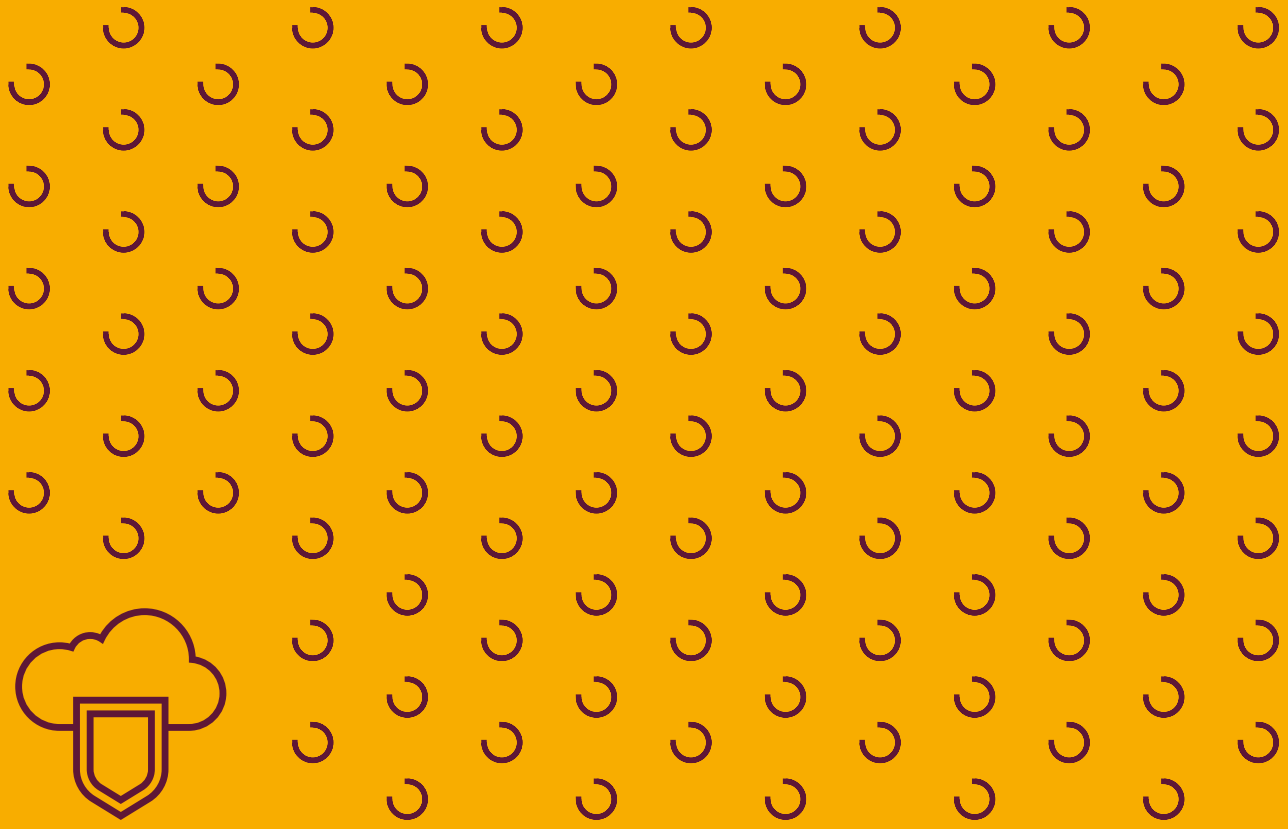


OD AUDYTU DO BEZPIECZNEJ INFRASTRUKTURY

Cyberbezpieczeństwo w praktyce

WSTĘP

„Cyberbezpieczeństwo w praktyce”

ma w pierwszej kolejności pełnić funkcje poradnikowe. Naszym zadaniem było przedstawienie kluczowych zagadnień wiążących się z cyberbezpieczeństwem w przemyśle i przekazanie w skrótowej formie najistotniejszych zagrożeń w obszarze IT oraz OT, a także zaleceń dotyczących odpowiedzi zakładów przemysłowych na te zagrożenia. Z dokumentu dowiesz się m.in.:

Jakich rodzajów zagrożeń może obawiać się współczesny przemysł w obszarze technologii informatycznych (IT)?

W części „Krajobraz zagrożeń infrastruktury IT” opisujemy takie zagrożenia jak malware, ransomware, ataki internetowe, wyłudzanie informacji, ataki DDoS, spam, botnety, wyciek danych, cryptojacking, cyberszpiegostwo i inne.

Przed jakimi zagrożeniami w przemyśle, w obszarze technologii związanych z produkcją - Operational Technology (OP) należy się chronić w szczególności?

W tej części omawiamy kategorie zagrożeń obejmujące m.in. procesy, ludzi i technologie. Opisujemy także znaczenie czynnika ludzkiego w całym systemie ochrony zakładów przemysłowych.

Na czym polega koncepcja głębokiego bezpieczeństwa – „Defense in Depth”?

Przedstawiliśmy na czym polega specyfika firm przemysłowych w obszarze bezpieczeństwa oraz opisaliśmy rozwiązania dedykowane dla przemysłu pod kątem infrastruktury krytycznej oraz elementów aktywnych infrastruktury, takich jak SCALANCE. Omówiliśmy też czym jest filozofia „Defence in Depth” Siemensa.

Jak przedsiębiorstwa radzą sobie z zagrożeniami?

Na przykładzie Constellation Brands i Sapa w Rackwitz pokazaliśmy jak firmy te przeciwdziałały zagrożeniom, jak zwiększyły bezpieczeństwo zakładu przed atakami i nieautoryzowanym dostępem.

Z jakich norm wynikają procedury i działania związane z oceną bezpieczeństwa?

W części dotyczącej oceny bezpieczeństwa opisaliśmy na czym polega ten proces. Omówiliśmy czym jest ocena cyberbezpieczeństwa, jakie normy określają postępowanie walidujące stan ochrony zakładu przemysłowego i jakie procedury są z nią związane.

Na czym polega ocena bezpieczeństwa w przemysłowej sieci OT? Jakie są cele oceny? Jakie aspekty brane są pod uwagę podczas oceny bezpieczeństwa?

Omówiliśmy zasady cyberbezpieczeństwa w odniesieniu do przemysłowych systemów sterowania (ICS - Industrial Control Systems) - w kontekście m.in. PLC i SCADA.

Czym jest CERT, i czym jest ProductCERT Siemensa?

Opisujemy czym są CERT czyli Computer Emergency Response Team i jaką rolę pełnią w wyszukiwaniu luk bezpieczeństwa w oprogramowaniu i w znajdywaniu odpowiedzi na istniejące zagrożenia.

O wypowiedzi poprosiliśmy grono ekspertów reprezentujących następujące organizacje: **ISSA Polska, Ministerstwo Cyfryzacji, Urząd Dozoru Technicznego, NASK, portal zajmujący się cyberbezpieczeństwem „Niebezpiecznik".**

PORADNIK POZWOLI PAŃSTWU:

1. Uzupełnić wiedzę w wybranych dziedzinach dotyczących bezpieczeństwa
2. Zapoznać się z narzędziami ułatwiającymi ochronę zasobów zarówno od strony procedur jak i technologii
3. Dowiedzieć się jakie, często niedoceniane aspekty decydują o przygotowaniu przedsiębiorstwa przemysłowego na cyberzagrożenia
4. Dzięki case studies zapoznać się z metodami, za pomocą których inne przedsiębiorstwa rozwiązują problemy związane z bezpieczeństwem
5. Zapoznać się z opinią ekspertów

BEZPIECZEŃSTWO W CENTRUM UWAGI

DOMINIKA BETTMAN

PREZES ZARZĄDU SIEMENS POLSKA

Bezpieczeństwo w centrum uwagi

Współczesny przemysł cechuje się dużą zmiennością wynikającą z potrzeby dostosowywania się producentów do wymagań ze strony klientów. Oprócz trendów sezonowych mają miejsce także zdarzenia zupełnie nieprzewidywalne, o zasięgu lokalnym lub globalnym, które mogą zachwiać podstawami całej światowej gospodarki. Współczesny przemysł musi być przygotowany na wszystkie te wyzwania – spodziewać się tego, co nieprzewidywalne.

Pojawiające się w zmiennych odstępach czasu zdarzenia losowe, takie jak pożary czy klęski żywiołowe, uświadamiają nam jak ważne jest szeroko rozumiane bezpieczeństwo. Równie nieprzewidywalne i dotkliwe dla przedsiębiorstw przemysłowych i ich klientów mogą być naruszenia cyberbezpieczeństwa: ataki hackerów zakłócające pracę systemów czy wycieki informacji. Firmy, które są w stanie przygotować obronę przed atakami, zabezpieczyć się na wypadek incydentów, będą w stanie uchronić się przed dużymi stratami.

Trendy technologiczne wpływające na rozwój przemysłu

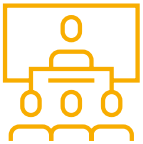
We współczesnym świecie o sukcesie przedsiębiorstw w przemyśle, decyduje przede wszystkim zdolność do tworzenia rozwiązań wyprzedzających konkurencję pod względem innowacji produktowych, obniżania kosztów produkcji lub tworzenia nowych modeli biznesowych. Przewagę taką daje Industry 4.0. Według najnowszego raportu z badań „Industry 4.0 Market by Technology" rynek Przemysłu 4.0 szacowany był w 2019 r. na 71,7 mld USD. Oczekuje się, że do 2024 r. osiągnie on wartość 156,6 mld USD, przy średniorocznym wzroście (CAGR) 16,9% w okresie od 2019 r. do 2024 r.[1]

Przyszłość przemysłu należeć będzie do innowacji w trzech następujących obszarach: sztucznej inteligencji (Artificial Intelligence), którą widzimy w fabrykach przyszłości, rozszerzonej rzeczywistości (Augmented Reality), której w Siemensie również poświęcamy dużo uwagi, bo pozwala na dostęp do informacji produkcyjnych z dowolnego miejsca na świecie oraz Edge Computing, który wspiera procesy związane z analizą danych. Także chmura jest ważnym elementem łączącym urządzenia i technologie, pozwalającym realizować wizję przyszłości. Zgodnie z wizją Siemensa wszystkie wspomniane elementy są istotne dla dalszego rozwoju przemysłu.

Rola informacji w przemyśle

Technologie te łączy wspólny mianownik: dane. Duże znaczenie dla działania współczesnego przemysłu ma zarządzanie danymi wspomagające m.in. optymalizację produkcji i zapobieganie awariom. Dostarczane informacje pozwalają usprawnić procesy produkcji, lepiej zarządzać zasobami i oszczędzać koszty. Predictive Maintenance to użycie danych do wyszukiwania anomalii w działaniu maszyn i linii produkcyjnych zapobiegające awariom. Odpowiednie wykorzystanie informacji i systemów służących do gromadzenia, obróbki i analizy danych pozwala przedsiębiorstwom stworzyć przewagę konkurencyjną.

Dane odgrywać będą coraz większą rolę w przemyśle. Ochrona informacji, zabezpieczenie procesów sterowanych w oparciu o dane bieżące, już obecnie jest krytyczna dla działania firm, a jej znaczenie z czasem będzie się tylko zwiększać. Firmy przemysłowe muszą być zatem odporne nie tylko na ataki na ich szeroko rozumiane systemy informatyczne (IT) tak samo jak pozostałe przedsiębiorstwa, ale powinny także w sposób szczególny zapewnić ochronę systemów stricte przemysłowych – OT, odpowiedzialnych za wytwarzanie, monitorowanie urządzeń i utrzymywanie ich w gotowości.



Świadomość kadr ma kluczowe znaczenie w strategii bezpieczeństwa

Pracownicy i menedżerowie muszą być przygotowani na nieprzewidywalne incydenty związane z szeroko rozumianym bezpieczeństwem. Lista potencjalnych zagrożeń dla działania firm jest długa, a ważne miejsce zajmuje wśród nich także cyberterroryzm. Siemens z najwyższą uwagą podchodzi do zagadnień związanych z ochroną informacji, zabezpieczeniem firmy przed różnymi rodzajami ataków i zagrożeń propagując koncepcję „Defense in Depth" wewnątrz organizacji, wśród partnerów i klientów.

Świadomość znaczenia zagadnień związanych z bezpieczeństwem ma dla organizacji kluczowe znaczenie. Według przeprowadzonej przez SANS ankiety „2019 State of OT/ICS Cybersecurity Survey"[2] to właśnie czynnik ludzki stanowi największe ryzyko naruszenia bezpieczeństwa systemów przemysłowych OT organizacji. Według 62% ankietowanych przez SANS jest on najważniejszą przyczyną zagrożeń i leży u podstaw najistotniejszych incydentów i naruszeń cyberbezpieczeństwa. Dlatego kształcenie, szkolenie i formowanie kadr jest w naszej opinii najważniejszym zadaniem w obszarze bezpieczeństwa.

KRAJOBRAZ ZAGROŻEŃ INFRASTRUKTURY IT

Przedsiębiorstwa przemysłowe, tak jak wszystkie inne organizacje, podlegają zagrożeniom wynikającym z otwarcia ich serwisów na świat i dostępu do ich zasobów poprzez sieć Internet. Dodatkowo, zagrożenie stanowi ich szczególna rola w zapewnianiu społeczeństwu dostępu do podstawowych usług, bez których niemożliwe jest obecnie funkcjonowanie ludności, takich jak energia elektryczna, woda pitna czy potrzebny do ogrzewania gaz. Rodzi to szczególne zagrożenie związane z cyberterroryzmem oraz cyberszpiegostwem. Przedsiębiorstwa przemysłowe nie mogą jednak ignorować także innych, powszechnych zagrożeń, takich jak malware, ataki DDoS czy ransomware, bo tak jak wszystkie inne organizacje są one na nie także narażone.

Firma Juniper Research prognozowała, że cyberprzestępczość w 2019 roku kosztować będzie firmy łącznie ponad 2 biliony dolarów[3]. Z raportu European Union Agency for Network and Information Security (ENISA)[4] dowiadujemy się o typach zagrożeń oraz ich znaczeniu dla bezpieczeństwa przedsiębiorstw.

Malware

Złośliwe oprogramowanie (malware) jest najczęściej spotykanym cyberzagrożeniem i według raportu ENISA odpowiada za 30% zgłoszonych w 2018 roku incydentów. Autorzy złośliwego oprogramowania dostosowują ich kod w taki sposób, by mógł być skuteczny także w atakach przynoszących korzyści z przestępstwa (ransomware).

Malware coraz częściej atakuje urządzenia Internet of Things (IoT). Jednym z godnych uwagi wydarzeń w 2018, roku był atak VPNFilter. VPNFilter to wielostopniowe złośliwe oprogramowanie, które zaatakowało ponad 500 tys. urządzeń na całym świecie, tworząc w ten sposób ogromną sieć ułatwiającą kolejne, anonimowe ataki na komputery i urządzenia mobilne.

W 2018 roku pojawiły się pierwsze malware o nazwie Triton atakujące systemy infrastruktury krytycznej Safety Instrumented Systems (SIS)[5]. Po raz pierwszy oprogramowanie o podobnym działaniu ujawniło swoje destrukcyjne działanie w ataku na saudyjskiego giganta naftowego Petro Rabigh w 2017 r. Według analityków z FireEye cyberprzestępcy stojący za Tritonem w 2019 roku po raz kolejny zaatakowali systemy kontroli przemysłowej (ICS) na Bliskim Wschodzie[6]. Triton podszywa się pod legalną aplikację Triconex Trilog służącą do przeglądania logów systemowych. Oprogramowanie jest zdolne do zakłócania działania zakładu, powodując przestoje w funkcjonowaniu usług. Te cechy stawiają je w jednym szeregu ze złośliwym oprogramowaniem Stuxnet powodującym przesyłanie błędnych informacji do sterowników PLC i odpowiedzialnym za awarie w różnego rodzaju fabrykach,

rafineriach czy elektrowniach oraz złośliwym oprogramowaniem Industroyer / Crash Override, które doprowadziło do przestojów w działaniu ukraińskiej sieci energetycznej.

Ransomware i wyłudzenia pieniędzy od przedsiębiorstw

Słowem ransomware określamy cyber-szantaż. Przestępca włamuje się do komputera ofiary i szyfruje zawartość dysków, uniemożliwiając dostęp do danych. Na ekranie zainfekowanych urządzeń wyświetlany jest komunikat o tym, co zrobić, by szantażysta umożliwił nam powrót do korzystania z systemów i dostęp do danych. W przypadku ataków pierwszych wersji ransomware wystarczyły czasami zmiany w rejestrze systemu operacyjnego, by użytkownik odzyskał kontrolę nad maszyną. Obecnie stosowane, najbardziej zaawansowane formy ransomware szyfrują pliki ofiary w taki sposób, że ich odzyskanie bez posiadanego przez przestępców klucza jest praktycznie niemożliwe. Jest to atak szczególnie groźny dla przedsiębiorstw, które nie tylko nie zapewniają właściwego zabezpieczenia przed tego typu złośliwym oprogramowaniem, ale przede wszystkim - zaniedbują backup. Ataki ransomware obserwowane są już od ponad 20 lat.

W ostatnim czasie ich częstotliwość nasiliła się ze względu na większe możliwości szantażystów pozostania anonimowymi, dzięki metodom płatności kryptowalutami. Jednym z najbardziej znanych ransomware jest WannaCry – złośliwe oprogramowanie typu ransomworm, które opiera się na kombinacji prostych technicznie exploitów. WannaCry replikuje się samoczynnie, bez ingerencji człowieka i rozprzestrzenia się z jednego komputera na inny w tej samej sieci. Globalny atak WannaCry na organizacje opieki zdrowotnej rozpoczął się w maju 2017 roku i doprowadził do zainfekowania 200 000 komputerów w 150 krajach.

Przedsiębiorstwa przemysłowe są narażone na ransomware w podobnym stopniu, jak inne firmy. Ataki ransomware nasiliły się w 2019 roku, o czym świadczą dane statystyczne przedstawione na dorocznej konferencji United States Conference of Mayors. Według stanu na lipiec 2019[7] , od 2013 roku, co najmniej 170 systemów miejskich, powiatowych lub stanowych w USA doświadczyło tego rodzaju ataku. Dwadzieścia dwa z nich miały miejsce w ciągu pierwszych sześciu miesięcy 2019 roku. Ransomware uniemożliwia pracownikom zaatakowanej firmy dostęp do systemów. W marcu 2019 roku w wyniku tego rodzaju ataku norweski producent aluminium, Norsk Hydro[8] poniósł straty szacowane na 71 mln USD. Natomiast w listopadzie 2019 zaatakowana została duża meksykańska firma naftowa Pemex[9] z obrotami rzędu 120 mld USD rocznie. W ataku tym szantażyści zażądali okupu w wysokości 565 bitcoinów, czyli ponad 4 mln dolarów.

Ataki internetowe

Ataki bazujące na możliwościach sieci wykorzystujące systemy i usługi sieciowe jako główną powierzchnię podatności ofiary. Obejmują one wykorzystanie przeglądarki w celu dodawania złośliwego kodu poprzez jego wstrzyknięcie (injection) na strony internetowe. Wykorzystują systemy zarządzania (CMS) i usługi sieciowe. Ataki oparte na sieci muszą być postrzegane jako jedno z najważniejszych zagrożeń ze względu na ich znaczny potencjał: od kampanii spamowych związanych z reklamami po trojany i Advanced Persistent Threat (APT).

W atakach na aplikacje internetowe stosowane są bezpośrednie lub pośrednie próby wykorzystania luki w zabezpieczeniach w usługach i aplikacjach w Internecie, nadużywanie interfejsów API i środowisk lub usług.

Wyłudzanie informacji (phishing)

Wyłudzanie informacji to mechanizm wykorzystujący techniki inżynierii społecznej, dzięki którym odbiorca zostanie zwabiony i „chwyci przynętę". Phisherzy próbują zachęcić odbiorców do reagowania na wiadomości e-mail, SMS lub treści internetowe, doprowadzając do otwarcia przez ofiarę złośliwego załącznika, kliknięcia w niebezpieczny adres URL lub sprawiając, że użytkownik przekaże swoje dane uwierzytelniające za pomocą wiarygodnie wyglądających stron phishingowych służących rzekomo np. do przelewów pieniężnych. Według przygotowanego przez Europol raportu Internetorganised Crime Threat Assessment[10] przypadki phishingu dotyczą 75% państw członkowskich UE.

Ataki DDoS

Ataki DDoS polegają na nieustannym nękaniu infrastruktury ofiary sztucznym, generowanym przez boty, ruchem internetowym. W efekcie uniemożliwiają one rzeczywistym użytkownikom dostęp do stron przedsiębiorstwa i powodują znaczące straty. W ataku DDoS (Distributed Denial-of-Service) uczestniczy zwykle bardzo wiele urządzeń klienckich (np. komputerów, smartfonów, sprzętu sieciowego), które próbują dostać się do zasobów atakowanego urządzenia. Atak realizowany jest z wielu zainfekowanych urządzeń (tzw. botnetu) zalewającego atakowane przedsiębiorstwo ruchem sieciowym. Jaki jest koszt ataku DDoS? Źródła podają zwykle od 20 tys. do 40 tys. USD za godzinę unieruchomienia strony, ale koszt ten zależy od wielkości firmy, znaczenia jej obecności w sieci oraz wielkości sprzedaży usług/produktów poprzez Internet. W przypadku każdego przedsiębiorstwa potencjalne straty będą inne. Na stronie Akamai[11] dostępny jest kalkulator potencjalnych kosztów takiego ataku[12],

można też skorzystać z innych kalkulatorów[13], by oszacować koszty DDoS dla własnej firmy. Jak podają serwisy zajmujące się atakami DDoS w 2019 roku udało się znacznie ograniczyć źródła tych zagrożeń[14]. Po aresztowaniu administratorów i zamknięciu Webstresser.org w kwietniu 2018[15] - jednego z najbardziej znanych serwisów oferujących „usługi" DDoS – liczba ataków zmalała i statystki znacznie się poprawiły. Niestety nie ustały zupełnie, bo w miejsce zamkniętych przestępczych przedsięwzięć i aresztowanych właścicieli pojawiły się nowe podmioty świadczące przestępcze usługi oraz nowi „przedsiębiorcy". Śledczy dotarli jednak nie tylko do bezpośrednio odpowiedzialnych za ataki, ale także do ich klientów. Pod koniec stycznia 2019 roku Europol poinformował o aresztowaniu ponad 250 użytkowników w Wielkiej Brytanii i Holandii. Inne źródła podają, że prowadzone jest dochodzenie w sprawie wszystkich 150 000 klientów Webstresser zamieszkałych w 20 różnych krajach.

Spam

Spam polega na wykorzystywaniu poczty elektronicznej e-mail do przesyłania niechcianych przez odbiorcę wiadomości. Spam pochodzi z początków Internetu i jest obecnie dystrybuowany głównie przez duże botnety spamowe. Mimo, że zjawisko z czasem straciło na znaczeniu spam jest nadal jednym z głównych wektorów ataku. W ciągu ostatnich lat spam ewoluował (pojawił się na przykład spam za pośrednictwem mediów społecznościowych i komunikatorów). Spam jest uważany za zagrożenie głównie dlatego, że powoduje utratę czasu odbiorców, a zatem jest źródłem kosztów przedsiębiorstwa. Wpływa też na zmniejszenie przepustowość sieci, obciąża zasoby obliczeniowe i pamięci masowe. Niechciana korespondencja mailowa może przenosić także malware.

Botnety

Botnet to inaczej sieć komputerów zainfekowanych złośliwym oprogramowaniem, nad którymi atakujący przejmują kontrolę. Z maszyn tych dokonywane są następnie inne ataki, w tym wysyłanie spamu, rozprzestrzenianie wirusów lub przeprowadzanie ataków DDoS.

W raporcie „Spamhaus Botnet Threat Report 2019" [16]przedstawiającym sytuację w ubiegłym roku, badacze ze Spamhaus Malware Labs zidentyfikowali i zablokowali 17 602 serwery Command & Control (C&C) botnetu hostowane w 1 210 różnych sieciach. Jest to ogromny wzrost, bo aż o 71,5% w porównaniu do 2018 roku. Od 2017 roku liczba nowo wykrytych botnetów prawie się podwoiła z 9 500 do 17 602. Spamhaus śledzi zarówno adresy IP, jak i nazwy domen wykorzystywanych przez serwery botnetów.

W 2019 roku Rosja, która odnotowała 143% wzrost ruchu C&C zajęła pierwsze miejsce pod względem lokalizacji botnetów, spychając z pozycji lidera Stany Zjednoczone.

Prawie 60% nowo wykrytych botnetów w 2019 roku powiązanych było z kradzieżą danych. Wśród najbardziej popularnych Lokibot nie tylko pozostał na pierwszym miejscu, ale także zwiększył zasięg o 74% w porównaniu do danych z 2018 roku. Drugi na liście „złodziej danych" – botnet AZORult, dołączył do Lokibota na szczycie listy, na pozycji nr 2.

Naruszenie danych i wyciek danych

Naruszenie danych to celowe lub niezamierzone doprowadzenie do wycieku poufnych informacji. Incydenty obejmują zarówno skoordynowane ataki w celach zarobkowych związanych z przestępczością zorganizowaną, działania polityczne lub wymierzone w rządy krajowe, po przypadkowe pozbywanie się zużytego sprzętu komputerowego lub nośników danych prowadzące do wycieku danych. W 2019 roku doszło do kilku znacznych incydentów tego rodzaju. W styczniu odkryto, że w sieci znalazło się blisko 780 mln rekordów – adresów mailowych oraz przypisanych im haseł i zdaniem ekspertów wyciek ten można uznać za jeden z największych w historii. Zbiór wykradzionych informacji został opublikowany m.in. na forach przestępców zajmujących się nielegalnym wykorzystaniem danych. Incydent oraz zasób informacji, które wyciekły nazwano „Collection#1". Kilka miesięcy później, w październiku 2019 roku[17] serwisy zajmujące się cyberbezpieczeństwem poinformowały o odkryciu w sieci 4 terabajtów danych użytkowników, z takimi informacjami jak adresy e-mail, numery telefonów, dane profilowe LinkedIn i Facebook. To drugi co do wielkości wyciek danych w historii, który liczbowo przewyższa jedynie wyciek danych użytkowników serwisu Yahoo (3 mld rekordów, 2013 rok). Jakby tego było mało, w maju 2019 roku, zajmujący się cyberbezpieczeństwem dziennikarz Brian Krebs poinformował o znaczącym wycieku danych – blisko 900 mln dokumentów amerykańskiej firmy zajmującej się nieruchomościami – First American Financial. Pomimo wzrostu świadomości na temat ochrony danych i rozwoju technologii – wycieka ich coraz więcej. Z zestawienia incydentów w ostatnich latach wynika, iż w 2019 roku odnotowano 23 duże wycieki danych dotyczące około 2,4 mld rekordów.

Z perspektywy całego państwa infrastruktura elektroenergetyczna jest infrastrukturą krytyczną. Pozwala na prawidłowe funkcjonowanie gospodarki, a w konsekwencji obsługuje praktycznie wszystkie gałęzie przemysłu. Większość zakładów zobowiązana jest do wdrożenia procedur w zakresie cyberbezpieczeństwa w oparciu o ustawę opracowywaną przez Ministerstwo Cyfryzacji i odnoszącą się do tzw. „infrastruktury krytycznej". Obecny trend preferuje otwarte rozwiązania komunikacyjne, standaryzację wymiany danych i pełną transparentność na poziomie obiekt wykonawczy – systemy Scada/MES. Liczne raporty pokazują, że stacje PLC/HMI są regularnie „testowane" przez zorganizowane ataki hackerskie. Pozwala to stwierdzić, że praktycznie każdy zakład jest lub powinien być zainteresowany wdrożeniem zasad cyberbezpieczeństwa celem ochrony danych produkcyjnych, swojego know-how, ale przede wszystkim niedopuszczenia do zatrzymania samej produkcji. W konsekwencji nie sposób wskazać konkretnego klienta, który nie byłby zainteresowany rozwiązaniami minimalizującymi cyberzagrożenia.

RAFAŁ BIEŃ

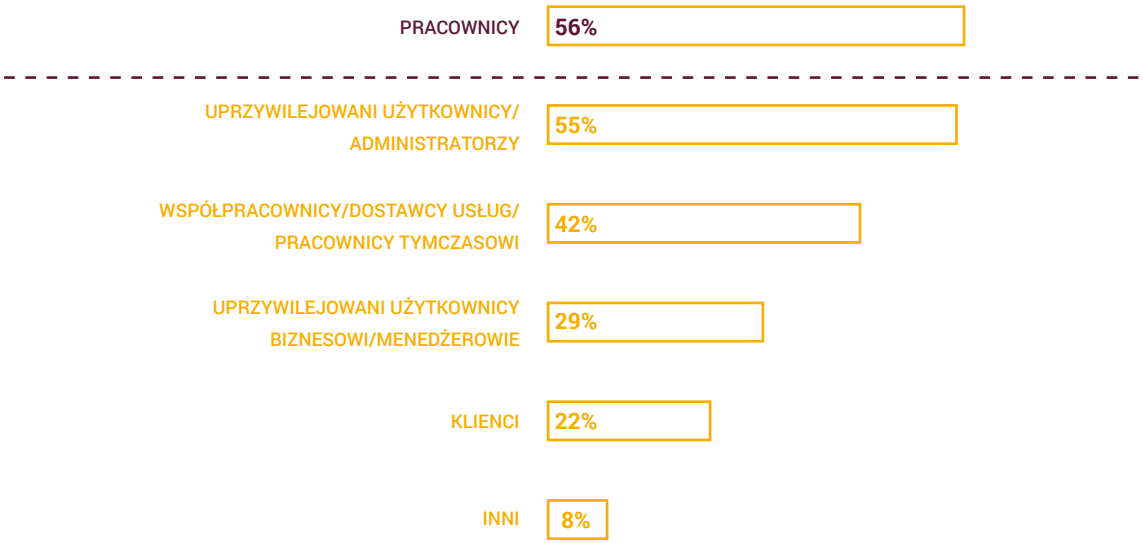
SIEMENS POLSKA

Zagrożenie od wewnątrz

Praktycznie wszystkie firmy i organizacje narażone są na zagrożenie z wewnątrz. Każdy obecny lub były pracownik, partner lub podwykonawca, który miał lub ma dostęp do zasobów organizacji, może celowo lub przypadkowo nadużyć udzielonego mu wcześniej uprawnienia do danych. Trzy najczęstsze rodzaje zagrożeń związanych z wykorzystaniem informacji poufnych to:

- **złośliwy informator** – działający umyślnie pracownik lub współpracownik, partner
- **wyciek w wyniku zaniedbania** – następuje wówczas, kiedy pracownik lub partner nie przestrzega zasad i instrukcji bezpieczeństwa
- **wyciek za pośrednictwem pracownika,** który działa nieumyślnie, ale jest przez atakującego wykorzystywany

ŹRÓDŁA ZAGROŻEŃ WEWNĘTRZNYCH DLA BEZPIECZEŃSTWA PRZEDSIĘBIORSTWA



Kradzież tożsamości

Kradzież tożsamości następuje w wyniku wycieku danych osobowych. W obecnych czasach konta bankowe, adresy domowe, dokumenty księgowe, dane medyczne i mnóstwo innych danych osobowych przechowywanych w urządzeniach własnych lub w bazach danych firm narażonych jest na działalność cyberprzestępczą. Atakujący potrzebują kilku elementów danych osobowych, aby dokładnie „zbudować" pełny profil konkretnej osoby. Jeśli „fragmenty informacji" nie są wystarczające do uzyskania pełnego profilu, dane są wymieniane między atakującymi za pośrednictwem Dark Web. Zagrożenie kradzieżą tożsamości jest silnie związane z naruszeniami danych w firmach lub organizacjach we wszystkich sektorach gospodarki. Naruszenie danych w większości przypadków ukierunkowane jest na dane klientów firmy. Informacje wyciekające podczas tych ataków mogą być wystarczające do następnego kroku, jakim jest oszustwo tożsamości.

Cyberszpiegostwo

Raporty globalnych organizacji zajmujących się badaniami nad bezpieczeństwem ujawniły, że cyberszpiegostwo staje się coraz większym zagrożeniem. Zagrożenie to zazwyczaj dotyczy sektora przemysłowego, infrastruktury krytycznej i strategicznej, obejmując jednostki rządowe, koleje, dostawców usług telekomunikacyjnych, firmy energetyczne, szpitale i banki. Cyberprzestępczość koncentruje się na kreowaniu zdarzeń z obszaru geopolityki, kradzieży tajemnic państwowych i handlowych, własności intelektualnej i informacji zastrzeżonych w strategicznych dziedzinach. W ostatnim czasie wzrosła liczba finansowanych przez wrogie sobie państwa cyberataków, które koncentrowały się głównie na gospodarce. Ataki te wykorzystują luki w urządzeniach przemysłowego Internetu Rzeczy (IoT) i dotyczą w szczególności sektora usług użyteczności publicznej, przemysłu przetwórstwa ropy naftowej i gazu ziemnego oraz produkcji.

Cryptojacking

Cryptojacking (znany również jako cryptomining) to stosunkowo nowy termin, który odnosi się do oprogramowania wykorzystującego moc obliczeniową urządzenia ofiary (procesora - CPU lub karty graficznej - GPU) do wydobywania kryptowalut bez zgody ofiary. Moc obliczeniowa służy do rozwiązywania równań kryptograficznych zapisanych w blockchainie.

Grupy działające na zlecenie wrogich państw używają różnych środków do anonimizacji ataków, co sprawia, że przypisywanie autorstwa konkretnemu atakowi jest niezwykle trudne. Ponadto, prawodawstwo poszczególnych krajów może sprzyjać kradzieży własności intelektualnej. Na przykład amerykańskie firmy działające w Chinach muszą uwzględniać, że cenne dane firmowe działających w tym kraju przedsiębiorstw przechowywane są wyłącznie w Chinach i przed przekazaniem tych danych poza Chiny wymagana jest zgoda rządu. Innym przykładem jest Rosja, która żąda recenzji kodu źródłowego oprogramowania dla wszystkich zagranicznych technologii sprzedawanych w tym kraju. Według brytyjskiego National Cyber Security Centre (NCSC), większość ataków przeprowadzają hakerzy finansowani przez wrogie państwa. Jedną z wciąż aktywnych grup zagrożeń cyberszpiegowskich jest PIPEFISH (znana również jako OilRig). Atakuje ona głównie podmioty z Bliskiego Wschodu działające w sektorze energetycznym.

Jak się zabezpieczać przed zagrożeniami?

Wirusy i złośliwe oprogramowanie można wykryć za pomocą odpowiedniego oprogramowania antywirusowego. W Siemensie automatyzacja tego procesu polega na instalacji narzędzi McAfee. Zarządzaniem oprogramowaniem – klientami antywirusowymi – w systemach PC i zapewnianiem bieżących sygnatur wirusów zajmuje się dedykowany do tego zadania serwer. Serwer ten może również wysyłać powiadomienia e-mailem do personelu serwisowego.

Wybierając kontrolery, komputery i inne systemy, z których należy korzystać, warto zwrócić uwagę, czy zawierają one mechanizmy ochronne i zostały przetestowane pod kątem luk w zabezpieczeniach. Takie testy są zazwyczaj znormalizowane. Na przykład certyfikat Achillesa wskazuje, że system pomyślnie przeszedł testy obciążenia i podatności. Ponadto, producent powinien zapewnić, że jego produkty spełniają wysokie standardy jakości. Proces rozwoju produktów Siemensa został przetestowany i stwierdzono, że spełnia on wymagania określone w IEC 624434[18].

Siemens ProductCERT

Siemens dysponuje zespołem ekspertów ds. bezpieczeństwa wspomagającym także klientów w wykrywaniu luk w zabezpieczeniach. Zespół ten nazywa się Product Computer Emergency Response Team (ProductCERT). Zgłoszone luki w zabezpieczeniach są natychmiast weryfikowane i analizowane przez ekspertów.

Siemens ProductCERT analizuje wszystkie raporty dotyczące problemów z bezpieczeństwem i publikuje porady dotyczące ochrony informacji i weryfikowanych luk, które bezpośrednio wpływają na produkty Siemensa i wymagają aktualizacji oprogramowania lub innych działań ze strony właściciela zakładu przemysłowego.

Ocena obejmuje waluację istniejącej instalacji pod względem środków ochrony, ryzyka i słabych punktów. Eksperci Siemensa przeprowadzają 2-dniową ocenę instalacji u klienta na podstawie normy IEC 62443 i przedstawiają zalecenia dotyczące minimalizacji ryzyka. Na potrzeby wdrożenia środków bezpieczeństwa oferowane są szkolenia mające na celu budowanie świadomości na temat cyberbezpieczeństwa w przemyśle. Można z nich również skorzystać w postaci kursów internetowych. Siemens doradza również w zakresie procesów, procedur i instrukcji pracy, a także skutecznej ochrony sieci. Ponadto zapewnia usługi konfiguracji Automation Firewall Next Generation i instalacji oprogramowania antywirusowego oraz wdrażania rozwiązań do monitorowania. Oferuje również usługi, które można wykorzystać w zakładzie w celu poprawy jego bezpieczeństwa. Obejmują one systemy do zarządzania oprogramowaniem antywirusowym, poprzez które zakład podłączony jest do centralnego serwera w firmie Siemens zapewniającego aktualne sygnatury wirusów.

O ENISA

European Union Agency for Network and Information Security (ENISA) jest jednostką, której celem jest gromadzenie wiedzy specjalistycznej w zakresie bezpieczeństwa informacji w UE, jej państwach członkowskich, w sektorze przedsiębiorstw i dla dobra obywateli państw członkowskich UE. ENISA opracowuje porady i zalecenia dotyczące dobrych praktyk w zakresie bezpieczeństwa informacji. Pomaga państwom członkowskim UE we wdrażaniu przepisów UE i działa na rzecz poprawy odporności na zagrożenia europejskiej infrastruktury i sieci informacji o znaczeniu krytycznym. ENISA dąży do zwiększenia istniejącej wiedzy w państwach członkowskich UE poprzez wspieranie rozwoju społeczności zaangażowanych w poprawę bezpieczeństwa sieci i informacji w całej UE.

ZAGROŻENIA INFRASTRUKTURY W PRZEMYŚLE

Oceniając bezpieczeństwo przemysłowych systemów Operational Technology (OT), należy zwrócić szczególną uwagę na „czynnik ludzki" – tak wynika z ankiety „2019 State of OT/ICS Cybersecurity Survey" przeprowadzonej przez SANS. Zdaniem respondentów szczególnie ważnym elementem, który należy brać pod uwagę w kwestiach ochrony zakładów przed zagrożeniami, są urządzenia dodane do sieci przemysłowej, zwłaszcza te wyposażone w technologie mobilne.

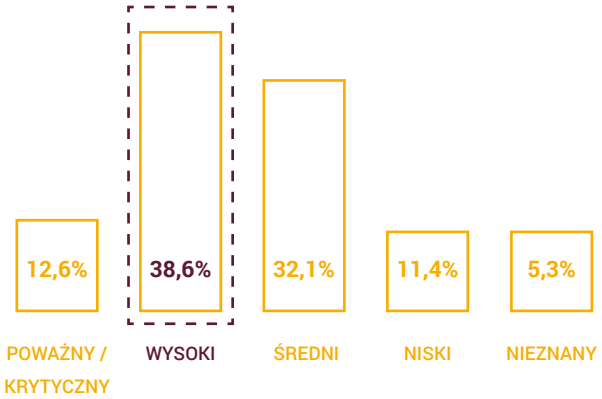
Zdaniem analityków SANS przeprowadzone przez tę organizację badanie bezpieczeństwa OT / ICS z 2019 r. świadczy o wzroście dojrzałości organizacji w obszarze ochrony systemów, poprawie identyfikowania przez nie potencjalnego ryzyka oraz wykrywania i reagowania na zdarzenia. Za najważniejszą przyczynę wywołującą zagrożenie dla bezpieczeństwa organizacji uważany jest czynnik ludzki, co oznacza, że szczególny nacisk należy położyć na rozwiązania problemu cyberbezpieczeństwa OT / ICS uwzględniające ryzyka związane z pracownikami, nie rezygnując jednak z obrony przed zagrożeniami zależnymi od wykorzystywanych technologii. Inicjatywy o najwyższym priorytecie (najwyżej budżetowe) związane były z systemem kontroli i bezpieczeństwa sieci. Działania te świadczą o zrozumieniu zasad funkcjonowania systemów bezpieczeństwa i konieczności sporządzenia mapy środowiska ICS. Wraz ze wzrostem znaczenia sieci w przemyśle zwielokrotniła się skala powodowanego przez nią zagrożenia. Łączność sieciowa otworzyła granice systemów przemysłowych – Industrial Control System (ICS), które historycznie były zamknięte, co spowodowało potrzebę kontroli działania komunikacji w przemyśle i przepływających przez sieć informacji, zwłaszcza w bezprzewodowych rozszerzeniach architektury ICS.

Wzrasta znaczenie architektur i usług opartych na chmurze. Kompleksowa kontrola zasobów systemowych, zwłaszcza urządzeń przemysłowych, staje się jeszcze trudniejsza, co wynika z coraz bardziej zacierających się granic systemów i dostępu do zasobów wirtualnych, co prowadzi do wzrostu ryzyka i wpływa na współczesne systemy ICS. Świadomość, edukacja i szkolenie zarówno pracowników OT, jak i IT staje się podstawą skutecznego wykorzystania ludzi, procesów i technologii w obszarze bezpieczeństwa systemów przemysłowych. Realizacja tych inicjatyw może być jednak trudniejsza niż się spodziewano. Pracownicy odpowiedzialni za obronę swojego środowiska przed różnymi czynnikami ryzyka koncentrują się zwykle na obecnymi bezpośrednim zagrożeniu. Przybywa im jednak pracy, bo do już obecnych czynników dochodzą zagrożenia związane ze wzrostem znaczenia Internetu Rzeczy (IoT), problemy z łańcuchem dostaw i podmiotami zewnętrznymi, które mogą naruszyć bezpieczeństwo.

Czynnik ludzki najistotniejszą przyczyną zagrożeń

Ryzyko oczywiście wpływa na podejście organizacji do bezpieczeństwa systemu OT. Nieco ponad 50% respondentów postrzega poziom cyberbezpieczeństwa OT / ICS jako poważny / krytyczny lub wysoki (rysunek 1).

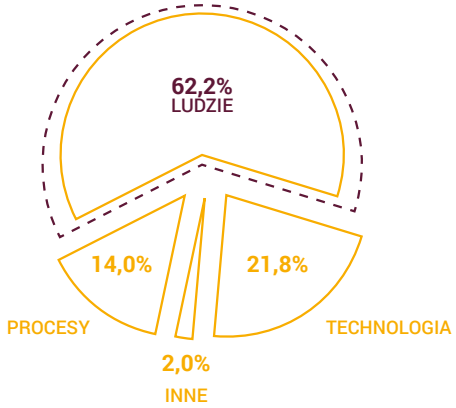
JAK ORGANIZACJA OCENIA POZIOM CYBERZAGROŻEŃ?



Rys. 1. Postrzeganie poziomu zagrożeń w przemyśle.

Czynnik ludzki stanowi największe ryzyko naruszenia bezpieczeństwa systemów OT organizacji. Według 62% ankietowanych jest on najistotniejszą przyczyną zagrożeń i leży u podstaw najważniejszych incydentów i naruszeń cyberbezpieczeństwa. Pozostałe czynniki - technologie (22%) i procesy (14%) wymieniane są przez respondentów dużo rzadziej (rys. 2).

JAKA KATEGORIA RYZYKA STANOWI NAJWIĘKSZE ZAGROŻENIE?



Rys. 2. Percepcja ryzyka w przemyśle.

„Czynnik ludzki" to szeroka kategoria ryzyka, obejmująca podmioty zewnętrzne i wewnętrzne oraz szerokie spektrum działań: od zamierzonych (złośliwych) do niezamierzonych (przypadkowych, nieostrożnych). Według raportu VerizonData Breach Investigations Report (DBIR) z 2018 r.[19] czynniki zewnętrzne, w tym przestępczość zorganizowana oraz cyberterroryzm odpowiadają za większość (72%)

naruszeń. Jednak potencjalnie bardziej niepokojące są dane o 28% naruszeń przez osoby wewnątrz organizacji. Zabezpieczenie przed czynnikami wewnętrznymi w przestrzeni OT / ICS jest szczególnie trudne. Co więcej, pracownicy dopuszczający się naruszeń bezpieczeństwa nie są o nic podejrzewani, bo na ogół dysponują właściwym dla ich stanowiska poziomem uprawnień dostępu do danych i systemów. Sytuację dodatkowo pogarszają ograniczenia kadrowe i technologiczne powodujące częste rotacje na tych stanowiskach.

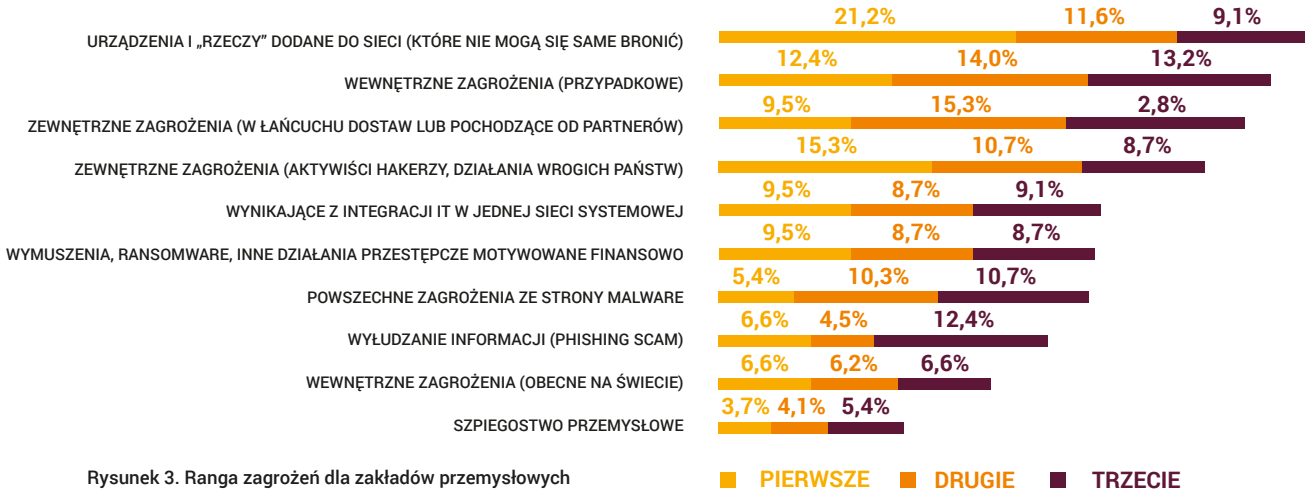
	2017		2019		ZMIANA
CZYNNIK	**PROCENT**	**MIEJSCE**	**PROCENT**	**MIEJSCE**	**MIEJSCA**
Zapewnienie niezawodności i dostępności systemów sterowania	52,3%	1	52,3%	1	—
Zapewnienie zdrowia i bezpieczeństwa pracowników	**32,7%**	**3**	**42,2%**	**2**	**1**
Obniżenie ryzyka / poprawa bezpieczeństwa	33,3%	2	34,8%	3	-1
Zapobieganie uszkodzeniom systemów	**24,8%**	**4**	**27,7%**	**4**	**—**
Spełnianie wymogów prawnych	17,0%	7	22,3%	5	2
Ochrona osób i mienia zewnętrznego	**16,3%**	**8**	**20,7%**	**6**	**2**
Zapobieganie stratom finansowym firmy	21,6%	6	18,8%	7	-1
Ochrona reputacji i marki firmy	**21,6%**	**5**	**17,6%**	**8**	**-3**
Zapobieganie wyciekom informacji	15,7%	9	14,8%	9	—
Zabezpieczanie połączeń z systemami zewnętrznymi	**13,7%**	**12**	**11,7%**	**10**	**2**
Zapewnianie lub koordynowanie programów edukacji i podnoszenia świadomości pracowników w zakresie cyberbezpieczeństwa	13,7%	11	10,5%	11	—
Minimalizowanie wpływu na akcjonariuszy	**5,9%**	**14**	**9,8%**	**12**	**2**
Tworzenie, dokumentowanie i zarządzanie politykami i procedurami bezpieczeństwa	14,4%	10	8,2%	13	-3
Ochrona tajemnic handlowych i własności intelektualnej	**9,8%**	**13**	**7,8%**	**14**	**-1**

Tabela 1. Najważniejsze czynniki biznesowe związane z cyberbezpieczeństwem. Główne obawy dotyczące biznesu związane z bezpieczeństwem i zarządzaniem ryzykiem OT pozostawały zasadniczo takie same w 2019 r. jak w 2017 r.

Znaczenie systemów sterowania

Według respondentów najistotniejszym wyzwaniem jest zapewnienie bezpieczeństwa, niezawodności i dostępności systemów sterowania. Równie istotną kwestią jest troska o zdrowie i bezpieczeństwo pracowników, której znaczenie wzrosło z 33% w 2017 r. do 42% w 2019 r., co stanowi największą zmianę w porównaniu do poprzedniej ankiety. Należy jednak zwrócić uwagę, że wszystkie wymienione przez respondentów obawy, o niezawodność, dostępność, zdrowie i bezpieczeństwo - łączą się ze sobą. W większości przemysłowych systemów sterowania dostępność sieci (w niektórych przypadkach wysoka dostępność [HA]) niezbędna jest do utrzymania ciągłości i bezpieczeństwa pracy. Co więcej, to właśnie zależna od działania sieci informacja o poprawności działania systemów zapewnia operatorom możliwość monitorowania, diagnozowania, konserwacji i przywracania do stanu użyteczności elementów sterowania oraz kontroli nad wykonywanymi przez systemy operacjami. Ponad 30% wzrost (do 22,3% w 2019 w porównaniu do 17% w 2017 r.) znaczenia kwestii określanych jako zgodność z przepisami jest prawdopodobnie wskazówką, że dotychczasowe regulacje były dotąd nieskuteczne w eliminowaniu zagrożeń w obszarze bezpieczeństwa. Kontrastuje to jednak ze zmniejszeniem o 43% (8,2% vs. 14,4%) znaczeniem dokumentowania i zarządzania politykami oraz procedurami bezpieczeństwa. Może to również wskazywać na wyższy stopień dojrzałości, z jakim firmy obecnie podchodzą od tworzenia dokumentów polityki bezpieczeństwa w porównaniu do wcześniejszego okresu. Stąd może wynikać mniejsze znaczenie tego czynnika w ostatnich badaniach.

NAJWAŻNIEJSZE KATEGORIE ZAGROŻEŃ USZEREGOWANE PRZEZ RESPONDENTÓW WEDŁUG RANGI



Rysunek 3. Ranga zagrożeń dla zakładów przemysłowych

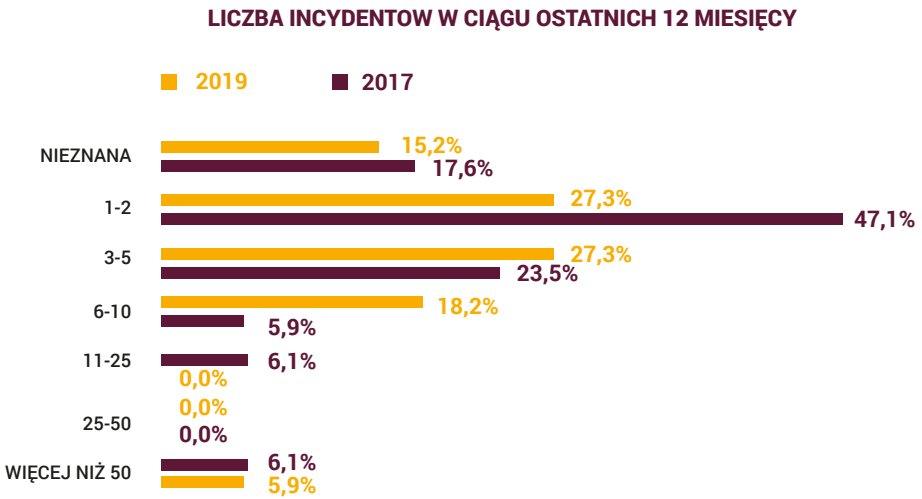
Bezpieczeństwo „rzeczy" w sieci przemysłowej

Zdaniem respondentów najważniejszą kategorią zagrożeń ogółem są urządzenia i „rzeczy" dodawane do sieci (które nie mogą same się chronić), co ponownie uświadamia nam jak ważne jest bezpieczne połączenie części produkcyjnej z infrastrukturą ICS, a także jak istotna jest potrzeba identyfikowania tych elementów, które są dołączane do sieci krytycznych. Oszustwa związane z phishingiem oceniono jako mniej istotne od innych zagrożeń OT / ICS, chociaż wciąż istnieją dowody (badania ataków ICS), że ta taktyka przestępców jest nadal preferowanym mechanizmem łamania początkowych zabezpieczeń, także w zakładach przemysłowych i przenikania do systemów sterowania w domenie OT. W 2017 r. oszustwa związane z wyłudzaniem informacji należały do pięciu najpopularniejszych kategorii, a dla 30% respondentów były jednym z najważniejszych zagrożeń. W 2019 r. już tylko mniej niż 25% respondentów wyraziło podobne obawy. W tej części badania wraca temat czynnika ludzkiego. Ponad 62% zagrożeń dla OT / ICS powiązanych jest z ludźmi. Dlatego spadek obaw o phishing w 2019 r. (czyli czynności mających na celu skłonienie pracowników do działań powodujących udzielenie atakującym dostępu do systemu) nie wydaje się racjonalnie uzasadniony.

Zdaniem badanych duże znaczenie mają zagrożenia zewnętrzne. Zagrożenia te mogą stwarzać incydenty w łańcuchu dostaw prowadzące do zakłóceń i efektu kaskadowego, wpływającego na pozostałych uczestników tego łańcucha dostaw, zależnych bezpośrednio lub pośrednio od produktów lub usług. Zdaniem SANS cyberprzestępczość w sektorze przemysłowym osiągnęła już znaczne rozmiary, co wynika częściowo z eksplozji Internetu Rzeczy oraz coraz większej liczby urządzeń podatnych na ataki. Dlatego zakłady przemysłowe muszą nadal koncentrować się na obronie przed rosnącym potencjałem ataku, w tym także ze strony podmiotów inspirowanych przez wrogie państwa, które prowadzić mogą do uszkodzeń lub zniszczenia systemów krytycznych dla zakładu i spowodować niedostępność usług dla społeczeństwa. Inni atakujący, ze świata przestępczego, starają się wyłudzać pieniądze, przejmując kontrolę nad systemami przemysłowymi, urządzeniami i krytycznymi informacjami. Dotyczy to zagrożenia określanego mianem ransomware, gdzie złośliwe oprogramowanie służy do szantażowania dużych zakładów przemysłowych. SANS zaleca, by przykładać większą rolę do świadomości pracowników OT w organizacjach, by grupa ta stała się gronem, do którego kierowane są kompleksowe kampanie uświadamiające w zakresie bezpieczeństwa i programy edukacyjne. Pozwoli to wzmocnić czujność i uodpornić organizację na niektóre zagrożenia.

Warto także zadać pytanie, czy rzeczywiście nastąpiła poprawa zabezpieczeń przemysłowych systemów sterowania i coraz bardziej konwergentnych sieci OT / IT oraz powiązanych z nimi urządzeń? Porównanie między 2017 r. a 2019 r. pokazuje, że chociaż sytuacja niekoniecznie jest lepsza, wydaje się, że trend zmierza

we właściwym kierunku – w kierunku dojrzewania organizacji do efektywnego wykrywania nowych i ewoluujących zagrożeń. Według respondentów badania z 2019 r. zgłaszających incydenty związane z ich systemami sterowania, w ciągu ostatnich 12 miesięcy ich liczba znacznie wzrosła (patrz rysunek 4). Przyczyny mogą wynikać ze zmian w statystykach, częstszego ich wykrywania, lepszego reagowania na incydenty oraz poprawniejszej kategoryzacji zdarzeń przez podmioty podejmujące działania.



Rys. 4. Liczba incydentów bezpieczeństwa.

Filozofia „Defense in Depth" to niejako zbiór dobrych praktyk i zasad określonych przez międzynarodowe stowarzyszenia, takie jak ISA (International Society of Automation) i bazuje na regulacjach – m.in. ISA-99 oraz IEC 62443, stanowiących wytyczne dla osób odpowiedzialnych za wdrożenie kwestii bezpieczeństwa w zarządzanych przez siebie obszarach. Metodyka „Defense in Depth" opiera się na 3 głównych zasadach i politykach bezpieczeństwa. Są to: ochrona zakładu, integralność sieci biurowej z siecią produkcyjną OT w aspektach stosowania segmentacji, wprowadzenie stref zdemilitaryzowanych i zabezpieczeń dostępu fizycznego do infrastruktury, a także powtarzający się proces aktualizacji oprogramowania samych elementów automatyki, w tym wiedzy i procedur reagowania zespołów obsługujących poszczególne działy.

W podejściu „Defense in Depth" znajdziemy zarówno aspekty związane z zagwarantowaniem ochrony fizycznej samego dostępu do zakładu oraz szaf sterowniczych, jak i procedury obejmujące osoby z obsługi. Koncepcja dostarcza także wytycznych, jak tworzyć bezpieczną infrastrukturę OT z zachowaniem ciągłości procesu i realizacją bezpiecznego zdalnego dostępu do elementów wykonawczych. W codziennej praktyce inne problemy napotyka oficer bezpieczeństwa danych, inne wymagania ma zespół IT, a jeszcze innych trudności z zagwarantowaniem bezpiecznej komunikacji doświadcza dział utrzymania ruchu i automatyki. Te wszystkie aspekty stanowią wykładnię dla wdrożenia rozwiązań wg. „Defense in Depth", którymi kieruje się Siemens.

RAFAŁ BIEŃ

SIEMENS POLSKA

Rośnie zagrożenie ze strony hackerów oraz błędów popełnianych przez podwykonawców zewnętrznych

Tabela 2 wskazuje autorów ataków, osoby przyczyniające się do naruszeń bezpieczeństwa, które były źródłami incydentów OT w 2017 i 2019 r. Podzielono ich na trzy szerokie kategorie: umyślnie złośliwi, nieumyślnie złośliwi oraz obydwie te grupy wraz z sytuacjami kiedy przyczyny są nieznane. Z badań wynika, że w 2019 r złośliwi hakerzy nadal byli wiodącymi autorami ataków, a liczba nieznanych źródeł spadła prawie o połowę. Wreszcie, niezamierzone szkodliwe działania dostawców usług, konsultantów i podwykonawców wzrosły ponad dwukrotnie.

	2017	2019
Incydenty zamierzone		
Hakerzy	**56,3%**	**44,8%**
Wrogie państwa lub podmioty sponsorowane przez te państwa	0,0%	27,6%
Przestępczość zorganizowana	**0,0%**	**24,1%**
Aktywiści, organizacje aktywistów, hakerzy	12,5%	17,2%
Konkurencja	**12,5%**	**10,3%**
Byli pracownicy	0,0%	10,3%
Byli dostawcy sprzętu	**0,0%**	**6,9%**
Incydenty zamierzone i niezamierzone / nieznane		
Obecni pracownicy	**31,3%**	**34,5%**
Nieznany (źródła nie zostały zidentyfikowane)	31,3%	17,2%
Incydenty niezamierzone		
Obecni usługodawcy, konsultanci, kontrahenci	**12,5%**	**31,0%**
Nieszkodliwi autorzy incydentów (wewnętrzni)		20,7%
Obecni dostawcy sprzętu	**18,8%**	**13,8%**
Służby wywiadowcze	0,0%	6,9%
Dostawcy lub partnerzy	**12,5%**	**6,9%**

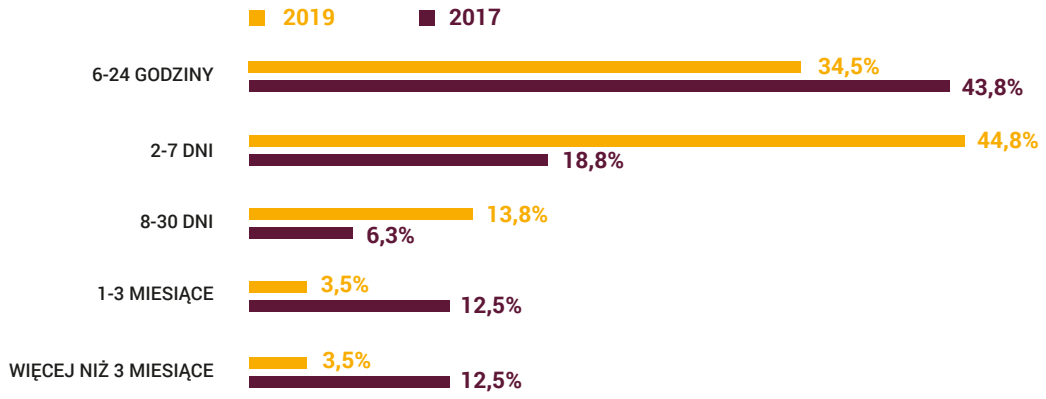
Tabela 2. Podmioty zaangażowane w incydenty w podziale na incydenty bezpieczeństwa zamierzone i przypadkowe.

Ustalenie źródła ataku jest często jednym z najtrudniejszych zadań w analizie incydentów. Najprawdopodobniej odpowiedzi respondentów to w rzeczywistości ich spekulacje co do faktycznej tożsamości źródła zagrożenia i niekoniecznie zawsze opierają się na bezpośrednich dowodach. Jednak są przesłanki ku temu, by stwierdzić, że wzrasta dojrzałość w wykrywaniu ataków na OT. Wzrost dojrzałości przejawia się m.in skróceniem okresu między incydentem a jego wykryciem (patrz – rysunek 4). Tabela 4 z kolei ilustruje początkowe wektory ataków wykonywanych w 2019 roku.

Dostęp fizyczny (pamięć USB, bezpośredni dostęp do sprzętu)	56,3%
Zdalny dostęp (z pominięciem docelowej architektury)	**40,6%**
Zaufany zdalny dostęp (poprzez docelową architekturę)	37,5%
Konserwacja i doradztwo serwisowe (zmiany konfiguracji)	**34,4%**
Łańcuch dostaw (tj. zmieniony / zmodyfikowany sprzęt lub oprogramowanie / aktualizacje oprogramowania i łatki; narzędzia / sprzęt do konserwacji)	18,8%

Tabela 4. Początkowe wektory ataku w 2019 r.

CZAS KTÓRY UPŁYNĄŁ OD MOMENTU ATAKU DO JEGO WYKRYCIA



Rysunek 4. Czas od ataku do jego wykrycia.

Spojrzenie na systemy OT / ICS z punktu widzenia ryzyka pomaga ustalić, co jest potrzebne do ich ochrony. Obszary o największym wpływie na bezpieczeństwo nie zawsze bezpośrednio wiążą się z obszarami o najwyższym ryzyku. Uważa się, że odporność na złamanie zabezpieczeń sieciowych i wbudowanych w systemy sterowania komponentów, chociaż często nie docenia się ich znaczenia, ma w rzeczywistości znaczny wpływ na bezpieczeństwo zakładów przemysłowych oraz integralność procesów.

	RYZYKO	WPŁYW
Połączenia z sieciami sterowania (systemy SCADA)	36,1%	34,1%
Wbudowane sterowniki lub komponenty (np. sterowniki PLC, IED)	**22,9%**	**33,2%**
Zasoby serwera związane z systemem operacyjnym (Windows, UNIX, Linux)	57,6%	32,7%
Połączenia z innymi systemami wewnętrznymi (sieci korporacyjne)	**42,0%**	**31,2%**
Urządzenia sieciowe (firewall, przełączniki, routery, gateway)	30,2%	30,2%
Stanowiska inżynierskie	**38,0%**	**29,3%**
Stacje robocze operatora	33,20%	28,80%
Protokoły komunikacyjne systemu sterowania	**23,90%**	**20,50%**
Aplikacja do sterowania procesami	16,10%	20,00%
Urządzenia terenowe (czujniki cyfrowe i siłowniki)	**19,50%**	**19,00%**
Urządzenia do zdalnego dostępu (VPN)	25,40%	18,50%
Systemy dostępu fizycznego	**22,40%**	**16,60%**
Urządzenia i protokoły komunikacji bezprzewodowej	27,80%	13,20%
Monitorowanie zakładu	**14,60%**	**13,20%**
Urządzenia mobilne (laptopy, tablety, smartfony)	36,10%	12,20%
Modemy analogowe	**12,20%**	**6,30%**
Inne	5,90%	2,00%

Tabela 5. Cechy systemów sterowania OT / ICS – ryzyko i wpływ

Podsumowanie

Rośnie znaczenie systemów do gromadzenia i analizy informacji. Podobnie wzrasta też rola urządzeń mobilnych, które zastępują tradycyjne komputery stacjonarne lub rozszerzają ich możliwości. Urządzenia mobilne, które często obecnie wyręczają w zadaniach inżynierskie stacje robocze, mają równoważne im prawa dostępu i możliwości wpływania na działanie ICS. Dlatego wpływ urządzeń mobilnych powinien być ściślej powiązany ze znaczeniem stacji roboczych, z którymi wiąże się ten sam wpływ na bezpieczeństwo i ryzyko. Urządzenia mobilne to nie jedyne ryzyko. Niekomórkowa komunikacja bezprzewodowa jest de facto metodą łączności z urządzeniami mobilnymi o coraz większym znaczeniu, dlatego należy zwrócić szczególną uwagę na bezpieczeństwo urządzeń w tej technologii. W przeszłości okazywało się, że wiele protokołów – w tym WPA, posiadało podatności i mogło być użyte do ataku na systemy OT/ICS. Biorąc pod uwagę, że oczekiwany okres użytkowania ICS jest mierzony w perspektywie aż dwóch dziesięcioleci, nieuniknione jest, że aktualnie wykorzystywany system może posiadać luki, które zostaną w przyszłości wykryte przez przestępców i jeżeli nie zostaną na czas załatane stanowić będą wektor ataku na całą infrastrukturę.

Aby poprawić poziom bezpieczeństwa organizacje muszą wiedzieć więcej o stanie swoich zasobów i infrastruktury. Jako drugą z najważniejszych inicjatyw w obszarze bezpieczeństwa ankietowani uznali audyt systemów sterowania i sieci. Audyt implikuje formalną procedurę, często przeprowadzaną przez niezależną trzecią stronę, która ocenia polityki i procesy pod kątem zgodności z wymaganiami, specyfikacjami, standardami i procesami.

O SANS

Instytut SANS jest organizacją badawczo-edukacyjną założoną w 1989 roku. Jej programy docierają obecnie do 165 000 specjalistów ds. bezpieczeństwa na całym świecie. Dzięki SANS szereg osób, od audytorów i administratorów sieci, po szefów ds. bezpieczeństwa informacji, dzieli się zdobytymi doświadczeniami i wspólnie znajduje rozwiązania dla stojących przed nimi wyzwań. O sile SANS decyduje liczne grono praktyków w obszarze bezpieczeństwa działających w różnych globalnych organizacjach, od korporacji po uniwersytety, pracujących razem, mających za zadanie nieść pomoc całej społeczności zajmującej się bezpieczeństwem informacji.

KONCEPCJA „GŁĘBOKIEGO BEZPIECZEŃSTWA” W PRZEMYŚLE

Koncepcja firmy Siemens – „Defense in Depth" oznacza ciągłą pracę nad zabezpieczeniami stacji roboczych, sterowników i innych dostarczanych przez firmę urządzeń. Firma przywiązuje szczególną wagę do standardów security i zgodności z obowiązującymi normami oraz przepisami. Stworzono m.in. centra bezpieczeństwa zajmujące się wyłącznie analizą podatności i cyberzagrożeń czyhających na zakłady przemysłowe. Produkty i komponenty firmowe oraz zewnętrzne są stale monitorowane pod kątem bezpieczeństwa.

Na całym świecie nieustannie trwają prace nad analizą problemów związanych z bezpieczeństwem. Zajmują się nimi CERT – zespoły reagowania na incydenty (ang. Computer Emergency Response Team). Pierwszy CERT utworzony został w listopadzie 1988 r. przez amerykańską agencję DARPA, po incydencie z robakiem Morrisa. Także Siemens otworzył własny ProductCERT. Do firmy spływają dane o incydentach dotyczących security z całego świata. Kluczem do efektywnej ochrony przed zagrożeniami jest jednak wymiana informacji, dlatego Siemens poważnie zaangażował się we współpracę z siecią CERT na całym świecie.

Wśród urządzeń dostarczanych przez Siemensa, które w szczególny sposób są zabezpieczane, wymienić należy te współpracujące z TIA Ethernet: S7-1500, 1505S, S7-300, CP343-1 i SCALANCE S. Oferują one zwiększoną dostępność, odporność na awarie i zdefiniowane zachowanie w przypadku ataku. W Siemensie dużą wagę przywiązuje się do potwierdzania standardów bezpieczeństwa projektowanych architektur i konstrukcji urządzeń poprzez ich certyfikację. Proces rozwoju produktów Siemensa posiada certyfikat "Secure Product Development Lifecycle" w oparciu o normę IEC 62443-4-1. Sterowniki S7-1500 oraz urządzenia SCALANCE XM408-8C posiadają certyfikat pierwszego poziomu CSPN – Certification de Sécurité de Premier Niveau. SIMATIC PCS 7 zgodny jest ze standardami IEC 62443-4-1 oraz IEC 62443-3-3 i posiada certyfikat TÜV SÜD.

Koncepcja bezpieczeństwa firmy Siemens – „Defense in Depth”

Ochrona zakładów przemysłowych, systemów, maszyn i sieci przed zagrożeniami cybernetycznymi wymaga wdrożenia i ciągłego doskonalenia holistycznej koncepcji bezpieczeństwa przemysłowego „Defense in Depth”. Produkty i rozwiązania Siemensa stanowią jeden z elementów tej koncepcji. Podlegają one ciągłemu rozwojowi, dzięki czemu ustawicznie poprawia się poziom ich bezpieczeństwa.

Siemens z uwagą analizuje ryzyka, oceniając je w kontekście stanu bezpieczeństwa środowiska produkcyjnego. Elementy portfela Assessment zaspokajają szereg potrzeb, od szybkiego przeglądu, po dokładną analizę i ocenę ryzyka oraz podatności – w tym gromadzenia danych z hali produkcyjnej. Ocena bezpieczeństwa przemysłowego została opracowana z myślą o klientach, którzy chcą szybko zapoznać się z bieżącym stanem bezpieczeństwa swojej infrastruktury. Proces składa się z jednodniowej analizy na miejscu, koordynowanej przez konsultanta ds. bezpieczeństwa, mającej na celu zidentyfikowanie i sklasyfikowanie luk w zabezpieczeniach i dostarczenie raportu zawierającego zalecenia dotyczące środków zmniejszających ryzyko. Podejście oparte jest na wiedzy eksperckiej Siemensa w zakresie systemów automatyki i dostosowane do najbardziej znanych międzynarodowych standardów bezpieczeństwa – IEC 62443, ISO 27001. Ocena opracowana jest na podstawie doświadczeń zdobytych podczas wdrażania programów security w wielu typach obiektów przemysłowych na całym świecie. Usługa dostępna jest zarówno dla systemów Siemens, jak i innych firm.

Dzięki Automation Firewall - NG dostępny jest kolejny poziom ochrony sieci produkcyjnych. Konstrukcja ta została zatwierdzona do użytku z systemami Siemens PCS7 i oparta na najnowocześniejszych rozwiązaniach Firewall Palo Alto Networks. Zapewnia ścisłą kontrolę pakietów ze wsparciem uczenia maszynowego w sieciach przemysłowych, umożliwiając ochronę zarówno przed znanymi, jak i jeszcze nieznanymi zagrożeniami. Rozwiązanie dostarcza poziom wysokiej dostępności (HA) zapobiegając awarii pojedynczego punktu w sieci. Skonfigurowanie dwóch urządzeń Firewall w parze wysokiej dostępności zapewnia nadmiarowość i w efekcie gwarantuje dostępność systemów produkcji.

Firma zdecydowanie zaleca stosowanie aktualizacji produktu, gdy tylko będą one dostępne i stosowanie najnowszych wersji software. Dotyczy to nie tylko produktów Siemensa, ale wszelkich używanych w zakładzie urządzeń, podzespołów i oprogramowania.

Informacje o luce w zabezpieczeniach

Obecnie producenci i dostawcy technologii stosują wiele różnych komponentów oprogramowania i starają się ustalić, czy pojawiające się luki w zabezpieczeniach mają wpływ na produkty automatyki. Aby być na bieżąco z ciągle zmieniającym się krajobrazem zagrożeń potrzebny jest system, który stale śledzi komunikaty o usterkach mających wpływ na wykorzystywane produkty i aktualizacje usuwające luki w zabezpieczeniach. Pomoc w radzeniu sobie z tym trudnym zadaniem oferuje aplikacja Siemens SVI (Security Vulnerability Information). SVI jest usługą w chmurze zapewniającą automatyczne generowanie cyfrowych biuletynów bezpieczeństwa związanych z lukami wpływającymi na spersonalizowaną listę komponentów ICS użytkownika. Biuletyn bezpieczeństwa zawiera takie informacje jak status poprawek w systemie użytkownika w czasie rzeczywistym i Common Vulnerability Scoring System (CVSS). CVSS to wynik liczbowy odzwierciedlający dotkliwość danej podatności. Prezentowany w CVSS wskaźnik można następnie przełożyć na reprezentację jakościową (niska, średnia, wysoka i krytyczna) pozwalającą przekazać organizacjom w syntetycznej formie ocenę, na ile groźna jest dana podatność. Informacje dotyczące bezpieczeństwa obejmują luki w systemie ochrony wpływające na komponenty innych firm, oprogramowanie Open Source (OS), oprogramowanie Commercial Off the Shelf (COTS), urządzenia sprzętowe, a także produkty Siemensa. W bazie danych znajduje się obecnie już ponad 30 000 komponentów i baza ta stale się powiększa.

Przemysłowe wykrywanie anomalii

Dzięki ofercie „Przemysłowe wykrywanie anomalii" (Industrial Anomaly Detection) firma Siemens oferuje najnowocześniejsze narzędzie bezpieczeństwa przeznaczone dla środowisk produkcyjnych. Proces analizy rozpoczyna się od fazy automatycznej identyfikacji zasobów i inwentaryzacji, po której następuje ustalenie oczekiwanego wzorca (lub linii bazowej) komunikacji w sieciach przemysłowych. Następnie narzędzie wyświetla przejrzysty przegląd monitorowanych systemów i automatycznie wykrywa nietypowe zdarzenia. Zapewnia to szybką identyfikację zmian w systemie, które mogą stanowić zagrożenie bezpieczeństwa lub mieć wpływ na dostępność systemów produkcyjnych. Przemysłowe wykrywanie anomalii opiera się na Mikroboksach PC Siemens (SIMATIC IPC427E) z odpowiednim fabrycznie zainstalowanym oprogramowaniem. Po pierwszym uruchomieniu komponent może być lokalnie skonfigurowany i administrowany przez WebGUI. Jest to system uczenia maszynowego, więc szybkość wykrywania anomalii będzie się z czasem zwiększać.

Współczesna infrastruktura przemysłowa staje się coraz bardziej skomplikowana, obsługiwana przez wiele podmiotów, połączona wzajemnie i zewnętrznie. Dlatego zarządzający zakładem przemysłowym powinni pozbyć się przekonania, że granica między strefą bezpieczną i niebezpieczną przebiega na fizycznym ogrodzeniu oddzielającym zakład od świata zewnętrznego, czy też firewallu na brzegu sieci zakładowej. Ta granica biegnie teraz często poprzez urządzenia i aplikacje. Praktyczne rozwiązania, mogące relatywnie szybko poprawić bezpieczeństwo w wielu przedsiębiorstwach, to zapanowanie nad bazą zainstalowanych urządzeń i ich oprogramowania oraz nieustanne podnoszenie świadomości pracowników i managerów w zakresie cyberbezpieczeństwa.

Siemens oferuje usługi polegające na ocenie stanu bezpieczeństwa w firmach przemysłowych. Ich celem jest pomoc przedsiębiorstwom w znalezieniu obszarów, w których występują ryzyka niepożądanych incydentów. Analiza pozwala także oszacować potencjalny wpływ wystąpienia takich incydentów na procesy i infrastrukturę przemysłową przedsiębiorstwa. W kolejnym kroku konsultanci mogą zaproponować rozwiązania, które w sposób optymalny kosztowo zmniejszą prawdopodobieństwo lub wpływ wystąpienia incydentów. Wybrane rozwiązanie pozwoli obniżyć ryzyka w obszarze cyberbezpieczeństwa, wspierając tym samym ochronę produktywności, redukując koszty i zapewniając zgodność z regulacjami. Szczególną uwagę zwracamy na podejście możliwie całościowe, warstwowe, zgodne z zasadami Siemensa „Defense in Depth" – najlepszymi praktykami wypracowanymi przez naszą firmę oraz w organizacjach międzynarodowych odpowiedzialnych za standardy, takie jak ISO 27001 czy ISO/IEC 62443.

WALDEMAR CHLEBIK

SIEMENS POLSKA

Podejście holistyczne (Holistic Security Concept) odpowiada na kluczowe pytania dotyczące bezpieczeństwa w biznesie

Co muszę chronić najbardziej w mojej branży?
Najważniejszym elementem tej koncepcji jest identyfikacja kluczowych aktywów biznesowych

Jakiego poziomu bezpieczeństwa potrzebuję?
Wymagania dotyczące poziomu bezpieczeństwa, zgodnie z IEC 62443 do ochrony przed atakami

Jak chronić określone zasoby?
Do ochrony i monitorowania zasobów krytycznych stosowane są rozwiązania oparte na standardach

Podejście holistyczne (Holistic Security Concept) Siemensa do kwestii bezpieczeństwa w przedsiębiorstwie

Schemat działań ochrony zasobów zakładu przed zagrożeniami. Według metody C62443/ISO27001

	DOSTĘP FIZYCZNY	ORGANIZACJA	PROJEKTOWANIE	POZIOM OPERACYJNY	ZARZĄDZANIE CYKLEM ŻYCIA
PL4	Drzwi obrotowe z czytnikiem kart i kodem PIN; Monitoring wideo i / lub skaner IRIS przy drzwiach	Podwójna weryfikacja przy działaniach krytycznych	Firewalls z funkcją Fail Close (np. zapora nowej generacji)	...	Weryfikacja funkcjonalności zabezpieczeń online
			...	Monitorowanie wszystkich działań urządzenia	...
+					
PL3	Drzwi obrotowe z czytnikiem kart	...	...	...	Zautomatyzowane tworzenie kopii zapasowych / odzyskiwanie
		Brak dostępu przez e-maila, www itp. Bezpieczna komórka	2 komputery (Secure Cell / outside)	...	
		Osoby odpowiedzialne za bezpieczeństwo w ramach własnej organizacji	Fizyczna segmentacja sieci lub równoważna (np. SCALANCE)	...	...
				Ciągłe monitorowanie (np. SIEM)	Weryfikacja kopii zapasowej
		...	...		Ograniczenie dostępu zdalnego (np. zasada połączenia)
+					
PL2	Drzwi z czytnikiem kart	Obowiązkowa edukacja w zakresie bezpieczeństwa			
+					
PL1	Zamknięty budynek / drzwi z kluczami	Treningi uświadamiające (np. szkolenie uświadamiające operatora)	Firewall do segmentacjj sieci (np. SCALANCE S)	...	System tworzenia kopii zapasowych / odzyskiwania
		Obowiązkowe zasady dotyczące pamięci USB (np. biała lista)	...	Bezpieczne logowanie we wszystkich systemach	

Wybrane środki bezpieczeństwa według podejścia Holistic Security Concept od PL 1 do PL 4. Poziomy ochrony (PL) wpływają na kluczowe funkcje i procesy bezpieczeństwa.

STUDIUM PRZYPADKÓW

Bezpieczna sieć w Constellation Brands

Constellation Brands, właściciel takich marek piwa jak Corona i Modelo zdecydował o wdrożeniu rozwiązań do zabezpieczenia i monitorowania sieci w zakładzie produkcyjnym browaru Nava w oparciu o rozwiązania Siemens SCALANCE.

Amerykański producent i dystrybutor alkoholu Constellation Brands jest właścicielem takich marek jak Corona Extra, Modelo Especial, Kim Crawford, Meiomi, The Prisoner, SVEDKA Vodka i High West Whisky. W 2013 r. firma z USA przejęła Modelo Brands wraz z browarem Nava.

Zakupiony przez Constellation Brands zakład miał zwiększyć swoje możliwości produkcyjne potrajając je w ciągu następnych 5 lat poprzez zwiększenie liczby linii pakowania oraz linii wytwórczych. Wszystkie istniejące w zakładzie elementy sieciowe automatyki postanowiono wesprzeć technologią Siemens SCALANCE. Aby zwiększyć bezpieczeństwo firma zdecydowała się na wdrożenie segmentacji sieci na wypadek awarii, która mogłaby unieruchomić nie tylko pojedynczą linię pakowania, ale wszystkie z nich i w efekcie wstrzymać całą produkcję. Inicjatywa wymagała wsparcia ze strony Siemensa we wdrożeniu rozwiązań obejmujących implementację urządzeń i zapewnienie wysokiej dostępności oraz wizualizacji i monitorowania sieci.

Problemów w realizacji tego zadania nastręczały wąskie ramy czasowe oraz braki w personelu inżynierskim w zakładzie, konieczność integracji nowych elementów z już istniejącymi przy jednoczesnych niedostatkach infrastruktury do monitorowania sieci. Z pomocą we wdrożeniu przyszedł Siemens oferując kompletne rozwiązanie oraz pomoc techniczną.

„Constellation Brands posiadał własny zespół ds. bezpieczeństwa IT, który korzystał ze wsparcia amerykańskiego Computer Emergency Response Team (CERT). Jednak w kwestiach bezpieczeństwa Operational Technology (OT) Constellation Brands zaufał w tym projekcie firmie Siemens" – twierdzi Maximilian Korff, Kierownik Produktu Cyberbezpieczeństwo i zdalny dostęp w Siemens AG.

Architektura systemu

W sieci, monitorowanych jest obecnie ponad 200 urządzeń. Siemens zastosował we wdrożeniu rozwiązanie zapewniające zdalny dostęp do hali produkcyjnej. Wdrożono także Siemens SINEMA Cloud, Remote Connect (SINEMA RC) oraz standaryzację komponentów Bill Of Materials (BOM). Po fazie realizacji przeprowadzono testy akceptacyjne Factory Acceptance Testing (FAT) i On-Site Acceptance Testing (SAT), jak również wykonano diagnostykę sieci PROFINET dla CPU-300 i ET200SP. Zrealizowano także kompletny audyt sieci przemysłowych.

W rozwiązaniu wykorzystano urządzenia z serii SCALANCE, SINEMA Server do monitorowania sieci oraz rozwiązania Simotion i Sinamics. Wizualizacja linii wykonana została z użyciem SIMATIC WinCC i PCS7. SCALANCE S pozwala użytkownikom dokładnie określać reguły zapory, co wyznacza obecnie ramy bezpieczeństwa sieci przemysłowej w zakładzie. Topologia sieci obejmuje łączność z przemysłowymi routerami Siemensa (SCALANCE XM408) połączonymi z zaporami przemysłowymi (firewall SCALANCE S615). Konfiguracja nosi nazwę „One Arm Mode", co oznacza, że cały ruch w sieci (wychodzące i przychodzące dane) odbywa się poprzez jeden interfejs. Stworzone rozwiązanie chroni przede wszystkim dostęp do urządzeń i danych produkcyjnych. Uprawnienia i dostęp do chmury prywatnej poszczególnym pracownikom i współpracownikom nadaje zespół Beer Operations Technology. Zespół ten tworzy nazwy użytkowników i nadaje hasła dla każdej osoby w prywatnej chmurze SINEMA RC.

Korzyści

Dzięki wdrożeniu rozwiązań zwiększających bezpieczeństwo w fabryce należącej do Constellation Brands udało się zyskać wgląd w stan sieci i objąć zakład stałym monitoringiem, co w efekcie podniosło stan bezpieczeństwa działania. Wyższa niezawodność sieci dzięki zwiększonej dostępności przekłada się także na niższe koszty funkcjonowania przedsiębiorstwa. Dane z diagnostyki sieci przesyłane są do serwera centralnego, co ułatwia zarządzanie nimi i zabezpiecza przed ich utratą. Zastosowane rozwiązanie umożliwia także łatwą integrację z nowymi liniami do pakowania.

Siemens zapewnia wsparcie techniczne zdalne i na miejscu, przeprowadzając m.in. zbiorcze i zaplanowane aktualizacje oprogramowania urządzeń. Część administracyjna rozwiązania zapewnia wykonywanie

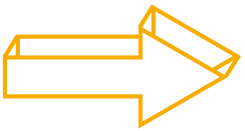
m.in. zadań tworzenia kopii zapasowych, aktualizacji oraz zmiany haseł. Oprogramowanie to odpowiada także za tworzenie raportów, monitoring błędów i wykrywanie nieprawidłowości w funkcjonowaniu sieci oraz jej pomiar utylizacji i siły sygnału WAN.

Zastosowane rozwiązanie przyjęte zostało przez globalnych producentów OEM współpracujących z browarem.

„Constellation Brands planuje w przyszłości rozszerzenie konfiguracji SINEMA Server. Chcemy rozbudować już istniejące rozwiązanie o SINEC NMS. Projekt migracji rozpoczął się już w lutym 2020 roku" – mówi Maximilian Korff.

Wykorzystane urządzenia, oprogramowanie i technologie

- **Przełączniki SCALANCE X200 (obecnie XC200)**
- **Przełączniki SCALANCE X307-3LD (obecnie XC216-4C)**
- **Routery SCALANCE XM408 (połączenie z IT)**
- **SINEMA Server v14.1 (monitoring sieci)**
- **PCS7 AS, S7 300/400, S7 1500, ET200SP, CP, HMI**
- **Simotion D445, Sinamics S120 i G120**
- **Sieć PROFINET**
- **Wizualizacja linii z użyciem SIMATIC WinCC, PCS7**



Producent profili aluminiowych Sapa w Rackwitz zwiększa wydajność i ochronę sieci przemysłowej

W zakładzie Sapa w Rackwitz wdrożono skalowalną i niezawodną technologię sieciową Siemensa. Dostosowane do potrzeb zakładu komponenty zapewniają wyższą wydajność sieci oraz skuteczną ochronę przed nieautoryzowanym dostępem.

Działający od 1958 r. zakład w Rackwitz pod Lipskiem w Niemczech należy do globalnej grupy Sapa. Fabryka Sapa Extrusion Deutschland GmbH produkuje wysokiej jakości profile aluminiowe przeznaczone do szerokiego zakresu zastosowań na dwóch w pełni zautomatyzowanych liniach prasowych. Od samego początku istnienia zakład polegał na technologii dostarczanej przez firmę Siemens.

Wyzwanie

W ramach procesu certyfikacji CE Sapa dokonano przeglądu infrastruktury w zakładzie. Z udziałem konsultantów Siemensa, wieloletniego dostawcy Sapa w dziedzinie technologii elektrycznej i automatyki, przeprowadzona została tak zwana szybka kontrola bezpieczeństwa. Zbadano dostępność całej sieci pod kątem oceny ryzyka awarii spowodowanych m.in. cyberatakami i ich wpływu na systemy produkcyjne. Analiza bezpieczeństwa ujawniła, że konieczna jest optymalizacja systemu ochrony poszczególnych elementów sieci, a także ochrona dostępu do przełączników, komputerów, kontrolerów i procesorów komunikacyjnych w fabryce. Istotne jest także zabezpieczenie komunikacji podczas pracy trzech wózków służących do transportu narzędzi prasowych i elementów poprodukcyjnych. W rezultacie opracowano środki

zapobiegawcze i praktyczne rozwiązania, a następnie rozpoczęto systematyczne ich wdrażanie.

Wdrożenie rozwiązania

Jednym z pierwszych podjętych działań było wdrożenie systemu zarządzania i diagnostyki sieci SINEMA Server firmy Siemens. Dzięki temu oprogramowaniu operator może szybko i wygodnie uzyskać wgląd w stan sieci przemysłowej i stale ją monitorować. System wyposażony jest w łatwy w użyciu interfejs użytkownika dostępny za pośrednictwem przeglądarki internetowej. Pozwala on automatycznie rozpoznawać komponenty sieciowe i automatycznie wizualizuje podwójnie przypisane adresy IP w sieci, co ułatwia zapobieganie konfliktom. System obrazuje aktualny stan urządzeń sieciowych, które można sortować według różnych kryteriów i pozwala na wykonywanie dostosowanych do potrzeb użytkownika raportów i analiz. Wyniki są wizualizowane także w panelu operatorskim HMI (Human Machine Interface). Wykonywanie raportów jest automatyczne i wysyłane pocztą elektroniczną do wybranych odbiorców, natomiast przypadki awarii są natychmiast zgłaszane przez SMS. Dzięki tym narzędziom sieć może zostać dostosowana do bieżących potrzeb i przeprojektowana w taki sposób, by spełniać oczekiwania zarówno specjalistów ds. produkcji, jak i IT w firmie.

W wyniku monitorowania sieci za pomocą SINEMA Server udało się stworzyć wydajny i niezawodny szkielet produkcyjny oparty na modułowych przełącznikach Ethernet SCALANCE XR324-12M. Przełączniki Ethernet SCALANCE XR-300, dostarczane także przez Siemensa zapewniają rozszerzone funkcje IT.

„Wybraliśmy przełączniki stelażowe, ponieważ pasują one do istniejących szaf 19" i urządzenia te można łatwo zintegrować z siecią za pomocą szerokiej gamy różnych rodzajów nośników optycznych i elektrycznych" – mówi Andreas Steinberg, odpowiedzialny za utrzymanie i automatyzację technologii środowiska produkcyjnego w Sapa.

Przełączniki firmy Siemens wykorzystują funkcję C-PLUG, pozwalającą zapisać na nośniku konfigurację urządzenia. Dzięki temu dane o parametrach danego urządzenia w sieci można szybko przenieść do urządzenia zapasowego.

Korzyści: bezpieczeństwo i wysoka wydajność sieci

Moduły SCALANCE S wyposażone zostały w zintegrowaną zaporę ogniową (firewall) zapewniającą separację systemów produkcyjnych, w szczególności od zewnętrznej sieci WWW. System gwarantuje, że jedynie autoryzowani użytkownicy mają dostęp do komponentów sieci produkcyjnej. Standardem jest również chroniony zdalny dostęp personelu wykonującego czynności konserwacyjne, który odbywa

się za pośrednictwem tunelowania VPN (Virtual Private Network) umożliwiając im szybką interwencję w przypadku awarii. Sieci: korporacyjna i produkcyjna są od siebie całkowicie odseparowane. Awaria w sieci korporacyjnej powoduje, że protokół RST (Rapid Spanning Tree) automatycznie trasuje sieć produkcyjną. Dzięki temu ataki na sieć korporacyjną i jej awarie nie wpływają na bezpieczeństwo produkcji.

„W sieci dozwolone są tylko wybrane protokoły komunikacyjne i mają do niej dostęp tylko wybrani użytkownicy. Prawa dostępu zredukowano do niezbędnego, bezpiecznego poziomu, który został wdrożony dzięki technologii sieciowej Siemensa" – wyjaśnia Karsten Konschak, szef działu IT w firmie Sapa.

Z systemem komunikacji zintegrowane zostało także napowietrzne rozwiązanie jednoszynowe do transportu narzędzi prasowych. Rozwiązanie realizowane przy pomocy komponentów Siemens i SCALANCE IWLAN umożliwia bezawaryjną komunikację za pośrednictwem dedykowanej sieci przemysłowej PROFINET / PROFIsafe, a tym samym bezpieczną obsługę w każdych okolicznościach.

W porównaniu do zastosowań biurowych, w przypadku produkcji oczekuje się od technologii sieciowych znacznie wyższej wydajności, niezawodności i dostępności.

„Niezawodność komunikacji jest teraz ważniejsza niż kiedykolwiek wcześniej, ponieważ wytwarzanie jest ściśle zorientowane na zamówienia realizowane w krótszych seriach, co powoduje częstsze zmiany produkcji i znacznie większą wymianę danych" – stwierdza Andreas Steinberg.

Postępująca wymiana komponentów PROFIBUS na PROFINET nieuchronnie zwiększy liczbę urządzeń sieciowych w zakładzie. W tych warunkach zarządzanie siecią staje się zatem niezbędne, co jest możliwe dzięki wdrożonym w Sapa w Rackwitz komponentom firmy Siemens. Zarówno IWLAN, jak i SINEMA Server wyróżniają się wydajnością, dostępnością i łatwością obsługi. W oparciu o te komponenty planowane są w zakładzie kolejne projekty modernizacyjne i integracyjne.

OCENA CYBERBEZPIE-CZEŃSTWA

Przed przystąpieniem do działań mających na celu utwardzanie systemów bezpieczeństwa, łatanie wszelkich możliwych luk – zarówno informatycznych jak i proceduralnych – konieczne jest wykonanie audytu lub oceny bezpieczeństwa. Ocena wykonywana jest w oparciu o standardy branżowe i normy, takie jak IEC 62443 i ISO 27001.

Ocena bezpieczeństwa cybernetycznego przedsiębiorstw przemysłowych obejmuje takie aspekty, jak: architektura sieci, przepływy danych, weryfikacja systemów i procesów produkcyjnych, a także wiedzy i podejścia do ochrony informacji przez pracowników. W większości przypadków przebiega to według podobnego planu, dlatego specjaliści Siemensa opracowali zarówno programy do pozyskiwania informacji, jak i kwestionariusze, które ułatwiają gromadzenie i przetwarzanie danych. Formularze wypełniane są wspólnie z menedżerami odpowiednich działów, takich jak produkcja, konserwacja, planowanie i bezpieczeństwo.

Wyniki przeprowadzonej oceny umożliwiają identyfikację tych obszarów, w których istnieje pilna potrzeba działania. Siemens opracowuje końcowy raport w oparciu o zebrane dane. Zawiera on konkretne propozycje i koncepcje, dostosowane do zadań analizowanych działów, mające na celu stopniową poprawę bezpieczeństwa przemysłowego.

Kontrola bezpieczeństwa przemysłowego

Ta metoda oceny opiera się na koncepcji głębokiej obrony (Defense in Depth) połączonej z najlepszymi praktykami i doświadczeniem w zakresie międzynarodowych standardów, takich jak IEC 62443 i ISO 27001.

Uwzględnia ona takie elementy jak:

- **Lista kontrolna (checklista) oparta na wywiadach pozwalających zidentyfikować i klasyfikować ryzyka**
- **Najlepsze praktyki oceny przemysłowej**
- **Zwięzły raport z zaleceniami dotyczącymi środków ograniczających ryzyko**

Ocena bezpieczeństwa według standardów IEC 62443

Norma IEC 62443 to wiodąca seria standardów bezpieczeństwa w środowisku automatyki. W dokumencie opisano ogólnie obowiązujące, uniwersalne rozwiązania przeznaczone do ochrony urządzeń produkcyjnych i systemów automatyki. **IEC 62443 zakłada:**

- **Ocenę stanu bezpieczeństwa opartą na wywiadach**
- **Stosowanie w przypadku całkowicie zautomatyzowanych systemów**
- **Stworzenie raportu z zaleceniami dotyczącymi eliminacji zidentyfikowanych luk w zabezpieczeniach**

Ocena bezpieczeństwa według normy ISO 27001

ISO 27001 jest wiodącym standardem obejmującym wymagania systemów zarządzania bezpieczeństwem informacji. **Zakłada on:**

- **Ocenę stanu bezpieczeństwa opartą na wywiadach zgodnie z wymaganiami ISO 27001**
- **Stosowanie w przypadku systemów automatyki opartych na całkowicie zintegrowanej automatyzacji (Totally Integrated Automation)**
- **Stworzenie raportu z zaleceniami dotyczącymi eliminacji zidentyfikowanych luk w zabezpieczeniach**

Oceny ryzyk i podatności

Podejście zakłada początkowy wybór zagrożeń, które mają podlegać ocenie. Następnie ma miejsce wyszukiwanie możliwych luk, klasyfikacja i ocena ryzyka.

Metoda ta zakłada:

- **Obsługiwane przez narzędzie pozyskiwanie i gromadzenie danych związanych z bezpieczeństwem systemów automatyki**
- **Klasyfikację i ocenę ryzyka zgodnie z systemem oceny podatności Common Vulnerability Scoring System (CVSS)**
- **Kompleksowy raport jako podstawę mapy drogowej bezpieczeństwa opartego na ocenie ryzyka**

Prowadzone przez Siemensa oceny stanu bezpieczeństwa zakładów produkcyjnych zwykle zaczynają się od spotkania organizacyjnego, po czym następuje realizacja oceny wspólnie z odpowiednimi przedstawicielami przedsiębiorstwa, zakończona sporządzeniem raportu i jego prezentacją. Sam proces sporządzania oceny rozpoczyna się od jednodniowej analizy dokonywanej przez Konsultanta Bezpieczeństwa, przeprowadzanej na miejscu przy użyciu kwestionariusza i metody klasyfikacji ryzyka. Zakończenie tego etapu finalizowane jest sporządzeniem raportu. W drugim kroku wykonywana jest dwudniowa ocena przeprowadzana na miejscu, oparta o normę ISO/IEC 62443 i koordynowana przez Konsultanta Bezpieczeństwa przy udziale Inżyniera Bezpieczeństwa. Kończy się ona około trzydziestostronicowym raportem opisującym ryzyka i rekomendowane środki zaradcze. Podobnie realizowana jest kolejna jednodniowa analiza, przeprowadzana w oparciu o normę ISO 27001. Kolejny etap to wielodniowa, całościowa i szczegółowa identyfikacja oraz ocena ryzyka przedsiębiorstwa i jego infrastruktury technicznej. Praca konsultantów Siemensa na tym etapie kończy się przygotowaniem około stustronicowego raportu, często będącego podstawą do wdrożenia lub uaktualnienia programu bezpieczeństwa. Wreszcie ostatnia faza to inwentaryzacja i skanowanie aktywne przy pomocy narzędzia SiESTA lub badanie pasywne podatności infrastruktury przemysłowej.

W realizacji często korzystamy ze wsparcia partnerów, takich jak firma ATOS, a także – w zależności od potrzeb – innych partnerów. Jesteśmy także pomysłodawcą inicjatywy „Charter of Trust" wypracowującej standardy bezpieczeństwa we współpracy z partnerami.

WALDEMAR CHLEBIK

SIEMENS POLSKA

OCENA BEZPIECZEŃSTWA W PRZEMYSŁOWEJ SIECI OT

Zasady cyberbezpieczeństwa w odniesieniu do przemysłowych systemów sterowania

Wizja Przemysłu 4.0 i Internetu Rzeczy (IoT) oznaczają dla świata przemysłu kolejny etap rozwoju interakcji między światem wirtualnym i fizycznym. Wiążący się z tym wzrost zagrożeń i wynikająca z nich konieczność poprawy zabezpieczeń w odniesieniu do przemysłowych systemów sterowania (ICS - Industrial Control Systems), w tym m.in. sterowników przemysłowych PLC i systemów SCADA (Supervisory Control And Data Acquisition) wymaga od przedsiębiorstw prewencyjnej i specyficznej dla branży strategii obrony.

Dzięki Siemens Industrial Security Services firmy przemysłowe mogą korzystać z wszechstronnego know-how, a także wiedzy technicznej globalnej sieci specjalistów w zakresie automatyzacji i cyberbezpieczeństwa. Całościowe podejście do koncepcji obrony opiera się na najnowocześniejszych technologiach, a także obowiązującym stanie prawnym i standardach w obszarze bezpieczeństwa. Dzięki szczegółowej analizie podatności i zastosowaniu właściwych, kompleksowych środków bezpieczeństwa zagrożenia i złośliwe oprogramowanie wykrywane są już na wczesnym etapie. Ciągły monitoring zapewnia przedsiębiorstwom stały wgląd w stan bezpieczeństwa ich zakładu przemysłowego i optymalną ochronę inwestycji.

Siemens, będąc globalnym dostawcą technologii i liderem także w kwestiach bezpieczeństwa zakładów przemysłowych, zapewnia kompleksowe doradztwo w obszarze planowania działań ochrony systemów przemysłowych.

Kompleksowa analiza zagrożeń i ryzyka

Doradztwo w zakresie bezpieczeństwa obejmuje całościową analizę zagrożeń i słabych punktów obrony przedsiębiorstwa, identyfikację zagrożeń i zalecenia odnośnie środków bezpieczeństwa pozwalających usuwać zidentyfikowane luki. **Zakres ten obejmuje:**

- **Analizę zagrożeń**
- **Identyfikację ryzyka**
- **Badanie i klasyfikację słabych punktów**
- **Doradztwo w zakresie bezpieczeństwa zgodnie z normami IEC 62443 i ISO 27001**
- **Inwentaryzację zasobów i wykrywanie podatności przez usługi skanowania**
- **Zalecenie odpowiednich środków bezpieczeństwa**
- **Doradztwo w zakresie bezpieczeństwa sieci**

Środki bezpieczeństwa redukujące ryzyko

Konsultacje świadczone przez Siemensa dotyczące planowania bezpieczeństwa przemysłowego obejmują:

- **Wieloetapową redukcję ryzyka**
- **Szkolenie w zakresie bezpieczeństwa i świadomości**
- **Zgodność z normą IEC 62443**
- **Instalację ochrony antywirusowej, białej listy i zapór ogniowych (firewall)**

Optymalizacja bezpieczeństwa zapewniająca kompleksową ochronę

Siemens dostarcza rozwiązania, które pozwalają proaktywnie monitorować i łatać luki w ochronie systemów. Według koncepcji „Defense in Depth" Siemensa konieczna jest stała optymalizacja bezpieczeństwa oznaczająca ciągłe monitorowanie i odnawianie wdrożonych środków z zastosowaniem scentralizowanych usług:

- **Wsparcia za pośrednictwem kompetentnej sieci ekspertów ds. bezpieczeństwa Siemensa**
- **Monitorowania i aktualizacji środków bezpieczeństwa**
- **Stałego informowania o odkrytych lukach i statusie dostarczanych do nich „łat" za pośrednictwem narzędzia Industrial Vulnerability Manager**
- **Systemów wykrywania anomalii w działaniu procesów przemysłowych.**

Niezawodne wykrywanie zagrożeń w sieciach przemysłowych – detekcja anomalii

Wraz z postępem cyfryzacji zakłady przemysłowe i pracujące w nich urządzenia coraz intensywniej komunikują się wewnętrznie i z otoczeniem. Często jednak złożone sieci przemysłowe dostarczające usługi pierwszej potrzeby dla ludności, takie jak woda bieżąca, prąd i gaz do ogrzewania, są znacznie mniej chronione przed cyberatakami, niż systemy biurowe.

W większości przypadków za obronę przed złośliwym ruchem odpowiadają zapory ogniowe (firewall). Zapewniana jest także ochrona punktów końcowych w niektórych urządzeniach oraz dokonywana jest szczegółowa inspekcja pakietów przechodzących przez Gateway do sieci produkcyjnych i biurowych. W wielu przypadkach brakuje jednak kontroli stanu komunikacji w sterownikach PLC lub innych urządzeniach przemysłowych poprzez odniesienie go do pracy „normalnej", czyli takiej, w której przez sieć nie przechodzi komunikacja mogąca świadczyć o istnieniu zagrożenia. Dzięki kontroli anomalii wykrywanie złośliwego oprogramowania w sieci zakładu produkcyjnego jest dużo łatwiejsze.

Wykrywanie anomalii

Rozwiązanie do wykrywania anomalii w komunikacji urządzeń przemysłowych Siemensa – **Industrial Anomaly Detection** - można bezproblemowo zintegrować z sieciami przemysłowymi. Pozwala ono ustalić, które zasoby należą do sieci, a także jak się ze sobą komunikują. Dzięki niemu pracownicy odpowiedzialni za bezpieczeństwo mogą łatwo wykryć i zbadać wszelkie odchylenia od normy w komunikacji w sieci przemysłowej. Proponowany przez Siemensa sprzęt wraz z oprogramowaniem obsługuje urządzenia wielu producentów i większość używanych obecnie w zakładach protokołów komunikacji. Software posiada funkcje uczenia maszynowego, co usprawnia konfigurowanie i korzystanie z Industrial Anomaly Detection.

w zakładach przemysłowych – **Industrial Anomaly Detection** – wykorzystuje machine learning, co umożliwia konfigurację systemu samouczącego się. Oprogramowanie automatycznie analizuje ruch danych w sieci podczas fazy uczenia, dzięki czemu może później wykrywać anomalie. Każde podejrzane zjawisko (nietypowy ruch) wykryte w sieci może oznaczać na przykład penetrację zakładu przez hakera lub kradzież danych. Anomalie mogą przypominać zmiany w konfiguracji sprzętu lub aktualizację oprogramowania, ale system za każdym razem ostrzega o nim personel techniczny. Reaguje zawsze, gdy wykryte zostanie odchylenie ruchu sieciowego od wzorca. Ma to szczególne znaczenie w farmacji, branży motoryzacyjnej, lotniczej, chemicznej, a także w przemyśle spożywczym.

Architektura rozwiązania

Obecne w zakładzie przemysłowym przełączniki łączą poszczególne systemy znajdujące się w topologii sieci. Topologia ta ma zwykle kształt pierścienia lub gwiazdy. Przełączniki umożliwiają także odwzorowanie całego ruchu danych przez tak zwany port SPAN, w którym czujniki anomalii zbierają dane i umożliwiają bieżącą ocenę i detekcję nieprawidłowości. Oprogramowanie jest zwykle instalowane na komputerze przemysłowym (IPC) firmy Siemens. Można je również łatwo zainstalować na innych platformach przemysłowych, takich jak IOT 2040 lub Ruggedcom RX1500. Wykrywanie anomalii

Usługa instalacji

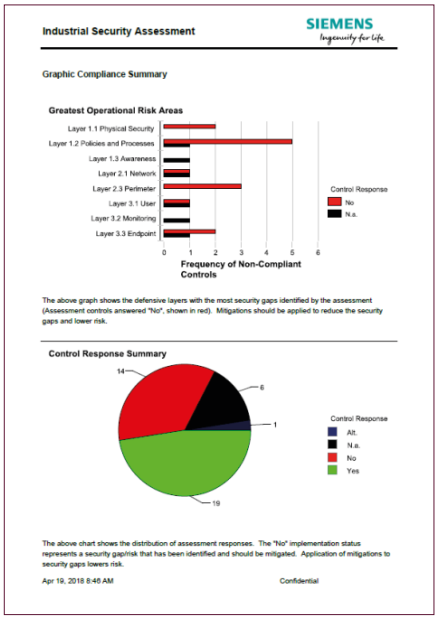
Dzięki przemysłowemu wykrywaniu anomalii Siemens zapewnia również usługę wspierającą płynną integrację produktu z infrastrukturą zakładu. Oferta ta obejmuje planowanie, wdrożenie i uruchomienie wykrywania anomalii w zakładach przemysłowych. Eksperci, którzy wykonują instalację rozpoczynają od planowania, poprzez wdrożenie, a kończą na szkoleniu zapoznającym pracowników z narzędziem.

Praktyczna ocena bezpieczeństwa w przemysłowej sieci OT

Na poziom zabezpieczeń zakładu przemysłowego wpływa nie tyle liczba utworzonych dokumentów na ten temat, co konkretne działania podejmowane przez specjalistów ds. bezpieczeństwa w przedsiębiorstwie. W tej części dokumentu przedstawiamy kilka usług dostępnych na rynku i świadczonych przez Siemensa, pozwalających przedsiębiorstwu przemysłowemu ocenić bezpieczeństwo posiadanej sieci przemysłowej i pomagających podjąć działania zwiększające poziom ochrony.

Industrial Security Assessment

Ocena bezpieczeństwa pozwala zidentyfikować luki w zabezpieczeniach i pomaga określić środki mające na celu ograniczenie ryzyka. Ocena oparta jest na standardach IEC 62443 i na koncepcji Defense in Depth Siemensa. Obejmuje ona identyfikację i łatanie bieżących luk bezpieczeństwa na podstawie dokonywanej oceny. Przygotowana przez Siemensa usługa zawiera analizę zarówno systemów i urządzeń dostarczanych przez tego producenta, jak i innych dostawców. Weryfikacja stanu obrony przed atakami odbywa się na miejscu u klienta i wykonywana jest przez Konsultanta ds. Bezpieczeństwa. Metodyka opiera się na przejściu przez listę kontrolną (checklistę) zawartą w specjalnie przygotowanym do tego celu kwestionariuszu. Pozwala ona zidentyfikować i sklasyfikować istniejące ryzyka. W efekcie klient otrzymuje zwięzły raport zawierający zalecenia dotyczące środków ograniczających ryzyko.



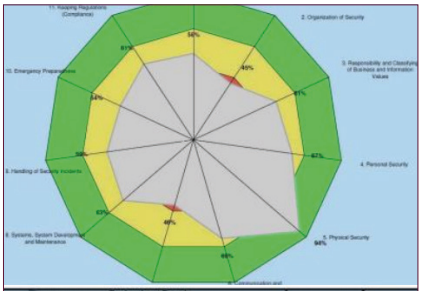
Fragment dokumentu Industrial Security Assessment

Ocena IEC 62443

Usługa pozwala odnaleźć luki w zabezpieczeniach i określać środki ograniczające ryzyko. Wykonywana przez specjalistów Siemensa ocena zgodna jest z wytycznymi zawartymi w międzynarodowej normie IEC 62443. Działania konsultantów koncentrują się na częściach: 2-1 dokumentu „Uruchomienie programu bezpieczeństwa automatyki przemysłowej i sterowania" oraz 3-3 „Bezpieczeństwo pomiarów i kontroli procesów przemysłowych – sieć i system bezpieczeństwa". Usługa ta obejmuje zarówno systemy Siemensa jak i innych firm. Konsultant ds. Bezpieczeństwa i Inżynier Bezpieczeństwa Siemensa pracują 2 dni w zakładzie klienta, wypełniając wspólnie z nim listę kontrolną opartą na kwestionariuszu pozwalającym identyfikować i klasyfikować ryzyka. W efekcie powstaje około trzydziestostronicowy raport zawierający zalecenia dotyczące środków zmniejszających ryzyko w zakładzie przemysłowym.

Ocena bezpieczeństwa zakładu zgodnie z międzynarodową normą ISO 27001

Usługa obejmuje jednodniowe warsztaty na miejscu z klientem umożliwiające identyfikację i klasyfikację ryzyka. Zajęcia prowadzone są przez Konsultanta ds. Bezpieczeństwa i Inżyniera Bezpieczeństwa. Ta forma szkolenia i konsultacji kierowana jest przede wszystkim do managementu oraz personelu odpowiadającego za produkcję, bezpieczeństwo IT, bezpieczeństwo fizyczne, konserwację oraz do inżynierów. Ocena wyników zajęć warsztatowych i ich podsumowanie następują off-line i udostępniane są w formie około 30 stron raportu zawierającego analizy, zalecenia dotyczące środków zmniejszających ryzyko i priorytetów działań powstałych na podstawie wyników scenariusza kosztów / korzyści.



	Security Areas	Evaluation / Result	Need for Action	Remarks (Priority)
Management	1. Instructions and Regulations		58%	1,0
	2. Organization of Security		45%	1,0
	3. Responsibility and Classifying of Business and Information Values		61%	1,0
	4. Personal Security		67%	0,9
Technique and Operation	5. Physical Security		94%	1,0
	6. Communication and Operational Security		69%	0,9
	7. System Access Monitoring		46%	0,9
	8. Systems, System Development and Maintenance		63%	0,9
	9. Handling of Security Incidents		59%	0,9
	10. Emergency Preparedness		54%	0,9
	11. Keeping Regulations (Compliance)		61%	1,0

Fragment dokumentu oceny bezpieczeństwa zakładu zgodnie z międzynarodową normą ISO 27001

Klasyfikacja i ocena ryzyka w programie bezpieczeństwa opartego na ryzyku – Risk & Vulnerability Assessment Identify

W tym przypadku dokonywana jest bardzo szczegółowa analiza, a raport końcowy liczy około 100 stron. Zawiera on takie elementy jak: dokumentacja projektu, opis zakresu, aktualna topologia sieci i architektura systemu, analiza ryzyka i metodologia punktacji, wnioski, wyniki analizy topologii sieci, rezultaty analizy Installed Base, ocena wyników krytycznych dla systemu (prawdopodobieństwo i wpływ na działalność zakładu), klasyfikacja ryzyka i poziom ryzyka, w tym punktacja (scoring), analiza potrzeb szkoleniowych oraz środki ograniczające ryzyko do każdego z wniosków. Powstaje także prezentacja dla zarządu jako pierwszy krok do ustalenia mapy drogowej bezpieczeństwa.

Vulnerability	Risk score
Flat network architecture/ No DMZ available	x.x
Flat network architecture/ No network segmentation	x.x
Unsecure/ Not controlled remote activities	x.x
No system hardening/Unneeded applications and services installed	x.x
Unpatched operating system	x.x
Obsolete Antivirus database	x.x
Windows firewall not active	x.x
Uncontrolled USB interfaces	x.x

Red (7.5 – 10) = Unaccaptable risk; Urgent action is necessary
Orange (5 – 7.5) = Unaccaptable risk; Acrtion is required
Yellow (2.5 – 5) = Accaptable risk; Subject to management approval
Green (0 – 2.5) = Accaptable risk; No action required

Risk & Vulnerability Assessment

W obszarze cyberbezpieczeństwa należy na każdy zakład spojrzeć globalnie: od fizycznego dostępu do zakładu po szyfrowanie danych na stacjach PC, przesyłanie tych danych, potencjalną pracę w chmurze, a kończąc na zabezpieczeniu poszczególnych bloków programowych w stacjach dyskretnych. Ponieważ najczęstsze w mojej pracy zawodowej są rozwiązania klasycznej automatyki przemysłowej bazujące na stacjach PLC oraz komunikacji w standardzie Ethernet i tworzenie sieci szkieletowych na potrzeby infrastruktury OT uważam, że w obecnym czasie głównym wyzwaniem dla osób zarządzających systemami automatyki jest realizacja bezpiecznego, zdalnego dostępu serwisowego i diagnostycznego. W tym przypadku niezbędne jest wdrożenie szeregu rozwiązań programowych typu Sinema Server, a także routerów typu Scalance S i M, które (poza opcją tzw. teleserwisu) pozwalają na ciągły monitoring ruchu w sieci zakładowej i urządzeń wykonawczych. Są to elementy kluczowe dla ciągłego procesu, a w przypadku potencjalnej awarii minimalizują czas reakcji odpowiednich służb.

Zachowanie ciągłości procesu i skrócenie do minimum potencjalnych czasów przestojów linii produkcyjnych jest dla przemysłu warunkiem koniecznym. Niejako „spycha" na dalszy plan potencjalne migrację i upgrade systemów wymagające od zakładu zatrzymania produkcji i przestoju parku maszynowego. Stosowana w przypadku klasycznych systemów IT tego typu metodyka jest naturalnym zjawiskiem polegającym na zatrzymaniu działania systemu i szybkiej aktualizacji oprogramowania, stąd też systemy IT wykazują większą odporność na potencjalne ataki w porównaniu do sieci produkcyjnych OT. W przypadku zakładów przemysłowych niestety takie działania niejednokrotnie są niemożliwe do zrealizowania, choćby ze względu na specyfikę procesów technologicznych, których nie da się łatwo zatrzymać. Siemens ze swoim systemowym podejściem daje gwarancję zachowania ciągłości procesu produkcyjnego i co ważne dla użytko-

wania końcowego – pozwala przewidywać poszczególne etapy implementacji wdrażania cyberbezpieczeństwa. Zgodnie z „Defense in Depth" wspieramy użytkownika na etapie przygotowania przez nasze służby audytu samej infrastruktury, oceny ryzyka zagrożeń i bezpieczeństwa, gdzie efektem jest raport końcowy i koncepcja wdrożenia zasad związanych z cyberbezpieczeństwem. Taka procedura w myśl „Defense in Depth" dotyczy każdego aspektu przedsiębiorstwa, linii produkcyjnej, infrastruktury IT/OT, standardów komunikacji do poziomu poszczególnych stacji PLC. Siemens przejmuje rolę „mediatora" pomiędzy „światem IT/OT". Wieloletnie doświadczenie w zakresie systemów przemysłowych ICS/SCADA, wsparcie produktowe praktycznie wszystkich obecnie oferowanych protokołów i standardów komunikacyjnych gwarantują stabilną platformę sprzętową. Dajemy możliwość stworzenia infrastruktury szkieletowej i segmentację sieci, co zabezpiecza dostęp do stacji PLC. Wykorzystujemy zapory ogniowe (firewall Scalance S), które realizują zdalny dostęp niezależnie od medium komunikacyjnego. Niemniej jednak, te procesy nie miałyby sensu, gdyby zostały pozbawione systemu typu SIEM (Security Information and Event Management), którego zadaniem jest ciągłe monitorowanie i wykrywanie anomalii w infrastrukturze zakładowej i natychmiastowa reakcja na niepożądane zachowanie na poziomie generowanych błędów, wystąpienia „obcych" pakietów danych. Konieczna jest także weryfikacja aktualizacji oprogramowania.

RAFAŁ BIEŃ

SIEMENS POLSKA

Zespół reagowania kryzysowego Siemens ProductCERT

CERT to jednostka skupiająca zespół ekspertów, których celem jest niesienie natychmiastowej pomocy, reagowanie na aktualne zagrożenia w obszarze bezpieczeństwa i rozwiązywanie problemów.

ProductCERT składa się z doświadczonych ekspertów zarządzających komunikacją wewnętrzną Siemensa w obszarze cyberbezpieczeństwa i obsługą zgłaszanych problemów dotyczących produktów, rozwiązań i usług firmy. ProductCERT stawia na wiarygodne relacje z podmiotami zajmującymi się ochroną systemów i ekspertami ds. bezpieczeństwa na całym świecie. Celem tej współpracy jest poprawa produktów Siemensa w zakresie szeroko rozumianego security, umożliwiająca wsparcie i rozwój najlepszych praktyk branżowych, a co najważniejsze – pomoc klientom Siemensa w zarządzaniu zagrożeniami.

ProductCERT jest odpowiedzialny za koordynację reakcji na incydenty związane z bezpieczeństwem cybernetycznym w firmie Siemens. Zespół pełni funkcję centralnego punktu kontaktowego dla ekspertów zajmujących się bezpieczeństwem, grup branżowych, organizacji rządowych i dostawców, którzy zgłaszają potencjalne luki w zabezpieczeniach produktów Siemensa. Koordynuje i utrzymuje komunikację ze wszystkimi zaangażowanymi stronami, zarówno wewnątrz organizacji, jak i z podmiotami zewnętrznymi. Dzięki pozyskiwanym informacjom reaguje na zidentyfikowane problemy bezpieczeństwa,

przekazując wszystkim potencjalnie zainteresowanym dane o podatnościach i problemach z ochroną danych przemysłowych.

Przekazywane przez ProductCERT komunikaty dotyczą bezpieczeństwa i mają na celu poinformowanie klientów o niezbędnych działaniach, które należy podjąć, by lepiej zabezpieczyć IT i OT, mając na uwadze nie tylko produkty i rozwiązania Siemensa, ale całą posiadaną infrastrukturę przemysłową. Jednostka monitoruje wszystkie znane obecnie zagrożenia zgodnie z koncepcją Cyber Threat Landscape for Siemens i ocenia ich potencjalny wpływ na przedsiębiorstwa. W oparciu o pozyskaną wiedzę i najnowsze trendy technologiczne ProductCERT konsultuje się z działem technologii informacyjnej w firmie Siemens w celu poprawy bezpieczeństwa IT. Realizując swoją misję, ProductCERT wykorzystuje relacje z wewnętrznymi i zewnętrznymi interesariuszami na całym świecie, takimi jak m.in. sieci CSIRT (Computer Security Incident Response Team) oraz innymi społecznościami zajmującymi się technologią i bezpieczeństwem. CERT Siemensa jest również uznawany za zaufanego partnera przez środowisko akademickie i przemysł, ma na koncie wiele projektów i publikacji eksperckich.

Siemens ProductCERT bada wszystkie zgłoszenia problemów związanych z bezpieczeństwem i publikuje porady dotyczące obszaru security pod kątem stwierdzonych luk w zabezpieczeniach. Mogą one dotyczyć bezpośrednio produktów Siemens wymagających zastosowania aktualizacji lub innych działań ze strony klienta. Siemens ProductCERT przekazuje także wszelkie informacje niezbędne do oceny wpływu luk w zabezpieczeniach na działanie systemów IT i OT.

KOMENTARZE EKSPERTÓW

ANDRZEJ ZIÓŁKOWSKI

PREZES URZĘDU DOZORU TECHNICZNEGO (UDT)

Każda nowoczesna i ważna organizacja narażona jest na szereg zagrożeń z zakresu cyberbezpieczeństwa. Od masowej, niechcianej komunikacji mailowej, przez skanowanie portów, po złośliwe oprogramowanie destabilizujące działanie organizacji. Nasze działania obejmują zarówno działania ukierunkowane na zewnątrz, jak i wewnątrz UDT. Wewnętrznie jako UDT staramy się minimalizować ryzyko dzisiejszych czasów, utrzymując aktualne wersje oprogramowania na wszystkich poziomach naszej infrastruktury. Modernizujemy także systemy zarządzania i ochrony naszego środowiska IT. Wprowadzamy zarówno oprogramowanie, które ogranicza potencjalny atak z zewnątrz, jak również wprowadzamy odpowiednie procedury ukierunkowane na nasze cyberbezpieczeństwo. Niestety najsłabszym ogniwem nierzadko jest człowiek. W naszych wewnętrznych systemach wykorzystujemy rozwiązania oparte o chmurę obliczeniową, gwarantującą elastyczność, ale także większą kontrolę i bezpieczeństwo danych.

Pracujemy z tymi, którzy mają doświadczenie, oferują nowoczesną i pewną technologię w tym zakresie. Na zewnątrz, dla naszych klientów uruchamiamy nową usługę związaną z audytami w zakresie cyberbezpieczeństwa. Audyt, pomimo że bazuje na uznanych standardach, to jednak ze względu na obszar cyberbezpieczeństwa przemysłowego opiera się na naszej wypracowanej metodologii.

Współpracujemy z innymi instytucjami w ramach członkostwa w Grupie Roboczej ds. cyberbezpieczeństwa przy Ministerstwie Cyfryzacji i NASK-PIB, gdzie uczestniczymy aktywnie w pracach Zespołu ds. certyfikacji w cyberbezpieczeństwie (CertiSecPL) oraz Zespołu ds. bezpieczeństwa Przemysłu 4.0. Nasza strategia dbania o bezpieczeństwo musi być wielowymiarowa i taką właśnie wielowymiarową strategię winny przyjąć polskie przedsiębiorstwa.

W myśl zapisów Ustawy o Krajowym Systemie Cyberbezpieczeństwa zakłady przemysłowe z sektora Energia - Operatorzy Usług Kluczowych, są odpowiedzialni za zapewnienie bezpieczeństwa świadczonych usług kluczowych oraz ciągłość ich świadczenia. W przypadku przemysłu procesowego zapewnienie bezpieczeństwa usługi kluczowej, a więc de facto procesu technologicznego oraz jego ciągłości, realizowanych za pomocą systemów automatyki przemysłowej, można osiągnąć tylko poprzez działania podnoszące poziom cyberbezpieczeństwa i jednocześnie bezpieczeństwa funkcjonalnego. Obszar cyberzagrożeń w przedsiębiorstwach przemysłowych dotyczy bowiem zarówno technologii informatycznych (IT), jak i operacyjnych (OT), odpowiedzialnych za fizyczne procesy przemysłowe. Nie sposób ograniczyć nasze działania tylko do układów zabezpieczających instalacje przemysłowe, abstrahując od sposobu sterowania tj. układów IT.

Naszym zdaniem pierwszym działaniem w kierunku ochrony systemów automatyki w obszarze OT powinien być audyt bezpieczeństwa określający poziom istniejących zabezpieczeń w organizacji, w takich obszarach jak np.: sprzęt, oprogramowanie czy zasoby ludzkie. Pomocną w tym zakresie jest analiza ryzyka i zagrożeń uwzględniająca podatności systemów automatyki. Prawidłowa ocena aktualnego stanu bezpieczeństwa IT/OT w firmie decyduje o kolejnych działaniach podnoszących jego poziom. Audyt poziomu zabezpieczeń tworzy podstawę do analizy całości zagadnień związanych z bezpieczeństwem, w tym także cyberbezpieczeństwa. W dzisiejszych czasach nikt nie może czuć się bezpieczny pod kątem potencjalnego cyberataku. Z tego też względu zwłaszcza w przemyśle do bezpieczeństwa trzeba podchodzić kompleksowo – holistycznie.

DR INŻ. WALDEMAR GRANISZEWSKI

ADIUNKT W INSTYTUCIE STEROWANIA I ELEKTRONIKI PRZEMYSŁOWEJ, WYDZIAŁ ELEKTRYCZNY, POLITECHNIKA WARSZAWSKA

Określenie ICS (ang. Industrial Control Systems) tak naprawdę jest pewnym skrótem szerszego pojęcia IACS (ang. Industrial Automation and Control Systems), które zostało zaproponowane w standardzie ISA-99/IEC 62443. Biorąc pod uwagę formalną definicję IACS: „a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process", mamy tu do czynienia ze złożonym zagadnieniem, zwłaszcza, że kluczowym wymogiem jest zapewnienie bezpieczeństwa osób i obiektów (ang. safety).

Zalecenia odnośnie cyberbezpieczeństwa systemów ICS / OT wynikają z :

- odpowiednich norm, np. ISA-99/IEC 62443 (wyżej wymienionej), czy też ISA84/IEC 61511;
- norm międzynarodowych dot. systemów zarządzania, np. ISO 22301, ISO 27001;
- innych norm branżowych;
- obowiązujących aktów prawnych;
- dobrych praktyk.

Systemy teleinformatyczne wspomagające funkcjonowanie przemysłu wytwórczego w zakresie ICT nie różnią się znacząco od systemów funkcjonujących w innych branżach. Dużym wyzwaniem jest jednak specyfika systemów ICS/OT. Stąd ważne jest holistyczne podejście do tematu, jak i korzystanie ze sprawdzonych modeli.

Tak jak w przypadku zagadnień ICT, wykorzystywany jest powszechnie model stosu protokołów TCP/IP, czy też ISO/OSI, czy też model warstwowy, tak w przypadku analizowania systemów ICS/OT dobrym modelem odniesienia jest zaproponowany przez prof. Theodore'a Joseph'a Williams'a model referencyjny Purdue (ang. The Purdue enterprise reference architecture). Model ten zakłada ścisłą segmentację poszczególnych systemów funkcjonujących w połączeniu z IT/OT dla przemysłu. W ostatnim okresie pojawiły się krytyczne głosy, że w związku z powszechnym zastosowaniem technologii IoT - Internetu Rzeczy (ang. Internet of Things) jak również IIoT - Przemysłowego Internetu Rzeczy (ang. Industrial Internet of Things) model stracił na aktualności. Jednak rozsądne podejście do projektowania i zarządzania systemami w branży przemysłowej powinno brać pod uwagę przede wszystkim kompleksowe zapewnienie cyberbezpieczeństwa dla całego procesu wytwarzania. Segmentacja i odpowiednia kontrola komunikacji w poszczególnych warstwach (tam gdzie jest to możliwe i nie zakłóci procesu), na styku warstw - w tym DMZ pomiędzy systemami IT a OT, jest jak najbardziej aktualna i zalecana.

Rekomendacje ISSA dla przedsiębiorstw wynikają bezpośrednio z obowiązujących aktów prawnych, m.in. w ramach Unii Europejskiej: „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" (Dyrektywa NIS), czy też „ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)".

W przypadku Polski kluczowym aktem prawnym jest „USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U. 2018 poz. 1560" (KSC) wraz z aktami wykonawczymi.

W przypadku dyrektywy NIS i odpowiednio KSC jednym z istotnych kroków, który powinien zostać przeprowadzony, jest szacowanie ryzyka i ocena jego wpływu na działanie organizacji. Jest to również jeden z kroków, który jest wymieniony w normie ISO 22301- System zarządzania ciągłością działania, jak i ISO 27001- System zarządzania bezpieczeństwem informacji. Audyty przeprowadzone zgodnie z ww. normami są jednym z elementów ciągłego iteracyjnego sposobu zarządzania ryzykiem w zakresie zapewnienia cyberbezpieczeństwa. Choć ustawa o KSC odnosi się do operatorów usług kluczowych, to wydaje się, że stosowanie podobnego podejścia do zarządzania ryzykiem przez pozostałe przedsiębiorstwa powinno skutkować znaczącym podniesieniem poziomu cyberbezpieczeństwa również w małych podmiotach.

Stosując analogię trwałości łańcucha dla elementów wchodzących w skład systemu IACS / ICS: cały system jest tak niezawodny jak poszczególne ogniwa tego łańcucha. Stąd też niezwykle ważne jest zastosowanie podejścia ochrony wielowarstwowej, która zapewni niezbędne zabezpieczenia dla najsłabszych ogniw, np. ochronę fizyczną i filtrowanie protokołów sieciowych do podatnych urządzeń, których z różnych powodów nie można zastąpić lub w inny sposób zabezpieczyć.

WOJCIECH WRZESIEŃ

HEAD OF PRODUCT MANAGEMENT TEAM, NASK S.A.

Cyberbezpieczeństwo, które jest jednym ze strategicznych obszarów działania NASK S.A., obejmuje również bezpieczeństwo sieci przemysłowych (OT). Korzystając z wieloletniego doświadczenia i współpracy z NASK Państwowym Instytutem Badawczym oraz NASK CSIRT, zapewniamy przedsiębiorstwom kompleksowe rozwiązania oparte na wielopoziomowym monitoringu, wykrywaniu i analizie incydentów. NASK S.A. Security Operations Center jest centrum kompetencyjnym zajmującym się analizą zdarzeń, detekcją zagrożeń i reagowaniem na wykryte incydenty. Częstotliwość ataków na sieci przemysłowe jest parametrem, który nieco paradoksalnie jest funkcją jakości systemu zabezpieczeń. Im większa świadomość zagrożeń, ich znajomość i wiedza o ewentualnych skutkach cyberataku, tym poważniejszy stosunek do konieczności zbudowania adekwatnej ochrony dla sieci przemysłowych.

Trudno jest też jednoznacznie ocenić, czy sektor przemysłowy jest częściej atakowany aniżeli inne dziedziny gospodarki, gdyż wymiana informacji w tym zakresie póki co nie ma charakteru powszechnego. Jedną z perspektyw, które można przyjąć jest ocena powyższego zagadnienia przez pryzmat rodzajów ataków. Z dostępnych danych wynika, że ataki masowe (np. phishing) są w podobnym stopniu udziałem szeroko rozumianego przemysłu, jak i innych branż ze względu na ich skalę, a nie konkretne cele ataku. Z drugiej strony ataki kierowane (targetowane) mogą mieć dużo groźniejsze konsekwencje. Informacje o atakach na np. infrastrukturę krytyczną bądź duże korporacje przemysłowe pochodzą wciąż raczej z poza granic Polski – w Polsce jest to ciągle swego rodzaju tabu.

Na podkreślenie zasługuje fakt, że przedsiębiorstwa coraz częściej są z mocy samych przepisów prawa obligowane do wdrożenia właściwych rozwiązań z zakresu cyberbezpieczeństwa, bowiem incydent, przed którym nie uda się uchronić może mieć krytyczny wpływ na wiele innych obszarów działania organizacji, w tym jej klientów oraz partnerów i kontrahentów. Ta świadomość daje wyobrażenie o skali „cyberskażenia" w obrębie całego teleinformatycznego ekosystemu naczyń połączonych.

Internet Rzeczy (Internet of Things, IoT) jest bez wątpienia furtką do tych części sieci, o których zdarza się zapominać zespołom odpowiedzialnym za infrastrukturę techniczną organizacji, a które przez brak właściwego monitoringu mogą stać się łatwym celem. Częstym problemem jest w ich przypadku brak wbudowanych mechanizmów ochrony, które są standardem w sieciach IT, takich jak zautomatyzowane – chronione aktualizacje, czy też kilkustopniowe uwierzytelnienia.

Do najczęstszych ataków dochodzi na skutek kilku rodzajów zaniedbań. Część zakładów przemysłowych jest podłączona do Internetu – co czyni je dostępnymi dla hakerów i złośliwego oprogramowania (malware) wykorzystującego luki i błędną konfigurację. W niektórych zakładach przemysłowych wciąż są stosowane systemy operacyjne, które nie są już wspierane przez producentów np. Windows XP. Przyczyną podatności na atak może być także stosowanie zbyt łagodniej polityki zmiany i używania haseł umożliwiających dostęp i przemieszczanie się w obrębie sieci OT, a także używanie nieszyfrowanych połączeń zezwalających na dostęp do sieci. Wciąż jeszcze wiele obiektów przemysłowych nie korzysta z systemów monitoringu – najważniejszych elementów infrastruktury, co także naraża je na ataki. Wreszcie, duża część zakładów ma co najmniej jedno nieznane lub obce urządzenie, które może być wyposażone w możliwość realizacji

połączeń bezprzewodowych, z których następuje atak. Jednymi z najtrudniejszych do opanowania i wykrycia są ataki typu ransomware i APT. W przypadku pierwszych motywacją są z reguły pieniądze, a zaszyfrowanie komponentów systemów klienta może skutecznie uniemożliwić sterowanie infrastrukturą przemysłową, powodując wymierne straty (por. atak na koncern NorskHydro w marcu 2019 r.). Drugi przywołany rodzaj ataku (APT) to przemyślany wielostopniowy atak, który może mieć wielowymiarowe przyczyny: okup, władza, przejęcie istotnego know-how. Jego wykrycie często zajmuje nawet do pół roku a skutki mogą być wielokierunkowe.

Z punktu widzenia NASK S.A. jest kilka elementów kluczowych dla możliwości realizacji skutecznych i efektywnych zabezpieczeń w organizacji.

Pierwszą, podstawową jest decyzja o zaplanowaniu, realizacji i wdrożeniu programów w obszarze bezpieczeństwa. Pierwszym aspektem takiej decyzji jest zaadresowanie obszaru proceduralno-prawnego, w tym stworzenie dokumentacji, np.: zgodnej z normami ISO 27001 i ISO 23001. Kluczową rolę w tym obszarze pełni również odpowiednia analiza ryzyka i jej projekcja w postaci Analizy Wpływu Biznesowego (BIA).

Drugim obszarem jest zaplanowanie narzędzi zarówno w postaci własnych systemów bezpieczeństwa. jak i usług zakupionych od zewnętrznych dostawców wraz z określeniem budżetu na ich realizację. Warto wspomnieć, że budżet powinien być zaplanowany w sposób skorelowany z uzgodnioną i przyjętą w organizacji analizą ryzyka.

Trzecim bardzo ważnym obszarem jest stałe podnoszenie świadomości i kwalifikacji pracowników. Ten etap to zarówno szkolenia specjalistyczne dla służb IT ale, co nie mniej ważne, także szkolenia dla wszystkich pracowników (w tym kadry zarządzającej) o tematyce bezpieczeństwa ogólnego związanego z pracą z użyciem komputerów i dostępem do sieci Internet (Security Awareness).

BIBLIOGRAFIA

1 Industry 4.0 Market by Technology (IoT, Artificial Intelligence, Industrial Metrology, Industrial Robotics, AR & VR, Blockchain, 3D Printing, Digital Twin, and 5G – Offering, Application, and End Users) and Geography-Global Forecast to 2024" https://www.marketsandmarkets.com/PressReleases/industry-4.asp

2 „2019 State of OT/ICS Cybersecurity Survey"

3 https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

4 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

5 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

6 https://threatpost.com/triton-ics-malware-second-victim/143658/

7 https://www.nytimes.com/2019/08/20/us/texas-ransomware.html

8 https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

9 https://www.reuters.com/article/us-mexico-pemex/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUSKBN1XM041

10 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

11 *Akamai* – duży, amerykański operator sieci dostarczania treści (CDN), zajmujący się także cyberbezpieczeństwem i świadczeniem usług w chmurze

12 https://www.akamai.com/us/en/products/security/calculate-the-cost-of-ddos-attacks.jsp

13 https://www.home.neustar/resources/tools/ddos-attack-cost-calculator

14 https://securelist.com/all/?category=911

15 https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

16 https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

17 https://www.pandasecurity.com/mediacenter/news/billion-consumers-data-breach-elasticsearch/

18 „Cyber Security for Critical Infrastructures" Siemens whitpaper https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/downloads/white-paper-infrastructures.html

19 https://teiss.co.uk/wp-content/uploads/2018/04/FINAL-FINAL-C739-Verizon-DBIR_2018-Main_report-180404-24-optimised.pdf

SIEMENS
Ingenuity for life

Ministerstwo
Cyfryzacji