Kamil Kowalczuk

Wdrożenie „Smart Metering" w kontekście cyberzagrożeń

„Smart metering", czyli inteligentne zarządzanie energią elektryczną. Staje się faktem w naszej rzeczywistości. Zgodnie z nowelizacją Prawa energetycznego wymienione zostaną liczniki prądu na tak zwane inteligentne liczniki AMI (*Advanced Metering Infrastructure*). W głównej mierze wymianie zgodnie z aktualnym Prawem Energetycznym i harmonogramem do 2028 r. ma podlegać 80% liczników stosowanych w gospodarstwach domowych, a do 2030 100% liczników.

Fot. American Public Power Association, Compaign Creators on unsplash

Główne korzyści dla OSD (Operatora Sieci Dystrybucyjnej):

- redukcja kosztów odczytu tradycyjnych liczników;
- uniknięcie kosztów legalizacyjnych liczników;
- ograniczenie różnicy bilansowej;
- korzyści z wcześniejszego wystawienia faktury odbiorcom;
- redukcja kosztów pozostałych operacji na licznikach (np. prace serwisowe).

Ponadto można zauważyć szereg korzyści dla przeciętnego „Kowalskiego", m. in.:

- efektywniejsza identyfikacja miejsca awarii oraz szybsze usunięcie awarii;
- możliwość monitorowania zużycia energii;
- zdalny odczyt.

W przyszłości prawdopodobnie będzie można również wdrożyć system, który pozwoli odbiorcom płacić za ilość faktycznie zużytej energii elektrycznej. Pojawi się wiele innych dodatkowych udogodnień dla odbiorców, które umożliwi interfejs HAN (Home Area Network).

Wyzwania Cyberbezpieczeństwa vs AMI

Całość systemu mocno wykracza poza tradycyjne zrozumienie systemów OT (Operation Technology).

Zmiany w odczycie i nowe możliwości jakie dają inteligentne liczniki wiążą się ze zmianami również w zakresie podejścia do cyberbezpieczeństwa danych obsługiwanych przez System. Dotyczy to zmian w architekturze rozwiązania na poszczególnych warstwach komunikacji w Systemie AMI (kompletne rozwiązanie Smart Metering).

Warstwa komunikacji z odbiorcą

Mowa tutaj o komunikacji bezpośrednio z odbiorcą poprzez interfejs HAN. Jednym z podejść jest budowa portalu i aplikacji na urządzenia mobilne dla klientów OSD. Wiąże się to z szeregiem zagrożeń w kontekście zachowania poufności, integralności i dostępności danych. W obszarze Home Area Network można się spodziewać zagrożeń:

- braki w aktualizacji oprogramowania np. aplikacja mobilna, czy portal www;
- złośliwe oprogramowanie, które wprowadzone do sieci HAN może w konsekwencji prowadzić do infekcji urządzenia lub nawet utraty kontroli nad nim;
- wyciek danych osobowych, których kradzież w konsekwencji może narazić konsumentów na szereg oszustw, łącznie z utratą tożsamości. Dane profilowe (trendy zużycia) również mogą być istotne dla przestępców, bo np. informują przestępców o cyklu życia domowników, co może ułatwić zaplanowanie włamania;
- ze względu na postępującą integrację sieci HAN nie tylko z licznikami, ale również w przyszłości z innymi urządzeniami - nie można wykluczyć ataków man-in-the-middle i podsłuchu danych, co może prowadzić do wycieku wielu poufnych danych;
- również z tego samego powodu jw. nie wykluczone są ataki na urządzenia IoT (inteligentne urządzenia takie jak: inteligentne zamki, termostaty, kamery). Przejęcie nad nimi kontroli może doprowadzić nawet do zmiany ich zastosowania i mogą być wykorzystane przez atakujących do innych celów, np. jako przyczółek do przejęcia kontroli nad routerem domowym, czy jako punkt pośredniczący w ataku na inne cele;
- ataki na infrastrukturę sieciową mogą otworzyć furtkę na dostęp do wszystkich urządzeń w sieci HAN, czy też zastosowanie ataku DDOS (*Destributed Denial of Service*) może uniemożliwić właściwą pracę sieci.

Jak w takim razie skutecznie dbać o bezpieczeństwo w/w warstwy?

Należy zwrócić uwagę na:

- ustanowienie silnego uwierzytelnienia, aby zapobiec nieautoryzowanemu dostępowi np. poprzez wieloskładnikowe uwierzytelnienie;
- wykorzystać zabezpieczenia sieciowe takie jak: firewalle, IDS, czy inne mechanizmy, które prewencyjnie utrudnią atakującemu dostęp do sieci;
- niezwykle ważne staje się edukowanie użytkowników, aby uniknąć potencjalnych zagrożeń, np. poprzez wydanie dla nich kanonu dobrych praktyk i zachowań w cyfrowym świecie, jest to w interesie OSD, jak i odbiorcy;
- aktualizować oprogramowanie możliwie często, aby uniknąć możliwości wykorzystania zidentyfikowanych podatności. System aktualizacji winien być najmniej angażujący użytkownika końcowego;
- ze względu na to, że sieć HAN jest siecią niezaufaną dla infrastruktury Systemu AMI, należy wdrożyć

> Jak widać, zagrożenia i niwelowanie ich w obszarze inteligentnych pomiarów jest problemem złożonym i wielowarstwowym. Ze względu na dokonywane zmiany w zakresie regulacji prawnych i wytycznych bezpieczeństwa - w tym również regulacje ogólnoeuropejskie, należy podejść do bezpieczeństwa Smart Meteringu w sposób holistyczny i oprzeć się na uniwersalnych zasadach

monitorowanie sieci co najmniej na elementach należących do OSD w celu identyfikacji potencjalnych zagrożeń:

- budowa zasad w postaci Polityki Bezpieczeństwa również jest korzystna dla OSD, ponieważ zdefiniuje kwestie ważne ze względu na sposób zarządzania urządzeniami, ich konfiguracją, jak i dostępem dla użytkowników.

Wyłącznie silna interakcja z użytkownikami, jak i kompleksowe podejście może zmitygować odpowiednio zagrożenia.

Warstwa komunikacji licznik, a koncentrator

Mowa tutaj o komunikacji pomiędzy licznikami w gospodarstwach, a koncentratorami oraz licznikami bilansującymi. W/w warstwa jest w kompetencjach OSD. Zagrożenia, które mogą wystąpić poza wymienionymi dla HAN to m. in.:

- ataki z wykorzystaniem błędów w protokołach transmisji, intruz może wykorzystać je w celu destabilizacji pracy urządzeń;
- podsłuch transmisji, w przypadku wykorzystania przestarzałych algorytmów szyfrowania lub jego brak przechwycenie danych przez intruza umożliwi mu ich odczyt i wykorzystanie;
- atak na integralność danych, np. poprzez wstrzyknięcie nieprawidłowych danych do systemu może doprowadzić do błędnych odczytów i obliczeń. W konsekwencji może to prowadzić dla OSD do utraty wizerunku i zaufania klientów, jak i do strat finansowych;
- ze względu na ograniczenia techniczne, atakujący może również podszyć się np. pod koncentrator i uzyskać dostęp do sieci lub danych.

W w/w warstwie, która jest pod kontrolą OSD skupić się należy na:

- wdrożeniu silnego szyfrowania do zabezpieczenia komunikacji, np. poprzez budowę własnego Centrum Autoryzacji (dalej CA) w oparciu o system KMS *(Key Managment System)*. Ważne jest, aby właściwe zarządzać cyklem życia kluczy szyfrujących i przeprowadzić odpowiednią separację CA od systemów dziedzinowych oraz urządzeń;
- należy rozważyć wdrożenie systemu klasy PAM *(Privileged Access Control)* w celu zarządzania dostępem uprzywilejowanym (np. konta administratorskie). Jest to o tyle istotne, że dostęp będą posiadali często nie tylko pracownicy, ale również pracownicy firm wspierających. Właściwie zarządzanie cyklem życia kont o podwyższonych uprawnieniach w kontekście skali jest krytyczne dla OSD.

Warstwa komunikacji koncentrator, a systemy OSD

Warstwa ta jest krytyczna dla funkcjonowania całego Systemu AMI. Koncentrujemy się na wymianie danych pomiędzy aplikacją AMI, a koncentratorami, jak i na wymianie danych z systemami dziedzinowymi istotnymi dla biznesu w ramach OSD oraz na udostępnieniu danych innym uczestnikom rynku - w tym komunikacji ze sprzedawcami i OIP (Operator Informacji Pomiarowej).

Zagrożenia dla w/w warstwy są tożsame z pozostałymi warstwami, przy czym mogą mieć zasięg globalny dla całego Systemu AMI. Niezwykle istotne staje się przeprowadzanie regularnych audytów bezpieczeństwa nie tylko w warstwie technicznej, ale też proceduralnej. Ponadto należy rozważyć cykliczne przeprowadzanie testów poszczególnych urządzeń wchodzących w skład systemu np. liczników, koncentratorów - szczególnie, gdy zmieniamy oprogramowanie wskazanych urządzeń.

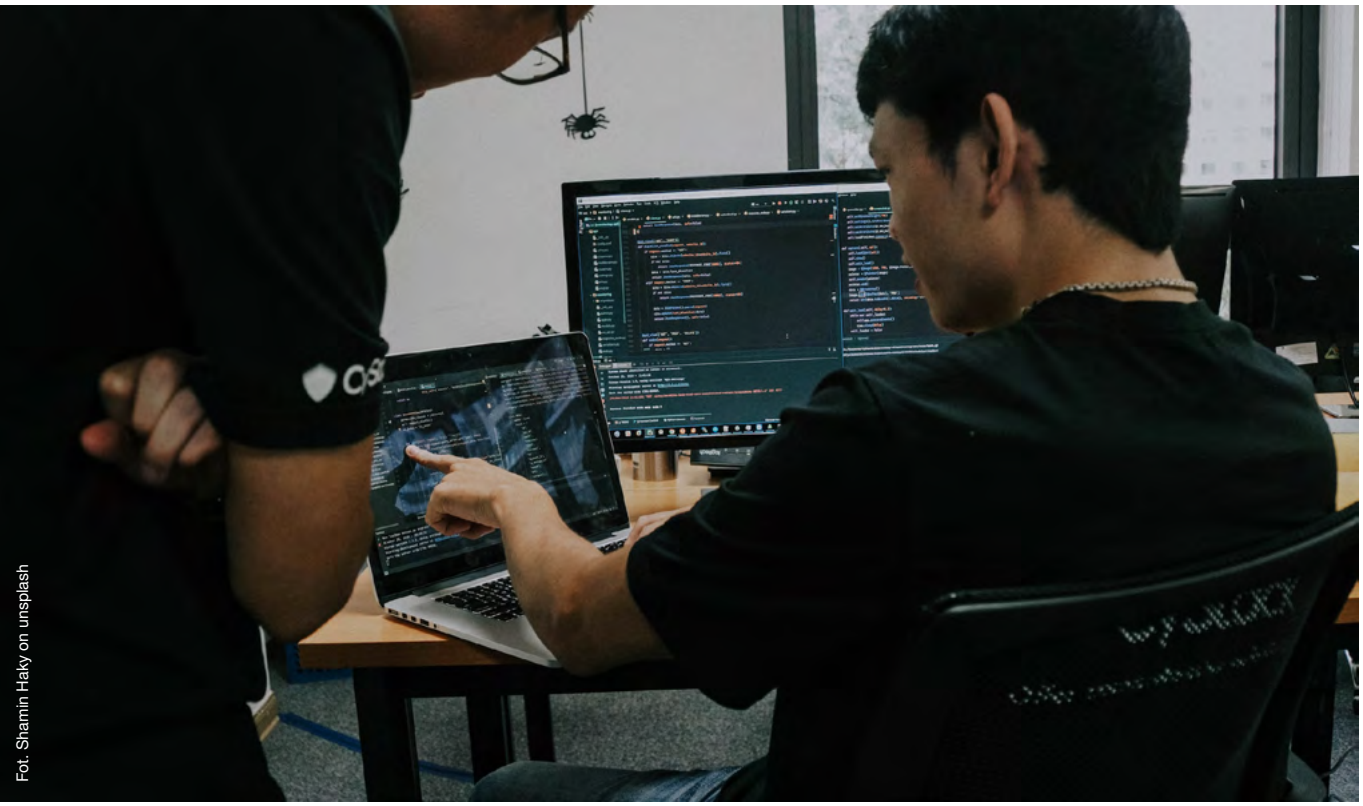
Jak widać, zagrożenia i niwelowanie ich w obszarze inteligentnych pomiarów jest problemem złożonym i wielowarstwowym. Ze względu na dokonywane zmiany w zakresie regulacji prawnych i wytycznych bezpieczeństwa - w tym również regulacje ogólnoeuropejskie, należy podejść do bezpieczeństwa Smart Meteringu w sposób holistyczny i oprzeć się na uniwersalnych zasadach.

Dobrym punktem wyjścia dla już eksploatowanych i nowo wdrażanych systemów jest oparcie się na standardach międzynarodowych, nie zależnie od otoczenia prawnego, zastosowanie wytycznych z normy ISO/IEC 62443, jako podstawy dla projektowania systemu (warstwa techniczna) oraz dla budowy polityk (warstwa proceduralna) umożliwi optymalne i właściwe zabezpieczenie Systemu AMI.

Kluczowe pryncypia standardu:

- Klasyfikacja ryzyka
  Polega to na określeniu potencjalnych zagrożeń i ich klasyfikacji. Na tej podstawie można określić ryzyko związane z systemem. Należy podejść do tego punktu z należytą staranością, ponieważ z niego będą wynikać adekwatne zabezpieczenia dla systemu - techniczne, jak i proceduralne.
- Kontrola dostawców
  Ustanowienie wymagań bezpieczeństwa w kontraktach z dostawcami oraz zapewnienie OSD możliwości kontroli spełnienia wymagań (np. testy odbiorowe, audyt dostawcy wykonywany przez OSD lub wskazaną przez niego firmę audytową - audyty

> Wdrożenie standardu jest procesem złożonym i wymagającym, często prowadzi do zmiany kultury organizacyjnej, ale korzyści z poprawy bezpieczeństwa są znaczne i długofalowe



Fot. Shamin Haky on unsplash

winny być cykliczne w trakcie cyklu życia systemu).

- Bezpieczne projektowanie Systemu
  Należy uwzględnić kwestie bezpieczeństwa w procesie projektowania systemu. W ramach segmentacji sieci należy już na tym etapie uwzględnić strefy oraz przepływ danych - w szczególności dotyczy to komunikacji z sieciami nie zaufanymi.
- Bezpieczeństwo w cyklu życia Systemu
  Uwzględnienie aspektów bezpieczeństwa w cyklu życia systemu od fazy projektowej do utrzymania, np. kwestie zarządzania podatnościami, czy cykl retencji kopii zapasowej. Należy uwzględniać kwestie tak zwanej „zimnej kopii bezpieczeństwa", która winna być odseparowana od Systemu produkcyjnego. Pozwoli to ograniczyć skutki potencjalnego ataku Ransomware - złośliwe oprogramowanie, które szyfruje dane i aplikację paraliżując System.
- Kontrola dostępu
  Implementacja odpowiednio silnego uwierzytelnienia i weryfikacji tożsamości oraz wdrożenie zasady najmniejszych niezbędnych uprawnień. Wskazane jest, aby zweryfikować dostęp nie tylko w warstwie aplikacyjnej, ale również systemu operacyjnego, kart ILO, czy warstwy wirtualizacyjnej. Dostęp winien być zweryfikowany na każdej płaszczyźnie uwierzytelnienia, dlatego należy również uwzględnić dostęp np. SNMP, czy konta lokalne dla kart ILO, czy też dostęp serwisowy do liczników, czy koncentratorów.
- Zarządzanie zmianami
  Wprowadzanie zmian w systemie w sposób kontrolowany i udokumentowany, aby uniknąć naruszeń bezpieczeństwa.
- Monitorowanie i reagowanie na incydenty
  System z punktu widzenia otoczenia jest kluczowy dla działalności OSD i dlatego należy go monitorować w trybie ciągłym i reagować na wszelkie nieprawidłowości. Właściwie zidentyfikowany zakres zagrożeń pozwoli zespołowi SOC (Security Operation Center) zbudować adekwatne scenariusze reakcji i zadbać o bezpieczeństwo, ale i właściwe działanie Systemu.

Wdrożenie standardu jest procesem złożonym i wymagającym, często prowadzi do zmiany kultury organizacyjnej, ale korzyści z poprawy bezpieczeństwa są znaczne i długofalowe.

Z punktu widzenia biznesowego wdrożenie standardu przekłada się na zwiększenie zaufania klientów i partnerów, ogranicza straty finansowe, czy ułatwia spełnienie wymogów regulacyjnych. W szerszej perspektywie poprawia również konkurencyjność OSD. Organizacje, które pokazują zaangażowanie w aspekty bezpieczeństwa budują swoją konkurencyjność, ponieważ coraz więcej partnerów i klientów zwraca na kwestie cyberbezpieczeństwa uwagę. □