Sicherheitslücke bei Mercedes, BMW und Co.: Schlüssellos, Auto los

Von Sandra Sperber, Robert Ackermann und Christoph Stockburger

Mit sogenannten Keyless-Systemen können Autobesitzer ihre Fahrzeuge öffnen und starten, ohne den Schlüssel aus der Hosentasche zu nehmen. Das ist komfortabel - vor allem auch für Diebe.

Wenig Zeit? Am Textende gibt's eine Zusammenfassung.

Wer einen Neuwagen kauft, kann bei vielen Modellen die Sonderausstattung Keyless Go wählen. Der Wagen lässt sich dann öffnen, ohne dass man den Schlüssel in die Hand nehmen muss. Es genügt, ihn einfach bei sich zu tragen. Nicht mal zum Starten wird er benötigt: Man drückt eine Taste, schon springt das Auto an. Die Signale werden über Funkwellen übertragen. Klingt praktisch? Ist es auch. Das Extra kostet je nach Hersteller allerdings bis zu 800 Euro Aufpreis - ein teures Vergnügen

Hinzu kommt: Wenn man es sich gönnt, freuen sich außer dem Fahrzeughändler vor allem Kriminelle. Denn für sie sind Autos mit Keyless-Go-Systemen leichte Beute. Eine Sicherheitslücke ermöglicht es Dieben, den Wagen innerhalb von Sekunden zu öffnen und damit abzuhauen.

Funksignale werden eingefangen und verlängert

Wie der geräuschlose Diebstahl funktioniert, demonstriert der Kriminologe Udo Hagemann am Beispiel eines von uns gemieteten Renault Espace mit Keyless-Entry-Funktion. Die Vorführung findet auf einer Straße in Berlin statt. Hagemann hat sich eine Laptop-Tasche umgehängt. Darin befindet sich die Gerätschaft für den Klau. Ein

Redakteur von **SPIEGEL ONLINE** trägt ebenfalls eine Laptop-Tasche, die mit Technik vollgestopft ist. Zu zweit knacken sie den französischen Familienwagen.

Die Funktechnologie des Schlüssels dient Udo Hagemann als Einfallstor. "Die Signale lassen sich sogar durch Wände hindurch abfangen und bis zu 400 Meter weit übertragen", sagt er. Das Prinzip funktioniert so: Die Autoknacker stellen sich mit einem Empfänger einfach vor die Haustüre des Fahrzeugbesitzers, fangen das Signal des Schlüssels dort ein und leiten es an einen Komplizen weiter, der am Wagen steht. Oder sie setzen sich im Café neben die Person mit dem Schlüssel. Durch die Anfälligkeit des Keyless-Go-Systems ist der Wagen dann schneller verschwunden, als der Besitzer seinen Espresso gekippt hat - obwohl der Schlüssel an Ort und Stelle bleibt.

Wenn das gestohlene Fahrzeug erst einmal in einem Versteck untergebracht ist, zapfen die Diebe über die Datenschnittstelle - die sogenannte OBD-Buchse, die beispielweise auch beim Service in der Werkstatt genutzt wird - die Software des Autos an. So können sie alle nötigen Fahrzeuginformationen auf einen leeren Schlüssel ziehen und das Auto fortan ganz normal öffnen, schließen und starten. Diese Schlüssel - laut Hagemann bekommt man sie "über Ebay oder in China und Südosteuropa" - werden "angelernt", heißt es im Jargon.

Hunderte Autobesitzer waren im vergangenen Jahr betroffen

Was genau in seinen beiden ominösen Laptop-Taschen steckt, verrät Hagemann nicht. Nur so viel: "Für rund 35.000 Euro kriegt man die Technik in Südosteuropa." Nach einem einzigen Autoklau hat man die Investition also wieder drin. Nicht nur Renault-Modelle lassen sich damit überlisten: "Es gibt keinen Hersteller, der ein hundertprozentig sicheres Keyless-Go-System bietet", sagt Hagemann.

Als ihm das Magazin "Autobild" vor Kurzem zehn verschiedene Modelle hinstellte - darunter eine Mercedes C-Klasse, ein VW Passat und ein Audi A4 -, konnte er mit seiner Methode jedes einzelne öffnen und starten. "Bei manchen Systemen unterscheiden sich zwar die Frequenzen, aber darauf kann ich meine Geräte einstellen."

Bei Autodieben hat sich die Sicherheitslücke längst herumgesprochen. Offizielle Zahlen, wie viele Fahrzeuge im vergangenen Jahr über das Keyless-Go-System gestohlen wurden, gibt es nicht. "Die Fälle werden in den Statistiken nicht gesondert ausgewiesen; außerdem ist die Art eines Diebstahls oft schwer nachzuprüfen", sagt eine Sprecherin des Bundeskriminalamts.

Diebstahlhochburgen im Osten und Norden /Süden relativ sicher

Doch es gibt Beispiele für spektakuläre Diebstahlserien, die das Ausmaß erahnen lassen: Im Main-Kinzig-Kreis wurden etwa allein im ersten Halbjahr 2015 mehr als 40 Autos geknackt. Die Täter hatten es dabei vor allem auf teure Modelle von BMW, Audi und Range Rover abgesehen. Der zuständige Kriminalhauptkommissar sprach dabei von "konkreten Hinweisen" darauf, dass eine "neue Methode" zum Einsatz kam: "Sogenannte Funkwellenverstärker." In Mecklenburg-Vorpommern führte die

Polizei den Klau von insgesamt 115 Autos ebenfalls auf die Anfälligkeit des Keyless-Go-Systems zurück.

Für Hagemann ist diese "neue Methode" eher ein alter Hut. "Ich habe schon vor acht Jahren mit solchen Geräten experimentiert", sagt er. Am Rande eines Seminars über Sicherheitslücken bei elektronischen Systemen, das Hagemann vor Polizisten hielt, habe ihn ein Beamter auf das Risiko von Keyless Go aufmerksam gemacht. "Das hat meinen Ehrgeiz geweckt."

Hagemann ist Gründer und Chef der Firma Bundpol Security Systems, er hat sich auf die Schulung von Behördenmitarbeitern und die Entwicklung von Sicherheitssystemen spezialisiert. Das Wissen um die Sicherheitslücke von Keyless Go hat er nach eigenen Angaben schon früh mit den Autoherstellern geteilt.

Das sagen die Hersteller

Wie die Tests zeigen, hat sich dabei aber nicht viel getan. Die Reaktionen der Autohersteller würden in einem Arbeitszeugnis wohl so zusammengefasst werden: Sie haben sich stets bemüht.

- "Wir nehmen das Problem sehr ernst und arbeiten laufend an der Verbesserung unserer Schutzsysteme", heißt es bei **Renault**. Auf Wunsch sei es auch möglich, die Keyless-Entry-Funktion auszuschalten.
- Ohne auf das Keyless-Problem direkt einzugehen, versichert **BMW** in einem Statement, "die Schutzmechanismen konstant weiter" zu entwickeln. Nach eigener Ansicht zähle ihr Schutzkonzept "zu den führenden in der Industrie". Eine ziemlich selbstzufriedene Meinung -schließlich tauchen in der jüngsten Diebstahlstatistik gleich drei BMW-Modelle in den Top-Ten auf.
- **Mercedes** teilt mit, dass sich bei Schlüsseln "neuerer Generation" die Keyless-Go-Funktion vom Nutzer ausschalten lasse.
- **Audi** stehe zu diesem Thema "mit den Behörden in Kontakt", sagt ein Pressesprecher. "Illegale Verwendung von Systemen zur Funkstreckenverlängerung" nehme man "sehr ernst".

In einem Schreiben, das SPIEGEL ONLINE vorliegt, teilt Matthias Wissmann, Präsident des **Verbands der Automobilindustrie** (VDA), beflissentlich mit:

- "Sicherheitsvorkehrungen gegen Fahrzeugdiebstahl (…) haben für die deutsche Automobilindustrie seit Jahren höchste Priorität." Wissmann spricht von einem "Wettlauf der Technologien 'Fahrzeug gegen Einbruchswerkzeug'".

Wer dabei derzeit die Nase vorn hat, zeigt Udo Hagemann mit seinen Laptop-Taschen.

Was hilft? Alufolie, dreilagig

Der 54-Jährige ist alles andere als ein Fortschrittsverweigerer, doch die aktuelle Entwicklung in der Autobranche stimmt ihn nachdenklich. "Je interaktiver die Fahrzeuge, desto verwundbarer ist ihre Sicherheit", sagt Hagemann. "Spätestens wenn die Autos von selbst fahren, wird es endgültig Zeit für vernünftige Firewalls."

Was Keyless Go betrifft: Wer in Zukunft noch viel Geld für ein hohes Diebstahlrisiko ausgibt, ist wohl selbst schuld. Und denjenigen, die sich bereits ein solches System eingebrockt haben, gibt Hagemann folgenden Tipp: "Wickeln Sie ihren Schlüssel in drei Lagen Alufolie ein, dann können die Funksignale nicht mehr abgefangen werden." Beim Renault Espace funktionierte der simple Trick.

Wenn man den Schlüssel bei jeder Fahrt wie eine Butterstulle ein- und auspacken muss, kann von Komfort allerdings keine Rede mehr sein.

Zusammengefasst: Keyless-Go-Systeme, durch die sich Autos automatisch öffnen, schließen und starten lassen, sind eine Sicherheitslücke. Gegen den elektronischen Diebstahltrick von Kriminellen ist derzeit kein Hersteller immun. Deshalb sollte man auf das meist teure extra verzichten - oder man muss seinen Schlüssel mit Alufolie umständlich gegen das Risiko schützen.