Poufne dane w autach na celowniku hakerów

Poufne dane osobowe, numery telefonów, treści przesyłanych SMS lub adresy naszych codziennych podróży autem mogą paść łupem hakerów. Wartość tych danych wzrośnie w ciągu najbliższych 10 lat z 2,19 miliarda dolarów w 2022 r. do ponad 14 miliardów dolarów w 2032 r. *Nasze pojazdy stały się kopalnią wiedzy i danych o naszym prywatnym życiu. Teraz UE wprowadza nowe przepisy, aby chronić kierowców – ujawnia analiza European Security Group (ESG) i firmy Check Point Software Techologies.

Micki Boland, ekspertka i ewangelista firmy Check Point Software*,* wskazuje na wiele luk w zabezpieczeniach motoryzacyjnych związanych ze wszystkim - od platform telemetrycznych, motoryzacyjnych interfejsów API i infrastruktury, w tym infrastruktury chmurowej i platform DevOps, kont klientów i samych pojazdów. Ekspertka ostrzega - hakerzy włamują się do systemów informacyjno-rozrywkowych aut od wielu lat.

Ilość i wartość poufnych danych przechowywanych w samochodach rośnie z roku na rok, stając się obiektem rosnącego zainteresowania ze strony cyberprzestępców. Jak podaje McKinsey, do 2030 roku ponad 95% sprzedanych samochodów osobowych prawdopodobnie będzie miało wbudowaną łączność internetową, a monetyzacja danych samochodowych może przynieść branży od 250 miliardów do 400 miliardów dolarów rocznego przychodu do 2030 roku. Nie bez powodu analitycy tej firmy ocenili, że samochody stanowią „*najgorszą kategorię produktów*" pod względem prywatności.

Poufne dane ukryte w naszych samochodach to nie tylko informacje wprowadzane bezpośrednio przez kierowców (adresy lokalizacji, numery telefonów, hasła dostępu) lecz dane automatycznie zbierane przez producentów w ramach wbudowanego fabrycznie systemu informatycznego. Tymczasem rezygnacja z udostępniania danych często jest ukryta w ustawieniach i menu, a użytkownicy rzadko mają świadomość tego typu zagrożeń. Na szczególna uwagę zasługują, coraz bardziej popularne w ostatnich latach, pojazdy elektryczne (EV) i tzw. pojazdy połączone (Connected Cars), wyposażone w dostęp do Internetu.

Teraz Unia Europejska wprowadza przepisy, które mają ograniczyć skalę ryzyka dla kierowców i zwiększyć ochronę ich danych.

Nowe przepisy dotyczące cyberbezpieczeństwa w motoryzacji weszły w życie Europie w lipcu. *Surowsze wymagania dotyczące bezpieczeństwa elektroniki i procesów aktualizacji oprogramowania, zmuszają producentów samochodów do udoskonalenia systemów zabezpieczeń w pojazdach i stanowią ogromne wyznawanie dla całej branży* – ujawnia Leszek Cieloch, podkreśla Leszek Cieloch z European Security Group (ESG), członek Polskiego Stowarzyszenia Dziennikarzy Motoryzacyjnych (PSDM).

Unia Europejska chce położyć kres rosnącym zagrożeniom bezpieczeństwa związanym z nowoczesną technologią samochodową, zwłaszcza pojazdami elektrycznymi (EV). Urządzenia elektroniczne w samochodach nie tylko służą wygodzie kierowców i przyczyniają się do bezpieczeństwa na drogach, ale także pozwalają na coraz większą kontrolę samochodów i ich użytkowników.

Nowe przepisy (*regulacje UE uznające rozporządzenia ONZ R155 i R156*), nakładają wyższe wymagania na firmy samochodowe i ich dostawców w zakresie ograniczenia zbierania informacji i bezpiecznego

przechowywania i przetwarzania danych zbieranych przez systemy aktualizacji oprogramowania wbudowanego w pojazdach.

Jak wynika z danych ujawnionych przez UE, dzisiejsze samochody obsługują do 150 elektronicznych jednostek sterujących (ECU) i do 100 milionów linii kodu. W rezultacie dane przepływają do i z pojazdu z wielu źródeł. Vishak Raman, dyrektor działu Security Business z firmy Cisco, ocenia, że w 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 wyrażają obawę o bezpieczeństwo ich prywatności i danych. Najbardziej świadomi są Niemcy, najmniej kierowcy w Chinach.

Eksperci bija na alarm – ochrona danych osobowych w samochodach to prawdziwy koszmar – czytamy w raporcie firmy Mozilla *''Privacy not Included" (2023)*. W ostatnich latach przemysł motoryzacyjny w coraz większym stopniu opiera się na technologiach i usługach opartych na danych. Eksperci przestrzegają, że samochód zasadniczo gromadzi zbyt dużo danych osobowych. 84% producentów przekazuje lub sprzedaje dane użytkowników usługodawcom, brokerom danych i innym firmom. Z badania wynika, że nieco ponad połowa producentów samochodów oświadczyła nawet, że „na żądanie" przekaże dane rządom lub organom ścigania. I to bez orzeczenia sądu. https://foundation.mozilla.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/

Zagrożenia dla cyberbezpieczeństwa w branży motoryzacyjnej są nieuchronne – podkreślają autorzy badania zatytułowanego *„Automotive Cyber Security 2024"* – opracowanego przez niemieckie Centrum Zarządzania Motoryzacją (CAM) we współpracy z amerykańskim gigantem oprogramowania Cisco Systems. Z badania wynika, że ryzyko cyberataków na przemysł motoryzacyjny rośnie ze względu na coraz częstsze tworzenie sieci i cyfryzację samochodów, produkcji i logistyki. Badanie wyraźnie pokazuje, jak bezbronna jest ta branża. W ostatnich latach ofiarami ataków stały się koncerny i indywidualni kierowcy – ich poufne dane stanowią wartościowy łup dla cyberprzestępców. https://auto-institut.de/automotiveinnovations/cybersicherheit-immer-mehr-angriffe-auf-automobilbranche-studie-zu-automotive-cyber-security/

Przykładem cytowanym w badaniu jest amerykański pionier samochodów elektrycznych Tesla, który stał się celem w marcu 2023 r. W tym czasie hakerzy uzyskali dostęp do oprogramowania pojazdu sterującego funkcjami samochodu, takimi jak trąbienie klaksonem, otwieranie bagażnika, włączanie reflektorów i obsługę systemu informacyjno-rozrywkowego samochodu.

Jak zauważył Elon Musk, "*przyszłość transportu jest autonomiczna i elektryczna, ale musi być również bezpieczna"*. To stwierdzenie podkreśla wagę inwestowania w zabezpieczenia cybernetyczne i współpracę w celu stworzenia bardziej bezpiecznego i wydajnego systemu transportowego dla przyszłych pokoleń.

W opinii ekspertów dane z naszych samochodów to nie tylko informacje zbierane przez wewnętrzne systemy aktualizacji oprogramowania aut, lecz dane wprowadzane przez kierowców podczas użytkowania pojazdu. W konsekwencji auta używane, powracające na rynek wtórny (poleasingowe, pokredytowne, powracające do dealera w wyniku wymiany na nowszy model), stanowią kopalnię wiedzy o prywatnym życiu kierowcy.

Analizy ESG nie napawają optymizmem – zaledwie 10-20 proc. kierowców usuwa z systemu auta wprowadzone dane, ponad 50 proc. kierowców nie ma świadomości zagrożenia bezpieczeństwa ich danych w autach, większość leasingowanych aut ma synchronizowane dane GPS, ewidencjonujące podróże służbowe, do których przypisane jest firmowe auto. *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).

Tymczasem – jak wynika z danych Samar Polska - w 2023 roku sprzedano w Polsce ponad 730.000 używanych aut.

Dzisiejszy samochód to maszyna z większą liczbą linii kodu niż nowoczesny odrzutowiec pasażerski. 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 wyprzedażach, gdy mijamy ulubione sklepy, a pewnego dnia nawet same poprowadzą (autonomiczne auta). - *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 Głażewski, dyrektor firmy Check Point Software Technologies w Polsce.

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 zwiększają 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.** https://www.grandviewresearch.com/industry-analysis/automotive-cyber-security-market

Ataki na systemy aut obejmują manipulowanie pojazdem: odblokowywanie go, uruchamianie lub zatrzymywanie silnika, miganie reflektorów, znajdowanie lokalizacji pojazdu na podstawie numeru VIN w celu śledzenia pojazdu, przejmowanie konta internetowego właściciela pojazdu, hakowanie interfejsów API telemetrii i kradzież danych. Ponadto komercyjne platformy zarządzania flotą stały się celem ataków hakerskich wykorzystujących luki w zabezpieczeniach sieci i interfejsów API obsługujących te aplikacje.

Aby ograniczyć potencjalne zagrożenia i ataki, niezbędne są zapobiegawcze środki bezpieczeństwa. Środki te nie tylko ochronią bezpieczeństwo i integralność pojazdów elektrycznych, punktów kontrolnych i systemów OTA, ale także zagwarantują niezawodne i nieprzerwane funkcjonowanie naszego społeczeństwa. Wdrożenie solidnych protokołów bezpieczeństwa powinno być najwyższym priorytetem, aby chronić te technologie i zapewnić bezpieczną i zrównoważoną przyszłość – podsumowuje Micki Boland, ekspertka i ewangelista firmy Check Point.
https://community.checkpoint.com/t5/IoT-Protect/Electric-vehicle-cyber-security-risks-and-best-practices-2023/td-p/198820

Naruszenie bezpieczeństwa samochodu skutkuje nie tylko stratami finansowymi, przejęciem kontroli, zagrożeniem dla bezpieczeństwa, ale także naruszeniem prywatności. Złożona i 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 lub 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 Głażewski z firmy Check Point Software.

Dobrze zorganizowane zarządzanie cyberbezpieczeństwem musi iść w parze z rozwojem pojazdów definiowanych programowo. Deweloperzy oprogramowania muszą zapewnić zabezpieczenia w każdym obszarze, niezależnie od bezpieczeństwa konkretnej aplikacji. W Krakowie firma Aptiv pracuje nad zabezpieczeniami do urządzeń. Celem jest ochrona komunikacji wewnątrz pojazdu, np. Automotive Ethernet w taki sposób, aby tylko uprawnione urządzenia lub osoby miały dostęp do określonych danych. *Zajmujemy się również zabezpieczaniem oprogramowania za pomocą podpisów cyfrowych. Nasi inżynierowie upewniają się, że kod został prawidłowo skompilowany, przetestowany i pochodzący z zaufanego źródła. Wyzwaniem dla skutecznej ochrony systemów jest przewidywanie, jak zaprojektowane zabezpieczenia będą się zachowywały w przyszłości. Z punktu widzenia*

cyberbezpieczeństwa bardzo trudnym zadaniem jest tworzenie systemów, które będą bezpieczne nie tylko dzisiaj, ale również za rok, pięć, a może dziesięć lat – mówi Dariusz Mruk, dyrektor Centrum Technicznego Aptiv w Krakowie.

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.

Źródła:

*Precedence Research
Chceckpint Software Technologies - https://blog.checkpoint.com/securing-the-cloud/new-year-old-problems-an-inside-look-at-cloud-misconfigurations/
McKinsey Report - https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/automotive-r-and-d-transformation-optimizing-gen-ais-potential-value
Aptiv Polska - aptiv-white-paper-cyberbezpieczeństwo-dla-przyszłości-branży-motoryzacyjnej.pdf
Salesforce - https://www.salesforce.com/uk/solutions/industries/automotive/overview/
Forbes - https://www.forbes.com/sites/daveywinder/2024/01/27/tesla-hacked-as-electric-cars-targeted-in-1-million-hacking-spree/
Businessjournal.pl - Microsoft Word - Auta poleasingowe oczkiem w głowie hakerów - raport ESG i Check Point.docx (businessjournal.pl)
DW.com - https://www.dw.com/en/new-eu-cybersecurity-rules-push-carmakers-to-shun-old-models/a-68806605