



Privacy in de auto

Digitale veiligheid

Diversen | Een mobiele telefoon wordt door beveiligingsexperts gezien als een spion in de broekzak. Een smartphone heeft een camera, een microfoon en een GPS-ontvanger. Daarbij is het een geliefd doelwit van hackers, want een telefoon wordt ook nog eens gebruikt voor bankieren, heeft een lijst van alle contacten en een archief vol foto's. Een auto heeft zo mogelijk nog meer sensoren en menigeen brengt er uren per dag in door. Dus rijst de vraag: hoe is het gesteld met digitale veiligheid in de auto?

De computer is gaandeweg in het leven van de automobilist geslopen. De vertrouwde autoradio heeft plaats gemaakt voor een infotainment-systeem met audio, communicatie en navigatie. De gegevens van het navigatiesysteem kwamen aanvankelijk van een CD-ROM, DVD of geheugenkaart. Om gegevens actueel te houden, en te voorzien van recente verkeersinformatie, halen auto's hun data voortaan uit externe bronnen. En die bron weet dus precies waar de automobilist is en wat de dagelijkse patronen zijn.

"De regel is eenvoudig: hoe meer sensoren en hoe meer automatisering, hoe groter het risico"



Ooit werd voor veilig telefoneren in de auto een Bluetooth-carkit ingebouwd. Nu is zo iets standaard, maar het betekent dat de auto is uitgerust met microfoons en de bestuurder erop moet vertrouwen dat de autofabrikant daar geen misbruik van maakt. Diezelfde microfoons worden namelijk ook gebruikt voor een slimme assistent en die moet op ieder moment kunnen reageren op een "Hey [auto]"-commando (vul hier uw favoriete automerk in). Afgaande op de algemene voorwaarden is niet uit te sluiten dat een autofabrikant weet wat er gaande is in de cabine.

En gaandeweg kregen auto's steeds meer sensoren. Camera's die eerst alleen werden gebruikt om parkeren makkelijker te maken, herkennen nu ook verkeersborden en worden gebruikt voor zelfrijdende functies. Worden de beelden van die camera's ook gebruikt om kunstmatige intelligentie te trainen? En hoe wenselijk is het dat uw oprijlaan of garage ook in beeld wordt gebracht?



"Apps" bij de auto vormen een heel ander risico. Hiermee kan op afstand het laadproces in de gaten worden gehouden, kan worden gecontroleerd of de deuren op slot zitten of kan de verwarming voor aanvang van de rit worden ingeschakeld. Dat is allemaal heel handig, maar moderne autodieven kunnen apps hacken om toegang te krijgen tot gegevens van de auto (rit-logboek) of zelfs de gehele auto! En ook als de autofabrikant de digitale beveiliging goed op orde heeft, hoe goed is de beveiliging van uw telefoon? Daarop geïnstalleerde apps van onduidelijke ontwikkelaars of apps van sociale media verzamelen alle data die ze maar te pakken kunnen krijgen...

Toekomstgericht

Bij het beoordelen van deze risico's is het belangrijk om richting de toekomst te denken. Menigeen zegt "ik heb niets te verbergen", maar als dat echt zo is, zou u dan kunnen leven in een glazen huis zonder gordijnen? Of zou u uw ontgrendelde telefoon aan een vreemde uitlenen? Niet zo'n prettig gevoel toch? En gegevens die nu triviaal lijken, kunnen in de toekomst aan andere data worden gekoppeld en dan opeens van grote waarde zijn.

En wat te denken van data die in verkeerde handen valt? Een mooi voorbeeld is het faillissement van een bedrijf dat DNA-analyse deed. Tijdens het bestaan sprong het altijd zorgvuldig om met de (medische) gegevens van klanten, maar na het faillissement gingen de computers vol gegevens naar de hoogste bieder. En de vraag is wat die ermee doet. Een meer concreet voorbeeld: een Amerikaanse autofabrikant

bracht het rijgedrag van klanten in kaart en verkocht dat aan verzekeraars, die vervolgens de premie van de minder zorgvuldige piloten verhoogde.



Het verouderen van systemen vormt een risico voor de veiligheid en de bruikbaarheid van een auto. Indien een fabrikant een oudere versie van een besturingssysteem inbouwt, bestaat het risico dat updates binnen afzienbare tijd niet meer mogelijk zijn. Kort daarna zullen apps ook niet meer communiceren met hun centrale server en dan is zo'n systeem onbruikbaar. Concreet betreft dit auto's met een oudere versie van Android Automotive. Google zal updates blijven aanbieden, maar als de hardware onvoldoende capaciteit heeft om nieuwe versies te draaien, zal het systeem spaak lopen en/of zullen de updates niet kunnen worden geïnstalleerd. Een hint: globaal wordt ieder jaar een nieuwe versie van Google uitgebracht. Op het moment van schrijven (medio 2025) is Android bij versie 15. Na gemiddeld 6 jaar accepteert een toestel geen updates meer omdat de hardware ontoereikend is.

Oplossingen

Nu de problemen in kaart zijn gebracht, is het tijd om te denken in oplossingen. De meest rigoureuze oplossing is offline leven: telefoon uit, navigeren met een wegenkaart en luisteren naar FM-radio. Dat is decennia lang goed gegaan, maar anno 2025 weinig realistisch.

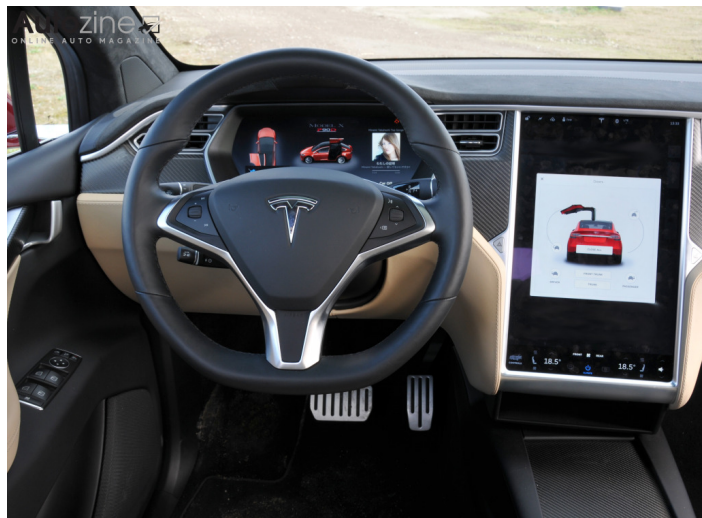
Daarom is het belangrijk om goed op te letten bij de keuze van een nieuwe auto. Is het infotainment-systeem door de autofabrikant zelf ontwikkeld, of is het uitbesteed aan een partij die er

bijbedoelingen mee heeft? In de algemene voorwaarden is eenvoudig terug te vinden wat de fabrikant wel of niet met de gegevens doet. En lees tussen de regels door. Zo geven Renault en Dacia aan zich het recht voor te behouden om ritgegevens te verkopen aan derden, maar dan wel geanonimiseerd. Dat klinkt mooi, maar wat is dat waard als de koper exact ziet waar iedere rit begint en eindigt? Zelfs met een ouderwets telefoonboek is eenvoudig te achterhalen wie er op dat adres woont! Einde anonimiteit.

Nieuwkomers

De gevestigde orde besteedt de ontwikkeling van software bijna altijd uit, omdat het de noodzakelijke kennis niet in huis heeft. Chinese autofabrikanten hebben in de praktijk meer computerkennis in huis dan het gemiddelde Europese softwarehuis en ontwikkelen daarom alles in eigen beheer. Bij navraag beloven de Chinese fabrikanten steevast alle data op een Europese server op te slaan, maar ze kunnen niet garanderen dat daar nooit een "backup" van wordt gemaakt in China.

Om er achter te komen wat systemen precies doen, volstaat het om de algemene voorwaarden te lezen. Fabrikanten zijn namelijk verplicht om hierin exacte uitleg te geven. Toen de testrijder tijdens het opladen van een Nio uit verveling door de vele menu's op het centrale beeldscherm bladerde, bleken beelden van hoge kwaliteit van iedere rit te zijn opgeslagen. Dit kwam als een onaangename verrassing. Echter, dit bleek duidelijk te staan in de eenvoudig leesbare (!) algemene voorwaarden van Nio en deze schok had dus voorkomen kunnen worden.



In kennis is Tesla vergelijkbaar met de Chinese merken. Ook de Amerikaanse fabrikant heeft een schat aan computerkennis in huis en neemt de automatisering daarom geheel in eigen hand. De klant is verplicht om Tesla te vertrouwen, want de auto functioneert niet zonder Tesla-account. En in tegenstelling tot de Chinese merken zijn Apple CarPlay en Android Auto niet beschikbaar bij Tesla.

Gevestigde orde

Renault, Dacia en Volvo hebben als eerste alles uitbesteed, en wel aan Google. En dat is een bedrijf dat het verzamelen van data als doel heeft. En het ergste is: het kan niet uit worden geschakeld. De meest recente modellen van deze merken vormen wat Autozine betreft het grootste gevaar voor de digitale veiligheid en het advies is om uiterst terughoudend te zijn met de aanschaf van deze auto's.

Zoals gezegd: de gevestigde orde besteedt vaak een deel van de ontwikkeling van het infotainment-systeem uit. Stellantis (Fiat, Peugeot, Opel, Citroën, DS Automobiles, Lancia, Jeep, Alfa Romeo) werkt samen met TomTom voor de navigatie en dus weet dat bedrijf waar de klant gaat en staat. Echter, TomTom functioneert zonder login en TomTom is geen bedrijf dat dataverzamelen als primair doel heeft. Opel en DS bieden in de allernieuwste modellen een aangename extra: een privacy modus waarmee alle luistervinken tijdelijk zijn uitgeschakeld.

Zeekr, Leapmotor en Smart zijn met respectievelijk de 7X en #5 schoolvoorbeelden van hoe het wel moet: ze hebben de vrij verkrijgbare broncode van Android genomen en op basis daarvan zelf een infotainment-systeem ontwikkeld. Ze zijn hiermee niet afhankelijk van Google en kunnen daarom een systeem op maat aanbieden. Bovendien is hiermee het risico kleiner dat de software ongevraagde updates krijgt die de hardware niet kan verwerken. Het half-Chinese Smart belooft plechtig dat alle data op Europese servers wordt opgeslagen.

Alternatieven

Een eenvoudige oplossing is het gebruik van de eigen telefoon middels Apple CarPlay of Android Auto. Dan wordt opnieuw een partij in vertrouwen genomen, maar in ieder geval heeft de gebruiker een vrije keuze. De echte computernerd (lees: de Autozine redacteur) gaat een stap verder: door Google's Android te vervangen door CalyxOS of GrapheneOS is geen Google-account meer aan de telefoon gekoppeld, terwijl beide wel functioneren met Android Auto. Door dan ook nog te navigeren met "TomTom Go" of "HERE We Go" kan min of meer anoniem worden genavigeerd.

Wat de apps van autofabrikanten betreft is er maar één oplossing: niet gebruiken. Voor het controleren van het laadproces biedt de aanbieder van de laadpas vaak ook een app. Die is net zo bruikbaar, maar heeft geen koppeling met de auto en dus is het risico dat kwaadwillenden toegang krijgen tot het voertuig een

stuk kleiner.

Gebruikte auto's

Gebruikte auto's vormen een heel ander risico. Let goed op dat de vorige eigenaar geen verbinding meer heeft met de auto. Anders kan deze u volgen of in het ergste geval zelfs de auto ontgrendelen en ermee weggrijden! Loop daarom alle lijstjes door van gekoppelde telefoons, elektronische sleutels, etc. en wis oude gegevens. Nog beter: geef de auto een fabrieksreset zodat de computer op nul staat voordat u de occasion in gebruik neemt.



Conclusie

Is digitale veiligheid van belang in de auto? Ja, want het gevaar is misschien wel groter dan op de PC thuis of met de mobiele telefoon. Immers, na het huis is de auto voor velen hun kostbaarste bezit. Daarbij heeft een auto meer sensoren dan een telefoon en voert menig een er (vertrouwelijke) gesprekken.

De regel is eenvoudig: hoe meer sensoren en hoe meer automatisering, hoe groter het risico. Daarom loont het om zorgvuldig onderzoek te doen naar de ingebouwde systemen en om de algemene voorwaarden te lezen. Dwingt de fabrikant af om met de voorwaarden akkoord te gaan, of is er een keuze? Kunnen online functies indien gewenst worden uitgeschakeld? Functioneert een auto of infotainment-systeem ook zonder login? En vooral: vertrouwt u de leverancier? Is het verzamelen van data het primaire doel van een bedrijf en is de aangeboden dienst slechts een excuus om dat te

doen? Of gaat het om de dienst en is het verzamelen van data een noodzakelijk kwaad voor het functioneren ervan?

Als alternatief kan Apple CarPlay of Android Auto worden ingezet, maar dat is slechts het verplaatsen van het risico naar een andere partij. Wie dat echt wil, kan kiezen voor een alternatieve versie van Android zonder Google (namelijk: CalyxOS of GrapheneOS). En wie volledig anoniem wil rijden, kiest een oudere auto zonder sensoren of computers. ■

