

Lokalizacja setek tysięcy aut elektrycznych, w tym policyjnych

6 stycznia 2025

W bezprecedensowym naruszeniu bezpieczeństwa danych, które wstrząsnęło europejskim przemysłem motoryzacyjnym, grupa Volkswagena stała się źródłem potężnego wycieku informacji dotyczącego ponad 800 tysięcy właścicieli pojazdów elektrycznych.

Wśród poszkodowanych znaleźli się nie tylko zwykli obywatele, ale również wysokiej rangi niemieccy politycy, prominentni przedsiębiorcy, a nawet całe jednostki policyjne, w tym flota Hamburg Police. Co szczególnie niepokojące, istnieją podejrzenia, że wyciek mógł również dotknąć pojazdów należących do służb wywiadowczych.

Skala wycieku jest porażająca – objął on dane właścicieli aut czterech głównych marek należących do koncernu: Volkswagen, Audi, Seat i Skoda, rozmieszczonych na terenie całej Europy. Szczególnie alarmującym aspektem tej sytuacji jest niezwykle precyzja danych lokalizacyjnych – w przypadku pojazdów marek Volkswagen i Seat, system był w stanie określić położenie auta z dokładnością do zaledwie 10 centymetrów.

Wyciek nie ograniczył się jedynie do danych lokalizacyjnych. Do sieci przedostały się również wrażliwe informacje osobowe właścicieli, takie jak adresy zamieszkania i numery telefonów. Co więcej, ujawnione zostały szczegółowe dane eksploatacyjne pojazdów, tworzące swoisty „billing” aktywności – zawierający informacje o czasie i miejscu uruchamiania oraz wyłączania pojazdów elektrycznych. Wszystkie te niezwykle wrażliwe dane były przechowywane w niedostatecznie zabezpieczonej infrastrukturze chmurowej Amazona.

Paradoksalnie, ujawnienie tego poważnego naruszenia bezpieczeństwa zawdzięczamy Chaos Computer Club (CCC) – stowarzyszeniu hakerów, które specjalizuje się w wykrywaniu i nagłaśnianiu problemów związanych z cyberbezpieczeństwem. Ich działanie miało na celu zwrócenie uwagi na poważne luki w systemie zabezpieczeń koncernu. Eksperci z CCC podkreślają jednak niepokojący fakt – istnieje duże prawdopodobieństwo, że nie byli oni pierwszymi, którzy uzyskali dostęp do tej bazy danych.

Ten incydent podkreśla rosnące zagrożenia związane z cyfryzacją przemysłu motoryzacyjnego i pokazuje, jak pozornie niewinne dane telemetryczne mogą stać się potężnym narzędziem w niepowołanych rękach. W przypadku służb policyjnych lub wywiadowczych znajomość dokładnej lokalizacji pojazdów może stanowić poważne zagrożenie dla bezpieczeństwa operacyjnego.

Źródło: ZmianyNaZiemi.pl