Nowe wyzwania związane z zapewnieniem bezpieczeństwa cybernetycznego przez operatorów usług kluczowych

Cezary Bryczek

1. Wprowadzenie

Rozwój nowych technologii i standardów spowodował z jednej strony ograniczenie kosztów eksploatacji związanych z przejazdami inżynierów na stacje energetyczne, uproszczenie infrastruktury komunikacyjnej, zwiększenie niezawodności i interoperacyjności pomiędzy urządzeniami różnych producentów, z drugiej strony zwiększyła się możliwość pojawienia się zagrożenia w postaci różnego rodzaju incydentów bezpieczeństwa, mających niekorzystny wpływ na infrastrukturę i urządzenia zainstalowane na stacjach energetycznych, zakładach przemysłowych, kopalniach, elektrowniach, a także na bezpieczeństwo i życie ludzi. Przykładami incydentów cybernetycznych odnotowanych w przeszłości są:

- **StuxNet Worm rok 2010** – atak na irańską elektrownię atomową w mieście Bushehr, gdzie w różnym stopniu zostały uszkodzone wirówki wzbogacające uran. Według analizy specjalistów firmy Symantec Stuxnet zaraził około 100 tysięcy komputerów na całym świecie, 60 tysięcy w Iranie w szczególności centralnych systemów komputerowych w obiekcie jądrowym Bushehr.

- **Rok 2014** – atak na niemiecką hutę stali, który polegał na przejęciu kontroli nad procesem produkcyjnym i awaryjne wyłączenie wielkiego pieca hutniczego. Atak spowodował poważne uszkodzenie infrastruktury i bardzo duże straty materialne.

- **BlackEnergy i KillDisk rok 2015** – atak na ukraińską sieć energetyczną, co skutkowało kilkugodzinną przerwą w dostawach prądu, która dotknęła od 80 tys. do 700 tys. odbiorców energii elektrycznej. Atakujący zablokowali możliwość zdalnego przywrócenia systemu, a także przeprowadzono atak DDoS na centrum obsługi klienta, opóźniając dotarcie informacji o blackoucie i uzyskanie informacji zwrotnej o tym,co się stało.

Biorąc po uwagę wyżej wymieniony przykład ataku na ukraińską sieć energetyczną, możemy sobie tylko wyobrazić, jakie skutki taka awaria spowodowałaby w naszym kraju. Brak dostarczonej energii elektrycznej dla zakładów przemysłowych, np.: rafinerii, spowodowałaby olbrzymie straty materialne w wyniku zatrzymania produkcji, a także mógłby spowodować

Streszczenie: Rozwój nowych technologii i standardów komunikacyjnych powoduje ograniczenie kosztów eksploatacji, uproszczenie infrastruktury komunikacyjnej, zwiększenie niezawodności i interoperacyjności pomiędzy urządzeniami różnych producentów. Z drugiej strony zwiększyła się możliwość pojawienia się zagrożenia w postaci różnego rodzaju incydentów bezpieczeństwa, mających niekorzystny wpływ na infrastrukturę i urządzenia zainstalowane na stacjach energetycznych, zakładach przemysłowych, kopalniach, elektrowniach, a także na bezpieczeństwo i życie ludzi. W niniejszym artykule przedstawiono zagrożenia i skutki, jakie mogą wystąpić w wyniku incydentów cybernetycznych, regulacje prawne, które wymuszają na operatorach usług kluczowych implementowanie rozwiązań zwiększających bezpieczeństwo cybernetyczne, oraz rozwiązania, które w znaczącym stopniu zwiększają odporność infrastruktury krytycznej na ataki cybernetyczne i pomagają zminimalizować ryzyko popełnienia błędu przez personel odpowiedzialny za obsługę urządzeń.

Słowa kluczowe: bezpieczeństwo cybernetyczne, zagrożenia cybernetyczne, operator usługi kluczowej, Dyrektywa NIS 2016/1148/U, ustawa o krajowym systemie cyberbezpieczeństwa

NEW CHALLENGES RELATED TO ENSURING CYBERSECURITY BY KEY SERVICES OPERATORS

The development of new technologies and communication standards results in reduction of operating costs, simplification of communication infrastructure, increase of reliability and interoperability between devices from different manufacturers, however, on the other hand, it increase the possibility of new threats occurrence, in the form of various types of security incidents, adversely affecting the infrastructure and devices installed on electrical substations, industrial plants, mines, power plants, as well as people's safety and life. This article presents threats and effects that may occur as a result of cyber incidents, regulations that force key services operators to implement solutions to enhance cybersecurity and solutions that significantly increase the resilience of critical infrastructure to cyber-attacks and help to minimize the risk of mistakes made by operators.

Keywords: cybersecurity, cyber threats, operator of key services (critical infrastructure operator), NIS Directive 2016/1148/U, the national cyber security regulation

uszkodzenia w instalacji technologicznej. Niedostarczenie energii do szpitali, banków, urzędów, domostw, systemu sterowania ruchem, trakcji elektrycznej itp. spowodowałoby olbrzymi chaos i zagrożenie dla bezpieczeństwa i życia ludzkiego.

Incydenty ze względu na charakter możemy podzielić na:

- celowe ataki, które mają na celu np.:
  - skompromitowanie systemu lub dostawcy usługi kluczowej,
  - spowodowanie awarii przez co zakłócenie ciągłości świadczenia usługi kluczowej,
  - destabilizację sytuacji w danym kraju,
  - wyłudzenie pieniędzy;
- incydenty przypadkowe, które wynikają z:
  - dostępu do obszarów krytycznych przez niedoświadczonych pracowników,
  - dostępu do niewłaściwych obszarów krytycznych przeszkolonego personelu,
  - błędów ludzkich.

Ataki na urządzenia i infrastrukturę mogą zostać przeprowadzone z zewnątrz, poprzez połączenia pomiędzy obiektem a np. centrum dyspozytorskim niezabezpieczone:

- szyfrowaniem,
- tunelowaniem,
- autoryzacją,
- uwierzytelnianiem,

jak i z wewnątrz poprzez intruzów, którzy uzyskali fizyczny dostęp do urządzeń, bądź też poprzez nieświadomy personel podłączający zainfekowane urządzenie do sieci.

2. Aktualne regulacje prawne

Z uwagi na rosnącą liczbę odnotowanych ataków i zagrożeń cybernetycznych oraz skutki, jakie mogą one mieć dla funkcjonowania Państw Członkowskich, a nawet całej Unii Europejskiej, Parlament Europejski i Rada (UE) przyjęły dnia 6 lipca 2016 r. **Dyrektywę NIS 2016/1148/UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii** [4]. Jednym z wymagań stawianych w dyrektywie **2016/1148/UE** [4] jest ustanowienie szczególnych wymogów dotyczących zapewniania bezpieczeństwa cybernetycznego przez przedsiębiorców z sektorów kluczowych, w tym z sektora energetyki. Wszystkie państwa członkowskie mają 21 miesięcy na wdrożenie postanowień dyrektywy do prawa krajowego i dodatkowe sześć miesięcy na opracowanie spisu operatorów usług kluczowych (infrastruktury krytycznej).

W ślad za Dyrektywą NIS została przyjęta Uchwała nr **52/2017** Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, a także w trakcie prac legislacyjnych jest **projekt ustawy z dnia 15 lutego 2018 r. o krajowym systemie cyberbezpieczeństwa** [2]. Ustawa 1 sierpnia została podpisana przez prezydenta. Wejdzie w życie 14 dni po ogłoszeniu.

W myśl projektu ustawy [2] operatorzy usług kluczowych muszą wdrożyć system zarządzania bezpieczeństwem, zapewniający w szczególności:

- prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie ryzykiem wystąpienia incydentu;
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
  - utrzymanie i bezpieczną eksploatację systemu informacyjnego,
  - bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
  - bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
  - wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz poufność, integralność, dostępność i autentyczność informacji,
  - objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej;
- zarządzanie incydentami;
- stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
  - stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
  - dbałość o aktualizację oprogramowania,
  - ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
  - niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
- stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa

Mając świadomość, że skutki incydentów bezpieczeństwa mogą zarówno mieć wpływ na ciągłość działania świadczonej usługi kluczowej, jak i skutkować znaczącą szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, zdrowia publicznego, utratą zaufania do instytucji publicznych i podmiotów gospodarczych, ustawodawca przewidział system kar pieniężnych, którym będzie podlegał operator usługi kluczowej. I tak przykładowo karze pieniężnej będzie podlegał operator, który:

- nie wdrożył systemu zarządzania bezpieczeństwem;
- nie opracował dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych;
- nie przeprowadził audytu bezpieczeństwa;
- nie realizuje wiążących poleceń wprowadzenia środków zaradczych;
- nie usunął w wyznaczonym terminie nieprawidłowości stwierdzonych w wyniku kontroli.

W **OSR** [1] do **projektu ustawy o krajowym systemie cyberbezpieczeństwa** [2] znajduje się wykaz operatorów usług kluczowych, których będą dotyczyły regulacje dotyczące cyberbezpieczeństwa z sektora energetyki, transportu, bankowości

i rynków finansowych, służby zdrowia, zaopatrzenia i dystrybucji wody pitnej, a także infrastruktury cyfrowej.

Przykładowo dla sektora energetyka wyszczególniono:

- podsektor energii elektrycznej:
  - operator sieci przesyłowej Polskie Sieci Energetyczne SA;
  - operatorzy sieci dystrybucji: Innogy Stoen Operator Sp. z o.o, PGE Dystrybucja SA, ENEA Operator Sp. z o.o., Tauron Dystrybucja SA, ENERGA – Operator SA,
  - dziewięć największych dla rynku przedsiębiorstw (m.in. dla portów morskich),
  - sprzedawcy energii;
- podsektor ropa naftowa:
  - operator ropociągów PERN SA,
  - przedsiębiorstwa zajmujące się wydobyciem, przetwarzaniem, magazynowaniem i przesyłem ropy naftowej: Polskie Górnictwo Naftowe i Gazownictwo i LOTOS Petrobaltic SA,
  - rafinerie: PKN „Orlen", Grupa LOTOS SA.

Należy nadmienić, że proces identyfikacji operatorów infrastruktury krytycznej nie został jeszcze zakończony i liczba operatorów, których będą dotyczyły regulacje, prawdopodobnie wzrośnie.

Podczas prowadzonych konsultacji dotyczących projektu ustawy pojawiła się wątpliwość dotycząca braku definicji incydentu bezpieczeństwa komputerowego, w ramach której rozróżniono by systemy IT oraz OT (technologiczne). W wyjaśnieniu tych wątpliwości [3] czytamy „Definicja systemu teleinformatycznego obejmuje zarówno systemy IT, jak i systemy OT – nie ma konieczności rozróżniania tych dwóch definicji. Warto zaznaczyć, że w automatyce przemysłowej mówi się jeszcze o wielu innych kwestiach, a nie tylko o łączności. IACS to nie tylko SCADA, ale też PLC, przetworniki wielkości nieelektrycznych na elektryczne, serwomechanizmy, transmisja danych w specjalizowanych sieciach (np. RS422/485, CANBus, ARING 429, mil-std-1553b, a także Ethernet)", co pokazuje, że intencją ustawodawcy jest zagwarantowanie bezpieczeństwa cybernetycznego nie tylko na poziomie systemów sterowania i nadzoru, centrów dyspozytorskich, ale także na poziomie sterowników polowych, układów automatyki i zabezpieczeń pracujących w polu i wykorzystujących do wymiany informacji różne protokoły komunikacyjne.

Biorąc pod uwagę zagrożenia dotyczące bezpieczeństwa cybernetycznego infrastruktury i urządzeń zainstalowanych na stacjach energetycznych, a także na regulacje prawne, które lada chwila wejdą w życie, należy już teraz na etapie projektowania zadbać o zapewnienie bezpieczeństwa sieciowego poprzez odpowiedni dobór rozwiązań umożliwiających monitorowanie oraz zarządzanie dostępem do sieci, a także dobór urządzeń, w tym sterowników i zabezpieczeń polowych, które będą miały zaimplementowane funkcje w istotny sposób zwiększające bezpieczeństwo cybernetyczne, aby po wejściu w życie ustawy nie być zmuszonym do zmian projektowych.

Przy doborze urządzeń należy zwrócić uwagę, czy urządzenia były testowane pod kątem bezpieczeństwa cybernetycznego, ich odporności na cyberataki. Istnieją ośrodki, które wykonują takie testy i wystawiają certyfikaty bezpieczeństwa, np.: certyfikaty Achilles (rys. 1).


Certificate Of Compliance

This is to certify that the:
WebField ECS-700
FCU712-S01

Manufactured by:
Zhejiang Supcon Technology Co.,Ltd.

Is in compliance with the requirements set forth by:
Achilles Level II Certification

CERTIFICATE NO. CERT-194-020714
FCU712-S_V11.1x.00
HARDWARE VERSION
FCU712-S_V11.1x.00
FIRMWARE VERSION
N/A
CONTROL PROTOCOL
Embedded Device
CATEGORY

Nate Kube, CTO

wurldtech
A GE Company

Rys. 1. Przykład certyfikatu Achilles

Drugą ważną rzeczą jest zgodność urządzeń z powszechnie obowiązującymi normami, standardami opisującymi wymagania lub rekomendacje dotyczące zapewnienia bezpieczeństwa cybernetycznego dostarczanych urządzeń. Przykładem może tu być: NERC CIP, IEC 62443 (ISA99), IEC 62351.

3. Rozwiązania zwiększające bezpieczeństwo cybernetyczne stosowane w urządzeniach EAZ

Cyberbezpieczeństwo można uzyskać przez:

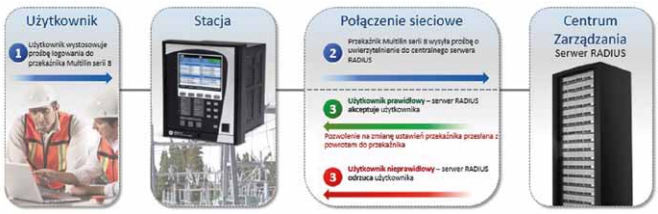
- **kontrolę dostępu** zarówno fizycznego, jak i elektronicznego;
- **poświadczenie/uwierzytelnienie** poprzez weryfikację czy osoba (lub coś) próbująca dostać się do systemu lub urządzenia jest do tego upoważniona;
- **upoważnienie** polegające na zapewnieniu, że każdy uwierzytelniony użytkownik ma uprawnienia tylko do tych czynności, które wykonuje. Możemy w tym celu wykorzystać systemy umożliwiające zdalne uwierzytelnianie i autoryzację użytkowników przy wykorzystaniu usługi RADIUS lub protokołu LDAP;
- **poufność** w celu zapewnienia, że wszelkie krytyczne informacje są przesyłane i utrzymywane w tajemnicy. Uzyskujemy to poprzez szyfrowanie i ochronę przed podsłuchaniem sieci;
- **integralność** poprzez zapewnienie, że otrzymana informacja od użytkownika lub zdalnego podmiotu nie została zmodyfikowana. W tym celu wykorzystujemy: szyfrowanie, certyfikaty i podpisy cyfrowe, uwierzytelnianie;
- **sprawdzanie – audyty** polegające na rejestrowaniu wszystkich zmian oraz operacji i przechowywanie ich w nieulotnej pamięci z zapewnieniem poufności i integralności;
- **wykrywanie incydentów i reakcję na nie**;
- podnoszenie świadomości, szkolenia, procedury, zrozumienie ryzyka i konsekwencji, skuteczne strategie.

W urządzeniach EAZ serii Multilin firmy General Electric zaimplementowano pod nazwą CyberSentry™ pakiet rozwiązań zwiększających bezpieczeństwo cybernetyczne. Rozwiązania te pozwalają na wykorzystanie narzędzi powszechnie stosowanych w systemach i sieciach IT do monitorowania i zarządzania bezpieczeństwem cybernetycznym oraz na

uzyskanie zgodności urządzeń serii Multilin z wymaganiami standardu NERC CIP, której stosowanie jest obligatoryjne w USA.

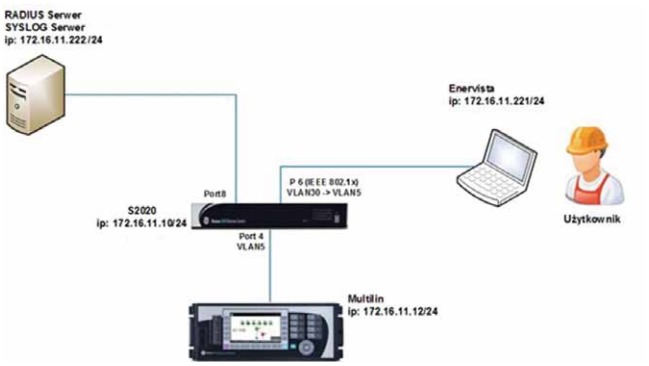
W skład pakietu rozwiązań CyberSentry™ wchodzą:

- **A Role-Based Access Control (RBAC)** – selektywny dostęp do funkcji i konfiguracji przekaźnika w oparciu o konkretne role przypisane do kont użytkowników. Dostępne role: Administrator, Supervisor, Inżynier, Operator i Obserwator. Dostęp do urządzenia może mieć wielu użytkowników, logując się na własne konto, a to rola określa, jakie mają uprawnienia i jakie operacje mogą być przez nich wykonywane.
- **An Authentication, Authorization, Accounting (AAA) Remote Authentication Dial-In User Service (RADIUS)** (rys. 2) – zdalne uwierzytelnianie i autoryzacja użytkowników żądających dostępu do urządzenia, centralne zarządzanie hasłami, kontami oraz rolami przypisanymi do danego konta. Możliwe jest okresowe udzielenie dostępu, np. w określonych godzinach. Użytkownik, logując się do przekaźnika Multilin, który jest jednocześnie klientem RADIUS, podaje swój login i hasło, które jest następnie przesyłane do centralnego serwera RADIUS w celu uwierzytelnienia i autoryzacji. Serwer RADIUS weryfikuje swoją bazę danych pod kątem użytkownika oraz hasła. Jeśli proces weryfikacji przebiegnie poprawnie, wystawia do klienta RADIUS zgodę na dostęp do urządzenia. Urządzenie Multilin przed rozpoczęciem logowania nawet nie wie o istnieniu takiego użytkownika. Wszystkie konta są na zdalnym serwerze RADIUS, co pozwala na utworzenie indywidualnych kont dla każdego użytkownika z osobna. Komunikacja pomiędzy serwerem a klientem w celu zapewnienia bezpieczeństwa sieciowego jest szyfrowana z wykorzystaniem metody EAP-TTLS.



Rys. 2. Etapy uwierzytelniania użytkownika

Usługa RADIUS umożliwia również konfigurowanie dostępu czasowego w połączeniu z zarządzaniem rolami (RBAC). Załóżmy, że na stacji elektroenergetycznej pojawia się zespół pracowników firmy zewnętrznej w celu przeprowadzenia badania okresowego urządzenia. Administrator bezpieczeństwa danej firmy, wiedząc, że polecenie na pracę zostało wystawione od godziny 9.00 do 16.00, wprowadza do serwera RADIUS użytkownika i hasło umożliwiając dostęp do urządzenia jedynie w tych godzinach i jedynie osobie znającej to hasło. Ponadto możemy wskazać, do których dokładnie urządzeń użytkownik będzie miał dostęp, wykluczając w ten sposób możliwość popełnienia błędu i np. wgrania nastaw do innego urządzenia. Osoba tworząca konto dostępu nadaje również uprawnienia (rolę RBAC) do konkretnych



Rys. 3. Użytkownik po poprawnym uwierzytelnieniu zostaje przypisany z VLAN30 do VLAN4, w którym znajduje się urządzenie

działań – zmiana nastaw zabezpieczeń, zmiana nastaw bezpieczeństwa, sterowanie, obserwacja.

Serwer RADIUS może zostać również wykorzystany do kontroli dostępu do sieci po uwierzytelnieniu użytkownika na porcie przełącznika sieciowego zgodnie ze standardem IEEE802.1x. Dodatkowo umożliwia to po poprawnym uwierzytelnieniu użytkownika przypisanie go do sieci VLAN, w której znajduje się urządzenie (rys. 3). W ten sposób, mając wydzielone sieci wirtualne VLAN np.: dla liczników, zabezpieczeń itp., możemy decydować, do której wirtualnej sieci użytkownik będzie miał dostęp, chociaż za każdym razem będzie fizycznie podłączony do tego samego portu przełącznika sieciowego.

- **Syslog** – raportowanie zdarzeń związanych z bezpieczeństwem cybernetycznym, takich jak: logowanie/wylogowanie, nieudane próby wprowadzenia hasła, zmiany nastaw, aktualizacja oprogramowania itp., poprzez standardowy protokół Syslog do centralnego systemu monitorującego (rys. 4). Zdarzenia klasyfikowane są pod kątem poziomu bezpieczeństwa i zawierają informację o dacie i godzinie wystąpienia zdarzenia, użytkowniku, adresie MAC oraz IP komputera, z którego ustanowiony był dostęp, jaki parametr został zmieniony,

Rys. 4. Monitorowanie bezpieczeństwa sieciowego z wykorzystaniem protokołu Syslog

Rys. 5. Przykładowe zdarzenia bezpieczeństwa zarejestrowane w serwerze Syslog

jaka wartość była przed i po zmianie (rys. 5). Istnieje także możliwość poinformowania o zdarzeniu bezpieczeństwa poprzez e-mail czy alarm przesłany do SSiN. Możliwe jest wygenerowanie raportu z zarejestrowanych zdarzeń w przypadku wystąpienia incydentu bezpieczeństwa i dołączeniu go podczas zgłaszania incydentu do właściwej komórki CERT (CSIRT), odpowiedzialnej za obsługę incydentów w danym sektorze operatorów usług kluczowych. Monitorowanie umożliwia niezbędną kontrolę nad urządzeniami na stacji, co stanowi kluczową rolę w przypadku wykrywania i zapobiegania wystąpienia incydentów bezpieczeństwa.

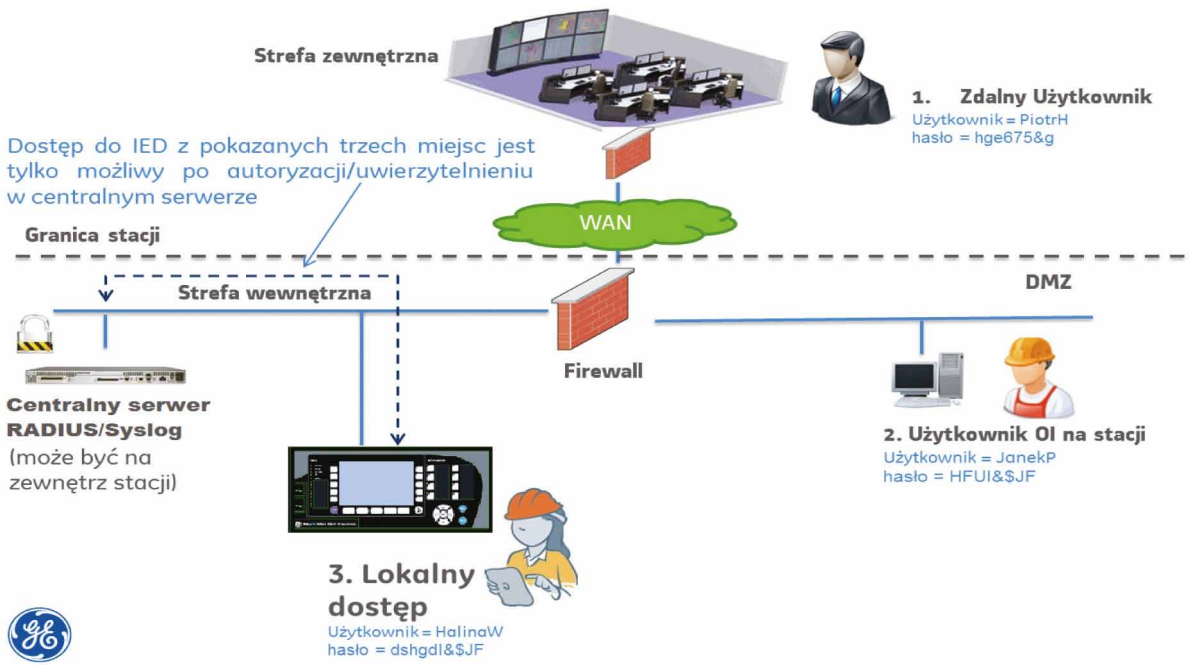
- **Szyfrowana komunikacja pomiędzy bezpłatnym oprogramowaniem inżynierskim EnerVista wykorzystywanym do zamiany nastaw, odczytu rejestratora zakłóceń oraz dziennika zdarzeń a urządzeniem serii Multilin** oparta o protokół the Secure Shell (SSH) ze standardem Advanced Encryption Standard (AES) i kluczem 128-bitowym w Galois Counter Mode (GCM). Dzięki szyfrowaniu chronimy przesyłane informacje, np.: nastawy zabezpieczeń, przed ingerencją osób trzecich, w wyniku czego mogłyby zostać zmodyfikowane i doprowadzić do błędnego działania urządzenia.

Ponieważ opisane tu rozwiązania są powszechnie stosowane w sieciach i systemach IT, istnieje wielu producentów oprogramowania do uwierzytelniania i autoryzacji z wykorzystaniem RADIUS\LDAP oraz do monitorowania, wykorzystując protokół Syslog. Daje to możliwość integracji urządzeń GE Multilin z narzędziami obecnie stosowanymi w przedsiębiorstwach do monitorowania zdarzeń bezpieczeństwa oraz centralnego zarządzania dostępem przez pracowników działów IT. Pozwala to na zastosowanie ujednoliconych narzędzi dla całej spółki.

Serwer RADIUS/Syslog może zostać zainstalowany zarówno na stacji energetycznej (rys. 6), jak i – co w przypadku zarządzania i monitorowania bezpieczeństwem wielu obiektów (całej infrastruktury krytycznej) wydaje się bardziej zasadne – w centralnym punkcie zarządzającym bezpieczeństwem, np.: ZE, RCN, CNE, w pomieszczeniu osoby odpowiedzialnej za cyberbezpieczeństwo itp. Ze względu na fakt, że serwer będzie pełnił kluczową rolę, należy zapewnić szczególną ochronę przed nieupoważnionym dostępem do pomieszczenia, w którym zostanie on zainstalowany oraz zapewnić bezpieczną i odporną na cyberataki łączność między serwerem a urządzeniami zainstalowanymi na przykład na stacji Elektro-Energetycznej poprzez szyfrowanie, tunelowanie, DMZ itp. W przypadku utraty komunikacji z serwerem RADIUS istnieje możliwość zalogowania się do urządzeń na konta lokalne. Jednakże konta te wraz z hasłami powinny być zabezpieczone i dostępne na żądanie jedynie w przypadkach awaryjnych, np. u dyspozytora w zabezpieczonej kopercie.

Podsumowanie

Z uwagi na rosnącą liczbę odnotowanych ataków i zagrożeń cybernetycznych oraz na skutki, jakie mogą one mieć dla funkcjonowania przedsiębiorstw a nawet państw, cyberbezpieczeństwo stało się obecnie jednym z kluczowych aspektów



Rys. 6. Dostęp do urządzenia z wykorzystaniem uwierzytelniania i autoryzacji w centralnym serwerze RADIUS

współczesnego świata. Nie tylko regulacje prawne, które lada chwila wejdą w życie w postaci ustawy o krajowym systemie cyberbezpieczeństwa, ale również świadomość przedsiębiorców dotycząca możliwych strat finansowych i wizerunkowych w przypadku wystąpienia incydentu cybernetycznego, powinna nas skłaniać do wyboru rozwiązań możliwie jak najbardziej odpornych na tego typu zdarzenia. Należy pamiętać, że rozwiązania podnoszące bezpieczeństwo cybernetyczne nie tylko chronią przed atakami cybernetycznymi, ale również zapewniają ochronę przed nieumyślnym spowodowaniem usterki przez niewłaściwe działania personelu odpowiadającego za obsługę urządzeń.

Prawdopodobieństwo wystąpienia zagrożenia cybernetycznego w przedsiębiorstwach energetycznych, zakładach przemysłowych (czy to uznanych za operatorów usługi kluczowej, czy też nie) jest w dzisiejszych czasach znaczące i nie powinno być ignorowane. Straty poniesione wskutek nieumyślnego incydentu czy też celowego ataku będą wielokrotnie przewyższać nakłady inwestycyjne związane z zastosowaniem urządzeń i systemów zwiększających poziom cyberbezpieczeństwa przedsiębiorstwa. Z uwagi na powyższe, jest zasadne stosowanie rozwiązań zwiększających bezpieczeństwo cybernetyczne bez względu na to, czy jest się zakwalifikowanym jako operator usługi kluczowej, czy też nie.

Literatura

[1] Ocena skutków regulacji z dnia 27 października 2017 r. do projektu ustawy o krajowym systemie cyberbezpieczeństwa.

[2] Projekt ustawy z dnia 15.02.2018 r. o krajowym systemie cyberbezpieczeństwa. Nr w wykazie prac legislacyjnych Rady Ministrów UD31.

[3] Tabela zawierająca odniesienie się Ministerstwa Cyfryzacji do uwag zgłoszonych w ramach opiniowania do projektu ustawy o krajowym systemie cyberbezpieczeństwa.

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

mgr inż. Cezary Bryczek – GE Power Sp. z o.o., Wałbrzych
e-mail: cezary.bryczek@ge.com