

Używane samochody oczkiem w głowie hakerów



Hakerzy chcąc pozyskać poufne dane o naszym życiu, numerach telefonów, treści przesyłanych SMS lub danych nie muszą już dokonywać skomplikowanych ataków na komputer, telefon czy skrzynkę mailową. Nasz samochód sprzedany innej osobie jest kopalnią wiedzy i danych o naszym prywatnym życiu – ujawnia analiza European Security Group i firmy Check Point Software.

- Numery telefonów, SMS, dane lokalizacyjne z używanych samochodów wpadają w ręce niepowołanych osób
- Tylko 1 na 10 kierowców aut leasingowych usuwa dane z pamięci auta
- Ponad 300.000 aut na rynku wtórnym co miesiąc w Polsce
- Ponad połowa kierowców nie ma pojęcia o zagrożeniu ich danych osobowych po sprzedaży auta
- Większość leasingowanych pojazdów ma synchronizowane dane GPS, związane z firmowymi podróżami oraz prywatne dane użytkowników, do których przypisane jest firmowe auto

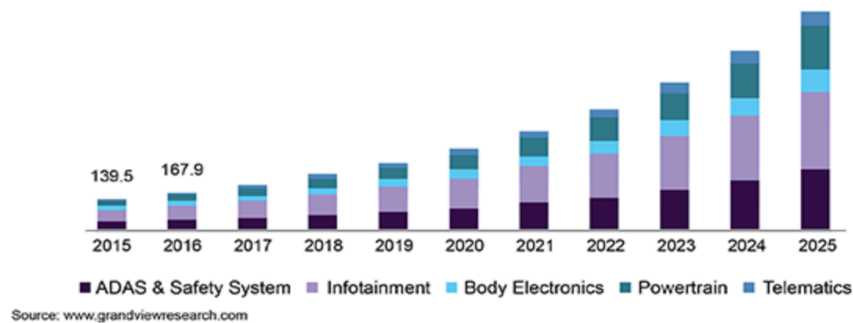
Samochody są coraz bardziej zaawansowane technologicznie i powiązane ze światem zewnętrznym. Funkcje, które kiedyś były dostępne tylko w luksusowych markach premium, są teraz dostępne praktycznie we wszystkich podstawowych samochodach miejskich. Funkcje te obejmują łączność Bluetooth do parowania telefonów komórkowych, nawigację GPS, hotspoty Wi-Fi, systemy unikania kolizji, zdalną diagnostykę i wiele innych. Dzięki tym możliwościom samochody szybko stają się bazami danych na kołach – zaznacza Wojciech Głazewski, przedstawiciel Check Point Software Technologies.

Skala zagrożenia utratą poufnych danych w przypadku samochodów z drugiej ręki lub poleasingowych jest przerażająca. Na polskim rynku co miesiąc pojawia się ok. 300 tysięcy ofert samochodów używanych. Tylko w marcu 2021r. rynek samochodów używanych w Polsce obejmował 248 612 ofert sprzedaży pojazdów i było to o 33 854 aut więcej niż w lutym br., wynika z raportu AAA Auto, opartego na analizie danych dotyczących sprzedaży aut używanych w komisach, na stronach internetowych oraz u dealerów samochodów używanych.

Jak wynika z obserwacji PZDM, zaledwie 1 na 10 właścicieli samochodów leasingowych oddaje pojazd usuwając zapamiętane dane z pamięci wewnętrznej auta. Znakomita większość używanych (3-4 letnich) aut, będących w ofercie na rynku wtórnym posiada w komputerze pokładowym informacje o książkach telefonicznych poprzednich właścicieli, destynacjach wprowadzonych podczas użytkowania, ulubionych wykonawcach i utworach czy treści wysyłanych wiadomości SMS – podkreśla Leszek Cieloch z European Security Group (ESG), członek zarządu Polskiego Stowarzyszenia Dziennikarzy Motoryzacyjnych (PSDM).

Największy rynek cyberbezpieczeństwa samochodowego w USA był wart 1,44 mld USD w 2018 roku i będzie rósł w tempie powyżej 20 proc. rocznie do 2025 roku – oceniają eksperci firmy Grand View Research. Automatyzacja procesów i rosnąca popularność autonomicznych pojazdów zwiększa skalę zagrożeń dla rynku motoryzacyjnego i ryzyka naruszenia danych przez hakerów. **Co ciekawe, najszybciej rosnącą kategorią rynku motoryzacyjnego na największym rynku na świecie (USA) ma być właśnie system informacyjno-rozrywkowy (Infotainment), odpowiedzialny za przechowywanie większości informacji z naszych urządzeń mobilnych, które podłączamy do auta.**

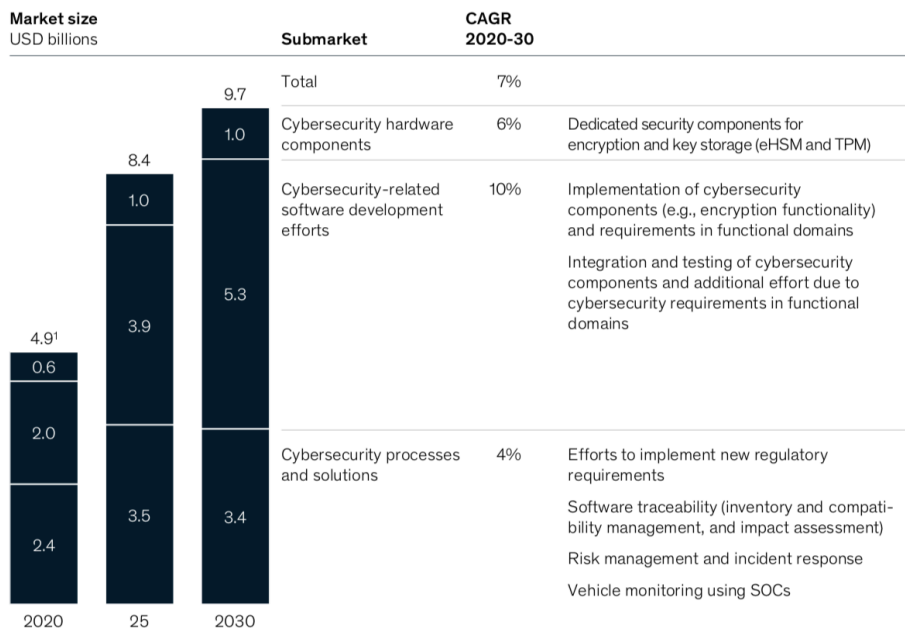
U.S. automotive cyber security market size, by application, 2015 - 2025 (USD Million)



Dzisiejszy samochód to maszyna z większą liczbą linii kodu niż nowoczesny odrzutowiec pasażerski. Dzisiejsze samochody i ciężarówki z łączem internetowym mogą dostarczać raportu o pogodzie, płacić za paliwo, znajdować miejsce parkingowe, omijać korki i słuchać stacji radiowych z całego świata. Wkrótce będą ze sobą rozmawiać, ostrzegać o wypadkach, gdy mijamy ulubione sklepy, a pewnego dnia nawet same poprowadzą (autonomiczne auta).

I choć konsumenci mogą kochać te funkcje, hakerzy doceniają je jeszcze bardziej.... To spędza sen z oczu wielu specjalistów branży motoryzacyjnej, którzy obawiają się blokady lub masowych kradzieży poufnych danych i dostępu do pojazdów przez nieupoważnione osoby.

Wyzwanie to może okazać się większe niż zabezpieczenie światowych linii lotniczych. Według raportu McKinsey & Company 2020 na temat cyberbezpieczeństwa w motoryzacji, nowoczesne pojazdy zawierają około 150 elektronicznych jednostek sterujących i około 100 milionów linii kodu a wraz z pojawieniem się funkcji autonomicznej jazdy i tak zwanej komunikacji między pojazdami, liczba wierszy kodu może się potroić. Analitycy firmy McKinsey szacują, że całkowity rynek cyberbezpieczeństwa motoryzacyjnego wzrośnie z 4,9 mld USD w 2020 r. do 9,7 mld USD w 2030 r., co odpowiada rocznemu wzrostowi o ponad 7%.



¹ Sum does not add up due to rounding
Source: Analysis based on data from "Automotive software and electronics 2030 – mapping the sector's future landscape," McKinsey, 2019

Badanie McKinsey 2020 wykazało, że 37 procent kierowców zmieniłoby markę samochodu, aby osiągnąć poprawę w obszarze zastosowania większej ilości technologii, łączności, elektryfikacji i współdzielonej mobilności. W niektórych krajach odsetek konsumentów chętnych do zmiany marki w celu uzyskania lepszej łączności był jeszcze wyższy (na przykład 56% w Chinach). Podobnie 39 procent konsumentów było zainteresowanych odblokowaniem dodatkowych funkcji cyfrowych po zakupie pojazdu - liczba ta wzrasta do 47 procent w przypadku klientów segmentu premium.

Wraz z szybkim rozwojem zaawansowanych technologii, takich jak mobilny internet, duże zbiory danych, sztuczna inteligencja i przetwarzanie w chmurze, **samochód stopniowo stał się nowym rodzajem inteligentnego środka transportu. Dzięki wzajemnym połączeniom i inteligencji samochód przekształca się z systemu zamkniętego w otwarty.** Niemniej jednak zapewnia również więcej opcji technologicznych i dostępu do globalnej sieci - usług podatnych na ataki (zwłaszcza gdy dostęp do Internetu jest aktywowany).

Naruszenie bezpieczeństwa samochodu skutkuje nie tylko stratami finansowymi, przejęciem kontroli, zagrożeniem dla bezpieczeństwa, ale także naruszeniem prywatności. Ta złożona połączona infrastruktura może wystawiać pojazdy na działanie szeregu wektorów. Uszkodzenie lub utrata wrażliwych danych w chmurze, awaria systemów, zasilania lub błędy w oprogramowaniu, przechwycenie informacji, takich jak zamykanie drzwi lub garażu, manipulowanie kontrolami pojazdu i fałszowanie / kradzież tożsamości to możliwe zagrożenia.

Oprócz samego wewnętrznego systemu Infotainment, coraz większym zagrożeniem stają się urządzenia mobilne będące kluczem i metodą sterowania wieloma kluczowymi funkcjami, takimi jak zamki, reflektory, system informacyjno-rozrywkowy, klimatyzacja, wycieraczki, klakson, a nawet ruch pojazdu.

- Urządzenia te i aplikacje mają szereg luk w zabezpieczeniach. Na przykład słabe wymagania dotyczące hasła, błędy kodu, przestarzałe systemy operacyjne, podatność na złośliwe oprogramowanie lub wirusy i słabe praktyki użytkowników stanowią istotne zagrożenie dla bezpieczeństwa jazdy i danych – podkreśla Wojciech Głazewski z firmy Check Point.

Potwierdzają to obserwacje PZDM. *- Niepowołana osoba może zainstalować aplikację na urządzeniu użytkownika pojazdu i uzyskać dostęp nie tylko do systemu pamięci pojazdu, lecz do numeru identyfikacyjnego pojazdu (VIN). Po uzyskaniu VIN osoba atakująca może zainstalować legalną aplikację i potencjalnie przejąć kontrolę nad pojazdem – informuje Leszek Cieloch z ESG.*

Początkowo bezpieczeństwo motoryzacyjne dotyczyło głównie systemów zamykania i immobilizerów ze względu na stosowanie systemów dostępu bezkluczykowego. Wiele badań wykazało możliwość dostępu do systemu bez pozwolenia. Wraz z rosnącą implementacją technologii, komunikacja zewnętrzna pojazdu stała się nową powierzchnią ataku. Istnieje szereg połączeń zewnętrznych, takich jak USB, Bluetooth, WiFi, ZigBee, GPS, Wave, 3/4/5G, OBD, GSM i wiele innych, stanowiących nowe wektory podatności samochodów i ukrytych w nich informacji....

W ocenie ekspertów najbardziej narażone na ataki są systemy audio, nawigacyjne i telefoniczne. Aby chronić je i bardziej wrażliwe systemy, na każdym etapie łańcucha produkcyjnego, od oprogramowania po projektowanie sprzętu, podejmowane są środki bezpieczeństwa. Główni dostawcy oprogramowania i sprzętu dla światowych producentów wbudowują zapory ogniowe, aby uniemożliwić takim elementom, jak systemy informacyjno-rozrywkowe, przekazywanie kodu do systemów, które regulują prędkość, sterowanie i inne krytyczne funkcje. To jednak może okazać się skutecznym rozwiązaniem do momentu fizycznego przekazania (sprzedaży) samochodu.

W momencie wejścia w posiadanie używanego, *nieoczyszczonego pojazdu*, niepowołana osoba może dowolnie skanować poufne dane i wykorzystać je przeświadczenia prywatnego życia poprzedniego właściciela....

- Ponad połowa analizowanych kierowców nie miała pojęcia o zagrożeniu ich danych osobowych po sprzedaży auta. Jednocześnie większość leasingowanych pojazdów ma synchronizowane dane GPS,

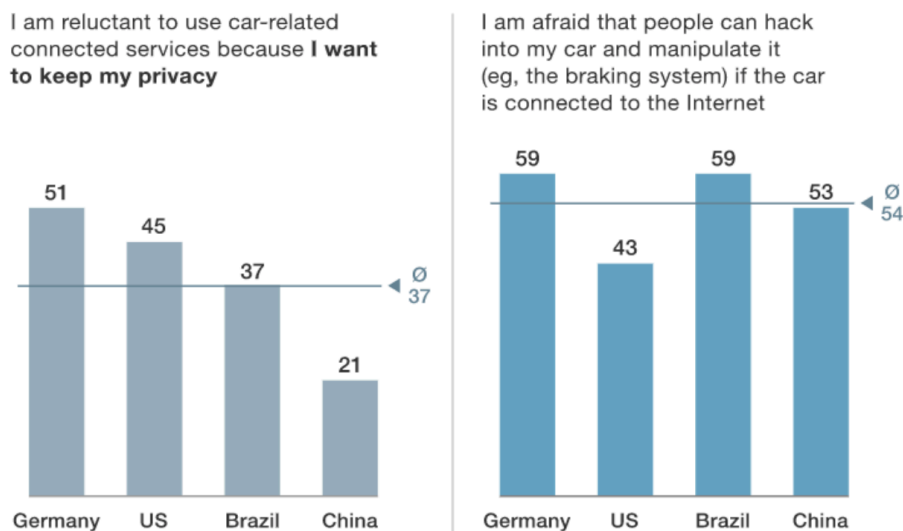
związane z firmowymi podróżami oraz prywatne dane użytkowników, do których przypisane jest firmowe auto – wynika z obserwacji ESG .

Podobne dane prezentuje badanie firmy HSB przeprowadzone na grupie 1.500 posiadaczy samochodów w USA. <https://us.acrofan.com/detail.php?number=448649>. Pokazuje ono, że 37 procent konsumentów było bardzo zaniepokojonych cyberbezpieczeństwem i bezpieczeństwem zautomatyzowanych pojazdów. **Ponad połowa badanych (55 procent) przyznało się do synchronizowania smartfonów lub innych urządzeń z systemem auta i nie mają oni pewności, jakie dane osobowe są przechowywane w systemie rozrywki ich samochodu.**

- Nasze samochody są bardziej połączone niż kiedykolwiek. Konsumentom trudno jest nadążyć za szybko rozwijającą się technologią pojazdów i zastanawiają się, czy ich prywatność i dane osobowe są chronione - twierdzi Timothy Zeilman, wiceprezes HSB, dostawcy usług i ubezpieczeń cybernetycznych.

Wtórnie mu Vishak Raman, Dyrektor działu Security Business z firmy Cisco, mówiąc, że „do 2024 r. na całym świecie ponad 300 milionów pojazdów na drogach będzie mogło otrzymywać scentralizowane aktualizacje. Pojazdy będą rejestrować i udostępniać wiele rodzajów danych, w tym geolokalizację, osiągi pojazdu, zachowanie kierowców i dane biometryczne”. Badani przez tę firmę użytkownicy samochodów obawiali się łączenia urządzeń mobilnych z systemem pojazdu, wyrażając obawę o bezpieczeństwo ich prywatności i danych. Najbardziej świadomi byli Niemcy, najmniej kierowcy w Chinach. Kierowcy są bowiem coraz bardziej świadomi zagrożeń wynikających z połączenia auta z Internetem – ponad połowa wskazuje na to niebezpieczeństwo.

% of new-car buyers that (strongly) agree with the statement



Źródło: prezentacja zagrożeń Cisco India 2020 <https://auto.economictimes.indiatimes.com/news/auto-technology/untangling-the-maze-of-connected-vehicles-before-taking-a-plunge/71214785>

- Możliwe, że w przyszłości samochody będą opatrzone specjalnymi naklejkami na szybach, które będą wskazywać, że pojazd spełnia normy cyberbezpieczeństwa. „Powinniśmy oceniać pojazdy pod kątem cyberbezpieczeństwa, tak samo jak oceniamy je pod kątem ochrony przed wypadkami - powiedział Jason K. Levine, dyrektor wykonawczy Center for Auto Safety.

W tym roku weszło w życie stosowne rozporządzenie ONZ w sprawie cyberbezpieczeństwa pojazdów, które zobowiązuje producentów do przeprowadzania różnych ocen ryzyka i zgłaszania prób włamań w celu poświadczenia gotowości do cyberbezpieczeństwa. Rozporządzenie wejdzie w życie we wszystkich pojazdach sprzedawanych w Europie od lipca 2024 r., a w Japonii i Korei Południowej w 2022 r.

Pytaniem pozostaje zachowanie kierowców. Czy wraz ze zmianami regulacji w stosunku do nowych pojazdów będzie rosła świadomość kierowców sprzedających swoje auta na rynku wtórnym? Czy

zaczniemy dbać o bezpieczeństwo przechowywanych danych w systemach samochodowych tak samo jak w przypadku komputerów? Specjaliści ESG są pełni obaw. Podkreślają, że łącząc system audio czy komputer pokładowy z przenośnymi urządzeniami, takimi jak smartfon, smartwatch czy nawigacja GPS, kierowcy potencjalnie otwierają furtkę hakerom i udostępniają informacje dotyczące zwyczajów posiadacza samochodu i nie tylko. Aby to zmienić, musimy zmienić postrzeganie auta jako urządzenia technicznego a nie tylko środka transportu.