

Hakerzy czyhają na samochody

data aktualizacji: 2017.05.12



Producenci samochodów w Europie przeznaczają rocznie na innowacje ponad 44 miliardy euro - według danych z Automotive Industry Report 2016. Firmy z branży motoryzacji planują swój strategiczny wzrost i rozwój, stawiając na nowe technologie związane z inteligentnymi i autonomicznymi pojazdami. Ekspertsi przewidują, że rynek zmieni się w ciągu kilku kolejnych lat bardziej niż kiedykolwiek, co przełoży się na istotne przemiany funkcjonujących w nim modeli biznesowych oraz wywoła bezprecedensowe wyzwania.

Komputery na kołach

Mają ponad 100 milionów linii kodu oraz ponad 100 różnych jednostek sterujących równocześnie przetwarzających dane. Co więcej, ich liczba zauważalnie rośnie, a one odgrywają coraz istotniejszą rolę w ramach segmentu internetu rzeczy (IoT). Oczywiście mowa o autonomicznych samochodach. Tego typu maszyny niosą ze sobą obietnicę wielu ekonomicznych i społecznych korzyści. Jednak w parze z nimi idą nowe zagrożenia, na które rynek motoryzacji nadal nie jest wystarczająco przygotowany.

Kiedy latem 2015 roku dziennikarz Andy Greenberg wsiadał do Jeepa Cherokee nie spodziewał się, że w konsekwencji Chrysler wycofa z rynku 1,4 miliona pojazdów. Podczas przejażdżki autostradą, nagle i bez ingerencji kierowcy wycieraczki zaczęły chodzić, radio zmieniło stację, a klimatyzacja zaczęła wyrzucać z siebie lodowate powietrze. Na dodatek próba wyłączenia urządzeń spełzała na niczym. Wszystko za sprawą dwóch legalnie działających hakerów, którym w ramach eksperymentu udało się zdalnie przejąć kontrolę nad pojazdem. To wtedy po raz pierwszy pojęcie carhackingu odbiło się szerokim echem po świecie.

- Od tamtej pory branża motoryzacyjna musiała na nowo przemyśleć swoje strategie zapewnienia bezpieczeństwa, szczególnie przyglądając się od nowa całemu procesowi

produkcji inteligentnych aut. Samochody coraz bardziej przypominają już nie tylko komputery, lecz całe sieci komputerowe. Są podłączone do internetu, komunikują się ze sobą, korzystają z licznych aplikacji. Konsekwencją podłączenia do internetu może być jednak otworenie drzwi dla potencjalnych hakerów, a najczarniejsze scenariusze ataku obejmują utratę kontroli nad hamulcami, silnikiem, czy wręcz całym pojazdem – mówi Marek Puchalski ekspert ds. bezpieczeństwa z Capgemini Software Solutions Center.

Zagrożenie na każdym etapie produkcji

Cyberbezpieczeństwo w motoryzacji staje się więc priorytetowym zagadnieniem dla tej branży. Nie tylko ze względu na możliwe ataki hakerskie na samochody w trakcie ich użytkowania. Problem zapewnienia bezpieczeństwa samochodów wymaga przemyślenia i przeorganizowania całego procesu produkcyjnego ze szczególnym uwzględnieniem fabryk i innych miejsc, w których samochody i ich części są wytwarzane.

Kai Grambow, Global Head of Automotive w Capgemini,: "Wszyscy, którzy pracują dla firm motoryzacyjnych, zdają sobie sprawę, jak ważne jest cyberbezpieczeństwo - poczynając od pracowników, aż do dyrektorów zarządzających. Nieudana próba udaremnienia ataku może oznaczać masowe zwroty zakupionego towaru, utracone dochody, grzywny regulacyjne, a nawet zagrożenie dla bezpieczeństwa klienta."

Mądre zarządzanie ryzykiem związanym z tym zjawiskiem zakłada ocenę bezpieczeństwa poprzez audyt, projektowanie strategii zabezpieczeń oraz wdrożenie odpowiednich procedur. Firma Capgemini, globalny lider konsultingu i outsourcingu, wprowadziła te elementy do swojej oferty rozwiązań dedykowanych producentom samochodów oraz ich dostawcom. Dodatkowo zapewnia organizacjom dostęp do sieci centrów bezpieczeństwa SOC (Security Operation Center) Capgemini, które świadczą szereg wyspecjalizowanych usług związanych z monitorowaniem pojazdów i ich produkcji. Przeprowadza również mini ataki hakerskie sprawdzające działanie aplikacji samochodowych jeszcze przed masowym wdrożeniem ich w pojazdach.

Źródło: