

Ciepło to poczucie bezpieczeństwa

orange™



Wszechobecne elektronika i cyfryzacja upraszczają zarządzanie nawet najbardziej skomplikowaną infrastrukturą, jednocześnie jednak stanowią wyzwanie w zakresie bezpieczeństwa. Problemów z próbą wyłudzenia pieniędzy doświadczyło gliwickie Przedsiębiorstwo Energetyki Ciepłej. Dzięki szybkiej reakcji i audytowi bezpieczeństwa przeprowadzonemu przez Orange udało się ograniczyć straty i zabezpieczyć infrastrukturę firmy na przyszłość.

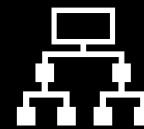
PEC Gliwice zajmuje się wytwarzaniem, przesyłaniem i dystrybucją ciepła na potrzeby centralnego ogrzewania i ciepłej wody na terenie Gliwic. Produkcja odbywa się w Ciepłowni Gliwice oraz w dwóch lokalnych kotłowniach.



Odbiorcy ciepła to liczne instytucje, zakłady przemysłowe, obiekty usługowo-handlowe oraz ponad 45 tysięcy mieszkań, w tym 18,5 tysiąca mieszkań odbiorców ciepłej wody użytkowej. W sumie PEC Gliwice zaopatruje w ciepło systemowe 100 tysięcy gliwiczian. Firma zatrudnia 251 pracowników.

Wyzwania i cele

Gliwicka sieć dystrybucji ciepła posiada rozbudowane zaplecze informatyczne wykorzystujące transmisję danych między innymi do zdalnych odczytów. Zarządzanie siecią wspiera infrastruktura sieciowa wyniesionych urządzeń rozmieszczonych na terenie miasta, które zbierają informacje dotyczące prowadzonego procesu dystrybucji ciepła systemowego, takie jak temperatura, ciśnienie wody. Tego typu punkty dostępowe stają się coraz częściej celami ataków hakerskich. Incydenty, jakich doświadczyliśmy, były właśnie związane z przejściem takiego punktu wymiany węzła komunikacyjnego przez osoby trzecie. Zaistniały incydent zmotywował zarząd firmy do kompleksowego przeglądu posiadanych zasobów informatycznych i przeprowadzenia kompleksowego audytu cyberbezpieczeństwa. Audyt przeprowadziła grupa 6 specjalistów z firmy Orange.



Wdrożenie

Orange współpracuje z PEC Gliwice Sp. z o.o. od wielu lat, dostarczając rozwiązania zarówno w zakresie telekomunikacyjnych usług stacjonarnych, jak i mobilnych. PEC Gliwice Sp. z o.o. korzysta również z 30-kanalowego traktu PRA Orange wykorzystywanego do funkcjonowania cyfrowej centrali telefonicznej. Incydent bezpieczeństwa skłonił zarząd PEC Gliwice Sp. z o.o. do przyjrzenia się kwestiom bezpieczeństwa kompleksowo. Wybór wykonawcy audytu padł zatem na długoletniego usługodawcę teleinformatycznego – firmę Orange. Przeprowadzono audyt cyberbezpieczeństwa, którego przedmiotem było skontrolowanie całego zaplecza informatycznego, od komputerów osobistych po serwery baz danych i aplikacje mobilne. Przyjrzenie się zarówno części sprzętowej, jak i oprogramowaniu zaowocowało zbudowaniem tabel podatności na zagrożenia. Przeprowadzony audyt pozwolił na wykrycie wielu potencjalnych zagrożeń w firmie.

W konsekwencji wprowadzono nowe procedury bezpieczeństwa, zaplanowano nakłady inwestycyjne na rozwiązania informatyczne, wymieniono przestarzały sprzęt i zmodernizowano oprogramowanie. Orange dostarczył również nowoczesne karty SIM – M2M – przeznaczone do transmisji danych dla wyniesionych punktów pracujących w trzeciej warstwie OSI.

Efekty i korzyści



Podstawową korzyścią przeprowadzonego audytu było uzyskanie obiektywnej opinii na temat stanu audytowanych obiektów przygotowanej przez zewnętrznych ekspertów oraz wykrycie wszelkich uchybień i ryzyk związanych z infrastrukturą informatyczną.



Raport okazał się niezwykle pomocny przy podejmowaniu decyzji w ramach wdrożenia zaleceń w nim zawartych w zidentyfikowanych obszarach potencjalnego usprawnienia systemów bezpieczeństwa. Raport wskazał również możliwości usprawnienia procesów, poprawy efektywności, racjonalizacji działań oraz optymalizacji kosztów.



Co niezwykle istotne, wydatki na poprawę bezpieczeństwa nie miały wpływu na opłaty wnoszone przez odbiorców ciepła systemowego, a co więcej – wprowadzone zmiany pozytywnie wpłynęły na obsługę i poprawę ochrony danych osobowych.

Plany na przyszłość



Okiem klienta

W mojej ocenie audyt został przeprowadzony bardzo profesjonalnie, a jego wyniki były bardzo surowe, na czym nam zależało – zarówno stosowane wcześniej rozwiązania z zakresu bezpieczeństwa, jak i sprzęt zostały poddane krytyce. Po zapoznaniu się z wynikami wprowadziliśmy zalecane zmiany, a po kolejnych 4 miesiącach ponowiliśmy audyt. Uważam, że ponowna analiza bezpieczeństwa jest niezbędna, aby należycie ocenić efekty wprowadzonych zmian i aktualny poziom zabezpieczeń. Co więcej, zamierzamy w kolejnym roku przeprowadzić następny audyt bezpieczeństwa. Jest to szczególnie istotne, gdyż nasza firma może zostać zakwalifikowana przez Departament Bezpieczeństwa i Zarządzania Kryzysowego przy Ministerstwie Energii do grupy operatorów kluczowych, co oznacza zwiększenie wymagań w obszarze bezpieczeństwa. W takiej sytuacji nasza współpraca z Orange jeszcze bardziej się zacieśni.

Krzysztof Szaliński, Zastępca Dyrektora ds. Technicznych