośliwym oprogramowaniem. Zainfekowane wirówki (a dokładnie kontrolujące je programowalne sterowniki logiczne) zaczęły pracować zgodnie z harmonogramem ustalonym przez atakujących. Doszło do uszkodzenia ok. 11–17% wirówek w ośrodku w Natanz[8], co spowodowało spadek produkcji paliwa jądrowego o 15%[9]. Ponadto podejrzewa się, że zostało zainfekowanych ok. 100 000 innych urządzeń, gdy Stuxnet nieplanowanie rozprzestrzenił się na świecie za pomocą sieci Internet[10]. Jest to najprawdopodobniej najbardziej znany przypadek ataku na system teleinformatyczny przeprowadzony przeciwko innemu państwu oraz jego infrastrukturze energetycznej.

---

[6] M. Baezner, P. Robin, *Hotspot Analysis: Stuxnet*, Zürich 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf, s. 7–8 [dostęp: 16 VII 2025].

[7] Tamże, s. 4.

[8] Tamże, s. 9.

[9] T.M. Chen, *Stuxnet, the Real Start of Cyber Warfare?*, „IEEE Network" 2010, t. 24, nr 6, s. 3. https://doi.org/10.1109/MNET.2010.5634434.

[10] N. Falliere, L.O. Murchu, E. Chien, *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf, s. 5 [dostęp: 16 VII 2025].

Innym przykładem oddziaływania w cyberprzestrzeni na elementy sektora energetycznego państwa był atak w 2012 r. na spółkę Królestwa Arabii Saudyjskiej – Saudi Aramco Oil Company (dalej: Saudi Aramco), największą na świecie firmę z sektora surowcowego. Zgodnie z wyliczeniami Europejskiego Banku Centralnego z 2011 r. – do 2009 r. na Arabię Saudyjską przypadało ok. 12% światowej produkcji ropy naftowej (z czego za większość wydobycia odpowiadała Saudi Aramco)[11]. Atak na Saudi Aramco został przeprowadzony najprawdopodobniej przez grupę cyberprzestępców APT33, powiązaną z Islamską Republiką Iranu. Systemy teleinformatyczne spółki sparaliżowano za pomocą wirusa Shamoon. Zainfekowano ponad 30 000 stacji roboczych[12]. Program ten rozprzestrzeniał się na inne stacje robocze (jest to działanie typowe dla złośliwego oprogramowania klasyfikowanego jako robak, ang. *worm*) i nadpisywał pliki w systemie operacyjnym urządzenia, co wyłączało zainfekowany komputer z użytku[13].

Ofiarą kolejnego poważnego ataku wymierzonego w infrastrukturę energetyczną państwa padła Ukraina. Został on przeprowadzony 23 grudnia 2015 r. wobec trzech regionalnych dystrybutorów energii elektrycznej, tj. Prykarpattyaoblenergo, Kyivoblenergo oraz Chernivtsioblenergo. Byli oni odpowiedzialni za przesył energii elektrycznej odpowiednio na terenach obwodów iwanofrankiwskiego, kijowskiego oraz czerniowieckiego. Według informacji amerykańskiej Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (Cybersecurity and Infrastructure Security Agency) ok. 225 000 osób pozostało bez dostaw prądu na ok. sześć godzin[14]. Ponadto zostały zaatakowane instytucje z sektorów: rządowego, mediów, transportu kolejowego oraz górnictwa[15]. Atak rozpoczął się (po fazie rozpoznania otwartoźródłowego infrastruktury przedsiębiorstw i wstępnych przygotowań do przeprowadzenia operacji) przez dystrybucję kampanii phishingowej do pracowników wymienionych instytucji. Pracownicy przez otwarcie załącznika do wiadomości

---

[11] A. Nakov, G. Nuño, *Saudi Aramco and the Oil Market*, „Working Paper Series" 2011, nr 1354, s. 9.

[12] G. Siboni, S. Kronenfeld, *Iran and Cyberspace Warfare*, „Military and Strategic Affairs" 2012, t. 4, nr 3, s. 90.

[13] Warto dodać, że od listopada 2022 r. spółka z grupy kapitałowej Saudi Aramco (Aramco Overseas Company B.V.) jest właścicielem 30% udziałów w Rafinerii Gdańskiej. Zob. *Saudi Aramco przejmie udziały w gdańskiej rafinerii*, CIRE, 12 I 2022 r., https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [dostęp: 14 XII 2024].

[14] *Cyber-Attack Against Ukrainian Critical Infrastructure*, CISA, 20 VII 2021 r., https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 28 XI 2024].

[15] J. Styczynski, N. Beach-Westmoreland, *When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [bmw] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, s. 5–7, 30–39 [dostęp: 16 VII 2025].

e-mail nieświadomie zainfekowali sieci swoich instytucji złośliwym oprogramowaniem typu trojan[16] o nazwie BlackEnergy 3[17]. Połączyło się ono z serwerami C2[18], po czym cyberprzestępcy zaimplementowali na zainfekowanych stacjach roboczych narzędzia do ekstrakcji danych uwierzytelniających oraz przeprowadzili rozeznanie sieci wewnętrznych zaatakowanych firm. Uzyskali możliwość zalogowania się do tych systemów i sieci oraz dokonania przeglądu widniejącej tam infrastruktury teleinformatycznej. Następnie załadowali kolejne złośliwe oprogramowanie, o nazwie KillDisk, które miało się uruchomić po restarcie systemu operacyjnego. Atakujący wyłączyli zasilacze awaryjne (ang. *uninterrupted power supply*, UPS) dla wybranych serwerów, w tym odpowiedzialnych za usługi telekomunikacyjne, a potem uruchomili wyłączniki prądu. Odłączyli w ten sposób od sieci co najmniej 27 podstacji elektrycznych oraz przerwali dostawy energii elektrycznej dla wspomnianych ok. 225 000 osób[19]. Wgrali następnie własną poprawkę systemu zarządzania przełącznikami, aby powstrzymać ich dalsze zdalne sterowanie, po czym przeprowadzili atak typu DoS[20] na infolinię kijowskiego dystrybutora energii. Uniemożliwiło to klientom zgłoszenie braku dostaw prądu. Ostatnim etapem działań było zaplanowane wcześniej wyłączenie się urządzeń typu UPS, co spowodowało uaktywnienie złośliwego oprogramowania KillDisk przy ponownym uruchomieniu systemów. Miało ono zniszczyć wszelkie dane i logi znajdujące się na urządzeniach, aby znacznie utrudnić późniejszą analizę, która mogłaby ustalić przyczyny zdarzenia i środki zaradcze.

Zakłada się, że za cyberatakiem na ukraińskich dystrybutorów energii stała co najmniej jedna grupa cyberprzestępcza sponsorowana przez państwo (ang. *state-sponsored group*), tj. APT44 powiązana z rosyjskim aparatem państwowym[21]. Przypisuje się jej zależność od Głównego Zarządu Wywiadowczego Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (Главное управление Генерального штаба

[16] Trojan – typ wirusa komputerowego imitujący rzeczywiste programy i funkcje.

[17] Jest to trojan typu RAT (ang. *remote access trojan*) umożliwiający atakującemu zdalny dostęp do stacji roboczej ofiary.

[18] Serwer C2 (ang. *command & control*) – infrastruktura służąca atakującemu do kontroli i zarządzania systemami i urządzeniami mu podległymi, w tym zaatakowanej infrastruktury.

[19] SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf, s. 11 [dostęp: 6 VIII 2025].

[20] DoS (ang. *denial of service*) – rodzaj ataku mający na celu przerwanie dostępności wybranej usługi.

[21] J. Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016 r., https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [dostęp: 15 XII 2024].

Вооруженных Сил Российской Федерации, GRU)[22]. Grupy tego rodzaju nierzadko stanowią narzędzie polityczne będące do dyspozycji państwa rosyjskiego.

Do następnego ataku w sferze teleinformatycznej na różne sektory ukraińskiego państwa, w tym energetyczny, doszło w 2017 r. Podobnie jak w przypadku ataków z 2015 r. działania te przypisano grupie APT44[23]. Nazwa ataku pochodzi od wykorzystanego w nim złośliwego oprogramowania NotPetya, które charakteryzowało się łatwością w tzw. ruchu lateralnym, szyfrowaniu dysków oraz dużą destruktywnością. Początkowo NotPetya zidentyfikowano jako typ ransomware'u[24], nie przewidywał on jednak kluczy deszyfrujących, mogących sprawić, że zainfekowane urządzenie stałoby się ponownie zdatne do użycia, a pliki na nim zawarte byłyby w nienaruszonym stanie. Takie programy określa się mianem *wiper*. Celem ataku było państwo ukraińskie i szeroko pojęta infrastruktura teleinformatyczna zlokalizowana na jego terytorium. Jednak ze względu na obecność w Ukrainie wielu oddziałów spółek zagranicznej proweniencji oraz specyfikę użytego oprogramowania (jak najszybsza propagacja przez sieć) zasięg ataku szybko przekroczył granice cyfrowe Ukrainy i wirus rozprzestrzenił się po świecie w tempie dotąd niezaobserwowanym[25]. Rząd federalny Stanów Zjednoczonych Ameryki w związku z cyberatakiem pociągnął do odpowiedzialności karnej sześciu obywateli Federacji Rosyjskiej – oficerów GRU[26].

Jak wspomniano, atak miał na celu infekcję jak największej liczby urządzeń teleinformatycznych na terytorium Ukrainy, więc nie został wymierzony bezpośrednio w sektor energetyczny, ten jednak nie uchronił się przed wirusem. Ofiarą ataków padły Kyivenergo oraz Ukrenergo – firmy odpowiedzialne za dystrybucję energii elektrycznej w Ukrainie na szczeblach: lokalnym i krajowym[27]. To zdarzenie pokazuje, że podmioty sektora energetycznego muszą chronić się nie tylko przed zagrożeniami ukierunkowanymi, lecz także przed zagrożeniami ogólnymi, na jakie są narażone inne sektory. Znacznie zwiększa to zakres monitoringu zagrożeń.

---

[22] G. Roncone i in., *APT44: Unearthing Sandworm*, Mandiant, 17 IV 2024 r., https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf, s. 2, 7 [dostęp: 16 VII 2025].

[23] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf, s. 3–4 [dostęp: 16 VII 2025].

[24] Ransomware – typ złośliwego oprogramowania, które blokuje dostęp do danych na komputerze lub w sieci i żąda okupu za ich przywrócenie.

[25] Łatwe infekowanie kolejnych stacji roboczych czy serwerów przez oprogramowanie NotPetya okazało się możliwe przez połączenie dwóch narzędzi, tj. Mimikatz oraz EternalBlue.

[26] M. Kerttunen, J. Hemmelskamp, *Major Cyber Incidents*…, s. 3–4.

[27] C. Krasznay, *Case Study: The NotPetya Campaign*, w: *Információ- és kiberbiztonság*, B. Török (red.), Budapest 2020, s. 486.

Agencja prasowa Reuters informowała w 2023 r., że po inwazji na Ukrainę Federacja Rosyjska za priorytetowy cel ataków teleinformatycznych obrała sektor energetyczny tego państwa[28]. Zgodnie z doniesieniami tej agencji Służba Bezpieczeństwa Ukrainy (ukr. Служба безпеки України, SBU) ustaliła, że Rosja przeprowadza średnio 10 ataków dziennie, m.in. podejmuje próby wyłączenia części infrastruktury energetycznej Ukrainy. To pokazało, że cyberprzestrzeń działa jak system naczyń połączonych. Przykładem jest atak na ukraińskiego satelitę, który spowodował niedostępność systemu zdalnego nadzorowania pracy ponad 5800 turbin wiatrowych w Niemczech[29].

Od rozpoczęcia rosyjskiej inwazji na Ukrainę są prowadzone działania ofensywne w cyberprzestrzeni wymierzone w infrastrukturę energetyczną innych państw europejskich. Jednym z nich była seria ataków w 2023 r. na duńskich operatorów IK. Opisał je w raporcie SektorCERT – zespół reagowania na incydenty bezpieczeństwa komputerowego odpowiedzialny za ochronę duńskiej IK[30]. Wynika z niego, że był to największy, a zarazem najbardziej kosztowny w historii atak przeprowadzony na tę infrastrukturę. Sprawcy zaatakowali część systemów zarządzania środowiskami automatyki przemysłowej (ang. *industrial control systems*, ICS) w przedsiębiorstwach i uzyskali dostęp do infrastruktury teleinformatycznej 22 podmiotów z sektora energetycznego. Ataków na wszystkie cele dokonano jednocześnie, były one przygotowane starannie i z dużym wyprzedzeniem, a atakujący miał rozeznanie, gdzie należy uderzyć[31]. SektorCERT miał problemem z jednoczesną obsługą 16 zaatakowanych instytucji oraz kolejnych sześciu, które padły ofiarą drugiej fali ataków. Te kolejne ataki SektorCERT przypisał innej, bliżej niezidentyfikowanej grupie cyberprzestępczej, wykorzystującej nowe narzędzia do ataku, w tym liczne podatności typu 0-day[32]. To wskazuje, że sprawca dysponował dużymi umiejętnościami w odkrywaniu tych podatności lub środkami pieniężnymi na zakup od innych grup cyberprzestępczych informacji o lukach bezpieczeństwa[33].

---

[28] N. Buli, N. Chestney, Ch. Steitz, *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023 r., https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [dostęp: 5 XII 2024].

[29] Tamże.

[30] SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [dostęp: 5 XII 2024].

[31] Tamże, s. 10.

[32] Podatność typu 0-day – podatność, która nie została publicznie potwierdzona przez producenta i nie istnieje dla niej oficjalna aktualizacja oprogramowania, która neutralizowałaby tę podatność.

[33] *Behind the Rise of the Million Dollar Zero-Day Market*, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [dostęp: 14 XII 2024].

Przypuszcza się, że za atakami (a przynajmniej częścią z nich) stała grupa APT44[34]. Co warte uwagi, SektorCERT ustalił, że w momencie największego nasilenia ataków źródłami były adresy IP wskazujące swoją geolokalizacją na Polskę i Ukrainę[35].

Identyfikacja zasobów sektora energetyki w obszarze morskim RP

W PEP2040 duży nacisk położono na podsektor energetyki morskiej i okołomorskiej państwa. Świadczą o tym działania wymienione w tym dokumencie:

- utworzenie morskich farm wiatrowych w polskiej wyłącznej strefie ekonomicznej, które do 2040 r. mają osiągnąć zdolność generowania energii elektrycznej o mocy ok. 11 GW,
- stworzenie głównego terminalu instalacyjnego (portu) specjalizującego się w obsłudze łańcucha dostaw dla morskich farm wiatrowych,
- rozbudowa sieci przesyłowej w północnej i północno-zachodniej części Polski w celu przystosowania systemu elektroenergetycznego Polski do odbioru i przesyłu energii wytworzonej m.in. w morskich elektrowniach wiatrowych,
- pozyskiwanie gazu ziemnego gazociągiem Baltic Pipe od 2022 r. Możliwy import 10 mld m^3 gazu ziemnego i eksport – 3 mld m^3,
- zwiększenie zdolności regazyfikacji terminalu LNG w Świnoujściu do 8,3 mld m^3 gazu ziemnego,
- budowa terminalu regazyfikacyjnego gazu ziemnego w Zatoce Gdańskiej (terminal FSRU[36]) o przepustowości nominalnej 4,5 mld m^3 gazu,
- rozbudowa gazociągów w północnej i centralnej części Polski w celu umożliwienia transportu gazu z terminalu FSRU w głąb kraju,
- możliwa rozbudowa Podziemnego Magazynu Gazu Kosakowo w Dębogórzu,
- zwiększenie zdolności przechowywania ropy naftowej w terminalu naftowym oraz bazy PERN w Gdańsku do ok. 1,9 mld m^3,
- budowę drugiej nitki Rurociągu Pomorskiego w celu optymalizacji przesyłu ropy naftowej z Naftoportu w Gdańsku w głąb kraju,
- zwiększenie mocy produkcyjnych Rafinerii Gdańskiej w obszarze petrochemii,

[34] SektorCERT, *The attack against Danish, critical infrastructure*…, s. 14–16.

[35] Tamże, s. 26.

[36] FSRU (ang. *floating storage regasification unit*) – jednostka pływająca służąca do regazyfikacji gazu.

- wydobycie ropy naftowej ze złóż zlokalizowanych na Morzu Bałtyckim oraz norweskim szelfie kontynentalnym,
- identyfikacja nowych złóż ropy naftowej i gazu ziemnego na Morzu Bałtyckim i norweskim szelfie kontynentalnym,
- stworzenie możliwości bunkrowania LNG w czterech największych portach Polski: Gdańsk, Gdynia, Szczecin i Świnoujście,
- ustanowienie podmorskiego połączenia stałoprądowego między Polską a Litwą (i szerzej krajami bałtyckimi) o planowanej mocy 700 MW (220 kV),
- możliwe wykorzystanie potencjału hydroenergetycznego.

Do tej listy można by dopisać istniejącą infrastrukturę energetyczną, która nie została wymieniona w PEP2040, ale poniekąd jest skoncentrowana wokół energetyki morskiej lub okołomorskiej państwa, tj. połączenie podmorskie Szwecji oraz Polski przez linię kablową SwePol Link o mocy 600 MW (450 kV) oraz bazy paliwowe ropy naftowej i paliw ciekłych: Dębogórze, Świnoujście, Trzebież, Szczecin, Koszalin, Ugoszcz, Gdańsk. Prawdopodobnie niemal całość zapotrzebowania Polski na gaz ziemny będzie mogła być pokrywana przez dostawy od strony Morza Bałtyckiego, przede wszystkim przez Baltic Pipe. Morskie farmy wiatrowe mają stanowić jeden z trzech filarów podstawy przyszłego miksu energetycznego RP i zaspokajać ok. 18% zapotrzebowania energetycznego[37]. Ponadto można byłoby uwzględnić energię elektryczną wytwarzaną w planowanej elektrowni jądrowej w województwie pomorskim, ponieważ system elektroenergetyczny (głównie infrastruktura przesyłowa) budowany w północnej części Polski będzie rozbudowywany i modyfikowany w taki sposób, aby współdzielić infrastrukturę przesyłową z tą elektrownią oraz m.in. z morskimi farmami wiatrowymi zlokalizowanymi w co najmniej dwóch ławicach: Ławicy Środkowej i Ławicy Słupskiej. To sprawia, że wszelkie zagrożenia cyberbezpieczeństwa w kontekście dystrybucji energii elektrycznej z planowanych morskich farm wiatrowych oraz elektrowni jądrowej będą w istotny sposób wpływać na oba przedsięwzięcia i tym samym znacznie utrudniać ich funkcjonowanie.

W ramach identyfikacji zasobów sektora energetyki w obszarze morskim RP oraz związanych z tym zagrożeń zostały uwzględnione dodatkowe podmioty mające wpływ na kształt sektora energetycznego RP w kontekście energetyki morskiej i okołomorskiej, w postaci: urzędów morskich w Gdyni i Szczecinie oraz

[37] *Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski*, Polityka, 2023 r., https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [dostęp: 15 XII 2024].

Ministerstwa Klimatu i Środowiska (jako urzędu obsługującego ministra odpowiedzialnego za sektor administracji publicznej „energia")[38].

Rodzaje potencjalnych adwersarzy dla zasobów teleinformatycznych przedsiębiorstw sektora energetycznego RP

Przewiduje się, że inwestycje podjęte w polskim sektorze energetycznym będą przynosić stosunkowo duże zyski, szczególnie dla firm stanowiących trzon tego sektora. Dla cyberprzestępców może to być zachętą do działań ofensywnych wobec tych podmiotów. Nie wszystkie próby ataku muszą być jednak motywowane chęcią zysku. Poważnym zagrożeniem mogą się okazać grupy APT, grupy cyberprzestępców sponsorowane przez podmiot państwowy lub powiązane z nim, rywale biznesowi i haktywiści.

Największe zagrożenie, które należy uwzględniać przy ocenie odporności własnych systemów i sieci teleinformatycznych, stanowią obecnie grupy APT. Celem ich precyzyjnych ataków są zazwyczaj najbardziej krytyczne podmioty i instytucje. Działania te mogą trwać wiele miesięcy czy lat, z uwzględnieniem etapu rozpoznania celu, przygotowania właściwych narzędzi pod zidentyfikowane słabości ofiary, utrzymania uzyskanego dostępu do jej systemów i unikaniem wykrycia.

Zagrożeniem są również grupy cyberprzestępcze sponsorowane przez podmiot państwowy lub powiązane z nim. Funkcjonują one (tak jak grupy APT) nierzadko na zasadzie zleceniowości, w tym sprzedaży swoich usług. Cyberprzestępcy sponsorowani przez państwo niewliczający się do kanonu grup APT prowadzą działania krótkoterminowe i/lub średnioterminowe, które skupiają się np. na utrudnieniu funkcjonowania organizacji lub na propagandzie.

Rywale biznesowi mogą okazać się zagrożeniem w kontekście kradzieży lub innych prób uzyskania informacji o stanie realizowanych projektów i wykonujących je firm. Jest to zjawisko nieuczciwej konkurencji – na podstawie wykradzionych informacji (ang. *data theft*) można próbować zaszkodzić planowanej inwestycji, realizującej ją spółce lub modyfikować własne plany inwestycyjne stosownie do działań adwersarza. Takie szkodliwe działania rywal biznesowy może prowadzić sam, ale znacznie częstszą praktyką jest zlecanie ich podmiotowi zewnętrznemu (grupie cyberprzestępczej), niepowiązanemu ze zleceniodawcą.

Ostatnimi z wymienionych są haktywiści, których działania w cyberprzestrzeni są motywowane względami ideologicznymi. Pobudką do podjęcia akcji są

[38] § 1 ust. 2 pkt. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 19 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Klimatu i Środowiska*.

zazwyczaj wydarzenia polityczne. Haktywiści mogą atakować zarówno instytucje państwowe, m.in. w tzw. afekcie (np. po nieakceptowanej przez nich decyzji władz), jak i przedsiębiorstwa, których polityka biznesowa, ekologiczna, cenowa, wizerunkowa wzbudza ich sprzeciw.

Wymienione podmioty mogą dokonać prób sabotażu, infiltracji czy zniszczenia infrastruktury teleinformatycznej obsługującej projekty energetyczne. Konieczne jest więc, aby podmioty odpowiedzialne ze te projekty oraz decydenci przeprowadzili analizy ryzyka i przygotowali plany zabezpieczeń, tak aby zagrożenie atakiem teleinformatycznym sprowadzić do akceptowalnego poziomu.

Warto zaznaczyć, że obecność na polskim rynku energetycznym spółek z zagranicznym kapitałem może być dla adwersarzy zachętą do podjęcia działań ofensywnych względem ich kapitału ulokowanego w inwestycjach energetycznych w Polsce. Przykładem jest Rafineria Gdańska, w której znaczną część udziałów posiada spółka zależna z grupy kapitałowej Saudi Aramco. Takimi działaniami mogą być zainteresowani zwłaszcza haktywiści i rywale biznesowi.

Zasoby teleinformatyczne przedsiębiorstw sektora energetyki morskiej oraz rodzaje ataków na nie

Aktywa, jakie organizacja z sektora energetycznego, w tym energetyki morskiej, musi chronić, aby uniknąć wystąpienia incydentu bezpieczeństwa teleinformatycznego, można podzielić na dwie grupy tzw. środowisk infrastruktury teleinformatycznej. Są to środowiska: korporacyjne oraz automatyki przemysłowej.

Różne systemy i urządzenia, ze względu na specyfikę spełnianych funkcji, mogą być wykorzystywane do wykonywania czynności biurowych oraz czynności zapewniających funkcjonowanie maszyn przemysłowych niezbędnych do produkcji lub dystrybucji energii elektrycznej. Mimo teoretycznej możliwości zupełnego odseparowania tych dwóch środowisk często są one od siebie zależne. Przykładem może być konieczność podjęcia działań korygujących w środowisku automatyki przemysłowej przez uprawnionego użytkownika z sieci korporacyjnej lub użytkownika z firmy zewnętrznej świadczącej usługi utrzymania maszyn przez zdalny dostęp do środowiska automatyki przemysłowej.

Środowisko korporacyjne w dojrzałej organizacji korzysta z takich systemów i urządzeń, jak: własna domena, kontroler domeny, serwery web, serwery e-mail, serwery bazodanowe, aplikacje biznesowe oraz punkty końcowe (stacje robocze, drukarki) itd. Niezależnie od specyfiki środowiska korporacyjnego powinno być ono odpowiednio chronione ze względu na zagrożenia ciągłości działania przedsiębiorstwa oraz wpływ na środowisko automatyki przemysłowej i zależność od niego.

W środowisku automatyki przemysłowej w dużych przedsiębiorstwach, do których można zaliczyć podmioty zapewniające produkcję oraz dystrybucję energii elektrycznej, powinny występować systemy i urządzenia takie jak: terminale zdalnego dostępu typu RTU (ang. *remote terminal unit*), interfejsy HMI[39], system SCADA[40], kontrolery, sterowniki PLC[41], konwertery sygnałów, diody optyczne czy sensory i czujniki. Te z kolei powinny być chronione systemami i urządzeniami odpowiadającymi tym wskazanym dla środowiska korporacyjnego lub wyspecjalizowanymi dla środowisk automatyki przemysłowej – w zależności od potrzeb. Przedstawione przykłady nie są wyczerpujące ze względu na odmienną specyfikę środowisk w różnych przedsiębiorstwach. Mogą one stosować rozmaite podejścia do projektowania i utrzymania swojej infrastruktury teleinformatycznej, w zależności od nakładów finansowych czy zasobów ludzkich, którymi dysponują.

Częstymi problemami występującymi w obu środowiskach są: nieaktualne wersje oprogramowania podatne na ataki[42], brak świadomości użytkowników na temat zagrożeń oraz niestosowanie dobrych praktyk i standardów z dziedziny teleinformatyki i cyberbezpieczeństwa. Przykładowo w ataku za pomocą złośliwego oprogramowania WannaCry wykorzystywano m.in. niezaktualizowane oprogramowanie w postaci protokołu SMBv1[43].

Stosunkowo częstym typem ataków na środowiska automatyki przemysłowej są ataki na łańcuch dostaw. Atakujący podejmują takie działania, gdy nie mogą uzyskać bezpośredniego dostępu, czyli punktu wejścia (ang. *point of entry*), do docelowej infrastruktury. Mniejsi podwykonawcy, z zazwyczaj proporcjonalnie mniejszymi nakładami na bezpieczeństwo teleinformatyczne swojej firmy, są łatwiejszym celem. Do tego rodzaju ataku może dojść np. w przypadku, gdy dostawca – na podstawie umowy z daną organizacją – ma zdalny dostęp do jej przemysłowej infrastruktury teleinformatycznej. Atakujący mogą w ten sposób pozyskać dane uwierzytelniania do kont serwisowych w środowisku automatyki przemysłowej wybranej organizacji i prowadzić już bezpośrednio w niej dalsze działania ofensywne.

---

[39] HMI (ang. *human-machine interface*) – interfejs występujący między maszyną a jej operatorem, najczęściej w postaci graficznej reprezentacji procesu.

[40] SCADA (ang. *supervisory control and data acquisition*) – system teleinformatyczny nadzorujący przebieg procesu produkcyjnego.

[41] PLC (ang. *programmable logic controller*) – programowalny sterownik logiczny, służący do sterowania pracą maszyny.

[42] *Outdated Software*, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [dostęp: 15 XII 2024].

[43] M. Akbanov, V.G. Vassilakis, M.D. Logothetis, *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, „Journal of Telecommunications and Information Technology" 2019, t. 75, nr 1, s. 114–115. https://doi.org/10.26636/jtit.2019.130218.

Mechanizmy ochronne zasobów teleinformatycznych sektora energetycznego RP

Sposoby zabezpieczania zasobów teleinformatycznych sektora energetycznego RP, w tym sektora energetyki morskiej i okołomorskiej, można podzielić na zabezpieczenia indywidualne oraz państwowe, związane z działaniem określonych służb i instytucji.

Zabezpieczenia indywidualne operatora infrastruktury krytycznej

Istotnymi sposobami przeciwdziałania skutkom ewentualnego ataku mogą okazać się m.in. stosowanie urządzeń typu firewall, segmentacja sieci pozwalająca wyizolować potencjalnie zaatakowane urządzenia oraz restrykcyjna kontrola uprawnień kont użytkowników (ang. *identity and access management/privileged access management*, IAM/PAM) zgodnie z dobrymi praktykami środowiska branżowego[44]. Zdarza się, że panele sterowania infrastruktury środowisk automatyki przemysłowej są dostępne z poziomu sieci Internet – czasami nawet bez konieczności uwierzytelnienia użytkownika, co stwarza poważne ryzyko dla takiego systemu[45].

Ze względu na możliwość oddziaływania na siebie środowisk korporacyjnych oraz środowisk automatyki przemysłowej powinny być one zabezpieczone w sposób spójny, nietraktujący żadnego z obszarów jako mniej istotnego wymiaru bezpieczeństwa. Oba środowiska zazwyczaj wykorzystują wspólne elementy infrastruktury teleinformatycznej przedsiębiorstwa, choćby w postaci domeny. Oba zatem mogą stać się ofiarą ataku w przypadku niewłaściwego ich zabezpieczenia. Rozwiązania te powinny być chronione – jako niezbędnym minimum – m.in. za pomocą urządzeń typu firewall, mechanizmów uwierzytelniania wieloskładnikowego (ang. *multi-factor authentication*, MFA), systemów: antyDDoS; zarządzania informacjami i zdarzeniami zabezpieczeń (ang. *security information and event management*, SIEM); zarządzania, automatyzacji i reagowania na zdarzenia bezpieczeństwa (ang. *security orchestration, automation and response*, SOAR); wykrywania nieautoryzowanego dostępu (ang. *intrusion detection system*, IDS); zapobiegania nieautoryzowanemu dostępowi (ang. *intrusion prevention system*, IPS); zapobiegania wyciekowi danych (ang. *data loss prevention*, DLP); ochrony punktów końcowych (ang. *endpoint detection and response*, EDR); typu antywirus, a także IAM/PAM, serwerów z kopiami bezpieczeństwa (backup), filtrów poczty elektronicznej oraz UPS.

---

[44] *Security and Privacy Controls For Information Systems and Organizations*, NIST, September 2020, s. 19–20. https://doi.org/10.6028/NIST.SP.800-53r5.

[45] *Raport roczny z działalności CERT POLSKA 2023*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf, s. 57–58 [dostęp: 16 VII 2025].

Co istotne, zgodnie z procedowanym projektem ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw przewiduje się m.in. wyznaczenie operatorom IK minimalnych standardów cyberbezpieczeństwa[46]. Może to skutkować poprawą bezpieczeństwa teleinformatycznego instytucji najważniejszych z punktu widzenia państwa. Te wymagania będą bazować na wynikach oceny ryzyka rozwiązań organizacyjno-technicznych przeprowadzonej przez dany podmiot. Jest to nowe podejście, w którym uwzględniono ewolucję zagrożeń i dezaktualizację w czasie zastosowanych zabezpieczeń, aby zapewnić ciągłość działań zabezpieczających.

Ponadto w ramach projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa[47] przewiduje się dokonywanie oceny ryzyka w odniesieniu do łańcucha dostaw w postaci dostawców i klientów biznesowych, z którymi podmiot chce współpracować. Celem jest zabezpieczenie sieci i systemów teleinformatycznych przedsiębiorcy przed potencjalnym atakiem na ten łańcuch. Zapisy zawarte w nowelizacji mogą się jeszcze zmienić w zakresie oceny ryzyka, zwłaszcza te dotyczące podmiotów określonych mianem dostawców wysokiego ryzyka. Zmiany mogą być podyktowane m.in. obawami społecznymi co do zgłoszonych propozycji, w tym arbitralnych i motywowanych politycznie decyzji skutkujących uznaniem podmiotu za dostawcę wysokiego ryzyka[48].

Państwowe formy zabezpieczenia operatora infrastruktury krytycznej

Pomimo rosnącego zagrożenia atakami na IK państwa rolą przedsiębiorcy nie jest przeznaczanie wszelkich dochodów z działalności na uodparnianie swojej spółki na dany typ zagrożenia. To państwo powinno ochraniać swoje interesy, w tym dbać o ciągłość funkcjonowania przez zapewnienie bezpieczeństwa procesom wytwarzania i dystrybucji energii elektrycznej na swoim terytorium. Te działania są realizowane m.in. przez Siły Zbrojne RP na podstawie art. 26 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* i aktów prawnych niższego rzędu, Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu na podstawie art. 5 i 6 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* oraz przez Policję na podstawie art. 1 ust. 2 pkt. 2–4 *Ustawy z dnia 6 kwietnia 1990 r.*

---

[46] *Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw*, nr UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [dostęp: 16 VII 2025].

[47] *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa*...

[48] M. Fraser, *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki*, CyberDefence24, 9 XI 2021 r., https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [dostęp: 18 VII 2025].

o Policji. Zadaniem tych instytucji jest rozpoznawanie zagrożeń bezpieczeństwa państwa i reagowanie na nie.

Działania z zakresu ochrony interesów sektora energetyki morskiej i okołomorskiej RP realizują m.in.:

- Marynarka Wojenna RP – jako rodzaj sił zbrojnych odpowiedzialny za zapewnienie bezpieczeństwa morskiego państwa,
- Morski Oddział Straży Granicznej – prowadzący bieżący nadzór i kontrolę nad obszarami morskimi,
- Wojska Specjalne w postaci jednostek wojskowych GROM oraz Formoza, które umożliwiają szybką odpowiedź na asymetryczne działania kinetyczne;
- Agencja Bezpieczeństwa Wewnętrznego – realizująca zadania zapobiegawcze związane z bezpieczeństwem państwa, IK oraz interesów ekonomicznych RP,
- Agencja Wywiadu – realizująca zadania przeciwdziałania zagrożeniom zewnętrznym względem RP oraz jej interesów i mienia,
- Policja – jako organ odpowiedzialny za zapewnienie ochrony bezpieczeństwa i porządku publicznego państwa,
- CSIRT GOV – odpowiedzialny za zabezpieczanie IK państwa w kontekście zagrożeń cyberbezpieczeństwa.

Większość wymienionych instytucji realizuje zadania ochronne, głównie związane z zagrożeniami o charakterze kinetycznym, zarówno symetrycznymi, jak i asymetrycznymi. Z kolei CSIRT GOV, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w ramach ABW, wykonuje swoje zadania na podstawie art. 26 pkt 3 i 7 oraz art. 27 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa i chroni m.in. operatorów IK w sferze cyfrowej państwa. Pozwala to na udzielanie pomocy tym operatorom w przypadku ataków ze strony m.in. grup APT czy sponsorowanych przez państwa.

Państwo polskie dostrzega zagrożenia dla swoich interesów w rejonie Morza Bałtyckiego i realizuje politykę ich zabezpieczania. Przykładem jest nowo sformowany zespół bojowy Jednostki Wojskowej Formoza, który ma umożliwić bardziej efektywne przeciwdziałanie zagrożeniom kinetycznym o wymiarze asymetrycznym w rejonie Morza Bałtyckiego[49].

[49] *Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej*, Ministerstwo Obrony Narodowej, 22 VIII 2023 r., https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [dostęp: 10 XII 2024].

Należy pamiętać, że najprawdopodobniej nie wszystkie wskazane w artykule obiekty i inwestycje energetyczne wejdą w skład IK na podstawie kryteriów określonych w niejawnym załączniku nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej[50]. Może to wynikać z tego, że obiekty te, jako jeszcze niegotowe, mogły nie przejść procedury wyłonienia obiektów IK spośród ogółu infrastruktury państwa. Ze względu na unikatowy charakter inwestycji typu morskie farmy wiatrowe można rozważyć, czy państwo polskie nie powinno działać wyprzedzająco i uznać takie obiekty, ich instalacje czy części za IK jeszcze przed ich powstaniem. Dzięki temu już w momencie budowy lub modernizacji infrastruktury państwo objęłoby ją ochroną. Takie działania zapewniłyby kompleksowe podejście do problematyki zabezpieczenia interesów energetycznych państwa.

Podsumowanie

W związku z zagrożeniami, przede wszystkim ze strony grup APT oraz grup sponsorowanych przez państwo, dla obecnych i planowanych inwestycji w morską oraz okołomorską infrastrukturę energetyczną konieczne jest, aby państwo polskie zapewniało wsparcie w utrzymaniu predefiniowanego poziomu bezpieczeństwa narażonych organizacji i ich infrastruktury teleinformatycznej, w tym bezpieczeństwa w cyberprzestrzeni. Przy strategicznych projektach realizowanych na podstawie PEP2040 należy zabezpieczyć infrastrukturę teleinformatyczną od początku jej powstawania, zgodnie z podejściem *security by design*. Infrastruktura ta powinna być tworzona zgodnie z najlepszymi praktykami w branży cyberbezpieczeństwa, aby zminimalizować ryzyko skutecznego ataku.

Na podstawie przedstawionych materiałów można wywnioskować, że obecnie państwo polskie może w stopniu podstawowym zapewniać cyberbezpieczeństwo sektora energetyki morskiej oraz okołomorskiej. W czasach bezwzględnej rywalizacji w cyberprzestrzeni może to być niewystarczające, zwłaszcza jeśli weźmie się pod uwagę zagrożenia, jakie mogą się pojawić w przyszłości, oraz dostępne sposoby ich mitygacji. Brakuje działań wyprzedzających, które sprawiłyby, że projekty energetyczne o znaczeniu strategicznym dla bezpieczeństwa państwa byłyby zabezpieczane od początku ich cyklu rozwojowego (fazy planistyczno-koncepcyjnej). Ponadto, jak zostało to wskazane, zagrożenie może się zmaterializować w postaci nie tylko bezpośredniego ataku teleinformatycznego na organizację, lecz także – co staje się coraz częstsze – ataku na łańcuch dostaw. Podwykonawca może się

[50] *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

okazać dogodnym punktem dostępowym do infrastruktury organizacji docelowej. Bez poszerzenia działań zabezpieczających zarówno ze strony operatorów IK, jak i państwa ochrona może się okazać nieskuteczna i nieprzystająca do realiów. Konieczna może być ocena skutków proponowanych regulacji prawnych – w postaci nowelizacji ustaw o zarządzaniu kryzysowym oraz o krajowym systemie cyberbezpieczeństwa – w odniesieniu do ich skuteczności względem obecnych i przyszłych wyzwań w obszarze cyberbezpieczeństwa. Dzięki temu będzie można bardziej kompleksowo podejść do tej problematyki.

Bibliografia

Akbanov M., Vassilakis V.G., Logothetis M.D., *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, „Journal of Telecommunications and Information Technology" 2019, t. 75, nr 1, s. 113–124. https://doi.org/10.26636/jtit.2019.130218.

Chen T.M., *Stuxnet, the Real Start of Cyber Warfare?*, „IEEE Network" 2010, t. 24, nr 6, s. 2–3. https://doi.org/10.1109/MNET.2010.5634434.

Krasznay C., *Case Study: The NotPetya Campaign*, w: *Információ- és kiberbiztonság*, B. Török (red.), Budapest 2020.

Nakov A., Nuño G., *Saudi Aramco and the Oil Market*, „Working Paper Series" 2011, nr 1354.

Security and Privacy Controls For Information Systems and Organizations, NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

Siboni G., Kronenfeld S., *Iran and Cyberspace Warfare*, „Military and Strategic Affairs" 2012, t. 4, nr 3, s. 77–99.

Źródła internetowe

Baezner M., Robin P., *Hotspot Analysis: Stuxnet*, Zürich 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf [dostęp: 16 VII 2025].

Behind the Rise of the Million Dollar Zero-Day Market, SIRP, https://sirp.io/behind-the-rise-of-the-million-dollar-zero-day-market/ [dostęp: 14 XII 2024].

Buchholz K., *Baltic Sea Cable Incidents Pile Up*, Statista, 6 II 2025 r., https://www.statista.com/chart/33892/damage-to-underwater-cables-and-pipelines-in-the-baltic-sea/ [dostęp: 16 VII 2025].

Buli N., Chestney N., Steitz Ch., *Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war*, Reuters, 15 VI 2023 r., https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/ [dostęp: 5 XII 2024].

Cyber-Attack Against Ukrainian Critical Infrastructure, CISA, 20 VII 2021 r., https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 28 XI 2024].

Falliere N., Murchu L.O., Chien E., *W32.Stuxnet Dossier*, Cupertino 2011, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf [dostęp: 16 VII 2025].

Fraser M., *Organizacje przedsiębiorców krytycznie o nowelizacji KSC. Dostawcy wysokiego ryzyka do poprawki*, CyberDefence24, 9 XI 2021 r., https://cyberdefence24.pl/polityka-i-prawo/organizacje-przedsiebiorcow-krytycznie-o-nowelizacji-ksc-dostawcy-wysokiego-ryzyka-do-poprawki [dostęp: 18 VII 2025].

Hultquist J., *Sandworm Team and the Ukrainian Power Authority Attacks*, Mandiant, 7 I 2016 r., https://cloud.google.com/blog/topics/threat-intelligence/ukraine-and-sandworm-team [dostęp: 15 XII 2024].

Kerttunen M., Hemmelskamp J., *Major Cyber Incidents: NotPetya*, March 2023, https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf [dostęp: 16 VII 2025].

Lorenz W., Zaręba S., *Konsekwencje eksplozji rurociągów Nord Stream 1 i 2*, Polski Instytut Spraw Międzynarodowych, 29 IX 2022 r., https://pism.pl/publikacje/konsekwencje-eksplozji-rurociagow-nord-stream-1-i-2 [dostęp: 16 VII 2025].

Morskie farmy wiatrowe najważniejsze w transformacji energetycznej Polski, Polityka, 2023 r., https://polityka.co.pl/morskie-farmy-wiatrowe-najwazniejsze-w-transformacji-energetycznej-polski-3060556.html [dostęp: 15 XII 2024].

Outdated Software, Plurilock, https://plurilock.com/deep-dive/outdated-software/ [dostęp: 15 XII 2024].

Powstaje kolejny zespół bojowy w Formozie. To odpowiedź na współczesne zagrożenia militarne i niemilitarne związane z funkcjonowaniem infrastruktury krytycznej, Ministerstwo Obrony Narodowej, 22 VIII 2023 r., https://www.gov.pl/web/obrona-narodowa/powstaje-kolejny-zespol-bojowy-w-formozie-to-odpowiedz-na-wspolczesne-zagrozenia-militarne-i-niemilitarne-zwiazane-z-funkcjonowaniem-infrastruktury-krytycznej [dostęp: 10 XII 2024].

Roncone G., Black D., Wolfram J., McLellan T., Simonian N., Hall R., Prokopenkov A., Perez D., Aytes L., Wahlstrom A., *APT44: Unearthing Sandworm*, Mandiant, 17 IV 2024 r., https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [dostęp: 16 VII 2025].

SANS ICS, E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid. Defence Use Case*, March 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf [dostęp: 6 VIII 2025].

Saudi Aramco przejmie udziały w gdańskiej rafinerii, CIRE, 12 I 2022 r., https://www.cire.pl/artykuly/rynek-paliw/saudi-aramco-przejmie-udzialy-w-gdanskiej-rafinerii [dostęp: 14 XII 2024].

SektorCERT, *The attack against Danish, critical infrastructure*, November 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [dostęp: 5 XII 2024].

Styczynski J., Beach-Westmoreland N., *When the lights went out: a comprehensive review of the 2015 attacks on Ukrainian critical infrastructure*, [bmw] 2019, https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [dostęp: 16 VII 2025].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2024 r. poz. 1077, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122, ze zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2025 r. poz. 902).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. DzU z 2025 r. poz. 636, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 19 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Klimatu i Środowiska (DzU z 2023 r. poz. 2726).

Inne dokumenty

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2023.

Polityka energetyczna Polski do 2040 r., Ministerstwo Klimatu i Środowiska, Warszawa 2021.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, nr UC32, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3 [dostęp: 16 VII 2025].

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, nr UC47, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-zarzadzaniu-kryzysowym-oraz-niektorych-innych-ustaw5 [dostęp: 16 VII 2025].

Raport roczny z działalności CERT POLSKA 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf [dostęp: 16 VII 2025].

David Cybulski

Specjalista w dziedzinie cyberbezpieczeństwa. Doświadczenie zawodowe zdobywał na rynku prywatnym oraz w administracji państwowej. Pasjonat zagadnień związanych z innowacyjnymi rozwiązaniami z zakresu cyberbezpieczeństwa oraz nowych technik cyberataków grup APT, ze szczególnym uwzględnieniem ataków socjotechnicznych. Jego zainteresowania naukowe obejmują ochronę infrastruktury krytycznej, aktywność wybranych grup APT, tematykę bezpieczeństwa zjawiska Shadow IT oraz działania Cyber Threat Intelligence / Threat Hunting wobec wybranych grup cyberprzestępczych.

Kontakt: dcybulski@proton.me