Fot.: CoPilot

Adam Kampa, Rafał Kozieł, Maciej Piliński,
Polskie Stowarzyszenie Rozwoju Fotowoltaiki

Odpowiedź branży fotowoltaicznej na wyzwania z zakresu cyberbezpieczeństwa

Cyberbezpieczeństwo to obecnie nieodłączny element naszej codzienności. Choć temat funkcjonuje od lat, dopiero niedawno wprowadzono regulacje, które realnie wpływają na nasze życie zawodowe i prywatne. Obszar ten można rozpatrywać z dwóch perspektyw: wymogów formalnych - wynikających z przepisów prawa oraz praktycznych aspektów – wpływających bezpośrednio na poziom bezpieczeństwa systemów IT i OT.

Znaczenie cyberbezpieczeństwa

Od 2018 r. Unia Europejska sukcesywnie rozwija regulacje dotyczące ochrony informacji i danych osobowych. Punktem zwrotnym była eskalacja zagrożeń po rozpoczęciu wojny na Ukrainie, co wymusiło rozszerzenie przepisów szczególnie w odniesieniu do usług kluczowych dla funkcjonowania państw.

W szczególności sektor energetyczny, w tym fotowoltaika, stanął przed nowymi wyzwaniami. Z jednej strony mamy coraz bardziej zaawansowane technologie i regulacje prawne. Z drugiej - zróżnicowane systemy IT i OT oraz konieczność modernizacji starszej infrastruktury. W tym kontekście cyberbezpieczeństwo nie jest już wyborem - jest koniecznością.

IT i OT - podobieństwa i różnice

Systemy IT służą do zarządzania danymi - ich przechowywania, przetwarzania i przesyłania. Natomiast OT (technologie operacyjne) odpowiadają za kontrolę fizycznych procesów przemysłowych - produkcji energii, sterowania urządzeniami, automatyzacji.

IT koncentruje się na bezpieczeństwie informacji, OT - na bezpieczeństwie fizycznym i operacyjnym. Ataki na IT mogą prowadzić do wycieku danych, natomiast ataki na OT mogą mieć katastrofalne skutki - od zatrzymania produkcji, po zagrożenie życia i środowiska.

Chociaż IT i OT pełnią różne funkcje, muszą ze sobą współdziałać. Jednak z uwagi na różnice technologiczne, środowiskowe i bezpieczeństwa - nie powinny funkcjonować jako jeden system.

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to część technologii informacyjnych (IT) i operacyjnych (OT), której celem jest minimalizacja ryzyka utraty danych i kontroli nad systemami. Najważniejszym zasobem jest informacja - jej wartość stale rośnie, a liczba zagrożeń ze strony hakerów i grup przestępczych nieustannie się zwiększa.

W kontekście energetyki - a zwłaszcza systemów produkcji i dystrybucji energii, wody, ciepła, czy chłodu - cyberbezpieczeństwo ma kluczowe znaczenie. Wystarczy zadać sobie pytania:

- jakie konsekwencje niesie utrata kontroli nad takimi systemami?
- kto może być zainteresowany zdobyciem danych z tych obszarów?
- czy zakłócenia mogą doprowadzić do realnego zagrożenia dla państwa i obywateli?

Cyberbezpieczeństwo możemy określić jako jeden z elementów technologii informacyjnej oraz operacyjnej zajmującej się zapewnieniem możliwie najniższego poziomu ryzyka powstania zagrożenia w bezpieczeństwie informacji, dla systemów IT i OT. Najważniejszym elementem dla obu technologii jest informacja przechowywana i przetwarzana w systemach. W przypadku technologii operacyjnej dochodzi możliwości sterowania, modyfikowania, czy operowania kluczowymi elementami systemów produkcji i usług.

> Cyberbezpieczeństwo możemy określić jako jeden z elementów technologii informacyjnej oraz operacyjnej zajmującej się zapewnieniem możliwie najniższego poziomu ryzyka powstania zagrożenia w bezpieczeństwie informacji, dla systemów IT i OT

Ryzyka w energetyce

Energetyka jest jedną z najbardziej wrażliwych branż pod względem cyberzagrożeń. Awaria systemu sterowania przepompownią, jak w przypadku Colonial Pipeline, może sparaliżować dostawy paliwa i wywołać panikę społeczną.

Koszt przywrócenia funkcjonalności systemów OT może sięgać mln zł, a skutki prawne, reputacyjne i finansowe mogą być znaczne. Dlatego coraz większy nacisk kładzie się na inwestycje w zabezpieczenia, systemy monitorowania i wykwalifikowaną kadrę.

Cyberbezpieczeństwo w świecie energetyki ma dwojaką naturę. Z jednej strony mamy nowe przepisy, technologie oraz rozwiązania. Z drugiej strony - mamy różnorodne i zdywersyfikowane źródła wytwarzania, bazujące zarówno na systemach stworzonych stosunkowo niedawno, jak również sprzed wielu lat, których wymiana nie może być wykonana z dnia na dzień. W tym miejscu warto podkreślić sytuację w branży fotowoltaicznej, której towarzyszył w ostatnich latach dynamiczny rozwój, pojawienie się wielu nowych produktów, nowych producentów komponentów i mnóstwo nowych systemów je obsługujących. Wiele organizacji związanych z produkcją innych kluczowych i krytycznych usług nadal spotyka się z wyzwaniami dotyczącymi rozwiązywania problemów w systemach OT. Problemy te dotyczą zarówno doboru odpowiednich technologii, a także aspektów czysto finansowych. Dla operatorów usług kluczowych koszty modernizacji wszystkich systemów OT mogą sięgać wielu mln zł, w zależności jak wiele elementów systemowych należy wymienić i zmodernizować, aby ryzyko wystąpienia niebezpieczeństwa cyfrowego było możliwe najbardziej zminimalizowane.

Znane są przykłady organizacji, które nie zdążyła zmodernizować swoich zabezpieczeń i zostały celem poważniejszych ataków cybernetycznych.

Kilka lat temu, organizacja Colonial Pipeline ze Stanów Zjednoczonych Ameryki stała się ofiarą jednego z bardziej skutkujących negatywnie ataków przy wykorzystaniu szkodliwego oprogramowania, gdzie jedna z przepompowni ropy naftowej oraz paliwa samochodowe-

go została całkowicie zablokowana, uniemożliwiając dostawy produktów do klientów. Ten incydent spowodował, że okoliczne miasta nie otrzymywały paliwa na lokalne stacje paliwowe, co z kolei spowodowało, że okoliczne firmy oraz ludzie w desperacji i panice wykupywali paliwo. Natomiast, gdy dostęp do niego wyczerpał się po kilku dniach braku dostaw, dochodziło do panicznych ataków, napadów i kradzieży przez zdesperowanych ludzi. Organizacja była nieoperatywna przez praktycznie tydzień. Zapłacono okup o wartości ok. 4,5 mln USD w kryptowalucie bitcoin. Reputacja samej firmy została bardzo nadszarpnięta na długi czas. Organizacja została pozwana zbiorowo i cywilnie przez swoich klientów, opierając się m.in. o straty finansowe, wyciek danych osobowych, niespełnianie wymogów umów. Rząd Stanów Zjednoczonych Ameryki oraz Urzędy Inspekcyjne przyjrzały się incydentowi i nałożyły dodatkowo na przedsiębiorstwo karę finansową, w wysokości ok. 7 mln USD.

> Energetyka jest jedną z najbardziej wrażliwych branż pod względem cyberzagrożeń. Awaria systemu sterowania przepompownią, jak w przypadku Colonial Pipeline, może sparaliżować dostawy paliwa i wywołać panikę społeczną

W chwili obecnej jesteśmy w sytuacji, w której cyberbezpieczeństwo jako element bezpieczeństwa rozwija się w bardzo wysokim tempie. Jednakże, z drugiej strony mamy do czynienia ze zjawiskiem bardzo szybkiego rozwoju grup przestępczych. Szczególnie wykorzystywana jest sztuczna inteligencja jako system pozyskujący informacje, analizujący i atakujący. Dlatego wraz z rozwojem technologicznym, należy również odpowiednio zabezpieczyć się w sferze cyberbezpieczeństwa, nie tylko w kadrę wyszkolonych specjalistów, ale i narzędzia oraz systemy zabezpieczające.

Dyrektywa EU NIS2

Przykładem powyższego rozwoju jest również Dyrektywa EU NIS2, która to weszła w życie na przełomie września/października 2024 r. Dyrektywa nakłada obowiązki na podmioty świadczące usługę kluczową. Usługą kluczową nazywamy wszelkie usługi o znaczeniu krytycznym dla działalności społecznej i gospodarczej danego regionu, miasta i całego kraju, tj.: rozszerza obowiązek ochrony m.in. w podmiotach z typu podmioty niezbędne (Essential Entities) takie jak ENERGETYKA. Nowością jest wprowadzenie odpowiedzialności dla kierownictwa firmy za zgodność ze środkami zarządzania ryzykiem w cyberbezpieczeństwie. Dyrektywa wprowadza obowiązek tworzenia analizy ryzyka i polityki bezpieczeństwa systemów informatycznych, obowiązek obsługi incydentów, wliczając w to zapobieganie, wykrywanie, reagowanie i mitygowanie, zapewnienie ciągłości działania usług i zarządzania kryzysowego, zapewnienie bezpieczeństwa łańcucha dostaw, zapewnienie bezpieczeństwa w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych, zapewnienie posiadania polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa, wykorzystywania kryptografii i szyfrowania. NIS2 jest Dyrektywą, która nakłada na kraje oraz organizacje z tych krajów nowe wymogi, lecz ostatecznie każdy z krajów musi sam wprowadzić własne przepisy lokalne. W Polsce, lokalne przepisy Dyrektywy zostaną wprowadzone w najbliższym czasie. Warto jednocześnie wspomnieć, że Dyrektywa NIS2 oraz jej lokalne wersje przepisów przewidują rygorystyczne i bardzo wysokie kary finansowe dla podmiotów nierealizujących zapisów regulacji we właściwy sposób. Dyrektywa NIS1 miała w swoich przepisach podobne kary za niespełnianie wymogów, jednak ich forma polegała głównie na ostrzeganiu, a kary finansowe były rzadko nakładane.

W Polsce dyrektywę NIS2 implementuje Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC). Według kalendarza legislacyjnego, czas na wdrożenie jej zapisów minął w październiku 2024 r. Niestety zarówno w naszym kraju, jak i w kilku innych państwach UE proces ten nie został zakończony. Ustawodawca w projekcie nowelizacji KSC zaproponował ustanowienie definicji tzw. Dostawcy Wysokiego Ryzyka (ang. *High-Risk Vendor*), mającej swoje korzenie jeszcze w Toolbox 5G - pakiecie najlepszych praktyk związanych z cyberbezpieczeństwem opublikowanym przez Komisję Europejską u progu procesu wdrażania sieci telekomunikacyjnej 5G w krajach członkowskich. W Polsce dotychczas ta definicja prawnie nie obowiązywała, a szkoda - przepisy związane m.in. ograniczają działalność, a wręcz eliminują z rynku podmioty i dostawców urządzeń, wobec których udowodniono działania szpiegowskie, korupcyjne, czy inne przestępstwa, zagrażające bezpieczeństwu państwa. Dotyczy to również przypadków ujawniania danych wrażliwych osobom trzecim, czy unikanie odpowiedzialności za wykryte luki w zabezpieczeniach. W kontekście infrastruktury krytycznej, jaką niewątpliwie jest energetyka, tego typu ograniczenia wydają się zasadne i zgodne z interesem społecznym. Bezpieczeństwo i odporność europejskiego systemu elektroenergetycznego mają ogromne znaczenie, biorąc pod uwagę rozwój sytuacji geopolitycznej, rosnące wzajemne połączenia cyfrowe i scenariusze zagrożeń hybrydowych.

Branża fotowoltaiczna

Branża fotowoltaiczna, jako główny filar transformacji energetycznej, przyczynia się nie tylko do dekarbonizacji,

ale także w coraz większym stopniu bierze na siebie odpowiedzialność za bezpieczeństwo i stabilność dostaw energii elektrycznej. Biorąc pod uwagę obecny udział generacji słonecznej w miksie energetycznym w Europie, należy z najwyższą uwagą szacować ryzyka związane z potencjalnymi zakłóceniami pracy tych instalacji, np. jednoczesnego przejęcia kontroli nad ich pracą w wyniku cyberataku. Konsekwencje mogą dotyczyć wielu państw - w przypadku Europy, systemy energetyczne są ze sobą połączone. Z jednej strony jest to oczywiście korzystne, ze względu na możliwość wymiany energii i bilansowania nadwyżek / niedoborów. Z drugiej - niesie ryzyko propagacji zakłóceń powstałych w jednym kraju na inne. Według szacunków PSE, zakłócenie działania jednocześnie 3 GW jednostek fotowoltaicznych (szczególnie w słoneczny dzień, gdy źródła konwencjonalne pracują na minimach technicznych), może doprowadzić do destabilizacji systemu, a w skrajnym przypadku - nawet do blackoutu, jakiego doświadczyli niedawno Hiszpanie, czy nieco później, mieszkańcy Pragi.

Zagrożenia cybernetyczne w energetyce

Rodzaje zagrożeń cybernetycznych charakterystycznych m.in. dla energetyki:

- Atak na protokół komunikacyjny - polega na wykryciu i wykorzystaniu luk w oprogramowaniu, dzięki czemu osoba niepowołana uzyskuje dostęp do danego środowiska. To również atak po uzyskaniu danych dostępowych (loginów, haseł) w sposób nielegalny - poprzez wyłudzenie danych, phishing, czy inne metody socjotechniczne.
- Atak na łańcuch dostaw - zainstalowanie w urządzeniu, bądź oprogramowaniu złośliwego składnika, który w określonym czasie, bądź po otrzymaniu zdalnego polecenia uruchomi się i zacznie wykonywać określone działanie: będzie przesyłał dane w sposób utajony (bez wiedzy użytkownika), śledził aktywność, bądź też doprowadzi do uszkodzenia, czy destabilizacji danej funkcjonalności. To również wszelkiego rodzaju „backdoory" i konie trojańskie. Przykładem takich działań mogą być wypadki opisane m.in. przez Reuters - w chińskich falownikach zainstalowanych w USA odnaleziono podejrzane moduły komunikacyjne, nie występujące w specyfikacji technicznej. „Nielegalne komponenty zapewniają dodatkowe, nieudokumentowane kanały komunikacji, które mogą umożliwić zdalne obejście zapór sieciowych, co może mieć katastrofalne skutki, z destabilizacją systemu elektroenergetycznego włącznie" - czytamy w artykule[1].
- Atak DDoS - Wysyłanie bardzo dużej ilości zapytań do hosta, bądź sieci zarządzającej pracą infrastruktury energetycznej. Dostęp do interfejsów tak przeciążonej sieci

Fot.: pixabay.com

staje się niemożliwy, w szczególności nie może odbierać rzeczywistych sygnałów sterujących, czy poleceń obsługi.
- Przeciążenie infrastruktury sterującej uniemożliwiające dostęp do interfejsów, w szczególności - odbioru sygnałów sterujących, poleceń.
- Atak ransomware - złośliwe oprogramowanie blokujące dostęp do danego serwisu. Dla przywrócenia funkcjonalności, autorzy ransomware oczekują wpłacenia okupu. Możliwe są również inne formy nacisku, czy szantażu, np. ujawnienie kompromitujących informacji. Przykładem takiego ataku była sytuacja opisana we wstępie, dotycząca Colonial Pipeline.

Prosumeryzm, a cyberbezpieczeństwo

Całkowita moc zainstalowana źródeł fotowoltaicznych w Polsce przekroczyła już 20 GW. Więcej niż 50% z nich to mikroinstalacje, będące w posiadaniu prosumentów. Właśnie w tej grupie, właścicieli instalacji OZE, świadomość zagrożeń cybernetycznych jest najmniejsza. Oczywiście nie ma mowy o zagrożeniu dla stabilności systemu elektroenergetycznego w przypadku zakłóceń w działaniu jednego, czy kilku falowników o mocy do 50 kW. Należy jednak pamiętać, że skoordynowane wyłączenie kilkuset, czy nawet kilku tysięcy urządzeń wytwórczych małej mocy może dać podobny efekt jak wyłączenie dużego bloku energetycznego. Czy taki scenariusz w ogóle jest możliwy? Najlepszym potwierdzeniem jest sytuacja, która miała miejsce w USA i kilku mniejszych państwach w listopadzie 2024 r.[2]. Wszystkie falowniki jednego z chińskich producentów zostały zdalnie wyłączone - jednocześnie. Tłem tego zdarzenia był konflikt licencyjny pomiędzy producentem, a dystrybutorem. Abstrahując od przyczyn, przypadek ten jasno pokazał, że tego typu działanie ze strony producenta, bądź innego podmiotu, który ma kontrolę nad tymże producentem, jest jak najbardziej możliwe i może dotyczyć nieokreślonej liczby urządzeń. Im wyższe nasycenie systemu elektroenergetycznego urządzeniami „niewiarygodnego" producenta, tym konsekwencje podobnych działań będą bardziej dotkliwe.

Nierozważny dobór urządzeń pracujących w naszej domowej instalacji może mieć oczywiście również inne konsekwencje, odczuwalne w znacznie mniejszej skali, z perspektywy pojedynczych użytkowników. Słabo zabezpieczony przed dostępem inwerter może być cennym źródłem informacji dla potencjalnych włamywaczy. Wszak po profilu zużycia energii można zweryfikować, kiedy mieszkańcy znajdują się poza domem i zaplanować włamanie do budynku. W ten sam sposób można pozyskać wrażliwe dane osobowe, zapisane w pamięci urządzenia. Dlatego tak istotne jest korzystanie ze sprzętu wyposażonego w zaawansowane zabezpieczenia, obejmujące chociażby wielopoziomowe szyfrowanie dostępu, regularnie przeprowadzane aktualizacje, czy przechowujące dane pozyskane z falowników (za świadomą zgodą użytkownika) na serwerach zlokalizowanych w Europie, bez ryzyka dostępu do nich osób trzecich. Producenci powinni legitymować się zgodnością z europejskimi standardami ochrony danych, chociażby w zgodzie z normami ETSI EN 303645 czy ISO 27001. Użytkownicy i instalatorzy również mają tu swoje zadanie. Podstawową czynnością, po uruchomieniu czy to instalacji, czy sieci domowej - jest zmiana domyślnego hasła dostępowego do urządzenia. Niestety, jak pokazuje praktyka - nawet tak podstawowe działania często są zaniedbywane. Dlatego nieustanne uświadamianie i edukacja o zagrożeniach jest tak bardzo istotna.

Certyfikacja cyberbezpieczeństwa

Istotnym problemem, luką prawną w Polsce jest brak jednoznacznych wymagań i obowiązku certyfikacji pod kątem cyberbezpieczeństwa źródeł wytwórczych, w tym inwerterów fotowoltaicznych, czy bateryjnych. O możliwości przyłączenia do sieci decyduje obecność na tzw. Białej liście - wykazie certyfikowanych urządzeń, prowadzonej przez PTPiREE. Wymagania te dotyczą zgodności m.in. z Kodeksem Sieci (NC RFG), Instrukcjami Ruchu i Eksploatacji Sieci Przesyłowej i Dystrybucyjnej oraz innymi aktami prawnymi, zatwierdzonymi przez URE. Są to jednak wymagania związane z działaniem urządzeń w sieci, reagowania na zmiany parametrów takich jak napięcie, częstotliwość, czy też określające sposób działania po zaniku zasilania, bądź innej sytuacji awaryjnej. Powyższe dokumenty nie określają jednak jakichkolwiek wymagań związanych z bezpieczeństwem przetwarzania informacji. W połączeniu z „opieszałością" we wdrażaniu dyrektywy NIS 2 w naszym kraju, pozbawiamy się narzędzi do weryfikacji dostawców pod tym kątem. Pewne nadzieje budzi opublikowana niedawno inicjatywa Ministerstwa Cyfryzacji, związana z powstającym systemem certyfikacji cyberbezpieczeństwa [3]. Niestety jednak, zapowiadany program ma być dobrowolny, a nie obowiązkowy.

Opisywany problem dotyczy wielu branż i grup urządzeń pracujących w systemie elektroenergetycznym, nie tylko źródeł wytwórczych. Bardzo wrażliwymi punktami są również tzw. Inteligentne liczniki energii elektrycznej, wdrażane na znacznym obszarze (docelowo 100%) Polski. Oprócz możliwości zdalnego odczytu danych przez operatora, posiadają one możliwość otrzymywania poleceń sterujących, w tym - odłączenia odbiorcy. Masowe uruchomienie tej funkcji doprowadzi do znacznego niezbilansowania systemu (nagła nadwyżka mocy w systemie, wynikająca z zaniku poboru), a w konsekwencji do jego awarii. Ciekawostka: scenariusz takiego zdarzenia, dokonanego przez grupę przestępczą opisano w fabularnej powieści Marca Elsberga pt. „Blackout". Zgodnie z tytułem, m.in. te działania do-

prowadziły do blackoutu na znacznym obszarze kontynentu i chaosu społecznego związanego z brakiem dostępu do energii elektrycznej.

Odpowiedź Europy na dominację chińskich producentów

Według raportu Instytutu Energii Odnawialnej (IEO) „Rynek Fotowoltaiki w Polsce 2024”[4] ponad 90% instalowanych w Polsce inwerterów pochodzi od chińskich producentów. W odniesieniu do magazynów energii ten udział jest jeszcze wyższy. Taka dominacja w połączeniu z przypadkami działalności korupcyjnej i nielegalnego lobbingu, które zaowocowały nawet usunięciem jednego z czołowych chińskich producentów z głównego stowarzyszenia branżowego w Europie[5], budzi uzasadnione obawy i wątpliwości co do intencji takich producentów. O zagrożeniach informowano już dawno, najlepszym przykładem jest rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r. *w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(RSP).* Nie sposób jednak oprzeć się wrażeniu, że przez ostatnie 6 lat nie potraktowano tego ostrzeżenia zbyt poważnie, a nasycenie rynków sprzętem chińskim znacząco wzrosło. Dopiero w ostatnim czasie pierwsze państwa europejskie zaczynają dostrzegać problem. Od 1 maja 2025 r. na Litwie obowiązuje prawo ograniczające możliwość instalowania chińskich urządzeń wytwórczych o mocy powyżej 100 kW[6]. Z kolei w Estonii tamtejszy wywiad opublikował w 2024 r. raport dotyczący głównych zagrożeń dla tego państwa w najbliższej przyszłości. Oprócz agresywnej polityki najbliższego sąsiada - Rosji, na drugim miejscu sklasyfikowano zagrożenie chińskimi technologiami w infrastrukturze krytycznej (5G, energetyka), ale nie tylko - również nieuprawnione pozyskiwanie danych i skanowanie całych obszarów z wykorzystaniem technologii LIDAR (obecną chociażby w samochodach elektrycznych, czy samojezdnych urządzeniach AGD)[7]. Ponadto, dominacja chińskich urządzeń na bardzo chłonnym rynku szeroko rozumianej transformacji energetycznej, gdzie funkcjonują również mechanizmy wsparcia (np. w Polsce - Czyste Powietrze, Mój Prąd) oznacza, że europejskie środki finansowe przyczyniają się do rozwoju przede wszystkim tamtejszej gospodarki - zamiast rodzimej.

> NIS2 jest Dyrektywą, która nakłada na kraje oraz organizacje z tych krajów nowe wymogi, lecz ostatecznie każdy z krajów musi sam wprowadzić własne przepisy lokalne. W Polsce, lokalne przepisy Dyrektywy zostaną wprowadzone w najbliższym czasie

Konflikt przyszłości (teraźniejszości?) w cyberprzestrzeni

Niezaprzeczalnym faktem jest silna zależność społeczeństwa od dostaw energii elektrycznej, a wszelkie zakłócenia w stabilnym funkcjonowaniu systemu energetycznego stanowią skuteczne narzędzie nacisku. Poleganie na technologii dostarczanej przez jedno państwo godzi w jeden z filarów europejskiej transformacji energetycznej - dywersyfikację źródeł. W rezultacie, z jednej strony odchodzimy od energetycznej dominacji Rosji i jej paliw kopalnych, które przez dekady zasilały Europę, a z drugiej - stopniowo wpadamy w orbitę wpływów innego globalnego mocarstwa, co niesie ze sobą podobne co do zasady wyzwania i ryzyka.

Niewątpliwie jednym z celów konfliktów międzypaństwowych jest doprowadzenie do destabilizacji infrastruktury krytycznej przeciwnika. Działania tego typu mają miejsce również w cyberprzestrzeni, co pokazuje chociażby wojna w Ukrainie. Nieustannie dochodzi do prób włamania do ukraińskiego systemu elektroenergetycznego przez grupy sponsorowane zapewne przez rząd Rosji. Już w 2015 r., krótko po aneksji Krymu doszło do znacznych blackoutów na terytorium Ukrainy, spowodowanych wprowadzeniem złośliwego oprogramowania[8]. Tego typu działania znacząco nasiliły się po 24 lutego 2022 r., dotykając również państw europejskich i innych, wspierających Ukrainę. Potwierdza to raport opublikowany przez Microsoft w czerwcu 2022 r.[9], wskazujący znaczący wzrost liczby prób włamania do sieci i serwisów europejskich oraz amerykańskich organizacji rządowych i firm energetycznych. □

Przypisy:

1 Rogue communication devices found in Chinese solar power inverters | Reuters
2 Deye deaktiviert Solar-Wechselrichter in USA, UK und PakistanBorns IT- und Windows-Blog
3 Certyfikacja cyberbezpieczeństwa coraz bliżej - Baza wiedzy - Portal Gov.pl
4 Raport „Rynek Fotowoltaiki w Polsce 2024” - EC BREC Instytut Energetyki Odnawialnej | Fotowoltaika
5 Korupcja w Parlamencie Europejskim. Huawei pod lupą śledczych
6 Lithuania bans remote Chinese access to solar, wind, storage devices – pv magazine International
7 https://raport.valisluureamet.ee/2024/en/
8 Energetyka.Plus - Cyberbezpieczeństwo infrastruktury krytycznej – energetyka na celowniku hakerów
9 Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues