Cyberdefence 24

aut. Andrzej Kozłowski 08.01.2021

ERICSSON: BEZPIECZEŃSTWO TO ODPOWIEDZIALNOŚĆ CAŁEGO PRZEMYSŁU

"Bezpieczeństwo nie może być zaniedbywane i konieczne jest podejmowanie odpowiednich środków zapobiegających. Podłączając urządzenia do sieci, chcemy mieć pewność, że są one bezpieczne i możemy im zaufać" mówi Bodil Josefsson, Head of IoT Security w Ericssonie.

Dlaczego internet rzeczy będzie przełomem? Jakie korzyści przyniesie ta technologia?

Nagły wzrost urządzeń internetu rzeczy (IoT) jest niewątpliwym elementem postępującej cyfryzacji społeczeństwa, która polega m.in. na podłączaniu coraz większej liczby rzeczy do Internetu. Zmienia to na przykład nasze życie, pracę przemysłu i sposób w jaki urządzenia się ze sobą komunikują. To jest prawdziwy przełom, który wpłynie na funkcjonowanie społeczeństwa.

5G jest fundamentem tej transformacji, który de facto pozwala na dokonanie tych zmian. Dzięki temu nasze sieci mają o wiele większe zasoby oraz możliwości, są jeszcze bardziej odporne i darzymy je większym zaufaniem. Możemy podłączyć więcej urządzeń dzięki większej przepustowości oraz mieć mniejsze opóźnienie. Nie mam żadnych wątpliwości, że 5G to przełom.

Internet rzeczy jest już wdrażany na całym świecie. Jakie rozwiązania udało się zaimplementować Ericssonowi w tym obszarze?

Ericsson zapewnia łączność oraz sprzęt do sieci mobilnych operatorom telekomunikacyjnym. Mamy rozwiązanie: Ericsson IoT Accelerator i jest to platforma do zarządzania łącznością, którą hostujemy, sprzedajemy telekomom oraz oferujemy w modelu platforma jako usługa. Dzięki temu urządzeniu operatorzy telekomunikacji mogą sprzedać łączność IoT swoim klientom biznesowym. Można to podsumować w skrócie, że my sprzedajemy te technologie do telekomów, a oni oferują je firmom.

Przechodząc do głównego tematu naszej rozmowy jakim jest bezpieczeństwo IoT. W mediach wiele uwagi poświęca się apokaliptycznym scenariuszom związanym z tą technologią. Czy Pani uważa, że faktycznie mamy się czego obawiać? Jakie największe zagrożenia wiążą się z rozwojem IoT?

Musimy wyjaśnić klika aspektów, które powinny zostać wzięte pod uwagę. Po pierwsze, będziemy mieli o wiele więcej urządzeń podłączonych do Internetu. Jak już powiedziałam, obserwujemy zdecydowany wzrost zainteresowania internetem rzeczy. Ericsson w Mobility Report przewiduje, że będzie 27 miliardów urządzeń podłączonych do Internetu w 2026 roku i 6 miliardów z nich będzie bazowało na technologii komórkowej**.**

Taki zdecydowany wzrost ilości podłączonego urządzeń stanowi ogromne wyzwanie z punktu widzenia bezpieczeństwa. Wiele z tych urządzeń będzie miało ograniczoną pamięć, moc obliczeniową i dlatego może nie być zdolna do sprostania wymaganiom bezpieczeństwa, które stosujemy do komputerów

czy smartfonów. Należy pamiętać, że będą one jednak podłączone do sieci i chcemy uniknąć sytuacji, że ktoś wykorzystując ich słabość, przejmuje nad nią kontrolę. Dlatego ważne jest zapewnienie odpowiedniej ochrony tak, aby zmniejszyć to ryzyko.

Ilość urządzeń podłączonych do Internetu oraz ich możliwa niezdolność do sprostania wymaganiom bezpieczeństwa stanowi wyzwanie dla ekspertów od bezpieczeństwa i musimy o to zadbać. Dlatego też bezpieczeństwo komponentów krytycznych jest takie ważne. Dużo w tym obszarze daje również sieć 5G, która jest bezpieczniejsza od swoich poprzedników i ma wiele wbudowanych nowych funkcji.

Musimy wszystkie zagrożenia brać na poważnie, nawet te, które mogą wydawać się nieco przesadzone. Bezpieczeństwo nie może być zaniedbywane i konieczne jest podejmowanie odpowiednich środków zapobiegających. Podłączając urządzenia do sieci, chcemy mieć pewność, że są one bezpieczne i możemy im zaufać. W takim przypadku normy 3rd Generation Partnership Project (3GPP) są bardzo ważnym elementem bezpieczeństwa infrastruktury i podstaw łączności. Ważne jest również to, żeby podłączany sprzęt był bezpieczny i budowany w ramach koncepcji *security by design*. Firmy muszą być również świadome konieczności inwestycji w bezpieczeństwo kluczowych elementów i wydatków, które są z tym związane.

Jeśli te środki zapobiegawcze nie zostaną wdrożone oraz jeżeli nie będziemy przyłączać urządzeń w bezpieczny sposób do sieci to oczywiście istnieje ryzyko. Moim zdaniem kadra zarządzająca przedsiębiorstwami jest coraz bardziej świadoma tych narastających zagrożeń, dlatego też będą zwracali uwagę na tę kwestię. W szczególności przemysł tzw. connected cars jest bardzo świadomy tych ryzyk i niezwykle uważny przy wdrażaniu nowych systemów.

Wzrost liczby urządzeń to również o wiele większe wolumeny danych, które są wymieniane między nimi. Jak sobie z tym poradzić?

Oczywiście dane muszą być bezpieczne. Trzeba zapewnić ich integralność oraz poufność w trakcie magazynowania jak i przekazywania. Jesteśmy zaangażowani w ten proces, na przykład w zakresie szyfrowania danych i kontroli dostępu. Należy podkreślić, że bezpieczeństwo to odpowiedzialność całego przemysłu, operatorów, dostawców, a nie tylko Ericssona.

Co powinniśmy zrobić, żeby rozwinąć internet rzeczy jak najszybciej to możliwe, ale jednocześnie nie zaniedbując kwestii bezpieczeństwa?

Po pierwsze, musimy się zastanowić w jaki sposób połączymy urządzenia oraz jaką wykorzystamy do tego technologię. Stosując technologię komórkową do łączenia urządzeń, zapewniamy właściwy poziom bezpieczeństwa. Następnie dodajemy bezpieczne produkty sieciowe opracowane według zasady security-by-design. Kolejną warstwą jest bezpieczeństwo samych urządzeń internetu rzeczy. Jest wiele firm oferujących takie rozwiązania, ale musimy wybrać tę najbezpieczniejszą, która poradzi sobie z ochroną urządzeń oraz usług i zapewnia m.in. np. szyfrowanie i odpowiednią ochronę danych. Muszą one być bezpieczne oraz polegać na metodzie autoryzacji np. za pomocą kart SIM, tak jak ma to miejsce w sieciach komórkowych. Identyfikacja urządzenia jest bardzo ważnym elementem zapewnienia bezpieczeństwa.

W jaki sposób zapewnić bezpieczeństwo identyfikacji podłączanych urządzeń?

Wszystkie podłączone urządzenia internetu rzeczy powinny posiadać swój identyfikator. Musimy wiedzieć czy podłączyliśmy autonomiczny samochód czy smart meter, gdzie to zrobiliśmy i jak oraz, że nie ma możliwości ich sklonowania czy zhakowania.

Jakie działania podejmuje Ericsson, aby zabezpieczyć internet rzeczy?

Zapewnia telekomom infrastrukturę - Ericsson IoT Accelerator - aby ułatwić zarządzanie łącznością. Akcelerator IoT jest platformą, która została opracowana zgodnie z zasadami "security-by-design". Do Akceleratora IoT dodajemy usługę bezpieczeństwa służącą do monitorowania i ograniczania zagrożeń (usługi Threat Monitoring and Mitigation), która pozwala na zmniejszenie ryzyk cyberbezpieczeństwa. Umożliwiamy w ten sposób operatorom obserwowanie tego, co dzieje się w ich sieciach IoT, obniżając ryzyko ataku czy wskazując ewentualne anomalie w działaniach, co mogłoby być znakiem potencjalnego nieautoryzowanego dostępu.

Usługi Threat Monitoring and Mitigation bazują na Ericsson Security Manager, czyli platformie automatyzacji bezpieczeństwa. To narzędzie jest odpowiedzialne za ochronę zasobów, jak również wykrywanie niebezpieczeństw i reagowanie na ataki. Oferujemy je telekomom np. Swisscom jest jednym z głównych klientów używających tego rozwiązania od prawie 2 lat. Wykorzystywane jest ono do ochrony infrastruktury telekomunikacyjnej. Ericsson Security Manager to horyzontalne narzędzie, które może zostać użyte w wielu sytuacjach jak np. do wspomnianej już ochrony sprzętu telekomunikacyjnego, sprawdzając czy spełnia on standardy bezpieczeństwa i jest odpowiednio zabezpieczony oraz czy wprowadzone zostały odpowiednie rozwiązania i polityki bezpieczeństwa w sieciach.

Ericsson Security Manager używamy także w dedykowanych sieciach. Ostatnio rozwiązanie to zostało zakupione przez dostarczyciela usług sieciowych w Finlandii, który oferuje ją m.in. instytucjom publicznym czy służbom ratunkowym. Podmioty te potrzebują sieci i urządzeń o podwyższonym standardzie bezpieczeństwa. Ericsson dostarcza im 5G Core, NFVI oraz usługi Dynamic Orchestration.

W jaki sposób połączyć bezpieczeństwo sieci 5G i internetu rzeczy?

Wieloletnia wizja Ericssona dotycząca połączonego społeczeństwa stała się w ostatnich latach rzeczywistością, a systemy mobilne stanowią podstawę zarówno dla internetu rzeczy (IoT), jak i szybko rosnącego zakresu usług cyfrowych. Wierzymy, że cyfryzacja będzie nadal zmieniać nasz przemysł, życie i społeczeństwo. System 5G umożliwi wiele nowych zastosowań, dzięki którym krytyczna rola systemów mobilnych stanie się jeszcze bardziej widoczna niż obecnie. Połączone urządzenia i aplikacje mobilne wymagają bezprzewodowego dostępu do sieci, która jest odporna, bezpieczna i zdolna do ochrony prywatności osób, a system 5G został zaprojektowany z myślą o tych wymaganiach.

5G to najnowsza generacja łączności komórkowej i wnosi ulepszenia do wcześniejszych generacji, przede wszystkim bardzo małe opóźnienia i wysoką przepustowość. Nie w każdym przypadku potrzebujemy takiej sieci, ponieważ część usług i serwisów może funkcjonować w oparciu o 3G i 4G, ale infrastruktura krytyczna i krytyczne usługi, nie mogą poprawnie funkcjonować bez niskich opóźnień oraz nie poradzą sobie bez 5G. Jeżeli podłączamy robota w przemyśle czy w kopalni, wtedy potrzebujemy tej technologii. Umożliwia ona o wiele więcej praktycznych zastosowań różnych rozwiązań z wykorzystaniem IoT**.** Dzięki bardzo małym opóźnieniom, możliwości transmisji olbrzymiej ilości danych oraz wysokiemu poziomowi bezpieczeństwa. Internet rzeczy i 5G są ze sobą połączone, ale nie zawsze potrzebujemy sieci najnowszej generacji do podłączenia urządzeń internetu rzeczy.

[Oferta Sklepu Defence24]