Rozwiązania STORMSHIELD pomagają spełnić rekomendacje cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego

1. Należy zmniejszyć do minimum ekspozycję sieci przemysłowej, zarówno sieci lokalnej, jak i punktów styku, poprzez identyfikację i ograniczenie do koniecznych, połączeń ‘z’ i ‘do’ tej sieci – ograniczamy (lub wręcz uniemożliwiamy) w ten sposób nieautoryzowane połączenia z zewnątrz.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW realizują segmentację sieci wraz ze szczegółową ochroną transmisji pomiędzy segmentami. Izoluje sieć do tylko niezbędnego ruch sieciowego. W sposób zautomatyzowany chroni przed próbami ataków i zagrożeniami sieciowymi. SNS autonomicznie przeprowadza analizę ruchu sieciowego. Autoryzuje i kontroluje autoryzowany dostęp zarówno użytkowników, jak i szyfrowany ruch sieciowy VPN.

2. Należy oddzielić systemy OT od systemów IT zorientowanych na klienta oraz monitorować i kontrolować interakcje pomiędzy tymi dwoma obszarami.
   Rekomendowanym rozwiązaniem jest unikanie podłączeń urządzeń przemysłowych do sieci publicznych, w szczególności Internetu.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW kontrolują i zabezpieczają transmisję do poziomu poszczególnych komend, instrukcji, identyfikatorów, zgodności ruchu sieciowego zarówno dla ruch IT jak i OT. Głęboka analiza jest przeprowadzana na poziomie protokołów sieciowych w sieciach IT oraz w całej gamie na poziomie protokołów OT, tak jak: Modbus, UMAS, OPC Classic (DA/HDA/AE), OPC UA, EtherNet/IP, CIP, BACnet/IP, S7, Profinet, IEC 60780-5-104, DNP3, IEC 61850 (MMS/GOOSE).

3. W przypadku gdy zdalny dostęp jest niezbędny (np. do monitorowania i zarządzania rozległą infrastrukturą) powinien być zawsze realizowany za pomocą VPN z wykorzystaniem konfiguracji umożliwiającej zastosowanie uwierzytelnienia wieloskładnikowego (MFA).

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW realizują konfiguracje VPN i pozwalają na zastosowanie uwierzytelnienia wieloskładnikowego (MFA).

4. Należy dokonać przeglądu zdalnego dostępu i ograniczyć go do niezbędnego minimum, w szczególności należy zwrócić uwagę na modemy komórkowe i metody zdalnego dostępu podwykonawców.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW kontrolują zdalny dostęp do niezbędnego minimum pod względem czasu, grupy lub użytkowników, adresów i oraz portów, protokołów. Dodatkowo zbierają informacje i raportują metody zdalnego dostępu podwykonawców.

5. Należy zmienić domyślne dane uwierzytelniające stosując dobre praktyki silnych haseł (o ile urządzenie takie hasła wspiera), na wszystkich urządzeniach, w szczególności urządzeniach posiadających interfejs webowy oraz wyłączyć niewykorzystywane konta.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW wymuszają zastosowanie się do dobrych praktyk pod względem haseł dostępowych. Jest to automatycznie alertowane, monitorowane i rejestrowane.

6. Tam gdzie to możliwe, należy ograniczyć dostęp do VPN dla określonych adresów IP lub ich zakresów. Przykładowo gdy podmiot nie posiada współpracowników ani podwykonawców zagranicznych, rekomenduje się zastosować możliwość próby nawiązania sesji VPN tylko dla polskich adresów IP.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW ograniczają dostęp do VPN dla określonych adresów IP lub ich zakresów. Umożliwia również blokowanie pod kątem geolokalizacji, jak i reputacji adresów IP.

7. W przypadku, gdy niezbędny jest zdalny przesył danych telemetrycznych za pomocą sieci komórkowej należy korzystać z dedykowanych prywatnych APN.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW obsługują modemy 3G, jak i LTE. Istnieje możliwość zestawienia transmisji dedykowanej za pomocą równoważenia obciążenia, zapasowych łączy, z wykorzystaniem protokołów routingu dynamicznego oraz Policy Base Routingu i dedykowanych prywatnych kanałów APN.

8. Należy aktualizować oprogramowanie wykorzystywanych systemów i urządzeń, w szczególności podczas planowych postojów. Przed aktualizacją należy przeprowadzić analizę potencjalnego wpływu aktualizacji na utrzymanie ciągłości działania (w szczególności aktualizacja może wprowadzać elementy, które spowodują utratę zgodności np. z oprogramowaniem niskopoziomowym) – dlatego też przed dokonaniem aktualizacji należy przetestować ją w środowisku testowym, przed zastosowaniem w środowisku produkcyjnym.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW automatycznie informują o nowych wersjach oprogramowania. Istnieją możliwości zapisu różnych polityki bezpieczeństwa, jest możliwość zaimplementowania różnych scenariuszy od przeprowadzanych akcji zależności do serwisowych,

które umożliwią utrzymanie ciągłości działania. Systemy Stormshield są w pełni redundantne - odporne na awarie.

9. Należy stosować segmentację sieci - minimalnie na styku sieci przemysłowej, a preferencyjnie, zależnie od rozmiaru i złożoności zakładu, również wewnątrz.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW służą do segmentacji i głębokiej analizy na poziomie protokołów OT, tak jak: Modbus, UMAS, OPC Classic (DA/HDA/AE), OPC UA, EtherNet/IP, CIP, BACnet/IP, S7, Profinet, IEC 60780-5-104, DNP3, IEC 61850 (MMS/GOOSE). Portfolio urządzeń Stormshield to rozwiązania instalowane do szaf teleinformatycznych, jak i również urządzenia, które możemy instalować bezpośrednio przed urządzeniami i sterownikami PLC. Mają możliwość wstawienia w szyny DIN, są odporne na nieprzychylne warunki środowiskowe i zasilane z dwóch niezależnych źródeł zasilania prądem stałym.

Separację mogą realizować na poziomie mostu i będą przezroczyste dla transmisji. Mogą monitorować, alertować, ale przede wszystkim blokować niepożądany ruch nawet na poziomie komend i adresów przemysłowych charakterystycznych dla poszczególnych protokołów przemysłowych.

10. Należy prowadzić okresową analizę widoczności urządzeń poprzez zewnętrzne skanowanie zakresu adresacji należącej do obiektu, czy wykorzystanie narzędzi typu Shodan.

Komentarz inżyniera:

Urządzenia Stormshield UTM/NGFW blokują cały niepożądany ruch z zewnątrz, tak że narzędzia Shodan nie powinny nic wykryć. Jednocześnie rejestrują wszystkie próby skanowania i ataków. Urządzenie Stormshield może alertować bezpośrednio do administratorów i operatorów systemów. Tym samym, można ten ruch przedstawić w sposób graficzny, łatwy do analizy i wyciągania wniosków.

Dane są dostępne w repozytorium, które szybko można przeszukiwać. Dane są także eksportowalne do innych systemów.