LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/20360**

02.07.2026

Kleine Anfrage 8348

der Abgeordneten Enxhi Seli-Zacharias und Christian Loose AfD

Fahrzeugdiebstähle im Kreis Borken

Anfang Februar 2026 gelang der Polizei ein Schlag gegen professionelle Autodiebe. Fahrzeuge wurden u. a. in Haan, Neuss, Düsseldorf, Dortmund, Dorsten, Herne, Rheinberg, Duisburg und Gelsenkirchen entwendet. Die Autos wurden nach derzeitigem Stand der Ermittlungen entwendet, indem gezielt die elektronischen Schnittstellen angegangen wurden.[1] So machten sich Täter zuletzt in Gelsenkirchen eine Schwachstelle im Keyless-System zunutze.[2]
Moderne Fahrzeuge nutzen zunehmend funkbasierte Keyless-Zugangssysteme, die den Fahrzeugzugang und den Motorstart ohne aktive Interaktion mit dem physischen Schlüssel ermöglichen. Die Systeme basieren auf einer bidirektionalen Funkkommunikation zwischen dem Fahrzeug und einem Transponder im Schlüssel. Sobald der Transponder innerhalb eines definierten Empfangsbereichs detektiert wird, autorisiert das Steuergerät des Fahrzeugs das Entriegeln der Türen sowie den Startvorgang.
Keyless-Systeme arbeiten typischerweise mit einer Kombination von niederfrequenten LF-Signalen zur Distanzmessung und hochfrequenten HF-Signalen zur Authentifizierung. Das Fahrzeug sendet periodisch LF-Anfragen aus, auf die der Schlüssel mit einem HF-Antwortsignal reagiert. Die Fahrzeugsteuerung interpretiert die Antwort als Nachweis der Schlüsselpräsenz und gibt daraufhin die Schließ- und Startfunktionen frei.
Diese Architektur ist anfällig für sogenannte Relay-Attacken (Reichweitenverlängerungsangriffe). Dabei wird das legitime HF-Signal des Schlüssels über externe Geräte abgefangen, verstärkt und über größere Distanzen weitergeleitet. Ein Auto lässt sich so sekundenschnell illegal öffnen und starten.
Eine Schwachstelle entsteht durch das Fehlen einer verlässlichen Distanzverifikation zwischen Fahrzeug und Schlüssel. Das System checkt zwar die Authentizität des Signals, kann aber nicht anderweitig prüfen, ob der Schlüssel tatsächlich physisch in unmittelbarer Nähe ist. Relay-Geräte können Distanzinformation manipulieren, ohne die kryptografischen Inhalte des Signals zu verändern. Ein „Hacken“ der Daten selbst ist nicht erforderlich, da die Angreifer lediglich die Übertragungsschicht ausnutzen. Aktuelle Untersuchungen zeigen, dass ein Großteil der Fahrzeuge anfällig für Relay-Attacken ist. Nur ein geringer Prozentsatz verfügt über wirksame Schutzmechanismen.
Diese Sicherheitslücke ist unabhängig vom Standort des Schlüssels vorhanden. Das bedeutet, dass das System auch dann missbraucht werden kann, wenn der Transponder sich innerhalb eines Gebäudes befindet oder in einer Tasche getragen wird. Auch die Funkreichweite des

[1] https://mettmann.polizei.nrw/presse/schlag-gegen-professionelle-autodiebe-polizei-klaert-mindestens-zehn-taten-und-nimmt-zwei-tatverdaechtige-fest
[2] https://www.waz.de/lokales/gelsenkirchen/article411326839/hochwertige-suvs-in-gelsenkirchen-gestohlen-das-raet-die-polizei-autobesitzern.html

Datum des Originals: 02.07.2026/Ausgegeben: 03.07.2026

Schlüssels selbst ist dabei unerheblich, da die Relay-Geräte die Distanz künstlich überbrücken.
Ein weiterer kritischer Aspekt betrifft den Fahrzeugbetrieb nach dem Start. Sobald der Motor läuft, wird die Schlüsselpräsenz in vielen Systemen nicht kontinuierlich überprüft.
Relay-Attacken hinterlassen keine physischen Spuren am Fahrzeug. Es entstehen weder Beschädigungen an Türschlössern noch Manipulationsspuren an der Elektronik. Dies führt zu erheblichen Herausforderungen bei der forensischen Analyse. Bei wieder aufgefundenen Fahrzeugen fehlen typische Indikatoren eines Einbruchs, was zu Unsicherheiten bei der Schadensbewertung führen kann.
Keyless-Systeme weisen zusammenfassend strukturelle Schwächen in folgenden Bereichen auf:

- Fehlende Distanzmessung: Die Systeme verlassen sich auf Signalpräsenz statt auf physikalisch verifizierte Entfernung.
- Anfälligkeit der HF-Kommunikation: Die HF-Antwortsignale können ohne kryptografische Manipulation weitergeleitet werden.
- Unzureichende Laufzeitmessung: Die Signallaufzeit wird nicht präzise genug erfasst, um Relay-Angriffe zu erkennen.
- Fehlende kontinuierliche Schlüsselvalidierung: Nach dem Motorstart erfolgt oft keine erneute Authentifizierung.

Diese Faktoren ermöglichen es Angreifern, Fahrzeuge ohne direkten Zugriff auf den Schlüssel zu öffnen und zu starten.[3]
Ein weiterer Aspekt ist, dass der Fahrzeugschlüssel bei jeder registrierten Bewegung kontinuierlich codierte Funksignale aussendet. Darauf basierend existieren weitere Angriffsszenarien, z. B. das gezielte Blockieren („Jamming“) des Schließsignals. In so einem Szenario bleibt das Fahrzeug unverschlossen, wodurch ein Täter anschließend leichter Zugriff bekommt und sich Zugang auf die Fahrzeugsysteme verschaffen kann. Diese Methode kommt beispielsweise in Frankreich häufig zur Anwendung.

Wir fragen daher die Landesregierung:

1. Wie stellt sich in Bezug auf Fahrzeugdiebstähle die aktuelle Gefährdungslage für Fahrzeughalter im Kreis Borken dar?

2. Wie viele Fahrzeuge wurden seit 2022 im Kreis Borken gestohlen? (Bitte differenziert nach Jahr sowie nach Antriebsart listen und dabei auch angeben, inwiefern im Kreis Borken erfasst wird, ob gestohlene Fahrzeuge mit Keyless-Apps oder anderen Schließsystemen vor unberechtigtem Zugriff gesichert waren)

3. Welche konkreten Schutzmaßnahmen empfiehlt die Polizei im Kreis Borken Bürgern, die ihr Fahrzeug, insbesondere bei der Nutzung von Keyless-Apps, wirksam sichern möchten?

4. Welche Fahrzeugtypen oder -modelle sind nach bisherigen Erkenntnissen bei der Nutzung von Keyless-Apps im Kreis Borken besonders von Fahrzeugdiebstählen betroffen? (Bitte auch angeben, welche speziellen Erkenntnisse zur Vorgehensweise der Täter im Kreis Borken vorliegen)

[3] Vgl. https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/keyless/

5. Welche konkreten Maßnahmen planen Polizei und Verwaltung im Kreis Borken, um die Bevölkerung kurzfristig zu informieren, zu schützen und das Sicherheitsgefühl zu stärken?

Enxhi Seli-Zacharias
Christian Loose