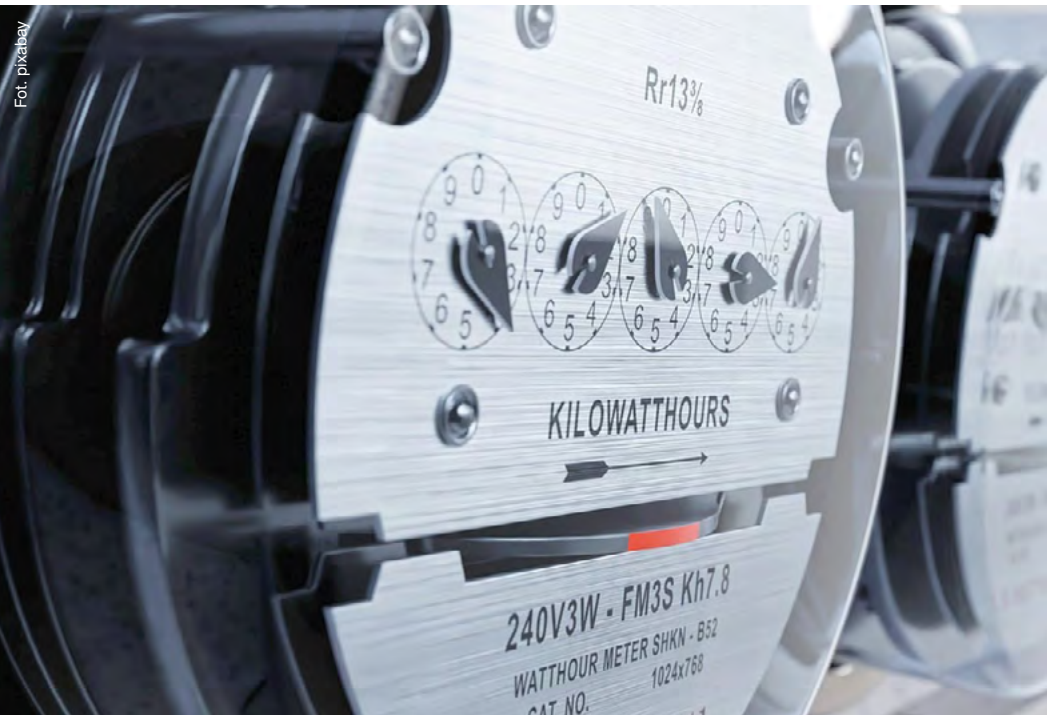
■ Sekcja Inteligentnych Sieci - Smart Grids,
Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Cyberbezpieczeństwo inteligentnych sieci

w kontekście rolloutu liczników smart

W Polsce trwa masowa wymiana liczników energii elektrycznej na urządzenia ze zdalnym odczytem (LZO). Do 2028 r. zostanie zamontowanych w sieci energetycznej ok. 16 mln liczników wyposażonych w moduł komunikacyjny. Z zainstalowanych do tej pory ok. 4 mln urządzeń ponad połowa pochodzi spoza Europejskiego Obszaru Gospodarczego. Liczniki smart to nowoczesne urządzenia cyfrowe z funkcją komunikacji. Zgodnie z obecnym stanem prawnym, muszą spełniać jedynie podstawowe wymagania formalne - niemal identyczne, jakie były stawiane w ubiegłym wieku prostym licznikom elektromechanicznym. W praktyce wystarcza certyfikacja MID (sprawdzana jest tylko niepełna metrologia) oraz znak CE (bezpieczeństwo fizycznego użytkowania). Dla komunikujących się liczników cyfrowych taki przestarzały system weryfikacji to stanowczo za mało. Robi się niebezpiecznie.



Fot. pixabay

W przeciwieństwie do takich krajów, jak Francja, Niderlandy, czy Wielka Brytania nie mamy w Polsce systemu weryfikacji i dopuszczania do naszego rynku urządzeń cyfrowych, które pracują w sieci energetycznej. Najwyższy czas podjąć pilne działania prewencyjne, zanim w naszych domach zostaną zainstalowane urządzenia, które potencjalnie mogą stwarzać ryzyko cyfrowego ataku - szczególnie, że sytuacja geopolityczna powinna specjalnie uczulać nas na takie zagrożenia.

Najbliższe miesiące mogą być decydujące dla przyszłości i bezpieczeństwa inteligentnych sieci w Polsce. Brak regulacji w zakresie cyberbezpieczeństwa liczników LZO stosowa-

nych w sektorze energii nie zwalnia nas z obowiązku rozsądnego doboru dostawców sprzętu. Postępujący proces transformacji energetycznej pociąga za sobą konieczność digitalizacji sektora, będącej warunkiem jego dynamicznego rozwoju, a jednocześnie rodzącej wyzwania związane z odpornością na fizyczne i cyfrowe zagrożenia. Technologie teleinformatyczne były, są i będą przedmiotem ataków grup przestępczych, aktorów sponsorowanych przez państwa lub wprost przez służby nieprzyjaznych państw. Suwerenność technologiczna dla sprzętu pomiarowego (LZO), który zawiera także podzespoły wykonujące komendy wydawane zdalnie, powinna być uwzględniona w procesie transformacji energetycznej na tych samych zasadach, jak w przypadku technologii informatycznych.

Liczniki inteligentne są istotnym ogniwem w łańcuchu zaopatrzenia w energię elektryczną, a ich zdalne lub zaplanowane zakłócenie może wywołać rozległe awarie energetyczne w sieciach dystrybucyjnych, wpływając negatywnie na duże grupy odbiorców i przedsiębiorstw. Motywacje i zasoby, by taki atak przeprowadzić, mają państwa rywalizujące, nieprzychylne lub wręcz wrogie szeroko rozumianemu Zachodowi, które sukcesywnie zwiększają swoją pozycję na polskim rynku zaawansowanej infrastruktury pomiarowej (AMI, z ang. *Advanced Metering Infrastructure)*. Tymczasem faktem jest, że zaczynamy w Polsce instalować urządzenia od producentów zlokalizowanych tysiące kilometrów stąd w krajach, które w sposób mniej lub bardziej jawny kontrolują na poziomie centralnym łańcuchy dostaw i opowiadają się za niedemokratycznymi sposobami zarządzania gospodarką. Jak to możliwe?

Przedstawiciele branży akcentują potrzebę podjęcia konkretnych działań ze strony Polskiego Rządu i powołanych do tego celu instytucji i służb, aby stworzyć optymalne warunki dla transformacji energetycznej, która wymaga bezpiecznej, odpornej na cyfrowe zagrożenia infrastruktury energetycznej.

Istnieje potrzeba doprecyzowania i uszczegółowienia wymagań dotyczących bezpieczeństwa cyfrowego liczników smart w już istniejących regulacjach, tj. w tzw. „Rozporządzeniach pomiarowych" (załącznik do nowelizacji Prawa energetycznego), tak aby stały się one w pełni funkcjonalną Specyfikacją Uzupełniającą (tzw. „Companion Standard"). Następnie powinniśmy jak najszybciej powołać/uruchomić profesjonalne krajowe niezależne laboratorium testujące konkretne wybrane typy urządzeń, które dany dostawca chciałby potencjalnie wprowadzić na nasz rynek. Wzorem mogą być np. krajowe laboratoria weryfikacyjne LAN we Francji, czy Tecnalia albo Instiituto Technologico la Energia w Hiszpanii lub DNV -GL dla Niderlandów. Laboratorium może być albo powołane przy którąś z renomowanych uczelni (politechnik), albo jako niezależna lecz notyfikowana przez instytucje Państwowe firma komercyjna.

Laboratorium testowałoby zgodność funkcjonalną z polskim „comapnion standard" (conformance), zdolność współpracy urządzeń od różnych producentów w jednej cyfrowej sieci energetyki zawodowej (AMI) i co najważniejsze - ich podatność na potencjalny atak cyfrowy z zewnątrz (nie tylko zdalny, ale także spowodowany przez potencjalne zaplanowane wcześniej „modyfikacje" sprzętu lun firmware (tzw. atak poprzez łańcuch dostaw).

Znanych jest wiele przykładów do czego może doprowadzić wprowadzanie na rynek krajowy i masowa instalacja urządzeń, które nie zostały wcześniej sprawdzone i zweryfikowane:

- **2001 r.** - dostawca energii elektrycznej California Independent System Operator - atakujący uzyskali dostęp do jednej z wewnętrznych sieci. Atak wpłynął na sieć elektroenergetyczną ofiary zanim został wykryty, w efekcie powodując przerwę w dostawie energii elektrycznej dla ok. 400 000 odbiorców. Prawdopodobnie był sponsorowany przez Chiny.
- **2015 r.** - Trzech operatorów sieci dystrybucyjnej (OSD) w Ukrainie - ponad 50 podstacji elektroenergetycznych zostało odłączonych od sieci. Braki w zasilaniu dotknęły ok. 225 000 odbiorców. System automatyki przemysłowej został fizycznie uszkodzony. Podstacje musiały być obsługiwane ręcznie przez kilka tygodni po zdarzeniu. Atakujący wykorzystał malware o nazwie BlackEnergy, atak prawdopodobnie sponsorowany przez Rosję.
- **2016 r.** - operator sieci przesyłowej (OSP) w Ukrainie - celem ataku stała się część systemu odpowiedzialna za dostarczanie energii do ukraińskiej stolicy. Konsekwencją ataku były poważne ograniczenia w dostawach prądu dla tysięcy odbiorców w północnej części Kijowa. Atak prawdopodobnie sponsorowany przez Rosję, co wykazało przeprowadzone międzynarodowe śledztwo (w 2016 r. doszło również do podobnych ataków na sieć energetyczną w USA przeprowadzonych przez tego samego aktora).
- **2016 r.** - sieci elektroenergetyczne w Izraelu - w wyniku ataku nie doszło do przerw w dostawach energii elektrycznej, jednak skompromitowano systemy rządowe związane z energetyką, brak atrybucji.
- **2022 r.** - seria ataków na turbiny wiatrowe różnych operatorów w Europie - w wyniku ataków jeden z operatorów utracił połączenie z 6000 turbin wiatrowych, inny padł ofiarą ataku ransomware, zaś kolejny na 24 godziny był zmuszony wyłączyć wszystkie urządzenia zarządzane zdalnie. Ataki te związane były prawdopodobnie z wybuchem wojny w Ukrainie i były realizowane przy wsparciu rosyjskim.

Atak atakowi nierówny

Należy zauważyć, że nie wszystkie potencjalne rodzaje ataków cyfrowych są w przypadku energetyki równie niebezpieczne. Ekspertyza przeprowadzona przez dwie polskie firmy Apator i ComCert (dostępna pod adresem: https://api.apator.com/uploads/cyberbezpieczenstwo/ekspertyza.pdf oraz pod adresem: https://api.apator.com/uploads/cyberbezpieczenstwo/fact-sheet-cyberbezpieczenstwo-.pdf wykazała że **Atak Fizyczny**, czyli włamanie poprzez manipulację komponentami sprzętowymi urządzenia i jego oprogramowaniem układowym jest wprawdzie łatwiejszy od innych rodzajów ataku, ale obejmuje on stosunkowo niewielką liczbę urządzeń (zazwyczaj jeden licznik), powodując stosunkowo niewielkie szkody w ujęciu społecznym. Jest on także stosunkowo łatwy do wykrycia, bo liczniki same zdalnie powiadamiają operatora o naruszeniu obudowy, plomby, czy innym sabotażu. Służby energetyczne reagują zazwyczaj w takim przypadku bardzo szybko i skutecznie.

Innym rodzajem ataku może być **Atak na Kanał Komunikacyjny**, w którym następuje przechwycenie lub/i manipulacja danymi/komendami przesyłanymi do i od licznika w kierunku systemu nadrzędnego infrastruktury AMI. Ten rodzaj ataku jest groźniejszy, bo daje efekt dla potencjalnie wielu liczników, jak i innych elementów sterowania sieci energetycznej. Jednak tutaj stosujemy już odpowiednie systemy szyfrowania przesyłanych informacji. Mamy także wdrożone aktywne systemy śledzące „podejrzany" ruch w sieciach informatycznych. Ponadto taki atak wymaga bardzo specjalistycznej wiedzy, ponieważ sieci cyfrowe energetyki są dedykowane i specyficzne i często fizycznie wydzielone. Różnią się one znacznie od powszechnie używanych sieci domowych i komercyjnych. Nawet kanały komunikacyjne i ich pasma są najczęściej inne niż te w sieciach informatycznych użytku powszechnego (np. wąskopasmowe PLC).

	Obecne środki ochrony	Potencjalne następstwa
Atak fizyczny	średnie	niskie
Atak na kanał komunikacyjny	wysokie	średnie
Atak na łańcuch dostaw	niskie	wysokie

Źródło: Ekspertyza Apator, ComCert

Jednym słowem ten rodzaj ataku - choć potencjalnie groźny - mamy dość dobrze zabezpieczony i monitorowany na bieżąco.

Przeprowadzona pogłębiona analiza wykazała, że prawdopodobnie największym obecnie zagrożeniem dla systemu elektroenergetycznego związanym m. in. z licznikami smart jest tzw. **Atak poprzez Łańcuchy Dostaw**. Ten rodzaj ataku może być przeprowadzony przez wykorzystanie backdoorów, bomb logicznych zaimplementowanych w samym oprogramowaniu układowym licznika podczas jego procesu produkcyjnego (świadome i zaplanowane działanie). Do takich narzędzi dostęp mają przede wszystkim producenci komponentów elektronicznych lub całych liczników.

Wykrycie takiej manipulacji jest oczywiście możliwe, ale może być niezmiernie trudne. Nawet producent licznika może nie być świadomym „zainfekowania" wytwarzanych przez siebie urządzeń. Klient końcowy (OSD), lub tym bardziej użytkownik licznika smart, ma minimalne szanse na zapobiegania takim planowanym na skalę krajową atakom.

Szereg zaleceń branżowych znalazło się także w Stanowisku Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, dotyczącym bezpieczeństwa liczników energii z dnia 4.08.2023. **Dokument ten dostępny jest pod adresem: https://kigeit.org.pl/FTP/if/SIS-SG/230804_Stanowisko_KIGEiT_Bezp_liczn_e.e.pdf**

Przedstawiciele branży polecają zastosowanie prostych, ale bardzo skutecznych przedsięwzięć zapobiegawczych, którymi jest niedopuszczanie do infrastruktury krytycznej Polski i UE dostawców z geograficznych obszarów wysokiego ryzyka (tych z poza EOG).

Zastosowanie tej prostej zasady prewencji wymaga nie tylko ostrożności i odpowiedzialności osób rozpisujących i rozstrzygających przetargi publiczne w energetyce, ale przede **wszystkim wydania natychmiastowych zaleceń lub przepisów prawnych przez odpowiednie służby Państwowe**. Tak właśnie postąpił niedawno czeski Urząd Bezpieczeństwa Cyfrowego (NUKIB), który w swojej rekomendacji zabronił zakładom energetycznym montowania liczników spoza Europejskiego Obszaru Gospodarczego, tym samym skutecznie przeciwdziałając narażaniu krajowej infrastruktury energetycznej na dodatkowe niebezpieczeństwo. Czasami takie proste, ale odpowiedzialne obywatelsko działanie może uchronić nas wszystkich przed poważnymi kłopotami.

Zespół specjalistów od cyberbezpieczeństwa i inżynierów tworzących zaawansowaną infrastrukturę pomiarową ostrzega: skoro **nie jesteśmy dziś w stanie sprawdzić szczegółowo, co dokładnie może zostać zainstalowane w elektronice profesjonalnej, którą kupujemy w masowych przetargach publicznych i instalujemy w sieci energetycznej, to kupujmy ją od zaufanych dostawców**. I czym prędzej przystąpmy do opracowania skutecznych regulacji w tym obszarze. □