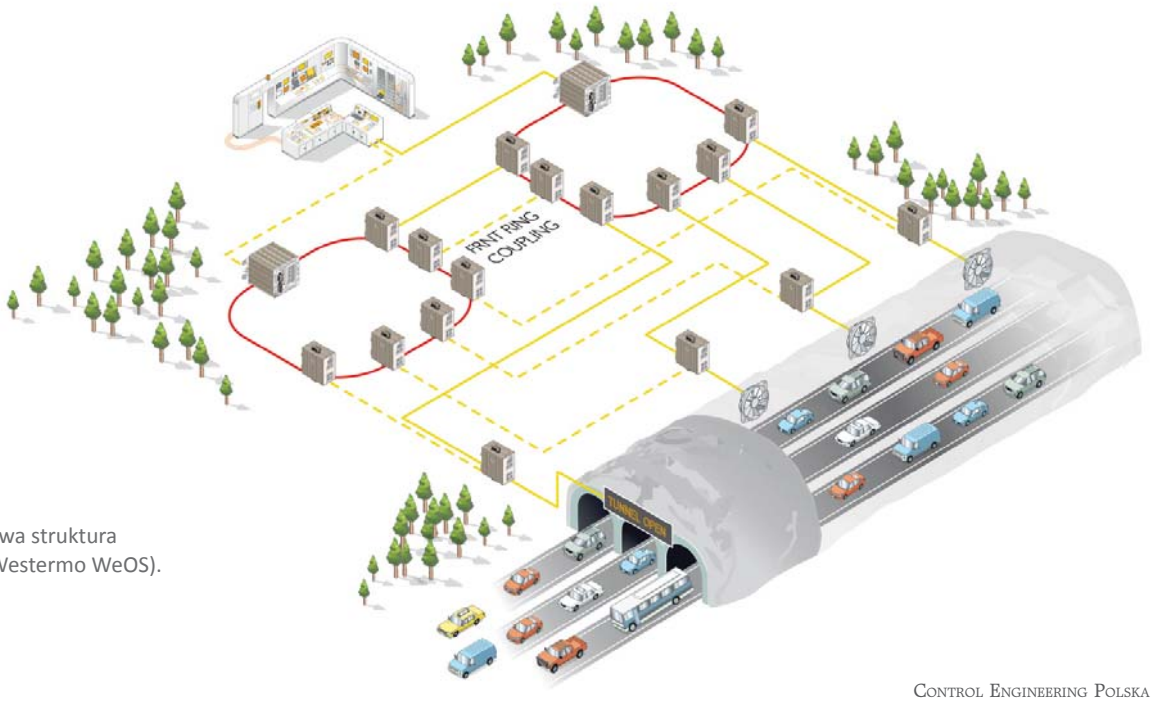
Cyberbezpieczeństwo przemysłowych systemów transmisji danych

W całym społeczeństwie oraz w społeczności branż przemysłowych rośnie świadomość zagrożeń atakami cybernetycznymi. Szczególnie narażone są krytyczne sektory, takie jak infrastruktura energetyczna, wodno-ściekowa, sektor finansowy czy też ochrony zdrowia i ubezpieczeń – ważne również dla bezpieczeństwa państwa. Wzrost tej świadomości ma pokrycie w tworzeniu lub modyfikacji odpowiednich regulacji prawnych, standardów technicznych oraz rozwoju technik zabezpieczeń. Również ryzyko związane z cyberbezpieczeństwem w systemach przemysłowych w końcu zostało dostrzeżone i potraktowane jako poważne. Wpisywane jest już na mapę kluczowych kwestii, istotnych do monitorowania przez zarządy firm.

Zuzanna Wieczorek
Kierownik działu technicznego
Tekniska Polska sp. z o.o.

Informacje związane z cyberbezpieczeństwem powinny trafiać do osób decyzyjnych, przede wszystkim odpowiedzialnych za finanse, informatykę, bezpieczeństwo, prywatność czy utrzymanie ruchu. Ważne są również szybkość i jakość reakcji na potencjalne zagrożenia i opracowanie w tym względzie odpowiedniej polityki. Porażające dane statystyczne mówią aż o kilkudziesięcioprocentowej stopie wzrostu wykrytych incydentów naruszenia bezpieczeństwa w ciągu ostatnich kilku lat! Jednocześnie ze statystyk tych wynika, że wydatki na jego zapew-



Ilustracja 1. Nadmiarowa struktura FRNT Ring Coupling (Westermo WeOS).

nienie stanowią średnio 4–6% budżetów przeznaczanych na informatykę. Określenie, czy jest to poziom wystarczający, musi być uzależnione od zidentyfikowania zagrożeń i ich potencjalnych konsekwencji biznesowych, politycznych oraz bezpośrednio związanych z bezpieczeństwem i zdrowiem ludzi.

Historia dość spektakularnych zdarzeń związanych z kształtowaniem świadomości cyberbezpieczeństwa w sektorze przemysłowym sięga przynajmniej 2007 r., kiedy to przeprowadzono eksperymentalny atak wykorzystujący lukę bezpieczeństwa w systemie SCADA, doprowadzając do autodestrukcji generatora energii. Kolejno następujące potem: kampania Stuxnet, NightDragon, ClearScada, ataki na sterowniki GE, Rockwell Automation, Schneider Electric, Koyo, Siemens, wirus Havex i kampania *cyber-espionage* (cyberszpiegowska) przeprowadzona przez grupę DragonFly, która dotknęła swoim zasięgiem infrastrukturę krytyczną kilkunastu Państw Azji, Ameryki i Europy (w tym także Polskę), aż po najświeższe doniesienia dotyczące dobrze zorganizowanych i przemyślanych ataków finansowanych przez państwa, które mają charakter destrukcyjny lub wyłącznie szpiegowski (i w związku z tym często pozostają niewykrywane) – ukierunkowane były na infrastruktury krytyczne i systemy przemysłowe.

W zeszłym roku miało miejsce bezprecedensowe oficjalne oskarżenie wystosowane przez amerykańskie ministerstwo sprawiedliwości (DOJ) w stosunku do chińskich hakerów, oskarżonych o cyberszpiegostwo gospodarcze. Wykryta została również kampania szpiegowska skierowana przeciwko dużym firmom z sektora energetycznego, m.in. polskim, a finansowana prawdopodobnie przez rząd rosyjski.

Zagrożenia dla przemysłu

Infrastruktura przemysłowych systemów sterowania (ICS – ang. *Industrial Control Systems*) praktycznie na każdym poziomie diametralnie różni się od typowych sieci teleinformatycznych i w związku z tym wymaga odmiennego podejścia do kwestii bezpieczeństwa komunikacji i samych treści danych. Inne są przede wszystkim priorytety w podejściu do zarządzania bezpieczeństwem i ryzykiem. Dla systemów przemysłowych będą to kolejno: dostępność i ciągłość działania, stabilność, integralność, poufność.

Systemy przemysłowe są stosunkowo łatwym celem, ponieważ przez wiele lat funkcjonowało przekonanie, że ich względna izolacja oraz nietypowe protokoły komunikacyjne stanowią same w sobie barierę ochronną. W konsekwencji systemy te mają niski poziom zabezpieczeń.

Ilustracja 2. Switch warstwy 3 z funkcją distributed micro-firewall, serwerem portów szeregowych. Westermo Lynx208-F2G-S2.

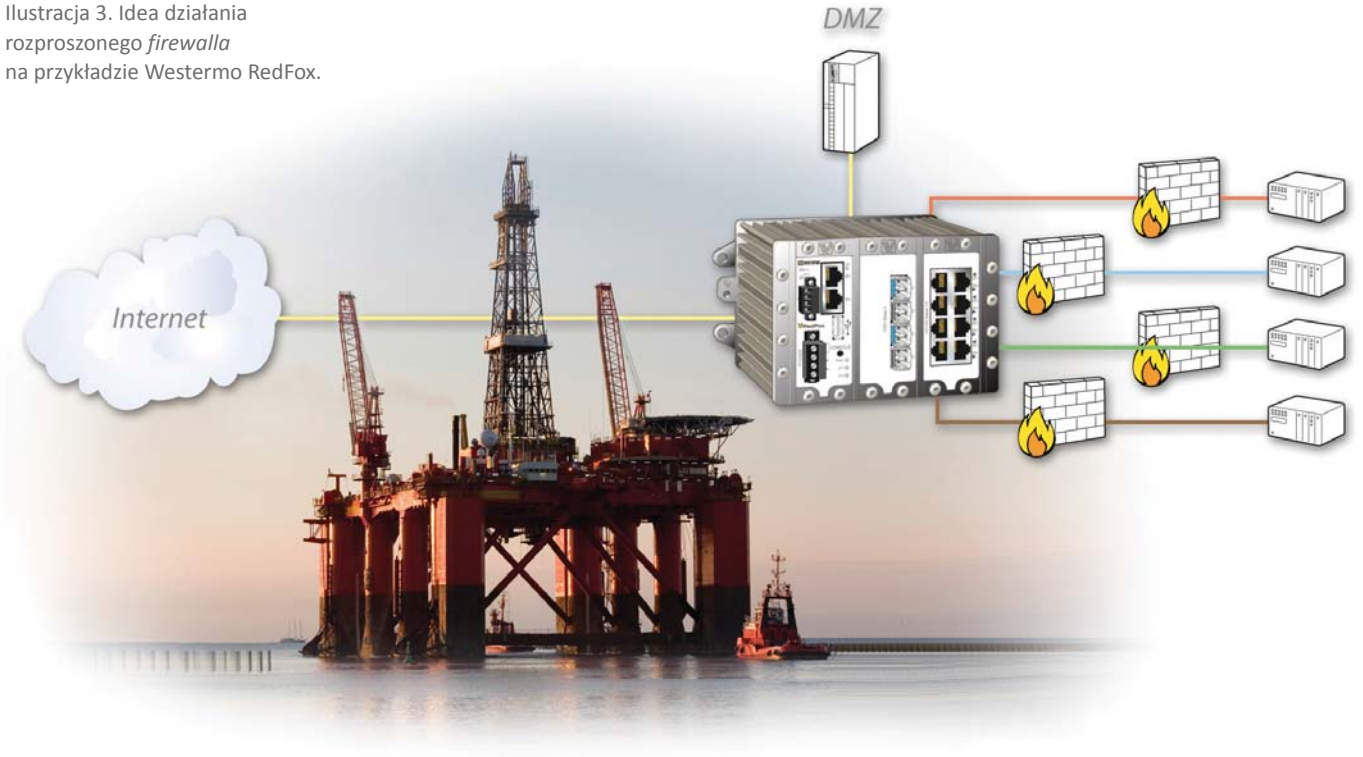
Systemy przemysłowe są stosunkowo łatwym celem, ponieważ przez wiele lat funkcjonowało przekonanie, że ich względna izolacja oraz nietypowe protokoły komunikacyjne stanowią same w sobie barierę ochronną. W konsekwencji oprogramowanie i sprzęt wykorzystywane do zarządzania oraz monitorowania procesów przemysłowych, poprzez nadzór i sterowanie urządzeniami automatyki, mają niski poziom zabezpieczeń. Tworzone są więc specjalne wirusy i oprogramowanie, skierowane do zainfekowania sterowników PLC i zdalnych terminali RTU, radzące sobie bez problemu ze specyfiką protokołów przemysłowych. Ze względu na wymogi biznesowe dotyczące dostępności danych z procesów przemysłowych w trybie rzeczywistym, sieci często nie są w pełni izolowane i mają połączenie z siecią korporacyjną.

Zniechęcająco na ambicje wprowadzania zaawansowanych rozwiązań bezpieczeństwa działa również fakt, że bardzo trudne jest opracowanie rozwiązań, które nie będą obniżać wydajności i degradować parametrów jakościowych procesów sterowania automatyką. Stosowane dotąd protokoły były projektowane do użytku lokalnego i nie przewidywano możliwości ich zdalnego serwisowania za pośrednictwem sieci publicznych (rozległych), w związku z czym brak w nich walidacji poprawności komend czy uwierzytelnienia ich źródła. Technologicznie infrastruktura informatyczna była oparta na łączach lokalnych (np. szeregowych) lub sieciach typu SDH/PDH, które mimo swoich wad w porównaniu z sieciami adresowalnymi są znacznie trudniejsze do penetracji i przeprowadzenia ataku. Obecnie, ze względu na zalety technologiczne czy ekonomiczne, powszechne jest stosowanie sieci wykorzystujących protokoły adresowalne (np. Ethernet, IP).

Sieci przemysłowe są również podatne na zagrożenia typu *zero-day*, takie jak np. niedawno opublikowane luki *shellshock* czy *heartbleed*. Naturalnym sposobem reagowania na informacje o takich lukach bezpieczeństwa w systemach operacyjnych jest tzw. *fast patching*, czyli szybka aktualizacja oprogramowania czy systemu operacyjnego urządzeń objętych zagrożeniem.

Dla systemów przemysłowych jest to jednak nie dość, że nierealne, to również niepożądane, ponieważ liczy się tu przede wszystkim ich stabilność. Nie można przeprowadzać eksperymentów na żywym organizmie lub definiować nadmiarowych reguł bezpieczeństwa, ryzykując, że będą one odfiltrowywać również prawidłowy ruch danych. Do niedawna brakowało tu w dodatku regulacji prawnych i wytycznych oraz audytów bezpieczeństwa, choć ten stan rzeczy powoli ulega zmianie (np. wprowadzane narzędzia NIST framework v1.0, NERC CIP).

Ilustracja 3. Idea działania rozproszonego *firewalla* na przykładzie Westermo RedFox.



Strategia wielowarstwowa

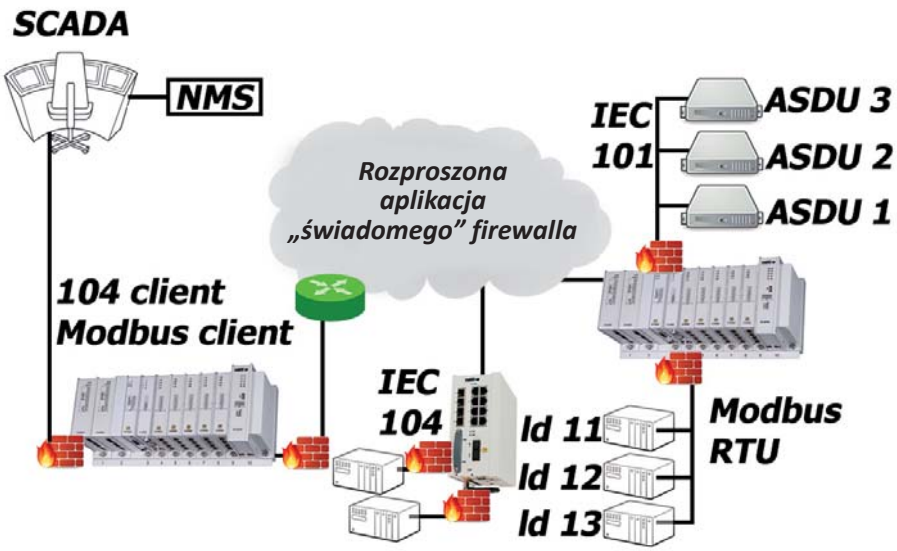
W dobrym systemie bezpieczeństwa sieci przemysłowej nie może zabraknąć narzędzi do profilowania i monitorowania zachowań, wykrywania włamań, skanowania pod kątem luk, wykrywania złośliwego kodu, korelacji zdarzeń dotyczących bezpieczeństwa.

Powiązanie informatycznych systemów korporacyjnych oraz przemysłowych sieci transmisji danych tworzy warstwową strukturę, w której każdy poziom ma inną specyfikę i wymagania, jak również architekturę połączeń „na zewnątrz". Naturalne jest więc, że najlepszym podejściem staje się wielowymiarowa/wielowarstwowa strategia bezpieczeństwa określana mianem Defence in Depth.

Pomysł w swoim założeniu jest prosty i opiera się na zastosowaniu dopasowanych zabezpieczeń na każdym poziomie sieci, począwszy od zabezpieczeń fizycznych obiektów, poprzez zabezpieczenia styku z siecią publiczną, aż po analizę i zabezpieczenie aplikacji przed złośliwym oprogramowaniem. Strategia bezpieczeństwa musi być zdywersyfikowana i uwzględniać:

- monitoring bezpieczeństwa i zarządzanie zdarzeniami (do analizy ex post),
- bezpieczeństwo fizyczne,
- odpowiednią architekturę sieci,
- zarządzanie dostępem do obiektów oraz powiązanie z prawami dostępu użytkowników do poszczególnych elementów systemu.

Strategia ta realizowana jest przez stosowanie systemów SIEM (*Security Information and Event Management*), specyfikację modelu dostępu i usług kryptograficznych, stosowanie sond monitorujących dany protokół przemysłowy (analiza historii sterowań), wykrywanie anomalii i działań nieuprawnionych, stosowanie odpowiednio skonfigurowanych, rozproszonych tzw. ścian ogniowych (*firewall*)



Ilustracja 4. Przykład działania SCADA *firewall*.

tekniska polska®
Przemysłowe Systemy Transmisji Danych Sp. z o.o.

Cyberbezpieczeństwo

DPI-SCADA firewall - analiza protokołów przemysłowych
DNP3, ModBus, IEC 104/101, **IEC 61850**

Łatwa konfiguracja zaawansowanych reguł SCADA firewall
fireall analizuje ruch i na jego podstawie przygotowuje reguły

VPN - bezpieczne przesyłanie danych
IPsec VPN, mGRE **DM-VPN**, GRE

Uwierzytelnianie
802.1x, Radius, TACACS+, X.509

Interfejsy
2 x100/1000 SFP, 8 x 10/100BaseT

Opcjonalne
Komunikacja 3G (2xSIM), SFP, RS-232, 8 x PoE+

Temperatura pracy -40°C do +75°C
Zasilanie 12 - 220VDC, 230VAC.

radiflow
Secure your Assets

Firewall - pozwala na tworzenie reguł pomiędzy wybranymi VLAN-ami

Łatwa konfiguracja zaawansowanych reguł firewall

VPN - bezpieczne przesyłanie danych
IPsec VPN, GRE, **SSL VPN**

Ciągłość komunikacji
FRNT (czas rekonfiguracji poniżej 20ms), RSTP, dwa wejścia zasilające.

Uwierzytelnianie
802.1x, Radius, X.509,

MTBF do 49 lat (MIL-HDBK-217K).

westermo®
Robust Industrial Data Communications – Made Easy

www.tekniska.pl

i systemów wykrywania/zapobiegania włamaniom. Dodatkowo pożądane jest wprowadzenie możliwości uwierzytelniania poleceń, autoryzacji dostępu (APA – ang. *Aplication Proxy Authentication*), archiwizacji i analizy logów.

Jednym ze sposobów jest zastosowanie rozproszonych, specjalnie opracowanych pod tym kątem „ścian ogniowych", tzw. *micro-firewall*. Dzięki temu każde z krytycznych dla systemu urządzeń końcowych może być izolowane przez *firewall* z określonym zestawem reguł dostępu „uszytych na miarę". Tego typu rozwiązania wymagają implementacji narzędzi *firewall* bezpośrednio w przemysłowych urządzeniach sieciowych, z których zbudowana jest infrastruktura. Oprócz możliwości uruchomienia i skonfigurowania *firewalla* na porcie lub dla wybranego VLAN, urządzenia te zapewniają wysoką dostępność dzięki możliwości tworzenia architektury nadmiarowej, bez pojedynczych punktów awarii **(ilustr. 1)**, z wykorzystaniem protokołów rekonfiguracji, takich jak np. FRNT, FRNT ring coupling, RSTP, OSPF.

Przykładem tego typu rozwiązań jest seria zarządzalnych, przemysłowych switchy warstwy 3: Lynx oraz RedFox firmy Westermo. Urządzenia te oparte są na systemie operacyjnym umożliwiającym przełączanie w warstwie drugiej (*switching* z możliwością tworzenia łatwo dostępnych topologii) oraz trzeciej (*routing*). Oprócz tego umożliwiają realizację procedur NAT, PAT, filtrowanie ruchu przez *firewall* z inspekcją stanu (*SPI firewall*), który można konfigurować niezależnie dla każdego interfejsu oraz wielu innych funkcji – a wszystko w jednym kompaktowym urządzeniu, przeznaczonym do pracy w trudnych warunkach środowiskowych.

Ilustracja 5. Kompaktowy SCADA *firewall* RADiFlow 1031.

Kolejnym krokiem jest *firewall* „świadomy" aplikacji, z funkcją analizowania wybranych protokołów przemysłowych, pozwalający śledzić i wykrywać anomalie. Takie rozwiązanie określa się mianem SCADA Deep Packet Inspection Firewall lub Application Aware Firewall, z możliwością scentralizowanego logowania zdarzeń. Umożliwia ono pełną analizę pracy sieci i jej zabezpieczenie niejako „od środka".

Urządzenie tego typu jest w stanie najpierw pracować w trybie uczenia się, by potem utworzyć model normalnej pracy, wykrywać anomalie i inicjować odpowiednie reakcje. Tryby pracy przykładowych rozwiązań tego typu marki RADiFlow to: uczenie się, blokowanie, logowanie.

Tryb logowania, praca *offline*, współpraca z systemami SIEM i systemami autoryzacji użytkowników jest szczególnie istotna w sieciach przemysłowych, w których zastosowanie klasycznego rozwiązania IT wiązałoby się z obniżeniem wydajności oraz zbyt dużym ryzykiem przerwania ciągłości procesu.

Dodatkowym atutem jest możliwość realizacji idei Role Base Access Control, czyli powiązania praw dostępu użytkownika z przeprowadzeniem wybranych działań, np. w ramach serwisu w określonym przez administratora czasie. Konieczną funkcją dla zapewnienia dostępu zdalnego jest również możliwość tworzenia szyfrowanych tuneli IPSec VPN. Przykład rozwiązania tego typu został przedstawiony na **ilustr. 4 i 5**.

Z punktu widzenia zarządzania bezpieczeństwem w systemach przemysłowych, kluczowe jest ciągłe monitorowanie i wykrywanie anomalii oraz możliwość szybkiej reakcji przez wprowadzanie sygnatur bezpieczeństwa w formie reguł *firewall*. Takie działania stanowią zabezpieczenie wewnętrzne i dają możliwość reagowania na zagrożenia *zero-day* oraz złośliwe oprogramowanie, którego celem może być penetracja systemu lub generowanie fałszywych komend dla systemów automatyki.

Zastosowanie rozwiązań *micro-firewall* i SCADA *firewall* jest jednym z elementów wprowadzania strategii bezpieczeństwa Defence in Depth. W połączeniu z odpowiednio przygotowaną polityką cyberbezpieczeństwa oraz scenariuszami reagowania na poszczególne zagrożenia umożliwia podwyższenie poziomu zabezpieczeń systemów przemysłowych, bez ryzyka utraty bądź obniżenia ich dostępności.

CE

Literatura:

1 „Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety 'Globalny stan bezpieczeństwa informacji'"; 2015 PWC
2 „Cyberespionage campaing hits energy companies"; 2014 Security Matters
3 „Cybersecurity for Power Utilities. Adefense primer for the operational network"; 2013 RAD
4 RADiFlow 3180 Security Appliance Review. a NERC CIP version 5 Compliance Enabler; 2014 RADiFlow
5 „Can we learn from SCADA security incidents? "; ENISA 2013
6 Materiały konferencyjne XVIII Seminarium Energotestu 2015 „Automatyka w elektroenergetyce: Niezawodność/bezpieczeństwo funkcjonowania systemów automatyki, sterowania i teletransmisji w elektroenergetyce generacyjnej oraz przesyle i rozdziale."
7 www.enisa.com
8 www.ics-cert.us-cert.gov
9 IEC 62351
10 „21 steps to Improve Cyber Security of SCADA Networks"; 2012 Departament Energii Stanów Zjednoczonych