aut. Andrzej Kozłowski 27.11.2019

CO PRZYNIESIE IOT? DUŻE PIENIĄDZE, ALE I KATASTROFALNE SKUTKI POTENCJALNYCH ZANIEDBAŃ

„Wymiana informacji o zagrożeniach w czasie rzeczywistym to klucz do bezpieczeństwa IoT" – powiedział Przemysław Kania, Managing Director, Cisco Polska podczas panelu zatytułowanego Secure & Resilient Industrial IoT (IIoT) – Mission Achievable na konferencji CYBERSEC 2019. Paneliści próbowali odpowiedzieć na pytanie czy zabezpieczenie Internetu rzeczy jest w ogóle możliwe.

W panelu udział wzięli: Przemysław Kania – Managing Director, Cisco Polska, Steve Purser – Head of Core Operations, ENISA; Bonnie Butlin – Co-founder & Executive director, Security Partners' Forum; Patrick Donahue – Director of Product, Cloudflare; Adam Roś – Samsung VP, R&D Institute Europe; Moderatorem był Patrick Tucker – Technology Editor, Defense One.

Do 2030 roku IoT ma dodać tryliony dolarów do światowej gospodarki, dlatego nie trzeba nikogo przekonywać jak ważna jest ta rewolucja, padło na rozpoczęcie debaty. "Kiedy mówimy o zabezpieczaniu IoT, jakie są największe ryzyka i wyzwania?" - zapytał Patrick Tucker Technology Editor, Defense One

„W CISCO, obserwujemy ostatnio bardzo wiele interesujących zjawisk, ze względu na fakt, że mamy przywilej współpracy z dużymi, średnimi i małymi przedsiębiorstwami od wielu lat. Pracujemy z nimi nad zabezpieczeniem sieci komputerowych. To co obserwujemy teraz, to trend podłączania sieci produkcyjnych OT (Operational Technology – przyp. red.), do Internetu, tak jak miało to miejsce w przypadku tradycyjnych sieci IT. Środowisko, do którego są one podłączane jest bardzo chaotyczne i niebezpieczne. Wprowadzanie podstawowych zasad bezpieczeństwa w tym środowisku jest kluczowe" - powiedział Przemysław Kania, dyrektor zarządzający Cisco Polska.

Adam Roś podzielił się spostrzeżeniami jak Samsung podchodzi do rewolucji IoT. „Koreański gigant produkuje ponad milion urządzeń elektronicznych codziennie, co daje prawie ponad pół miliarda urządzeń rocznie w fabrykach na całym świecie. Dlatego cyberbezpieczeństwo musi być częścią DNA firmy" – podkreślił. Przedstawiciel Samsunga zwrócił również uwagę, że IoT zwiększa tzw. powierzchnię ataku. Atakowanie urządzeń np. sensorów IoT czy systemów kontroli przemysłowej może w konsekwencji, w jego opinii, doprowadzić do katastrofy. „Innym ważnym aspektem jest kradzież tajemnic handlowych i technologii np. przemysłu półprzewodników. Rozwój takiej technologii, to wydatki sięgające dziesiątek milionów dolarów. Jeżeli ktoś je od nas ukradnie to straty są ogromne i mogą doprowadzić nawet do upadku biznesu" – zakończył Adam Roś.

„Podłączone do sieci urządzenia mają często wiele luk bezpieczeństwa, które są dobrze znane i do których istnieją już łatki. Proces aktualizacji oprogramowania milionów urządzeń jest jednak czasochłonny i bardzo trudny" – powiedział Patrick Donahue. Przedstawiciel Cloudflare przypomniał również atak na Stuxnet, kiedy to inżynierowie otrzymywali informacje, że wszystko pracuje sprawnie,

podczas gdy maszyny się psuły. Kończąc swoją wypowiedź ostrzegł, że manipulacja sensorami może doprowadzić do poważnych strat finansowych.

Z przedmówcą zgodził się Przemysław Kania z Cisco, który podkreślił, że musimy sobie zdać sprawę, że wszystkie zjawiska, o których mówimy, zachodzą w czasie rzeczywistym na masową skalę i mogą mieć dewastujący wpływ. Przedstawiciel Cisco zaproponował również rozwiązanie. „Nowoczesna architektura bezpieczeństwa musi być nieustannie podłączona do bazy wiedzy o zagrożeniach w czasie rzeczywistym. Rzeczy podłączone do Internetu muszą ze sobą rozmawiać, a zabezpieczenia powinny wykorzystywać techniki uczenia maszynowego w celu uczynienia środowiska IoT bezpieczniejszym" – powiedział. „W Cisco mamy ludzi, którzy monitorują ruch w sieci, widzą nowe zagrożenia, setki ataków i miliony nowych próbek złośliwego oprogramowania codziennie. Mogą aktualizować urządzenia na całym świecie o ten nowe informacje. Moim zdaniem to jest właśnie rozwiązanie problemów, o których mówimy. Musimy dzielić informacje pomiędzy maszynami w czasie rzeczywistym, ponieważ model, w którym dzieje się to już po wykryciu zagrożenia jest niewystarczający" - dodał.

Należy również spojrzeć na rozwój infrastruktury informacyjnej w ostatnich 25 latach „Rozwinęła się ona w tak szybkim tempie, że obecnie nie wiemy, gdzie znajduje się część naszych urządzeń podłączonych do Internetu, których są setki milionów, dlatego tak trudne jest ich zabezpieczenie. Po drugie, produkty te muszą być jak najszybciej dostarczone na rynek, co prowadzi do sytuacji, że nie ma czasu na sprawdzenie ich pod kątem bezpieczeństwa" – podkreślił Steve Purser z ENISY

Dyskutując o kwestiach związanych z IoT nie zabrakło pytania o rolę sieci 5G oraz jej zabezpieczenie. Przemysław Kani wskazał, że architektura 5G będzie o wiele bardziej rozpowszechniona niż poprzednie sieci telekomunikacyjne. Dlatego też będzie je o wiele trudniej zabezpieczyć. Jego zdaniem rozwiązaniem mogłoby być budowanie sieci 5G w najbardziej otwarty sposób, z punktu widzenia wymiany informacji o zagrożeniach pomiędzy podmiotami budującymi 5G.

Na zakończenie dyskusji, moderator zapytał przedstawiciela Cisco o rozbudowane relacje biznesowe z Chinami. „W Cisco zajmujemy neutralne stanowisko w obecnej sytuacji geopolitycznej, która ma miejsce pomiędzy USA i Chinami. Chcemy przede wszystkim dawać najwyższą jakość usług naszym klientom – zakończył swoją wypowiedź Kania.

Czytaj też: Infrastruktura krytyczna coraz bardziej zagrożona. Nawet elektrownie atomowe nie są bezpieczne [WIDEO]