

Bezpieczeństwo sieciowe – badanie sieci OT/ICS

Red Team: konsulting praktyczny

Czy wiesz, że ataki ransomware zdarzają się co 10 sekund, a aż 85% naruszeń wynika z błędu ludzkiego? Zainwestuj w cyberbezpieczeństwo swojej sieci OT/ICS – ale z konkretnym planem działania!

Eksperci Tekniska przeprowadzą Cię przez proces zbadania i podniesienia bezpieczeństwa sieciowego krok po kroku, wskazując najefektywniejszą drogę do osiągnięcia celu. Inwestycja w cyberbezpieczeństwo to inwestycja w ciągłość pracy Twojego przedsiębiorstwa, ochronę wrażliwych danych, zgodność z wymaganiami i normami oraz minimalizację potencjalnych strat finansowych.

Co zyskujesz?



Stabilność działań

Zagrożenie dla infrastruktury sieciowej to zagrożenie dla całej firmy. Awaryjne prowadzące do zaburzenia ciągłości działań przedsiębiorstwa skutkują realnymi, często dotkliwymi stratami – zarówno finansowymi, jak i wizerunkowymi. Dzięki badaniu bezpieczeństwa sieci minimalizujesz ryzyko i zapewniasz sobie stabilność biznesową.



Maksymalizacja ROI

Inwestuj w cyberbezpieczeństwo mądrze, stawiając na dopasowane rozwiązania, których skuteczność możesz zmierzyć i ocenić. Redukcja ryzyka zaczyna się od ustalenia priorytetów i dopasowania kierunku działania do Twoich potrzeb i ograniczeń. Tylko w ten sposób zbudujesz efektywny model bezpieczeństwa i zmaksymalizujesz zwrot z inwestycji. Buduj cyberbezpieczeństwo efektywnie – nie efektownie.



Spełnienie wymagań

Podczas badania eksperci Tekniska nie tylko określą, czy Twoja sieć spełnia wszystkie normy i wymagania, ale też przedstawią krok po kroku, gdzie występuje największe ryzyko i czym może skutkować. Wspólnie ustalimy priorytety i wskażemy drogę do realnej eliminacji problemów.



Bezpieczeństwo i ciągłość procesów

Bezpieczna sieć OT to bezpieczny proces produkcyjny. Wiemy, jak ważna jest ciągłość procesu i zdajemy sobie sprawę, że jego zaburzenie lub czasowe przerwanie nie wchodzi w grę – dlatego nasze badania możemy przeprowadzić z pełną skutecznością w sposób stuprocentowo pasywny, który nie zaburzy pracy Twojego przedsiębiorstwa.



Jak działamy?

Aby skutecznie zminimalizować ryzyko, jednocześnie maksymalizując zwrot z inwestycji w cyberbezpieczeństwo, na sieć przemysłową należy patrzeć z wielu perspektyw, uwzględniając możliwości i ograniczenia Twojego przedsiębiorstwa.

Dzięki obraniu odpowiedniej metodyki działań oraz wnikliwemu i pragmatycznemu podejściu nasi inżynierowie wskażą najbardziej narażone na atak fragmenty Twojej infrastruktury. Wraz ze wskazaniem potencjalnych wektorów ataku wskażemy Ci realną drogę do celu, bazując na podejściu praktycznym – nie na powielaniu schematycznych raportów i rekomendacji.

Analiza potrzeb - warsztat

1

W ramach warsztatu przedyskutujemy i zbadamy Twoje potrzeby. Dowiemy się, jakie masz oczekiwania, a Ty – jak będzie przebiegała cała usługa. Pamiętaj, że to od Ciebie – Twoich potrzeb oraz możliwości technicznych i finansowych – zależy zakres naszych działań. Na tym etapie poznajemy Twój zespół, stan techniczny oraz uwarunkowania i wspólnie definiujemy cele, zakres działań oraz sposób ich realizacji.

Inwentaryzacja

2

Aby kompleksowo i rzetelnie panować nad bezpieczeństwem swojej sieci, potrzebujesz pełnego obrazu infrastruktury – rzeczywistego, szczegółowego i zawierającego pełną listę urządzeń, wykorzystywanych protokołów czy logicznych i fizycznych połączeń. Taki obraz pozyskujemy w wyniku inwentaryzacji sieci. Metodologię, narzędzia i wynik tego etapu dopasowujemy do Twoich oczekiwań – inwentaryzacja może być zarówno usługą niezależną, jak również krokiem do dalszych działań oraz możliwości organizacji.

Badanie bezpieczeństwa

3

Posiadając pełen obraz infrastruktury i dane o firmie pozyskane podczas wywiadu, przeprowadzamy kompleksowe badanie bezpieczeństwa, podczas którego wskażemy obszary największego ryzyka i potencjalne zagrożenia. W zależności od obranej strategii, badanie może zostać przeprowadzone w sposób w pełni pasywny. Opcjonalnie możemy zrealizować pentesty dla wybranych części lub elementów infrastruktury – czerpiemy tu z naszego doświadczenia oraz metodologii dedykowanych dla OT/ICS.

Raport i rekomendacje

4

W wyniku badania otrzymasz od nas szczegółowy i precyzyjny raport zawierający listę potencjalnych wektorów ataków, efekt badania protokołów przemysłowych i elementów infrastruktury pod kątem podatności oraz rekomendacje naszych specjalistów wraz z priorytetem i odniesieniem do rozpoznanych w ramach zbadanych w kroku pierwszym możliwości oraz ograniczeń organizacji. Z nami zyskasz rzeczywisty i rzeczowy obraz swojej sieci przemysłowej i jej podatności z perspektywy cyberryzyka wraz z propozycją planu minimalizacji tego ryzyka uwzględniającego priorytety działań.



Dlaczego Tekniska?



Kompleksowo i indywidualnie

Na bezpieczeństwo Twojej sieci OT/ICS ma wpływ wiele czynników, dlatego to Ty decydujesz o ostatecznym zakresie usługi – możemy zatrzymać się na inwentaryzacji lub przeprowadzić Cię przez cały proces, uwzględniając pełne badanie bezpieczeństwa sieci.



Optyka na proces

Wiemy, że ciągłość procesu to podstawa działania Twojej firmy. Dlatego wybieramy sposób badania bezpieczeństwa sieci, którego przeprowadzenie nie wprowadza ryzyka awarii w działaniu infrastruktury przemysłowej i związanych z tym przestojów, a także nie odciąga Twoich pracowników od kluczowych dla firmy działań.



Doświadczenie i pragmatyzm

Nasz zespół tworzą doświadczeni inżynierowie, którzy podczas działań przyjmują wiele perspektyw, by w wyniku prowadzenia usługi spełnić wszystkie Twoje założenia biznesowe. Zbadamy Twoją infrastrukturę, stawiając się zarówno w roli atakującego, jak i zarządzającego siecią. Dzięki wielopłaszczyznowemu, praktycznemu podejściu jesteśmy w stanie wskazać wektory ataku i skuteczną drogę do ich eliminacji.

Jak zacząć?

Jesteś gotowy, by działać lub masz jeszcze jakieś pytania? Skontaktuj się z nami! Zespół Tekniska przygotuje dla Ciebie ofertę w oparciu o indywidualne potrzeby i możliwości. Po uzupełnieniu formularza w ciągu jednego dnia roboczego skontaktuje się z Tobą nasz specjalista. W międzyczasie otrzymasz potwierdzenie złożenia prośby o kontakt.



Kontakt

Marcin Skórka

Menedżer Projektów
Cyberbezpieczeństwa ICS/OT

✉ marcin.skorka@tekniska.pl

☎ +48 502 594 348

Tekniska Polska

Przemysłowe Systemy
Transmisji Danych Sp. z o.o.

ul. Łabędzka 9-9A
44-121 Gliwice

NIP: 6312631825
KRS: 0000383694

+48 32 33 111 06-09
tekniska@tekniska.pl

WWW.TEKNISKA.PL