Trzy problemy związane z bezpieczeństwem Internetu Rzeczy – i jak je rozwiązuje Telit

Wraz z pojawieniem się Internetu Rzeczy (IoT) na całym świecie pojawiły się nowe obawy dotyczące bezpieczeństwa. Liderzy projektów IoT muszą śledzić mnóstwo obiektów – czasami tysiące urządzeń rozmieszczonych na rozległych obszarach geograficznych. Zadania obejmują wszystko, od aktualizacji oprogramowania po monitorowanie fizycznej lokalizacji. Każde podłączone urządzenie stanowi nową powierzchnię ataku lub bramę umożliwiającą cyberprzestępcom wejście do sieci.

Obecnie obawy dotyczące bezpieczeństwa uniemożliwiają szersze zastosowanie rozwiązań IoT. Przyjrzyjmy się bliżej trzem zasadniczym obawom dotyczącym bezpieczeństwa.

1. Rosnąca liczba możliwości ataku

Wyobraź sobie, że Twoje dane są zamknięte w pokoju z jednymi drzwiami. To jedyny sposób, w jaki złodziej może wejść, dzięki czemu łatwo go strzec. Jeśli jednak przenosisz dane do dużego pokoju z setkami drzwi i okien, wprowadzasz o wiele więcej możliwości wejścia.

Kiedy firma wdraża projekt IoT, przechodzi od potencjalnie małej liczby podłączonych urządzeń do ogromnej floty czujników, które często są rozmieszczone w odległych lokalizacjach. Każde nowo podłączone urządzenie, bez względu na swoją rolę, staje się przedmiotem ataku, który przestępca może wykorzystać i potencjalnie włamać się do szerszej sieci.

2. Wyzwania związane z aktualizacją oprogramowania sprzętowego

Brak spójnych aktualizacji firmware i oprogramowania na urządzeniach IoT stanowi poważne zagrożenie bezpieczeństwa. Przestarzałe oprogramowanie sprzętowe może utrzymywać znane luki w zabezpieczeniach, zasadniczo pozostawiając otwarte drzwi dla napastników. Ale gdy aktualizacja wymaga fizycznego dostępu do każdego urządzenia, jej dostarczanie może być czasochłonne i kosztowne.

3. Zarządzanie urządzeniami i łącznością

Po wdrożeniu setek lub tysięcy urządzeń IoT, jak sprawdzić, czy urządzenia prawidłowo przesyłają dane do systemów i usług, które integrują? Liderzy projektów IoT potrzebują kompleksowej platformy, która pozwoli im zarządzać przepływem danych, uzyskiwać dostęp do informacji o połączeniach i otrzymywać powiadomienia, gdy urządzenie wykazuje nietypowe użycie lub problemy z połączeniem.

Liderzy IoT borykają się również z innymi problemami związanymi z bezpieczeństwem, w tym z domyślnymi lub takimi samymi hasłami, niewystarczającymi możliwościami szyfrowania i wyzwaniami związanymi z ręcznym uruchamianiem urządzeń.

Chociaż problemy z bezpieczeństwem IoT mogą być przytłaczające, to nie muszą takie być. Wiele zależy od znalezienia doświadczonego partnera z wiedzą i narzędziami, które zapewnią bezpieczne wdrożenie IoT.

Zestaw narzędzi bezpieczeństwa IoT

Firma Telit jako pionier i lider w zakresie produktów i oprogramowania IoT klasy korporacyjnej zapewnia szereg narzędzi zwiększających cyberbezpieczeństwo i skracających czas wprowadzania na rynek.

Jednym z przykładów jest uruchamianie typu zero-touch (bez dotykania), które umożliwia konfigurowanie urządzeń IoT z ustawieniami przechowywanymi w centralnym źródle. Gdy urządzenie pojawia się w sieci, jego ustawienia konfiguracyjne są instalowane automatycznie i zdalnie, zapewniając operatorom wdrożeń znacznie szybszą metodę wdrażania, jednocześnie minimalizując możliwość ataku.

Urządzenia IoT często są wyposażone w domyślne hasła, których użytkownicy nie zmieniają lub nie mogą zmienić, co czyni je szczególnie podatnymi na ataki. Wdrażanie typu zero-touch eliminuje potrzebę stosowania haseł, umożliwiając uwierzytelnianie urządzeń przy zachowaniu anonimowości, dzięki czemu osoby atakujące nie mogą uzyskać dostępu do informacji o uwierzytelnianiu urządzenia końcowego.

Automatyzacja konfiguracji urządzeń zmniejsza również złożoność zarządzania wdrożeniami i pomaga wyeliminować błędy charakterystyczne dla wdrożeń IoT o dużej skali. Ręczne wdrażanie wymaga znacznie więcej konfiguracji, od instalacji, przez ręczną konfigurację, po konfigurację zaplecza IT. Zero-touch eliminuje te opóźnienia i możliwości powstawania błędów, sprawiając, że urządzenia są w pełni funkcjonalne w kilka sekund po ich włączeniu. Administratorzy wdrożeń mogą regularnie dostarczać aktualizacje w dużych partiach, zapewniając, że urządzenia zawsze mają zainstalowane najnowsze poprawki zabezpieczeń.

Secure boot (bezpieczny rozruch) to kolejna funkcja zabezpieczeń na poziomie urządzenia, zapewnia ona, że tylko dostawca IoT, który wyprodukował moduł, tworzy oprogramowanie i je kontroluje. Jeśli haker spróbuje zmodyfikować oprogramowanie, moduł wyłączy się i stanie się bezużyteczny.

Moduły komórkowe Telit są zabezpieczane i „personalizowane" w momencie produkcji. Jeden z przykładów sprzętu to moduł 4G LTE-M/NB-IoT (Rel. 14) – ME310G1.
ME310G1 to ewolucja nowej rodziny produktów Telit xE310 z wbudowanym GNSS. Te moduły zapewniają wdrożenia IoT ze zoptymalizowanym zużyciem energii i zwiększonym zasięgiem. Przy wymiarach zaledwie 14,3×13,1 mm ME310G1 jest idealny do zastosowań IoT o ograniczonych rozmiarach. Opcjonalna możliwość awaryjnego połączenia z czterozakresowym 2G pozwala urządzeniom pozostać połączonymi, nawet gdy wychodzą z zasięgu LTE-M/NB-IoT.
ME310G1 umożliwia wdrażanie nowych projektów o małych rozmiarach zewnętrznych w wielu obszarach zastosowań, jak śledzenie przedmiotów, opieka zdrowotna, inteligentne pomiary, urządzenia przenośne, czujniki przemysłowe, automatyka domowa i wiele innych, korzystając z niskiego poboru mocy. Miniaturowa rodzina Telit xE310 obejmuje moduły 2G (GE310-GNSS), Cat M1/NB2 (ME310G1) i Wi-Fi/BLE (WE310F5) kompatybilne pin-to-pin, umożliwiając zaprojektowanie pojedynczego układu PCB i wdrożenie dowolnej kombinacji technologii 2G, 4G i krótkiego zasięgu. WE310F5 łączy Wi-Fi i Bluetooth Low Energy (BLE5), aby zapewnić niedrogie i szybkie rozwiązanie dla producentów urządzeń IoT, którzy chcą dodać łączność bezprzewodową do swoich aplikacji.

Kompleksowe zabezpieczenia IoT dzięki Telit OneEdge

Zero-touch i secure boot są częścią oprogramowania Telit OneEdge, wielokrotnie nagradzanego, innowacyjnego pakietu oprogramowania z wbudowanymi modułami, bezpiecznymi i łatwymi w użyciu narzędziami. OneEdge pozwala programistom uprościć projektowanie, wdrażanie i zarządzanie rozwiązaniem IoT, skracając czas wprowadzania na rynek i całkowity koszt posiadania. OneEdge zapewnia wszechstronne możliwości zarządzania urządzeniami. Umożliwiają one nadzorcom dostęp do danych o urządzeniu (np. modelu, numeru seryjnego, wersji sprzętu i oprogramowania, źródła zasilania, poziomu naładowania baterii i innych), zapewniając, że każde urządzenie ma najbardziej aktualne oprogramowanie, a także aplikację do monitorowania stanu i zdalnego rozwiązywania problemów.

Zdalne zarządzanie urządzeniami zapewnia prawidłowe i bezpieczne działanie urządzeń IoT po wdrożeniu. Ponieważ technicy nie muszą fizycznie odwiedzać urządzenia aby nim zarządzać lub go aktualizować, zmniejsza to wysiłek operacyjny wymagany do utrzymania floty urządzeń IoT.

OneEdge obejmuje również zarządzanie łącznością. Telit monitoruje łączność z siecią komórkową i jakość łącza każdego urządzenia, umożliwiając nadzorcy przeglądanie szczegółowych informacji o połączeniu z siecią komórkową za pośrednictwem bezpiecznego portalu internetowego.

Zapobiegaj cyberatakom, zanim się pojawią

Obawy związane z bezpieczeństwem IoT są uzasadnione, ale nie muszą zakłócać planów wdrożenia IoT. Ważne, aby podejmować odpowiednie wewnętrzne środki bezpieczeństwa i znaleźć partnera, który zapewni narzędzia i wiedzę, które pomogą zbudować bezpieczne i skalowalne rozwiązanie.