Données véhicule

Test TCS: applications à distance pour véhicules – sont-elles sûres?

Les applications à distance (en anglais «remote apps») pour véhicules sont à la mode. Elles permettent de lire en temps réel, via un smartphone ou une tablette, un grand nombre de données dites informatives sur la voiture ; comme le kilométrage, le niveau du réservoir d'essence, les intervalles entre les services, la pression des pneus, etc. Ces applications servent également à exercer certaines fonctions de commande comme le verrouillage et le déverrouillage des portes, ainsi que l'ouverture et la fermeture des fenêtres – un surcroît de confort, mais qui ouvre aussi un champ d'action aux criminels. C'est dire l'importance de la sécurité informatique. Le TCS et ses clubs partenaires ont donc soumis trois applis à distance (BMW, VW et Renault) à un dit test de pénétration.

Notons-le d'emblée: les trois applis examinées de BMW, Renault et VW sont en principe sûres et utilisables sans grand risque. Mais leur sécurité n'est pas totale, si bien qu'il reste des précautions à prendre: les trois applis présentent diverses faiblesses que l'on peut qualifier de risques moyens et qui, dans un cas extrême, peuvent permettre à des tiers d'accéder au compte d'utilisateur et à la commande de toutes les fonctions à distance.
Ce test a révélé les points faibles suivants:

Banque de données non codée

Renault My Z.E. sauvegarde des données sensibles dans une banque de données non codée sur le smartphone. Cette faiblesse permet à un éventuel utilisateur malveillant de lire dans certaines conditions des données comme le numéro d'identification du véhicule et un code d'activation grâce auquel il peut enregistrer le véhicule à son nom.

Absence de pinning de certificat

En outre, la liaison entre Renault My Z.E. et VW Car-Net et le cloud peut, dans certaines conditions, être captée et modifiée. La tâche du pirate sera d'autant plus facile si l'utilisateur a désactivé certaines fonctions de sécurité sur son appareil.

Informations d'enregistrement dans l'URL

L'appli BMW Connected communique avec plusieurs points terminaux du cloud. Pour permettre à l'utilisateur de ne s'enregistrer qu'une fois dans l'appli, les informations d'enregistrement sont d'abord modifiées. Malheureusement, le constructeur a choisi une méthode peu sûre pour la transmission de ces données d'enregistrement modifiées, de sorte que le compte peut éventuellement être piraté. Par ailleurs, des données sensibles sont stockées dans les fichiers de protocole du fournisseur, où des utilisateurs ayant qualité d'administrateurs peuvent les voir.

Mot de passe trop faible

La directive implémentée dans l'appli BMW Connected pour régler le mot de passe est trop faible. La longueur du mot de passe est limitée à huit signes au maximum et le nombre de signes spéciaux est également restreint. La force du mot de passe en est réduite, de sorte que l'attaquant peut plus facilement découvrir le mot de passe par des tentatives (ledit «bruteforcing»). Même des mots de passe simples comme «abcd1234» sont permis. BMW bloque cependant le compte d'utilisateur après plusieurs essais infructueux jusqu'à ce qu'il soit à nouveau libéré par un lien via courriel.

Pas de clôture effective de la séance

Les trois applis ont en commun le point faible suivant: la séance n'est pas véritablement clôturée après le logout. L'utilisateur ne peut donc pas simplement bloquer un pirate qui a réussi à s'infiltrer.

Conclusion

Les trois applis offrent certes une sécurité d'utilisation suffisante dans l'ensemble, mais présentent tout de même quelques points faibles. Conclusion évidente: les constructeurs doivent continuer d'optimiser la sécurité informatique. La multiplication des fonctions et services numériques disponibles augmente aussi les exigences en termes de sécurité, si bien que le thème de la sécurité informatique jouera un rôle croissant à l'avenir.

Recommandations

- L'utilisateur doit avoir la possibilité de désactiver complètement la transmission de données du véhicule.
- Les données récoltées par le constructeur doivent être librement accessibles au propriétaire du véhicule.
- Certaines fonctions comme l'activation du klaxon doivent être désactivées durant le trajet pour des raisons de sécurité.
- Les directives pour les mots de passe doivent être plus sévères.
- Les critères de sécurité informatique doivent répondre aux standards de sécurité actuels, idéalement sur la base d'une certification neutre (par ex., Common Criteria).

Conseils pour le consommateur

- Il existe de grandes différences au niveau des fonctions pouvant être commandées à distance non seulement entre les constructeurs, mais aussi entre les modèles et exécutions. Pour l'acheteur, il est donc important de toujours vérifier les fonctions effectivement supportées pour chaque cas particulier.
- Il faut utiliser des mots de passe aussi sûrs que possible, donc comprenant des minuscules et des majuscules, des chiffres, des signes spéciaux et ayant une longueur d'au moins 12 signes.