Stefan Bednarczyk,
GIAC GICSP

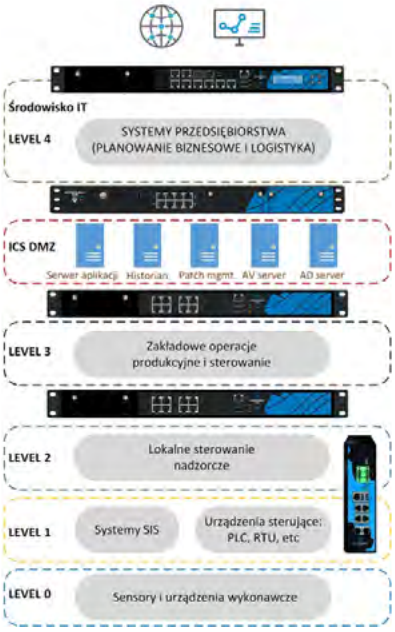
Bezpieczna sieć przemysłowa - studium przypadku

W artykule poruszono kwestię cyberzagrożeń w sieciach przemysłowych i zaprezentowano proces wdrażania stosownych zabezpieczeń. Od analizy ryzyka, zgodnej ze standardem IEC-62443, przez właściwą architekturę sieci, do implementacji przemysłowych firewalli DPI.

W ciągu ostatnich kilku miesięcy nasiliły się działania hakerskie, które obnażyły problemy dotyczące cyberbezpieczeństwa w systemach automatyki przemysłowej (ICS/OT) w różnych gałęziach gospodarki, również w infrastrukturze krytycznej (IK). Potwierdzają to ataki na systemy SolarWinds z grudnia 2020 r. oraz atak na infrastrukturę operatora rurociągów paliwowych Colonial Pipeline z maja 2021 r. W tym drugim przypadku cyberatak zmusił firmę do zamykania swoich systemów IT, co spowodowało zatrzymanie działania rurociągów. Dotychczasowe znalezione wskaźniki naruszenia bezpieczeństwa określają, że użyte zostało złośliwe oprogramowanie typu ransomware, a za atak odpowiada grupa hackerów DarkSide [1]. Można się w tym miejscu zastanowić, jakie systemy zaatakuje przeciwnik jeśli będzie silnie zmotywowany, aby zaszkodzić jakiemuś państwu? Zapewne będą to systemy energetyczne. Specjaliści z firmy Stormshield przeanalizowali ataki na takie systemy i w swoim opracowaniu [2] określili, że za 49% ataków odpowiadają cyberprzestępcy sponsorowani przez wywiady obcych państw. Taki przeciwnik jest bardzo silnie zmotywowany, posiada wysokie umiejętności oraz nieograniczone środki.

Czy w takim razie jesteśmy w stanie skutecznie chronić naszą infrastrukturę krytyczną?

Odpowiednie obowiązki np. analizę ryzyka i ciągłe monitorowanie, nakłada na operatorów IK ustawa o krajowym systemie cyberbezpieczeństwa. Właścicielom systemów ICS z pomocą przychodzi standard IEC-62443, w którym zawarte są rekomendacje m. in. w zakresie oceny ryzyka, podziału systemu na strefy i kanały, określania wymaganych poziomów bezpieczeństwa (SL-T) dla zgrupowanych w strefach zasobów oraz wprowadzania odpowiednich zabezpieczeń. Bardzo wiele można osiągnąć, gdy architektura systemu będzie zaprojektowana w odpowiedni sposób i zbudowana z właściwych dla przemysłowego środowiska elementów. Sieci oparte o standard Ethernet, jeśli są zbudowane z zarządzalnych przełączników,



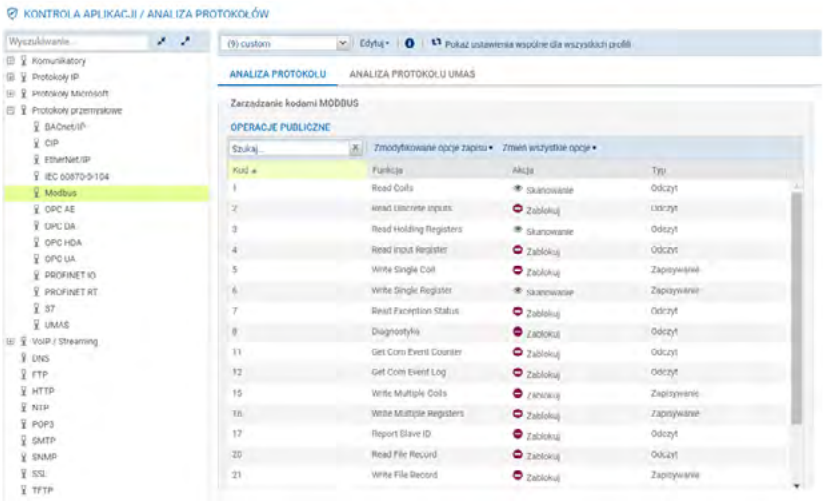
Rys. 1

można zacząć już zabezpieczać na ich poziomie. Przykładowo przemysłowe przełączniki Westermo [3] umożliwiają logiczną segmentację sieci z wykorzystaniem VLAN-ów, zapewniają kontro-

lę dostępu na poziomie portów, logują naruszenia do systemu SIEM oraz jeśli są modelami warstwy trzeciej (routerami) filtrują ruch pomiędzy VLAN-ami. Jeśli chodzi o architekturę, to norma IEC-62443 dla systemów ICS wykorzystuje referencyjny model Purdue, w którym cała sieć podzielona jest na warstwy pokazane na rys. 1.

Pomiędzy warstwami należy stosować rozwiązania służące do egzekwowania polityki bezpieczeństwa. Do tego zadania doskonale nadają się urządzenia klasy UTM firmy Stormshield [4]. Do dyspozycji są modele chroniące w konfiguracji wysokiej dostępności (HA) brzeg sieci przedsiębiorstwa na styku z Internetem. Inne modele posłużą do zbudowania strefy DMZ pomiędzy siecią biurową, a siecią OT. Do instalacji w sieci OT w celu podziału systemu na strefy bezpieczeństwa przeznaczone są dwa modele: SNi40 i SNi20. Urządzenia te posiadają funkcje UTM znane z modeli przeznaczonych dla sieci IT oraz wyposażone są w dodatkowe mechanizmy głębokiej analizy pakietów (DPI) dla protokołów przemysłowych: Modbus TCP, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), PROFINET, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). Funkcjonalność DPI pozwala na tworzenie bardzo precyzyjnych reguł filtrowania ruchu sieciowego - można dopuścić tylko określone kody funkcji protokołów przemysłowych, pomiędzy obiektami zdefiniowanymi za pomocą adresów IP oraz identyfikatorów i adresów urządzeń na poziomie aplikacji przemysłowej. Dla każdego z protokołów można użyć po dziesięć profili, w których określa się akcje (skanowanie, blokada) dla poszczególnych kodów funkcji protokołu (rys. 2).

Profile analizy protokołów następnie są wykorzystywane w regułach firewall-a. Oprócz twardego egzekwowania reguł w trybie IPS, każda reguła może też działać jako IDS. Wtedy ruch pasujący do reguły nie jest blokowany, a jedynie zdarzenie zapisywane jest w logach. Pozwala to na łatwe testowanie reguł przed ich implementacją, co ma szczególne znaczenie w środowisku przemysłowym. Częstym przypadkiem jest też sytuacja, w której pogrupowaliśmy urządzenia w strefy, ale sieć jest płaska, a musimy zabezpieczyć kanał pomiędzy urządzeniami. Rozwiązaniem jest dostępny w urządzeniach Stormshield transparentny tryb pracy. Wybrane porty Ethernet są zgrupowane i przypisane do mostka sieciowego (bridge). Urządzenia końcowe (np. HMI, PLC,..) podłączone do tych portów komunikują się ze sobą jakby były podłączone do przełącznika LAN, a dla komunikacji pomiędzy nimi będą działały wszystkie reguły tradycyjnego firewalla oraz analizy DPI.



Rys. 2

Wcześniej wspomniano o konieczności wykonywania cyklicznej analizy ryzyka, a pierwszym etapem w procesie jej automatyzacji jest inwentaryzacja sieci (urządzeń, połączeń, protokołów, ...) i stworzenie jej cyfrowego obrazu. Dane te powstają w systemie wykrywania zagrożeń Radiflow iSID (IDS dla OT) i dalej trafiają do systemu Radiflow CIARA *(Cyber Industrial Automated Risk Analysis)*. System ten automatyzuje proces dobierania właściwych mechanizmów bezpieczeństwa przeciw symulowanym setkom typów cyberzagrożeń jednocześnie modelując dziesiątki funkcji sieci cyfrowej, w tym protokołów, podatności, wersji firmware, topologii, typów urządzeń i innych. Cały ten proces jest realizowany zgodnie z algorytmem opisanym w standardzie IEC-62443 [5] i pozwala na planowanie terminu i kosztów wdrażania zabezpieczeń dla zmieniającego się w czasie poziomu ryzyka.

Odpowiadając na pytanie z początku artykułu - tak mamy szereg narzędzi, które prawidłowo skonfigurowane i zastosowane pomogą nam chronić sieci przemysłowe w systemach krytycznych, jednocześnie pamiętając, że najsłabszym ogniwem pozostaje człowiek, dlatego ważna jest jego edukacja. □

Literatura

1. Charlie Osborne. „Everything you need to know about the Colonial Pipeline ransomware attack".
2. Stormshield. "From 2015 to tomorrow: cyberintrusions in electrical grids. Whitepaper".
3. Westermo. "5 basic steps for improved industrial cybersecurity".
4. Stormshield Network Security.
5. Radiflow. „CIARA Cyber Industrial Automated Risk Analysis. IEC-62443-Based Risk Assessment in ICS/SCADA Networks".