Przestępczy potencjał samochodów autonomicznych

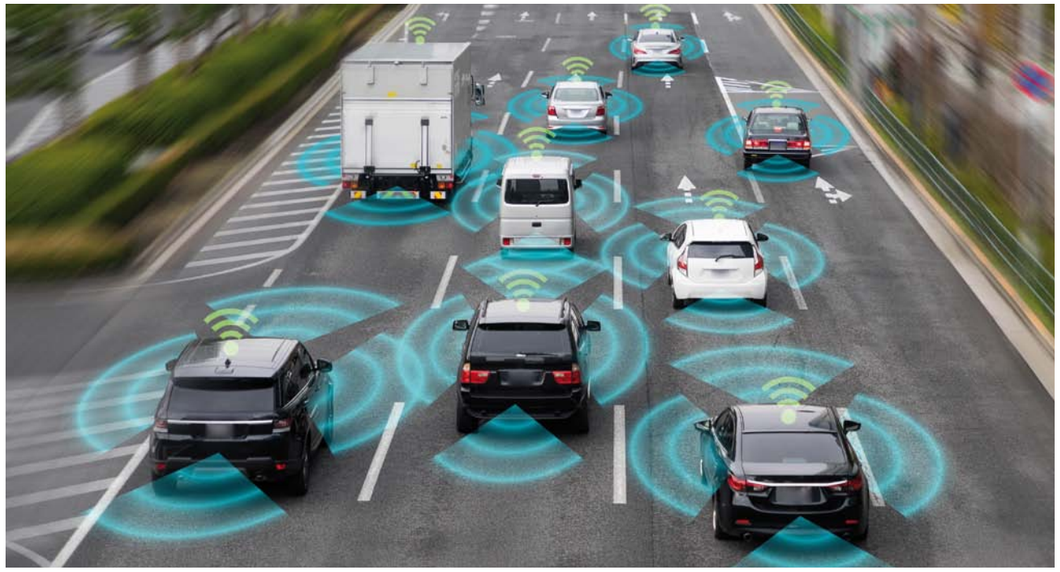
Szansa czy zagrożenie?

Aleksander Kostuch
Ekspert bezpieczeństwa Stormshield – europejskiego wytwórcy rozwiązań z obszaru bezpieczeństwa IT

Samochody autonomiczne to temat, który w ostatnim czasie przyciąga uwagę całego świata. Jednak nim w pełnym wymiarze zaczniemy korzystać z nowych technologii, eksperci z dziedziny cyberbezpieczeństwa ostrzegają przed zagrożeniami związanymi z potencjalnym wykorzystaniem tych pojazdów do celów przestępczych

Era pojazdów autonomicznych oznacza konieczność szczególnej dbałości o bezpieczeństwo cybernetyczne. Ponieważ stosowane obecnie rozwiązania nie są wystarczające, firmy z branży motoryzacyjnej powinny podjąć działania minimalizujące ryzyko ataków hakerów.

Wraz z rozwojem technologii, samochody stają się coraz bardziej zautomatyzowane, a implementacja systemów cyfrowych już dziś przynosi wiele korzyści. Kolejnym etapem w rozwoju motoryzacji będzie autonomiczność, która zmieni oblicze transportu. Firmy takie, jak Google, Tesla, Waymo czy Uber, coraz śmielej testują samojezdne pojazdy na drogach publicznych. Wkład w rozwój technologii mają również polskie firmy, na przykład start-up Blees z Gliwic, która konstruuje autonomiczny autobus. Wraz z testami pojawiają się prognozy dotyczące tego segmentu rynku. Według International Data Corporation do 2040 roku liczba autonomicznych pojazdów przekroczy 30 milionów i będą one spotykanie nie tylko w Kalifornii – kolebce autonomicznej jazdy – lecz na całym świecie.



Fot. topgear.com

Ataki hakerskie

Podłączenie pojazdów do sieci otwiera pole do działania dla cyberprzestępców. Pierwsze przypadki ataków hakerskich na systemy samochodowe miały miejsce już kilka lat temu. W 2015 roku, dwóch hakerów w ramach eksperymentu w łatwy sposób przejęło kontrolę nad samochodem marki Jeep Cherokee, wykorzystując lukę w oprogramowaniu. W wyniku ataku, hakerzy uzyskali kontrolę nad systemami klimatyzacji, hamulcami, pedałem gazu oraz radiem.

W maju bieżącego roku Toyota poinformowała o innym incydencie: przez ponad pięć miesięcy zasób chmurowy niewymagający autoryzacji żadnym hasłem był powszechnie dostępny. Zawierał ID samochodu, lokalizację auta oraz nagrania z zewnętrznych kamer samochodów. Dane mogły dotyczyć aż 2 milionów pojazdów, których użytkownicy subskrybowali usługi: T-Connect/G-Link/G-Link Lite/G-Book.

Śmiercionośny potencjał

Obecna sytuacja geopolityczna na świecie ukazuje potencjał możliwości nowych technologii. W konflikcie w Ukrainie drony są stałym elementem pola walki zbrojnej. Z kolei w mediach pojawiają się fake newsy tworzone w oparciu o sztuczną inteligencję. Samojezdne pojazdy mogą oferować duże możliwości na polu walki i poza nim. Nietrudno sobie wyobrazić auto przewożące ładunki wybuchowe lub inne niebezpieczne materiały. Cyberprzestępcy mogą również wykorzystać samochody do przemytu narkotyków albo broni, a nawet przeprowadzać ataki terrorystyczne. Wreszcie przejęty przez hakerów samochód może stać się narzędziem do szpiegowania i monitorowania.

Dlatego tak ważne jest, aby branże wykorzystujące autonomiczne technologie, w tym przemysł motoryzacyjny, miały świadomość konieczności większej niż dotychczas dbałości o bezpieczeństwo cybernetyczne. Nadchodząca era pojazdów autonomicznych wymaga szczególnej uwagi w tym zakresie. W sytuacji, gdy samochody mogą być zdalnie kontrolowane, cyberprzestępcy zyskują możliwość wykorzystania ich do własnych celów.

Cybernetyczne wyzwanie

Zapewnienie bezpieczeństwa w branży motoryzacyjnej zawsze było jednym z najważniejszych aspektów. Jednak wraz z upowszechnianiem pojazdów autonomicznych pojawia się wiele nowych wyzwań. Hakerzy, którzy potencjalnie przejmą kontrolę nad systemami pojazdów, mogą nie tylko zagrażać zdrowiu i życiu pasażerów, ale także stanowić zagrożenie dla ruchu drogowego. Dlatego konieczne jest opracowanie nowej polityki, która pozwoli stworzyć bardziej bezpieczną przestrzeń w branży motoryzacyjnej. Niezbędne są nowe regulacje oraz wdrażanie ulepszonych środków bezpieczeństwa przez producentów samochodów. Regulacje prawne powinny jasno określać odpowiedzialność producentów za cyberbezpieczeństwo pojazdów autonomicznych, w tym za zapewnienie aktualizacji i łatek oprogramowania w przypadku wykrycia zagrożeń.

Wymaga to współpracy między producentami samochodów, dostawcami oprogramowania oraz organami regulacyjnymi. Konieczne jest ustanowienie standardów bezpieczeństwa, audytów i testów, które będą obowiązujące dla wszystkich producentów samochodów. Bezpieczeństwo powinno być wprowadzane już na etapie projektowania i produkcji, a nie tylko w formie reakcji na istniejące zagrożenia. Wprowadzenie zabezpieczeń nie tylko fizycznych i technologicznych, lecz również takich, jak systemy wykrywania i ochrony przed atakami, aktualizacje zdalnego oprogramowania, separacja systemów wewnątrz pojazdu, powinno być integralną częścią procesu tworzenia samochodów.

W planowaniu powinny zostać określone trzy kluczowe obszary:

- **Ścisła separacja systemów** w pojazdach autonomicznych. Każdy system, zarówno ten związany z jazdą autonomiczną, jak i pozostałe (np. komunikacja i rozrywka), powinny być od siebie odizolowane, aby zapobiec potencjalnemu przenoszeniu się ataków. Bezpośrednie połączenie z siecią Internet w trakcie słuchania muzyki, nawigacji czy streamingu również sprzyja bezpośrednim atakom.

W sierpniu 2022 japoński programista ogłosił, że udało mu się uruchomić własne oprogramowanie w pokładowym systemie rozrywkowym IVI (*In-Vehicle Infotainment*) w samochodzie Hyundai Ioniq SEL z 2021 r. Odkrył on, że producent pojazdu zabezpieczył system Hyundai Mobis za pomocą kluczy, które były publicznie znane i dostępne w Internecie.

- **Procedury wprowadzania aktualizacji oprogramowania**. Systemy te powinny być tak zaprojektowane, aby zapewnić bezpieczeństwo i niepodatność na ataki w trakcie procesu aktualizacji. Po wykryciu luki w zabezpieczeniach, należy mieć możliwość sprawnego informowania i szybkiego reagowania na nowe zagrożenia. W 2017 roku (publicznie informację tę ogłoszono we wrześniu 2020) badacz podatności odkrył, że samochody Tesli łączyły się z siecią, wykorzystując OpenVPN. Okazało się, że te uniwersalne klucze dawały dostęp do każdego samochodu. Korzystając z API, można było np. lokalizować, otwierać czy uruchamiać dowolny samochód Tesli.
- **Implementowanie zaawansowanych systemów monitorowania** pozwalające identyfikować nietypowe aktywności i próby ataków.

Aby uniknąć zagrożeń, producenci samochodów i organy rządowe muszą wyprzedzać rozwój technologii, tworząc nowe rozwiązania i regulacje prawne. Powinny one obejmować procedury audytów i testów koniecznych na etapie projektowania, produkcji i użytkowania pojazdów pod kątem zagrożeń cybernetycznych.

Funkcjonujący obecnie Audyt IATF 16949 (będący międzynarodowym standardem jakości stosowanym w branży motoryzacyjnej) uwzględnia elementy związane z cyberbezpieczeństwem, choć nie jest to główny obszar ooceny. Audyt obejmuje sekcję, w której znajdują się wymagania dotyczące systemów informacji, w tym cyberbezpieczeństwa.

Zarówno wśród konsumentów, jak i pracowników branży motoryzacyjnej należy promować świadomość cyberbezpieczeństwa. Kierowcy powinni być uświadamiani o zagrożenich i uczeni odpowiednich praktyk, a pracownicy motoryzacyjni – przeszkoleni w zakresie identyfikacji i zarządzania ryzykiem cybernetycznym. Sensowne byłoby utworzenie wspólnych platform i mechanizmów wymiany informacji na temat zagrożeń i incydentów cyberbezpieczeństwa w branży motoryzacyjnej. ■