PROJEKTOWANIE I URUCHOMIANIE SIECI STACYJNYCH O BEZPIECZNEJ ARCHITEKTURZE

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1]OMICRON electronics GmbH, Klaus, Austria (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Lucerna, Szwajcaria (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Lucerna, Szwajcaria (stefan.mattmann@ckw.ch)

Słowa kluczowe: CYBERBEZPIECZEŃSTWO, IEC 61850, WYKRYWANIE NIEAUTORYZOWANEGO DOSTĘPU, AUTOMATYKA STACYJNA

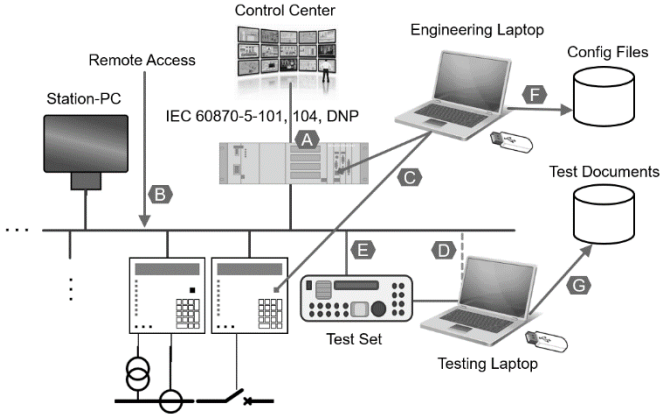
Streszczenie

Osoby przeprowadzające audyty związane z usługami i cyberbezpieczeństwem coraz częściej uważają, że nie tylko centra nadzoru są istotnym wektorem ataków. Również stacje elektroenergetyczne mogą potencjalnie stanowić cel przeprowadzenia cyberataków. Ważnymi czynnikami ryzyka są procesy, sposób uruchamiania systemów zabezpieczeń i sterowania oraz metody wdrażania dostępu umożliwiającego zdalne serwisowanie. Z tego powodu architektura systemu zabezpieczeń i sterowania musi być weryfikowana pod kątem bezpieczeństwa. Aby to osiągnąć, firma Centralschweizer Kraftwerke AG (CKW) – szwajcarski producent i dystrybutor energii elektrycznej – wdrożyła w latach 2016/2017 projekt mający na celu opracowanie nowej architektury referencyjnej dla obwodów wtórnych. Stworzony przez nią projekt rozwiązuje problem tych wektorów ataku za pomocą środków zaradczych, oferując jednocześnie rozsądną równowagę między łatwością serwisowania a bezpieczeństwem. Rozwiązanie to zakłada wiele poziomów ochrony, w tym wiele warstw zapory. Dodatkowo stosowany jest system wykrywania nieautoryzowanego dostępu (IDS). Wybór odpowiedniego IDS dla stacji elektroenergetycznych okazał się trudny, ponieważ wiele z tych systemów nie spełnia wymagań sieci stacyjnych. W pierwszej części niniejszego artykułu podano najważniejsze wektory ataku na stacje elektroenergetyczne, a w dalszej części opisano architekturę bezpieczeństwa wdrożoną po raz pierwszy w nowym projekcie stacji elektroenergetycznej 110 kV typu greenfield opracowanym przez CKW. Artykuł kończy się omówieniem doświadczeń w zakresie doboru odpowiedniego systemu IDS dla stacji elektroenergetycznych oraz wniosków wyciągniętych z wewnętrznego testu akceptacji przeprowadzonego dla tego projektu.

1. Wprowadzenie

1.1. Wektory ataku na stacje elektroenergetyczne

Dla pozostałej części niniejszego artykułu przyjmujemy, że cyberatak na stację elektroenergetyczną jest zdarzeniem, w którym przeciwnik modyfikuje, degraduje lub dezaktywuje działanie co najmniej jednego zabezpieczenia, sterownika polowego lub układu automatyki stacyjnej w stacji elektroenergetycznej. Aby to osiągnąć, osoba atakująca może użyć jednej ze ścieżek ataku, które przedstawia Rysunek 1 [1].



Rysunek 1: Wektory ataku na stacje elektroenergetyczne [1]

Osoba atakująca może uzyskać dostęp za pośrednictwem łącza z centrum nadzoru (**A**), tak jak miało to miejsce podczas pierwszego cyberataku na sieć elektroenergetyczną na Ukrainie, gdzie zmodyfikowano firmware urządzeń bramy (powodując ich zniszczenie) [2] lub za pomocą złącza zdalnego dostępu (**B**), tak jak miało to miejsce podczas drugiego cyberataku na Ukrainie przeprowadzonego w 2016 r. [3] oraz podczas cyberataku „TRITON" skierowanego na sterowniki PLC infrastruktury krytycznej [4].

Kolejnym punktem wejścia są komputery służące do prac inżynierskich (**C**), zarówno bezpośrednio podłączone do urządzeń stacji elektroenergetycznej, jak i do sieci stacyjnej. Gdy inżynier ds. zabezpieczeń podłącza swój komputer do przekaźnika w celu zmiany nastaw (zabezpieczeń), złośliwe oprogramowanie na komputerze może z kolei zainstalować złośliwe oprogramowanie w przekaźniku, tak jak miało to miejsce w przypadku sterowników PLC w słynnym cyberataku „Stuxnet" przeprowadzonym w 2010 roku [5].

Laptopy używane do testowania systemu IEC 61850 (**D**) są często bezpośrednio podłączane do szyny stacyjnej, co jest również potencjalnym sposobem zainfekowania inteligentnych urządzeń elektronicznych (IED). Z tego względu dostępne są nowe narzędzia testowe IEC 61850, które zapewniają bezpieczne pod kątem cybernetycznym odseparowanie komputera testowego od sieci stacyjnej elektroenergetycznej. Ostatnią metodą uzyskania nieautoryzowanego dostępu pozostaje zatem samo urządzenie testujące (**E**). Z tego powodu ważne jest, aby producenci testerów inwestowali w zabezpieczanie swoich urządzeń tak, aby ta metoda dostępu nie była atrakcyjna dla osoby atakującej.
Miejsce przechowywania nastaw (**F**) i dokumentów testowych (**G**) może również stanowić źródło infekcji. Ich serwer lub lokalizacja przechowywania również zaliczają się do obszaru krytycznego i nie powinny się znajdować w strefie informatycznej biura. Dlatego rozważne jest wdrożenie oddzielnego, izolowanego i chronionego rozwiązania do zarządzania takimi danymi.

2. Nowa propozycja dot. architektury stacji elektroenergetycznych

2.1. Najnowocześniejsze rozwiązania w dziedzinie cyberbezpieczeństwa technologii operacyjnej

Stowarzyszenie szwajcarskich firm energetycznych VSE powołało grupę roboczą ds. bezpieczeństwa technologii operacyjnej (OT), która w wyniku swoich prac opublikowała dokument z zaleceniami branżowymi: „Handbook on Basic Protection of Operational Technology in Power Systems" (Poradnik nt. podstawowej ochrony technologii operacyjnych w systemach elektroenergetycznych). Poradnik ten odwołuje się do dokumentu „Cyber Security Framework for Critical Infrastructure" (Ramy cyberbezpieczeństwa dla infrastruktury krytycznej) opracowanego przez amerykański Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology, NIST) [7], który jest stale dostosowywany i aktualizowany, a jego najnowsza wersja została opublikowana w 2018 r. Ramy wyznaczone przez NIST bazują na założeniu, że nigdy nie ma 100% ochrony przed cyberatakami. Przy odpowiednim poziomie wiedzy i odrobinie wysiłku wszystkie podjęte środki bezpieczeństwa mogą zostać zneutralizowane. Na tej podstawie ramy wyznaczone przez NIST zalecają wdrożenie procesu składającego się z następujących pięciu kroków: „Zidentyfikuj", „Chroń", „Wykryj", „Zareaguj", „Przywróć". Pierwszym z nich jest identyfikacja wektorów ataku (Zidentyfikuj), jak zostało to omówione w poprzedniej części niniejszego artykułu. Następnym krokiem jest zastosowanie środków zaradczych (Chroń). Jeśli osoba atakująca nadal jest w stanie przełamać te zabezpieczenia, atak musi zostać wykryty (Wykryj) i, w najlepszym wypadku, niezwłocznie odparty (Zareaguj), aby przywrócić normalny stan najszybciej, jak to tylko możliwe (Przywróć). Dzięki doświadczeniom wyniesionym z kroków „Wykryj" i „Zareaguj" można zidentyfikować nowe wektory ataku i wdrożyć nowe środki zaradcze. Proces się następnie powtarza.

Rekomendacje szwajcarskiej branży kładą duży nacisk na interakcję ludzi, technologii i procesów w ramach organizacji. Przykładowo stałe monitorowanie lub wykrywanie nieautoryzowanego dostępu (Wykryj) ma sens tylko wtedy, gdy odpowiednio zareagowano na komunikaty alarmowe. Dlatego komunikaty alarmowe muszą być zrozumiałe dla wszystkich osób zaangażowanych w proces reagowania: inżynierów ds. technologii operacyjnej i specjalistów ds. bezpieczeństwa IT. W przeciwnym razie proces reagowania jest nieskuteczny. Ponadto jeśli IDS generuje zbyt wiele fałszywych alarmów, wszystkie alarmy mogą zostać ostatecznie zignorowane.

2.2. Inicjatywy CKW na rzecz cyberbezpieczeństwa OT [6]

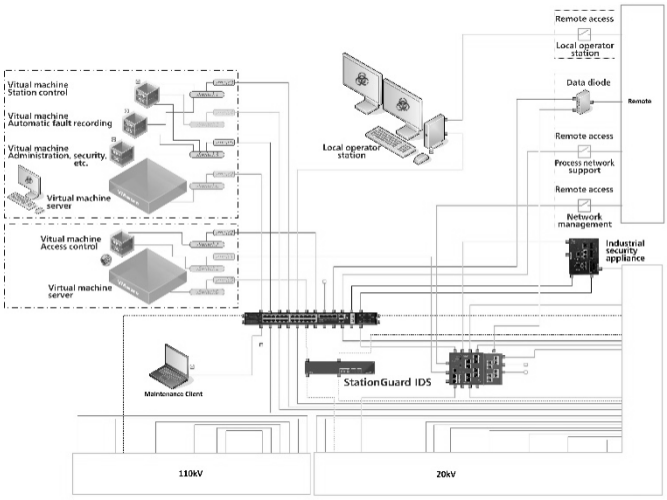
Temat bezpieczeństwa OT, zwłaszcza dot. systemów sterowania i zabezpieczeń, w ostatnich latach zyskał na znaczeniu w CKW. Było to spowodowane wspomnianymi zaleceniami branżowymi zaprezentowanymi w Szwajcarii, ale przede wszystkim wynikło z wyników ocen bezpieczeństwa OT przeprowadzonych przez CKW w ciągu ostatnich lat. Oceny te wykazały newralgiczne punkty zarówno w sieciach, jak i technologii sterowania stosowanej w stacjach elektroenergetycznych. Przykładowo znaleziono niebezpieczne przejścia między strefami i krytyczne metody uzyskania zdalnego dostępu na komputerach sterujących stacją. Ponadto nie można

było ocenić, czy atak obecnie jest przeprowadzany w sieci stacji, czy też w sieci występują podejrzane działania, które mogą wskazywać na dopiero zbliżający się atak.
Na podstawie tych ustaleń firma CKW postawiła sobie za cel wyeliminowanie istotnych słabych punktów i zaostrzenie wymagań dotyczących opracowywanej przez nią przyszłej architektury stacji elektroenergetycznych. Z tego powodu te konkluzje zostały zintegrowane z nowym standardem CKW w zakresie projektowania stacji.
Oprócz pracy nad tym standardem projektowym firma CKW brała czynny udział w pracach szwajcarskiej grupy roboczej nad wspomnianym już poradnikiem dot. bezpieczeństwa OT. W oparciu o tę wymianę informacji CKW całkowicie zintegrowała ustalenia grupy roboczej z własnymi standardami projektowymi.

W latach 2016/2017 zespół projektowy firmy CKW rozpoczął prace planistyczne nad budową nowej stacji elektroenergetycznej typu greenfield „US Rothenburg", która zostanie uruchomiona w 2020 roku. W tym projekcie wykorzystano nowy standard firmy CKW dot. bezpiecznej architektury i zastosowano się do najnowszych wytycznych zamieszczonych w szwajcarskim poradniku dot. bezpieczeństwa OT. Aby móc zaimplementować te wyrafinowane środki bezpieczeństwa, CKW podjęła decyzję o samodzielnym wdrożeniu architektury sieci i konfiguracji przełączników.

2.3. Projekt sieci

Projekt sieci US Rothenburg zakłada zastosowanie przeszkód w każdym obszarze, aby w jak największym stopniu utrudnić możliwość przeprowadzenia ataku. Rysunek 2 przedstawia sieć stacji US Rothenburg.



Rysunek 2: Architektura sieci US Rothenburg [6]

W ramach tej architektury wszystkie wektory ataku opisane w punkcie 1.1 niniejszego artykułu są rozwiązywane za pomocą całego wachlarza środków bezpieczeństwa. Zdalne połączenia w ramach zakładu zostały potraktowane z najwyższym priorytetem. Są one nie tylko zabezpieczone za pomocą zapór ogniowych i rozwiązań tunelowych, ale też domyślnie wyłączone. Połączenia realizowane w ramach zdalnego dostępu są aktywne tylko wtedy, gdy jest to konieczne. Oznacza to, że wiele osób jest zaangażowanych w realizację zdalnego dostępu, podobnie jak ma to miejsce w przypadku procesu uwierzytelniania dwuetapowego.
Komunikacja z systemem SCADA odbywa się przy użyciu protokołu szeregowego IEC 60870-5-101. Cały proces uzyskiwania dostępu do urządzeń stacji elektroenergetycznej w celach serwisowych odbywa się wyłącznie za pośrednictwem specjalnych stacji roboczych, które są odpowiednio zabezpieczone. Są one zwirtualizowane i umieszczone w lokalizacji centralnej. Ten zdalny dostęp na potrzeby serwisowe również musi być uzyskiwany zdalnie.
System SCADA, system rejestracji zakłóceń i serwery systemu bezpieczeństwa są zwirtualizowane i obsługiwane z poziomu komputera-hosta umieszczonego lokalnie w stacji elektroenergetycznej. Nawet lokalna stacja HMI uzyskuje dostęp do tych systemów za pomocą zdalnego pulpitu poprzez dodatkową lokalną zaporę ogniową. Stosowana jest kontrola dostępu oparta na rolach (RBAC). Oznacza to, że nie ma jednego hasła na urządzenie, ale jest jedno hasło na użytkownika. Ma to taką zaletę, że inżynier może używać

własnego hasła we wszystkich stacjach elektroenergetycznych. Jeśli pracownik opuści szeregi firmy, jego profil użytkownika można łatwo usunąć bez konieczności zmiany haseł. To zarządzanie użytkownikami jest realizowane za pomocą centralnego serwera Active Directory (AD) i lokalnego serwera RADIUS w stacji elektroenergetycznej. Użytkownicy muszą się logować przy użyciu usługi katalogowej AD, która przypisuje im niezbędne uprawnienia. W razie potrzeby dostęp do centralnej usługi AD można uzyskać z lokalizacji centralnej. Ponadto użytkownicy muszą się zalogować do każdego urządzenia IED przy użyciu indywidualnej nazwy użytkownika i hasła. Niniejszym urządzenia IED korzystają z lokalnego serwera RADIUS w celu sprawdzenia poprawności nazwy użytkownika i hasła oraz w celu uzyskania uprawnień przypisanych temu użytkownikowi. Dotyczy to zarówno dostępu do urządzeń z narzędziami inżynierskimi, jak i obsługi wyświetlacza urządzenia IED. Nie są stosowane żadne standardowe hasła.

Wszystkie komputery podłączone do sieci stacyjnej mają wzmocnioną ochronę. Jest to realizowane m.in. poprzez konfigurację zapory systemu Windows zgodnie z matrycą komunikacyjną stacji oraz, w zależności od roli tego klienta, poprzez blokowanie funkcji systemów operacyjnych, które nie są wymagane.

Rolą dodatkowego środka bezpieczeństwa jest kontrola dostępu do sieci realizowana poprzez ominięcie procesu uwierzytelnienia MAC, co oznacza, że tylko zarejestrowane urządzenia mogą się łączyć z przełącznikiem sieciowym.

W przypadku awarii przełącznik musi również rozpoznać i zaakceptować rezerwowe urządzenia z zapasu. W przełącznikach sieciowych i zaporze sieciowej stacji elektroenergetycznej listy kontroli dostępu są skonfigurowane tak, aby wymusić komunikację danego urządzenia z innym określonym uczestnikiem sieci. Obejmuje to również wykorzystany protokół i port przełącznika.

Sieć szyny stacyjnej oraz sieć do konfiguracji i serwisowania są logicznie (VLAN) i fizycznie oddzielone. Oznacza to, że na każdym urządzeniu IED typ komunikacji MMS i GOOSE wg IEC 61850 działa w ramach innego interfejsu sieciowego niż dostęp serwisowy. Ponadto cała sieć szyny stacyjnej jest podzielona na segmenty, a następujące segmenty oddzielone są zaporą:

- 110 kV (GOOSE i MMS),
- 20 kV (GOOSE i MMS),
- lokalny HMI,
- brama protokołu,
- systemy pomocnicze,
- sieci serwisowe dla urządzeń IED i klientów,
- sieć zarządzania, VM, RADIUS.

Komunikacja między stacją a obszarami sieci wyższego poziomu jest dodatkowo zabezpieczona za pomocą sieci jednokierunkowej. Zapewnia ona, że tylko sesje komunikacji wychodzącej mogą być inicjowane i stanowi kolejną warstwę zabezpieczeń.

System wykrywania nieautoryzowanego dostępu (IDS) monitoruje cały ruch sieciowy w systemie za pomocą białej listy, tj. wszelki nieznany ruch, który nie znajduje się na białej liście, domyślnie wygeneruje alarm. IDS zgłasza alarm do centrum nadzoru za pośrednictwem sterownika RTU oraz do centrum operacji bezpieczeństwa za pośrednictwem specjalnych protokołów do rejestrowania alarmów.

3. Wykrywanie nieautoryzowanego dostępu

Architektura bezpieczeństwa firmy CKW bazuje na tworzeniu segmentów sieci oddzielonych zaporą ogniową. Konfiguracja zapory dokładnie określa, które protokoły mogą być użyte do komunikacji między segmentami. Jednak protokoły dozwolone przez zaporę ogniową, takie jak MMS czy GOOSE stosowane w IEC 61850, oraz protokoły inżynieryjne specyficzne dla danego dostawcy mogą być również używane do atakowania urządzeń i infekowania ich. W takich sytuacjach firma CKW chciała zapewnić możliwość wykrycia nieautoryzowanego działania już na wczesnym etapie. Pod tym kątem podjęto decyzję, aby w ramach architektury referencyjnej firmy CKW zastosować IDS.

Aby móc analizować najbardziej krytyczny ruch, tj. komunikację między bramą a urządzeniami IED, przynajmniej cały ruch bramy powinien być dublowany do IDS. Przełączniki na poziomie pola rozdzielni zwykle nie muszą być uwzględniane, ponieważ zazwyczaj wychodzi od nich tylko ruch rozgłoszeniowy (multicast), taki jak GOOSE lub Sampled Values. Aby zapewnić, że analizowany jest również cały ruch przy emisji „unicast” we wszystkich gałęziach sieci, zalecane jest aby wszystkie przełączniki (switch’e) były odzwierciedlane w systemie IDS.

W architekturze firmy CKW IDS jest podłączony do „mirror" portów we wszystkich przełącznikach sieciowych. Oznacza to, że IDS analizuje ruch na szynie stacyjnej, a także ruch przychodzący z zewnątrz przed przejściem i po przejściu przez zaporę ogniową.

3.1. Wymagania dla IDS w stacji elektroenergetycznej

Proces doboru IDS odpowiedniego dla stacji elektroenergetycznych okazał się trudny. Ważnym wymogiem było to, aby IDS mógł być łatwo obsługiwany przez inżynierów ds. zabezpieczeń, sterowania i sieci, którzy są odpowiedzialni za wszystkie urządzenia IED i urządzenia sieciowe. Aby wesprzeć proces reagowania na alarm, musi być możliwe łatwe powiązanie alarmów IDS ze zdarzeniami w stacji elektroenergetycznej i dziennikami zdarzeń w HMI. Dlatego system IDS powinien udostępniać określone widoki dla stacji zamiast tylko zezwalać na stosowanie terminologii związanej z bezpieczeństwem informatycznym.

Do niedawna istniały tylko dwie główne metody stosowane przez IDS: metoda oparta na sygnaturach i metoda oparta na „zdolności uczenia się".

Metoda oparta na sygnaturach polega na stosowaniu czarnej listy. Podobnie rzecz ma się ze standardowymi skanerami antywirusowymi zainstalowanymi na komputerach osobistych. Przeprowadzane jest skanowanie w poszukiwaniu schematów znanych wirusów i złośliwego oprogramowania. Problem polega na tym, że znana jest tylko niewielka liczba cyberataków na stacje elektroenergetyczne, a nawet już pierwszy przypadek nowej formy ataku może się wiązać z poważnymi konsekwencjami. IDS stacji musi być w stanie wykryć ataki bez specyficznej wiedzy o tym, jak może wyglądać taki atak.

Dlatego coraz więcej systemów IDS stosuje metodę opartą na „zdolności uczenia się". IDS analizuje ogólne parametry różnych protokołów, aby poznać średnie wartości i częstotliwość każdego parametru. Podczas normalnej pracy alarm jest generowany, jeśli komunikacja sieciowa znacznie odbiega od wyuczonej średniej. W rezultacie wywoływane są fałszywe alarmy dla wszystkich zdarzeń, które nie wystąpiły podczas fazy nauki. Obejmuje to np. wyłączenia i operacje przełączania, a także rutynowe testy zabezpieczeń. Ponieważ system nie zna znaczenia telegramów w sieci, komunikaty alarmowe odnoszą się do ogólnych parametrów protokołu, takich jak „MMS confirmed-write-response failed". Powoduje to generowanie dużej liczby fałszywych alarmów, z których każdy wymaga sprawdzenia przez specjalistów ds. IT i IEC 61850. Taki wysiłek związany z procesem reagowania był nie do przyjęcia dla firmy CKW.

3.2. Wybrana metoda stosowana przez IDS

W przypadku stacji elektroenergetycznych IEC 61850 cały system automatyki, w tym wszystkie urządzenia IED, ich modele danych i wzorce komunikacji, opisano w ramach ustandaryzowanego formatu SCL. Informacja ta umożliwia zastosowanie innej metody wykrywania nieautoryzowanego dostępu: system monitorowania może utworzyć model systemu układu automatyki stacji i porównać każdy pakiet w sieci względem tego modelu. Nawet zmienne zawarte w przekazywanych komunikatach (GOOSE, MMS, SV) mogą być oceniane na podstawie oczekiwań wynikających z modelu systemu. Ten model systemu zawiera zatem białą listę, a wszystkie pakiety niezgodne z modelem systemu wywołają alarm. Firma CKW wybrała IDS oparty na tej metodzie (OMICRON StationGuard).

Jego zaletą jest to, że wykrywane są nie tylko zagrożenia cybernetyczne, takie jak źle sformułowane pakiety i niedozwolone sterowania MMS, ale także błędy komunikacji i problemy z synchronizacją czasu. W konsekwencji wykrywane i zgłaszane są niektóre awarie sprzętu.

Korzystając z sekcji stacji w pliku SCL, możliwe jest automatyczne utworzenie schematu stacji na którym mogą być przedstawiane alarmy. Taki widok może pomóc w ocenie, czy dana czynność, która wywołała alarm, została wykonana celowo. Przykładowo zdarzenie mogło zostać spowodowane przez inżyniera przeprowadzającego test lub może być powiązane ze złośliwymi działaniami zainfekowanego laptopa testowego.

W momencie opracowywania niniejszego artykułu przeprowadzono fabryczny test akceptacji (FAT) stacji US Rothenburg i obecnie trwa procedura jej uruchamiania. W przypadku FAT musiano przeprowadzić prawie całkowitą konfigurację sieci, aby możliwe było przetestowanie, czy system działa. Zrozumieliśmy również, że IDS potrzebuje wsparcia dla routingu wykonywanego przez wiele poziomów zapór ogniowych. Występuje wiele duplikacji ruchu przed i za zaporami ogniowymi, które mogą mylić wskazania IDS. Jednak wybrany

IDS poprawnie działał w ramach tego scenariusza. Ponadto tworzenie matrycy komunikacyjnej w celu konfiguracji zapory wiąże się z dużym wysiłkiem, ponieważ należy to wykonać ręcznie. Ponieważ IDS ma dostęp do takiej białej listy za pośrednictwem SCL, również ten proces może zostać zautomatyzowany w przyszłości.

4. Wnioski i perspektywy

Jeśli atakujący może wpłynąć na jedną lub więcej stacji elektroenergetycznych, może to mieć poważne konsekwencje dla całej sieci. Stacje mają kilka wektorów ataku, które mogą ominąć zaporę ogniową. Bezpieczna architektura sieci stacji elektroenergetycznych firmy CKW zapewnia liczne środki zaradcze dla wektorów ataku omówionych w niniejszym artykule. Środki bezpieczeństwa zapewniają wysoki poziom ochrony, a jednocześnie umożliwiają przeprowadzanie wydajnych procedur serwisowych i inżynieryjnych przy użyciu zdalnego dostępu. Architektura ta bazuje na wykrywaniu nieautoryzowanego dostępu wewnątrz sieci. W przypadku stacji IEC 61850 dostępna jest metoda IDS, która wykorzystuje SCL do automatycznego tworzenia białej listy całego dozwolonego ruchu sieciowego. Pozwala to również wyświetlać wykryte zdarzenia w języku stosowanym przez inżynierów ds. zabezpieczeń, automatyki i sterowania, aby mogli współpracować z inżynierami ds. bezpieczeństwa w celu skutecznego ustalania przyczyn zdarzeń.

Cyberbezpieczeństwo polega na uświadomieniu sobie tego, że każdy projekt można udoskonalić. Do ulepszeń można zaliczyć np. opartą na certyfikatach kontrolę dostępu do sieci zgodną z 802.1X [8] zamiast obecnie stosowanego podejścia opartego na MAC. Jednak w tym celu większa liczba urządzeń IED musi obsługiwać standard 802.1X, co obecnie nie ma miejsca. Dokumenty uzupełniające powinny omawiać wnioski wyciągnięte z uruchomienia tego projektu i przedstawiać wyniki przyszłych ocen bezpieczeństwa i testów penetracyjnych przeprowadzanych w ramach tej stacji elektroenergetycznej.

5. Bibliografia

[1] Klien, A.: „New approach for detecting cyber intrusions in IEC 61850 substations”, PAC World Conference Europe, Glasgow, 2019

[2] „Analysis of the Cyber Attack on the Ukrainian Power Grid”, SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, dostęp: listopad 2019 r.

[3] „WIN32/INDUSTROYER - A new threat for industrial control systems”, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, dostęp: listopad 2019 r.

[4] „Threat Research - Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure”, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, dostęp: listopad 2019 r.

[5] D. Kushner: „The Real Story of Stuxnet
How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program”, IEEE Spectrum, luty 2013 r.

[6] Gosteli, Y., Klien A.: „Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg”, bulletin.ch, 2019, 6, str. 50–52

[7] NIST: „Framework for improving critical infrastructure cybersecurity”, version 1.1, National Institute of Standards and Technology, kwiecień 2018 r.

[8] IEEE: „802.1X-2010 - IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control”, International Standard, luty 2010 r.

OMICRON to firma międzynarodowa służąca branży elektroenergetycznej innowacyjnymi rozwiązaniami w zakresie testowania i diagnostyki. Zastosowanie produktów firmy OMICRON pozwala użytkownikowi z dużą dozą pewności ocenić stan urządzeń podstawowych i dodatkowych zainstalowanych w systemie. Gamę produktów uzupełniają usługi w obszarze konsultacji, uruchomień, testowania, diagnostyki i szkoleń.

Klienci w ponad 160 krajach polegają na zdolności firmy do dostarczania najnowocześniejszej technologii o doskonałej jakości. Nasze centra serwisowe na wszystkich kontynentach zapewniają dostęp do obszernej bazy wiedzy oraz doskonałej obsługi klienta. Wszystko to, w połączeniu z rozległą siecią partnerów handlowych, sprawia, że nasza firma jest liderem w branży elektroenergetycznej.

Szczegółowe informacje, dodatkowe publikacje oraz dane kontaktowe naszych oddziałów na całym świecie można znaleźć na naszej stronie internetowej.

www.omicronenergy.com