



De moderne auto als mogelijke spion

Digitale dreigingen in slimme voertuigen

Moderne voertuigen worden steeds slimmer. In toenemende mate worden er digitale systemen in voertuigen geïntroduceerd die data verzamelen en verbonden zijn met internet. Dit levert aan de ene kant praktische voordelen op, maar aan de andere kant verzamelen deze systemen veel data over inzittenden, het voertuig zelf en over objecten en personen in de nabije omgeving. Verschillende partijen, waaronder statelijke actoren, kunnen toegang verkrijgen tot deze data. In deze publicatie roept de AIVD op om bewust om te gaan met spionagerisico's die gepaard gaan met moderne voertuigen. Ook geeft de AIVD aan via welke systemen deze risico's zich kunnen manifesteren en hoe u hiermee om kunt gaan.

Voor wie is dit advies relevant?

Over iedere inzittende van een modern voertuig kan via verschillende systemen informatie worden verzameld, maar er zijn personen van wie gesprekken, activiteiten of reisbewegingen met bijzondere interesse kunnen worden gemonitord. Te denken valt aan hoogwaardigheidsbekleders, mensen met sleutelfuncties in het bedrijfsleven of binnen de overheid en personen die anderzijds beschikken over gevoelige informatie. Onderstaande adviezen zijn gericht aan deze groep, met als doel hen te helpen hoe om te gaan met de gestelde spionagerisico's. Echter, de adviezen geven mensen daarbuiten ook handvatten om bewust om te gaan met brede dataverzameling door moderne voertuigen en zichzelf van de 'automatische piloot' af te halen. Niet alle adviezen zullen dekkend zijn op elke situatie, daarom is het goed om de risico's per situatie in te schatten en daarbij passende maatregelen te nemen.

Spionagerisico's in en via het voertuig

Moderne voertuigen verzamelen veel verschillende typen data. De gebruiker van een voertuig heeft vaak geen grip op de data die door het voertuig wordt opgeslagen of gecommuniceerd, omdat dit automatisch en ongemerkt gebeurt. Dit geldt zowel voor interne systemen als voor externe (camera)systemen. Voertuigfabrikanten hebben vaak toegang tot deze data, maar ook dealers, lease- en onderhoudsmaatschappijen, app-ontwikkelaars, producenten van voertuigonderdelen en clouddiensten kunnen toegang krijgen tot (een deel van) deze data. Hierdoor kunnen risico's ontstaan.

Naast deze bedrijven hebben kwaadwillende partijen interesse in en zeer waarschijnlijk ook toegangsmogelijkheden tot deze data. Voor statelijke actoren zijn deze datastromen een interessante bron van informatie. Sommige statelijke actoren kunnen deze data bij bedrijven opvragen of kunnen zelf hackoperaties uitvoeren om bij de data of de relevante systemen te komen. Ook voor 'gewone' cybercriminelen en hackers kunnen deze data interessant zijn om te verkrijgen, om deze bijvoorbeeld te gijzelen of te verhandelen.

**“Ga bewust om met spionagerisico's
die gepaard gaan met moderne voertuigen”**

Risicovolle systemen

Microfoons

Veel voertuigen zijn uitgerust met meerdere microfoons. Technisch is het mogelijk om de microfoons op afstand in te schakelen, waardoor kwaadwillenden gesprekken kunnen afluisteren.

Advies: Voer geen vertrouwelijke gesprekken in of rondom het voertuig.

Camera's

Moderne voertuigen zijn vaak voorzien van in- en externe camera's. Technisch is het mogelijk om de camera's op afstand in te schakelen. Hiermee kunnen kwaadwillenden opnames in en rondom het voertuig maken.

Advies: Wees je bewust van wat de camera in het voertuig mogelijk kan zien. Gebruik geen voertuig met een externe camera voor het reizen naar een gevoelige locatie.

Koppeling telefoon en overige apparaten

Er zijn verschillende methodes om een telefoon of andere apparaten met het voertuig te verbinden, zoals Bluetooth, Wi-Fi, een fysieke USB-aansluiting of het draadloos oplaadstation. Technisch is het voor kwaadwillenden mogelijk om via al deze verbindingen toegang te krijgen tot interne systemen van het voertuig en om vanuit het voertuig data uit de gekoppelde apparaten te halen.

Advies: Vermijd het (automatisch) verbinden met Bluetooth of Wi-Fi. Maak geen gebruik van draadloos laden. Koppel een mobiele telefoon niet zomaar aan een USB-aansluiting, maar maak gebruik van een datablocker.

Infotainmentsystemen

Het ingebouwde infotainmentsysteem is het centrale punt voor datavergaring en -opslag in het voertuig. Vanuit het infotainmentsysteem wordt (een deel van) de verzamelde data beschikbaar gesteld aan de voertuigleverancier en andere partijen. Deze datavergaring gaat ver, denk hierbij aan de unieke identificatienummers van gekoppelde apparaten, contactgegevens, internetverkeer, verstuurd berichten of navigatiegegevens. Technisch is het mogelijk om toegang te verkrijgen tot de data die in het infotainmentsysteem worden opgeslagen.

Advies: Wees terughoudend met het invullen van specifieke NAW-gegevens in het navigatiesysteem, zoals een thuisadres of het adres van een gevoelige locatie. Weeg het gebruik van ingebouwde navigatiesystemen af tegen het reisdoel en de invulling van de reis.

GPS & Track and trace

Voertuigfabrikanten gebruiken deze systemen om een voertuig live te volgen en reisbewegingen te registreren. Technisch is het voor kwaadwillenden mogelijk om de live-locaties van voertuigen te volgen.

Telematicamodule

In moderne voertuigen wordt gebruik gemaakt van een telematicamodule. Deze module heeft internettoegang vanwege file-informatie, locatiedata of updates van de fabrikant. Ook worden via deze module voertuigdata gedeeld met de fabrikant.

Laadpalen

Laadpalen voor elektrische voertuigen worden gebruikt voor het versturen van data over de voertuigen die zijn gekoppeld.

Advies voor bovenstaande: Risico's vanuit deze systemen zijn niet te voorkomen met techniek of door gedrag. Weeg daarom de risico's van gebruik van het voertuig af tegen het reisdoel en de invulling van de reis.

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
aivd.nl

september 2026