Orange Polska wspiera firmy w budowaniu bezpieczeństwa przemysłowej infrastruktury krytycznej

Case study Orange Cyberdefense

Infrastruktura krytyczna obejmuje maszyny, urządzenia i systemy, które są niezbędne do prawidłowo działającej produkcji. Te elementy mogą być narażone na różne zagrożenia, takie jak: katastrofy naturalne, sabotaż czy ataki cybernetyczne. Dlatego ważne jest, aby zapewnić odpowiednią ochronę oraz zarządzanie i zminimalizować ryzyko ich uszkodzenia lub zatrzymania.

Warto podjąć zawczasu działania zapobiegawcze, takie jak monitorowanie sieci, wykrywanie i usuwanie zagrożeń, zabezpieczanie systemów i danych oraz tworzenie planów awaryjnych na wypadek ataku.

Wprowadzenie

Ostatnie miesiące wskazują, że zagrożenie atakiem cyberprzestępców na infrastrukturę krytyczną firm rośnie. Przestępcy stają się niezwykle aktywni w tym obszarze. Są w stanie zaburzyć ciągłość działania całej firmy. Dlatego eksperci Orange Polska zostali zaproszeni do międzynarodowego zespołu Orange Cyberdefense, aby przeprowadzić audyt bezpieczeństwa infrastruktury OT amerykańskiego giganta.

Orange Cyberdefense (OCD) to wyspecjalizowana jednostka biznesowa Orange dostarczająca zaawansowane usługi cyberbezpieczeństwa dla międzynarodowych przedsiębiorstw.

Orange Cyberdefense to:

- ponad **25-letnie doświadczenie w dziedzinie bezpieczeństwa** informacji,
- ponad **250 badaczy i analityków**,
- **współpraca z 16 centrami bezpieczeństwa** (SOC Orange), 10 Cyber SOC oraz jednostkami CERT na całym swiecie,
- **wsparcie sprzedaży i usług w 160 krajach**.

Orange Cyberdefense, działając w ramach Grupy Orange, nawiązał współpracę z ekspertami ds. cyberbezpieczeństwa OT Orange Polska w celu przeprowadzenia audytu bezpieczeństwa w przedsiębiorstwie produkcyjnym, które ma wiele rozproszonych lokalizacji w USA i na świecie.

Wyzwania

Przedsiębiorstwo produkcyjne, które zdecydowało się na skorzystanie z rozwiązania od OCD i Orange Polska, ma na całym świecie ponad 220 lokalizacji, w których produkuje materiały niezbędne w branżach takich jak FMCG i handel. W ramach projektu pilotażowego przeprowadzono audyt bezpieczeństwa sieci i urządzeń OT (infrastruktury przemysłowej) pod kątem identyfikacji podatności, potencjalnych zagrożeń oraz wydania rekomendacji zmian w celu zminimalizowania ryzyka ich wpływu na ciągłość biznesową.

Zakres projektu obejmował:

- skanowanie całej sieci w lokalizacji klienta,
- identyfikację sieci i urządzeń OT,
- oszacowanie podatności infrastruktury OT na zagrożenia,
- oszacowanie zagrożeń i ryzyka ich wystąpienia,
- rekomendacje zmian w sieci IT i OT oraz w urządzeniach w celu bezpiecznego odseparowania obu sieci od siebie.

Wdrożenie

Projektem objęto w Stanach Zjednoczonych dziesięć lokalizacji klienta, które są oddalone od siebie o tysiące kilometrów.

W ramach audytu eksperci ds. cyberbezpieczeństwa Orange:

- przeprowadzali wywiady z klientami, rozpoznawali potrzeby i funkcjonujące procesy,
- oszacowali podatności infrastruktury OT, stosując odpowiednią wiedzę specjalistyczną oraz właściwe narzędzia,
- zidentyfikowali i przedstawili istotne zagrożenia mogące mieć wpływ na ciągłość biznesową klienta,
- zaproponowali zmiany w konfiguracji sieci i urządzeń klienta.

Eksperci Orange, używając sprawdzonych narzędzi i wykorzystując swoje doświadczenie, zidentyfikowali kluczowe miejsca w sieci klienta w celu podłączenia się do nich i analizy ruchu sieciowego. Narzędzia dostępne w laboratorium OT w Warszawie wspomagały na co dzień ich pracę.

Efekty i korzyści

Kompleksowy audyt bezpieczeństwa cybernetycznego infrastruktury OT jest ważnym narzędziem dla każdego przedsiębiorstwa produkcyjnego. Pozwala on na identyfikację potencjalnych zagrożeń i słabych punktów w sieci i systemach OT, a także na wprowadzenie rozwiązań, które pomogą w ich wyeliminowaniu lub zminimalizowaniu wystąpienia zagrożeń.
W ten sposób przedsiębiorstwo:

- zwiększy swoją odporność na ataki hakerskie i inne zagrożenia cybernetyczne,
- zminimalizuje ryzyko wystąpienia ataku, który powoduje zakłócenie lub utratę ciągłości biznesowej.

W efekcie przeprowadzonego audytu przygotowano szczegółowe zalecenia dotyczące znaczącego wzmocnienia poziomu bezpieczeństwa i klient uzyskał:

- spójny raport dotyczący zidentyfikowanej infrastruktury zawierający szczegółowe informacje na temat jej funkcjonowania w sieci,
- wiedzę na temat nowych zagrożeń oraz najnowocześniejszych technik cyberprzestępców,
- wiedzę o podatności swoich urządzeń na zagrożenia,
- informacje dotyczące ryzyka wpływu zagrożeń na ciągłość biznesową,
- wdrożenie odpowiednich rekomendacji w celu minimalizacji ryzyka utraty ciągłości biznesowej.

Okiem klienta

Dzięki współpracy z ekspertami z Orange Polska przeprowadzony audyt oraz rekomendacje z niego wynikające oznaczały właściwe rozpoznanie potrzeb w zakresie bezpieczeństwa OT kolejnych lokalizacji i spotkały się z wysoką oceną klienta.

John Dauphinais
Head of Consulting, Orange Cyberdefense