Dati del veicolo

Test TCS: applicazioni a distanza per veicoli - quanto sono sicure?

Le applicazioni a distanza per auto ("remote-apps" in inglese) sono di moda. Consentono di leggere in tempo reale, su smartphone o tablet, un gran numero di dati del veicolo, come: chilometraggio, livello del carburante, intervalli tra i servizi, pressione delle gomme, ecc.. Inoltre possono esercitare determinate funzioni di comando, quali il blocco e l'avvio del veicolo, l'apertura e la chiusura dei finestrini. Tutte funzioni confortevoli, ma danno anche l'opportunità ai malintenzionati di entrare in azione. Ecco perché la sicurezza informatica è importante. Il TCS e i suoi club partner hanno sottoposto tre applicazioni (app) a distanza (BMW, VW e Renault) a un test di intrusione abusiva.

Le tre app esaminate di BMW, VW e Renault sono in linea di principio sicure e utilizzabili senza grossi rischi. Tuttavia, la loro sicurezza non è completa ed è auspicabile prendere alcune precauzioni. Infatti, esse presentano diversi punti deboli, di rischio medio, ma, in caso estremo, permettono a terzi di accedere al conto dell'utente e al comando di tutte le funzioni a distanza. Il test ha evidenziato i seguenti punti deboli:

Banca dati non codificata

Renault My Z.E. salva dati sensibili in una banca dati non codificata sullo smartphone. Questa lacuna permette ad un malintenzionato di leggere, in certe condizioni, dati quali il numero d'identificazione del veicolo e un codice d'attivazione, con il quale può registrare l'automobile a proprio nome.

Pinning di certificato mancante

Il collegamento con il cloud corrispondente delle app di Renault My Z.E. e di VW Car-Net, in determinate condizioni, può essere captato e modificato. Il compito di un malvivente risulterà ancora più facile se sull'app dell'utente sono state disattivate certe funzioni di sicurezza.

Informazioni di registrazione nell'URL

L'app BMW Connected comunica con più punti terminali del cloud. Per permettere all'utente di registrarsi soltanto un'unica volta nell'app le relative informazioni sono dapprima modificate. Purtroppo, il costruttore ha scelto un metodo poco sicuro per la trasmissione di questi dati di registrazione modificati, tanto che il numero di conto può essere captato da un malintenzionato. Inoltre, dati sensibili sono immagazzinati negli schedari di protocollo del fornitore dove possono essere visionati da utenti con la qualifica di amministratori.

Fragili direttive per la password

La direttiva relativa alla password implementata nell'app BMW Connected è troppo fragile. La lunghezza della password è limitata ad un massimo di otto segni ed il numero dei segni speciali è ristretto. La forza della password risulta così indebolita, in quanto sono anche permesse password semplici come, per esempio, "abcd1234", che possono essere scoperte facilmente attraverso vari tentativi col "bruteforcing". Tuttavia, dopo pochi tentativi non riusciti, BMW blocca il conto dell'utilizzatore fino a quando sarà nuovamente liberato da un link via e-mail.

Manca la chiusura effettiva della seduta

Le tre app hanno in comune il seguente punto debole: dopo il logout, la seduta non risulta veramente conclusa. L'utente non può dunque semplicemente bloccare un pirata che è riuscito ad accedere ai suoi dati.

Conclusione

Nel complesso, le tre app offrono certamente all'utente una sufficiente sicurezza d'utilizzo, ma presentano ugualmente alcuni punti deboli. Ciò dimostra chiaramente che i costruttori devono continuare a ottimizzare la sicurezza informatica. Con il moltiplicarsi delle funzioni dei servizi numerici disponibili aumentano anche le esigenze in termini di sicurezza, tanto che il tema della sicurezza informatica assumerà in futuro sempre maggiore importanza.

Raccomandazioni

- L'utente deve avere la possibilità di disattivare completamente la trasmissione dei dati del veicolo.
- I dati raccolti dal costruttore devono essere liberamente accessibili al proprietario del veicolo.
- Per motivi di sicurezza, certe funzioni come l'attivazione del claxon devono essere disinserite durante il tragitto.
- Occorrono direttive più severe per le password.
- I criteri di sicurezza informatica devono rispondere agli attuali standard di sicurezza, idealmente sulla base di un attestato neutrale (per es. Common Criteria).

Consigli per il consumatore

- Non soltanto tra i costruttori, ma anche tra i singoli modelli e le varianti dell'equipaggiamento, esistono grandi differenze a livello delle funzioni che possono essere comandate a distanza. Per l'acquirente è dunque importante verificare sempre le funzioni effettivamente sostenute in ogni singolo caso.
- Occorre utilizzare password il più sicure possibile, ossia che comprendano lettere minuscole e maiuscole, cifre, segni speciali e che abbiano una lunghezza di almeno 12 segni.