Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 62

XIX Konferencja Naukowa

AKTUALNE PROBLEMY W ELEKTROENERGETYCE APE'19

Jastrzębia Góra, 12-14 czerwca 2019

doi: 10.32016/1.62.11

BEZPIECZEŃSTWO INFORMATYCZNE INTELIGENTNYCH SYSTEMÓW POMIAROWYCH W ŚWIETLE USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Aleksander BABŚ

Instytut Energetyki Oddział Gdańsk
tel.: +58 349 8230 e-mail: aleksander.babs@ien.gda.pl

Streszczenie: 28 sierpnia 2018 weszła w życie Ustawa o Krajowym Systemie Cyberbezpieczeństwa, implementująca wymagania europejskiej dyrektywy NIS.
Wszyscy operatorzy usług kluczowych będą zobowiązani do wdrożenia określonych w ustawie procedur dotyczących m.in. szacowania ryzyka w zakresie funkcjonowania świadczonych usług kluczowych, zarządzania incydentami a przede wszystkim zastosowania adekwatnych do oszacowanego ryzyka środków technicznych i organizacyjnych. Istotnym elementem szacowania tego ryzyka jest znajomość potencjalnych wektorów ataku możliwych do wykorzystania do naruszenia stabilności systemu realizującego określoną usługę kluczową.
Systemy inteligentnego opomiarowania, m.in. ze względu na fakt, iż wykorzystują liczniki energii elektrycznej pozostające fizycznie poza kontrolą operatora sieci, mogą być celem cyberataku o dużym zasięgu i istotnym, negatywnym wpływie na działanie sieci elektroenergetycznej i ciągłość dostaw energii elektrycznej.
Referat przedstawia wybrane scenariusze ataku na infrastrukturę inteligentnego opomiarowania oraz środki zapobiegawcze których zastosowanie może podnieść odporność na dotychczas zidentyfikowane metody cyberataku. W referacie przedstawiono sposób zapewnienia bezpieczeństwa informatycznego inteligentnych systemów pomiarowych. Określono procedury związane z badaniami poziomu bezpieczeństwa systemów inteligentnego opomiarowania w odniesieniu do poszczególnych warstw tych systemów.

Słowa kluczowe: inteligentne systemy pomiarowe, cyberbezpieczeństwo.

1. WPROWADZENIE WYMAGANIA USTAWOWE

W dniu 28 sierpnia 2018 weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa (KSC), wdrażająca wymagania dyrektywy europejskiej [1] NIS (Network and Information Systems Directive).

Nakłada ona nowe obowiązki na podmioty z sektorów energetyki, infrastruktury cyfrowej, zaopatrzenia w wodę pitną, bankowości, ochrony zdrowia i transportu. Ustawa ta wyodrębnia operatorów usług kluczowych (OUK), do których zalicza się m. in. firmy z sektora energetycznego, w tym również operatorów systemów dystrybucyjnych.

Przewidziany w ustawie harmonogram działań nakazuje operatorom usług kluczowych podjęcie takich działań jak:

- oszacowanie ryzyka w aspekcie zapewnienia ciągłości świadczenia usług kluczowych, a ponadto wdrożenie procedur zarządzania incydentami, usunięcie podatności systemów informatycznych oraz wyznaczenie osoby odpowiedzialnej za kontakt z innymi podmiotami zobowiązanymi do wdrożenia KSC (w terminie 3 miesięcy od dnia doręczenia decyzji o zaliczeniu w poczet operatorów usług kluczowych),
- wdrożenie środków technicznych i organizacyjnych odpowiednich do oszacowanego ryzyka oraz zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, zbieranie informacji o zagrożeniach i podatnościach oraz przygotowanie dokumentacji (w terminie 6 miesięcy, okoliczności jak wyżej),
- przygotowanie pierwszego audytu oraz przekazanie sprawozdania z audytu organowi wskazanemu w Ustawie o KSC (w terminie 12 miesięcy, okoliczności jak wyżej).

W świetle powyższych regulacji prawnych szczególnego znaczenia nabiera spełnienie tych wymagań w odniesieniu do systemów informatycznych określanych jako przemysłowe systemy sterowania [1] lub systemy technologiczne (systemy OT – Operational Technology). Niezakłócone działanie tych systemów w porównaniu do systemów informatycznych ogólnego przeznaczania (systemy IT - Information Technology), ma kluczowy wpływ na bezpieczeństwo całych dziedzin życia ze względu na swój sposób działania, tj. działanie w czasie rzeczywistym, rozległość terytorialną i obsługę takich dziedzin życia jak: dostawa energii, bezpieczny transport itp. W przewodniku poświęconym bezpieczeństwu systemów sterowania przemysłowego [1] zostały opisane wymagania dotyczące zapewnienia bezpieczeństwa informatycznego systemom OT oraz sposoby ich spełnienia.

Wymagania te zostaną opisane w odniesieniu do jednego z systemów krytycznych wdrażanych u krajowych OSD, systemu informatycznego zaliczanego do grupy systemów technologicznych OT – systemu akwizycji danych pomiarów z liczników inteligentnych (system AMI – Advanced Metering Infrastructure).

2. SPOSÓB REALIZACJI WYMAGAŃ USTAWY

Oszacowanie ryzyka

Zgodnie z wymogami ustawy konieczne będzie posiadanie sformalizowanego, systematycznego procesu oceny i zarządzania ryzykiem systemów SCADA.

Punktem wyjścia do oszacowania ryzyka (jak też wielu innych kluczowych procesów zarządzania cyberbezpieczeństwem) jest inwentaryzacja zasobów urządzeń teleinformatycznych odpowiedzialnych za działanie infrastruktury krytycznej. Inwentaryzacja zasobów systemów informatycznych głównie z grupy OT jest możliwa za pomocą specjalizowanego pakietu oprogramowania do pasywnej analizy sieci informatycznej. W wyniku działania takiego oprogramowania otrzymuje się mapę połączeń host-to-host sieci OT.

Kolejnym krokiem jest identyfikacja podatności systemów OT możliwa do wykonania za pomocą specjalizowanego pakietu oprogramowania. Szczególną rolę mają w tym względzie testy penetracyjne (pentesty), które są w istocie wieloaspektową próbą kontrolowanego włamania się do istniejących rzeczywistych systemów OT prowadzone w celu określenia podatności badanego systemu teleinformatycznego na ataki wewnętrzne i zewnętrzne poprzez wskazanie miejsca i sposobu takiego włamania. Rozbudowane oprogramowania specjalistyczne umożliwia wykonanie kilkuset testów już zdefiniowanych, przy czym w odniesieniu do systemów typu OT największą wartość mają testy dedykowane dla danego systemu uwzględniające jego specyfikę działania, wykorzystywanych protokołów czy też warstw architektury sprzętowej i programowej.

Testy penetracyjne są elementem pełnego audytu bezpieczeństwa, wykonywanego zgodnie z normą ISO 27001.

Specjalizowany pakiet oprogramowania składa się zazwyczaj z systemu centralnego, składującego dane oraz dokonującego ich szczegółowej analizy oraz trzech do pięciu sond, instalowanych w kluczowych węzłach sieci. System centralny pozwala na relokację sond do innych węzłów sieci, zgodnie z potrzebami.

Zidentyfikowane podatności podlegają analizie potencjalnych ryzyk związanych z cyberbezpieczeństwem infrastruktury krytycznej sieci OT.

Wdrożenie środków technicznych i organizacyjnych

Na podstawie wykonanej analizy ryzyk specyfikuje się wymaganie dla wdrożenia narzędzi informatycznych wspierających identyfikację przyszłych ryzyk w trybie ciągłym, zgodnie z wymaganiami Ustawy. Pod uwagę brane są następujące aspekty:

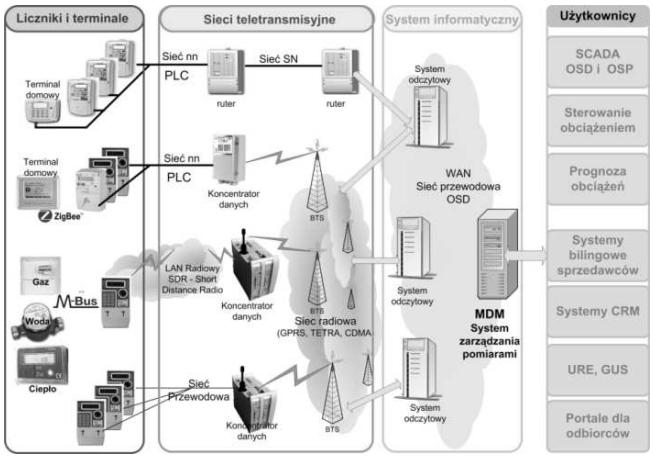
- odpowiednia architektura bezpieczeństwa,
- fizyczna lub/i logiczna separacja sieci teleinformatycznej OT od innych sieci a zwłaszcza IT
- zaprojektowanie miejsc instalacji w sieci OT i sposobu działania sond sieciowych badających ruch i stwierdzające anomalie sieci OT,
- wdrożenie zarządzania kluczami szyfrowania tj. regularnej wymiany kluczy, bezpieczna dostawa kluczy od producenta itp.,
- organizacja zasobów ludzkich dla bieżącej kontroli cyberbezpieczeństwa.

Końcowym etapem jest przygotowanie odpowiedniej dokumentacji zgodnej z rozporządzeniem Rady Ministrów.

3. WDROŻENIE PROCEDUR CYBERBEZPIECZEŃSTWA NA PRZYKŁADZIE SYSTEMU AKWIZYCJI DANYCH POMIAROWYCH Z LICZNIKÓW INELIGENTNYCH – SYSTEM AMI

Struktura systemu AMI

System inteligentnego opomiarowania składa się z części pomiarowej tj. liczników energii elektrycznej oraz koncentratorów komunikujących się z tymi licznikami z wykorzystaniem sieci elektroenergetycznej niskiego napięcia oraz systemu informatycznego OT - aplikacji centralnej AMI zbierającej i przetwarzającej dane pozyskane z liczników oraz udostępniającej te dane innym systemom np. do systemu rozliczającego odbiorców. Struktura systemu AMI została pokazana na rysunku 1. Zwraca uwagę wielowarstwowa struktura systemu i jego zasięg terytorialny. Elementy końcowe – liczniki inteligentne – zainstalowane są u odbiorców energii, a zatem fizyczny dostęp do nich jest również możliwy powszechnie.



Rys 1. Struktura systemu AMI

Sprawdzenie podatności systemu AMI

Podatność systemu AMI na cyberataki powinna być badana w odniesieniu do poszczególnych jego warstw (Rysunek 1):

- Liczniki AMI i koncentratory danych zainstalowane na stacjach SN/nn,
- Modemoroutery na stacjach SN/nn i łączność poprzez sieć komórkową i karty SIM pracujące w wydzielonym APN,
- Aplikacja centralna AMI.

Jeśli dane pomiarowe składowane w systemie AMI są udostępniane klientom poprzez serwis WWW, zasadne jest także badanie poziomu bezpieczeństwa takiego serwisu.

Wstępnym etapem realizacji audytu bezpieczeństwa jest analiza publicznie dostępnych dokumentów dotyczących charakterystyki systemu jak i informacji szczegółowych specyficznych dla danego systemu, które mogły się pojawić w takich źródłach jak:

- Specyfikacje i opracowania publikowane przez organizacje producentów sprzętu (np. PRIME Alliance OSGP Alliance, DLMS User Association),
- Informacje dostępne na stronach internetowych podmiotów, w których wdrożono system AMI tj. specyfikacje zakupowe (SIWZ) wraz z zapytaniami i odpowiedziami oraz specyfikacje techniczne i funkcjonalne sprzętu (np. DTR,

instrukcje użytkownika i administratora model danych, dokumentacja protokołów łączności).

Potencjalnymi zagrożeniami dla infrastruktury pomiarowej, które możliwe są do weryfikacji w toku realizacji testów są:

- okazjonalne lub systematyczne fałszowanie pomiarów,
- blokada akwizycji danych,
- nieuprawniony dostęp do bieżących danych pomiarowych,
- nieuprawniony dostęp do historycznych danych pomiarowych,
- przejęcie kontroli nad częścią infrastruktury AMI,
- zdalne wyłączenie i załączenie liczników.

4. PRZYKŁADOWY OPIS TESTÓW BEZPIECZEŃSTWA INFRASTRUKTURY SYTSTEMU AMI

Audyt bezpieczeństwa systemu AMI zrealizować można przeprowadzając dwa rodzaje testów:

- testy typu „whitebox" podczas którego wykorzystywane są wszystkie dostępne informacje dotyczące testowanego systemu takie jak: dane dostępowe, szczegółowa architektura systemu, klucze szyfrujące i tym podobne
- testy typu „blackbox" w którym badany system (fragment systemu) traktuje się jako czarną skrzynkę tj. tak jak może być widziany z perspektywy osoby atakującej dany system, nie posiadającej informacji zastrzeżonych lub niedostępnych publicznie.

Testy - zarówno typu „whitebox" jak też „blackbox" - dotyczyć mogą wszystkich urządzeń wykorzystywanych przez system AMI, a zatem liczników, koncentratorów danych oraz urządzeń komunikacyjnych (modemorutery) pełniących role styków tych elementów z pozostała częścią infrastruktury operatora sieci elektoenregetycznej. Zakres testów liczników inteligentnych może dotyczyć:

- możliwości enumeracji wszystkich obiektów modelu danych (np. COSEM, ANSI C.12),
- poprawności implementacji uprawnień do obiektów modelu danych,
- podatności na wysyłanie celowo błędnych danych (fuzzing).

Koncentratory danych testować można w następującym zakresie:

- weryfikacja zabezpieczeń, kont i uprawnień w systemie operacyjnym koncentratora
- sprawdzenie możliwości nieuprawnionego dostępu do koncentratora klientem protokołu odczytu danych zaimplementowanego w koncentratorze (np. DCSAP, P3.2)
- audyt podatności wbudowanego serwera WWW.

Testy bezpieczeństwa modemorouterów dotyczyć mogą:

- możliwości pozyskania istotnych danych (np. nazwa APN, SIM PIN),
- możliwości dostępu do innych urządzeń poprzez sieć komórkową - przypadku braku izolacji pomiędzy poszczególnymi węzłami w ramach wykorzystywanego APNa,
- weryfikacji zabezpieczeń, kont i uprawnień w systemie operacyjnym modemorouterów,
- audyt podatności wbudowanego serwera WWW.

Przeprowadzenie audytu bezpieczeństwa systemu AMI wymaga zastosowania zestawu narzędzi sprzętowych i programowych. Narzędzie te dzielą się na dwie kategorie – ogólnodostępne i specjalizowane, opracowane na potrzeby audytu danego systemu AMI.

Narzędzia ogólnodostępne to przykładowo:

- analizator protokołów Wireshark,
- analizator widma w paśmie CENELEC,
- zestaw narzędzi audytowych dostępnych w pakiecie Kali.

Narzędzia specjalizowane to przykładowo:

- emulator licznika AMI, umożliwiający zapis i analizę sesji odczytowych,
- generator zakłóceń o określonych właściwościach (zakłócenie jednej lub wielu częstotliwości w paśmie CENELEC),
- dekoder (dissector) danego protokołu dodany do pakietu Wireshark,
- klient protokołu odczytu danych zaimplementowanego w koncentratorze danych.

Typowy zakres testów typu „blackbox" obejmuje:

- próba podsłuchu i dekodowania strumienia danych PLC w celu pozyskania zapisu sesji protokołów wyższych warstw (np. DLMS),
- próba dekodowania protokołów wyższych warstw w celu pozyskania rzeczywistych danych pomiarowych,
- próba rejestracja obcego licznika (lub emulatora licznika) na koncentratorze,
- próba przejęcie liczników poprzez ich przerejestrowanie na podstawiony koncentrator,
- próba sterowania przejętymi licznikami,
- próba blokada akwizycji danych (np. poprzez zagłuszanie sieci w zakresie wykorzystywanych częstotliwości),
- przeprowadzenia ataku na koncentrator oraz modemorouter od strony złącza Ethernet i udostępnianych serwisów w warstwie TCP/IP,
- próba penetracji warstwy telekomunikacyjnej od strony modemoroutera.

Powyższe metody ataku możliwe są do przeprowadzenia przez ogólnodostępną sieć niskiego napięcia lub po uzyskaniu fizycznego dostępu do urządzeń zainstalowanych w stacji SN/nn. Stąd też konieczne jest stosowanie systemów sygnalizacji włamania do obiektów elektroenergetycznych w celu pozyskania informacji o nieautoryzowanym dostępie.

5. REKOMENDACJE DOTYCZĄCE MOŻLIWOŚCI PODNIESIENIA POZIOMU BEZPIECZEŃSTWA SYSTEMU AMI

Systemy AMI wykorzystujące ogólnie dostępną sieć elektroenergetyczną do przesyłania danych użytkowych z definicji udostępniają istotny wektor ataku, jakim jest możliwość podsłuchu i analizy przesyłanych danych a także wysyłanie w medium transmisyjnym własnych, spreparowanych danych. W połączeniu z technicznym brakiem kontroli nad węzłami transmisyjnymi – licznikami

energii elektrycznej oraz – po uzyskaniu fizycznego dostępu do stacji SN/nn – także koncentratorami danych i modemorouterami – powoduje to konieczność zastosowania określonych mechanizmów bezpieczeństwa systemu. Są to:

- Szyfrowanie danych przesyłanych w sieci elektroenergetycznej. Wszystkie wykorzystywane obecnie standardy transmisji danych poprzez sieć elektroenergetyczną umożliwiają szyfrowanie w warstwie MAC i/lub warstwie aplikacji. Niektóre standardy umożliwiają również cyfrowe podpisywanie przesyłanych pakietów danych. Stosowanie szyfrowania wiąże się z opracowaniem i stosowaniem polityki okresowej wymiany kluczy szyfrujących a także generowania, zmiany i unieważniania certyfikatów cyfrowych, o ile są stosowane.
- Uwierzytelnienie urządzeń w celu potwierdzenia, że dane urządzenie jest urządzeniem zainstalowanym przez operatora sieci dystrybucyjnej a nie urządzeniem podstawionym przez intruza. Odpowiednie mechanizmy dostępne są w odniesieniu dla transmisji danych poprzez sieć elektroenergetyczną (np. HLS jako jeden z mechanizmów objętych specyfikacją DLMS) jak też dla komunikacji poprzez sieć Ethernet (np. 802.1X).
- Odpowiednie zabezpieczenie koncentratorów danych i modemorouterów. Jest to konieczne by uniemożliwić pozyskanie istotnych danych, umożliwiających dalszą penetrację sieci – jak na przykład kluczy szyfrujących poszczególnych liczników, dostępu do innych urządzeń wykorzystujących dany APN. Jest to także istotne ze względu na fakt, iż dane pomiarowe odczytane z liczników są najczęściej tymczasowo składowane w pamięci nieulotnej koncentratora danych. Nieograniczony dostęp do takiego koncentratora umożliwiłby modyfikację tych danych – co przekładać się będzie na zaniżenie (lub zawyżenie) ilości zużytej przez klientów energii elektrycznej.
- Okresowe sprawdzenie obecności urządzeń na sieci. Brak danego urządzenia oznaczać może jego kradzież w celu przeprowadzenia analizy sprzętowej, na przykład w celu ekstrakcji kluczy szyfrujących. Istotne jest, by wszystkie klucze, zapisywane w pamięci nieulotnej urządzeń, nie były dostępne w jawnej postaci (ang. clear text). Ta sama zasada dotyczy wszystkich innych danych sensytywnych, jak na przykład danych pomiarowych, PINu do karty SIM, nazwy APN.
- Okresowa analiza integralności urządzeń – zwłaszcza koncentratorów danych oraz modemorouterów. Pozwoli to na wykrycie nieuprawnionych prób modyfikacji tych urządzeń, np. poprzez zainstalowanie oprogramowania do podsłuch danych
- Stosowanie systemu klasy AAA (authentication, authorization and accounting) w odniesieniu do koncentratorów danych i modemorouterów. Umożliwi to wyeliminowanie składowania lokalnych poświadczeń na urządzeniach oraz scentralizowane zarządzanie dostępem oraz szczegółowe logowanie istotnych zdarzeń.

6. BIBLIOGRAFIA

1. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 Revision 2. May 2015
2. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf

IT SECURITY OF SMART MEASUREMENT SYSTEMS IN THE LIGHT OF THE ACT ABOUT THE NATIONAL CYBERSECURITY SYSTEM

On August 28, 2018, the Act on the National Cyber Security System, implementing the requirements of the European NIS Directive, came into force.

All identified operators of key services are be required to implement the procedures laid down in the directive, including risk assessment in the scope of functioning of provided key services, incident management and most importantly the application of technical and organizational measures adequate to the estimated risk. An important element of estimating this risk is the knowledge of potential attack vectors that can be used to breach the stability of the system performing a specific key service.

Intelligent metering systems due to the fact that they use electricity meters that remain physically beyond the control of the network operator, may become a target of a cyberattack on a massive scale and therefore have a significant negative impact on the operation of the electric grid and continuity of energy supply.

The paper presents selected methods of the attack on smart metering infrastructure as well as preventive measures that may increase resistance to currently identified cyber-attack methods. Moreover the paper presents the methods of executing a security audit of AMI systems on their architectural levels.

Keywords: advanced metering systems, cyber security, AMI, cyber security directive.