

Rund sechs Millionen Teslas ohne UWB bleiben angreifbar — österreichische App TeslaKee schließt die Lücke im Bluetooth-Autoschlüssel

Das Salzburger IT-Sicherheitsunternehmen hinter der Marke IT-Wachdienst.com bringt Sicherheitsforschung ins Produkt: Policy-Engine gegen Relay-Diebstahl, Schutz vor der Ortung von Fahrerinnen und Fahrern und ein ortsabhängiger Auto-Sentry-Modus — vollständig ohne Cloud, ohne Konto und ohne Internetverbindung

Urstein bei Salzburg, 17. August 2026 — Der digitale Autoschlüssel am Smartphone ist bequem — und bei allen Tesla-Fahrzeugen ohne Ultra-Breitband-Technik (UWB) grundsätzlich angreifbar. Die **toothR new media GmbH**, ein österreichisches IT-Sicherheitsunternehmen mit Sitz im Wissenspark Urstein bei Salzburg, das unter der Marke **IT-Wachdienst.com** kleine und mittlere Unternehmen in Sicherheitsfragen berät, veröffentlicht mit **TeslaKee** eine Smartphone-App, die zwei seit Jahren dokumentierte Schwachstellen des Bluetooth-PhoneKey-Protokolls praktisch entschärft: den **Relay-Angriff, der zum Fahrzeugdiebstahl in Sekunden führt**, und die sogenannte **BlueBait-Attacke, mit der sich Fahrerinnen und Fahrer über gefälschte Fahrzeug-Signale orten lassen — selbst dann, wenn das eigene Auto kilometerweit entfernt steht**.

Das Problem: Das Handy antwortet, ohne nachzudenken

Tesla-Fahrzeuge entriegeln, sobald sich das gekoppelte Smartphone in Bluetooth-Reichweite meldet. Die eingesetzte Kryptografie ist solide. Die Schwachstelle liegt eine Ebene darüber, in der Logik: **Die offizielle App beantwortet jede Authentifizierungsanfrage — bedingungslos, ohne zu prüfen, ob die Situation überhaupt plausibel ist.**

Genau das macht zwei Angriffe möglich.

Gefahr 1: Relay-Angriff — Diebstahl in unter einer Minute

Bei einem Relay-Angriff arbeiten zwei Täter mit zwei handelsüblichen Funkmodulen zusammen. Einer folgt der Fahrzeughalterin ins Einkaufszentrum, der zweite steht am Auto auf dem Parkplatz. Die Funkstrecke zwischen beiden verlängert die Bluetooth-Reichweite künstlich um beliebige Distanzen. Für das Fahrzeug sieht es so aus, als stünde der Besitzer direkt daneben. **Das Auto entriegelt, lässt sich starten und wegfahren — während das Handy unberührt in der Jackentasche steckt.**

Der Angriff wurde von Sicherheitsforscher Martin Herfurt im Rahmen des Projekts TEMPA (trifinite.org) auf Sicherheitskonferenzen live demonstriert und ist als Video dokumentiert („The Tesla Parking Lot Job“, <https://youtu.be/eDbSzVTYqBY>). Er benötigt keine Kenntnis von Passwörtern, keinen Tesla-Account und hinterlässt keine Einbruchsspuren — ein Umstand, der in der Schadensregulierung regelmäßig zu Problemen mit Versicherungen führt.

Neuere Fahrzeuge begegnen dem mit UWB-Distanzmessung: Das Auto misst physikalisch, wie weit das Telefon tatsächlich entfernt ist, und ein weitergeleitetes Signal fliegt auf. **Diesen Schutz hat die große Mehrheit der Fahrzeuge jedoch nicht.**

Die weltweite Tesla-Flotte mit Bluetooth-PhoneKey wird derzeit auf **rund acht Millionen Fahrzeuge** geschätzt. Davon sind **nur etwa 20 Prozent mit UWB ausgestattet** — der Schutz kam erst mit den jüngsten Modellgenerationen und damit erst spät in eine Flotte, die seit Jahren wächst. **Für rund sechs Millionen Fahrzeuge bleibt Bluetooth allein die Grundlage des Zugangs**, verteilt nach Modellgeneration:

Modell	UWB erst ab	Ohne UWB (betroffen)
Model S / X	Modelljahr 2021 (Palladium)	alle älteren S/X
Model 3	Modelljahr 2024 („Highland“)	alle Vor-Highland-Model-3
Model Y	Modelljahr 2025 („Juniper“)	alle Vor-Juniper-Model-Y

Erschwerend kommt hinzu: UWB schützt nur, wenn **Fahrzeug und Smartphone** die Technik beherrschen. Ein Großteil der verbreiteten Android-Geräte hat keinen UWB-Chip. Selbst Besitzer eines neuen Fahrzeugs fallen damit still auf die ungeschützte Bluetooth-Ebene zurück.

Gefahr 2: Die BlueBait-Attacke — Fahrer werden ortbar, auch fernab ihres Fahrzeugs

Weniger bekannt, aus Sicht des Datenschutzes aber gravierender ist ein Angriff, den die Forschung als **BlueBait-Attacke** bezeichnet — nach dem Köder, mit dem gearbeitet wird: **Die offizielle App antwortet auch auf gefälschte Fahrzeuge**. Wer einen nachgebauten Tesla-Beacon betreibt — ein Gerät für wenige Euro — bekommt von jedem vorbeigehenden Tesla-Fahrer eine Antwort des Smartphones. Damit lässt sich zuverlässig feststellen: **Diese konkrete Person war zu dieser Uhrzeit an diesem Ort.**

BlueBait funktioniert vollkommen unabhängig davon, wo das Auto steht. Die Halterin muss nicht in der Nähe ihres Fahrzeugs sein — es genügt, dass sie ihr Telefon dabei hat. Mehrere solcher Beacons, verteilt über eine Stadt, ergeben ein Bewegungsprofil.

Die Anwendungsfälle sind unangenehm konkret: **Stalking, häusliche Gewalt und Nachstellung, verdeckte Beobachtung durch Dritte, kommerzielles Kunden-Tracking im Einzelhandel, das Ausspähen von Fahrzeugen als Vorbereitung eines Diebstahls**. Betroffene bemerken davon nichts — es gibt keine Anzeige, keinen Hinweis, kein Protokoll.

Eine technische Dokumentation des Angriffs ist unter <https://trifinite.org/stuff/bluebait/> veröffentlicht.

Entscheidend dabei: Gegen BlueBait hilft UWB nicht. Die Distanzmessung greift erst, wenn das Fahrzeug die Nähe des Telefons überprüft — sie verhindert den Diebstahl. Die Ortung entsteht aber schon eine Stufe davor, allein dadurch, dass das Telefon auf eine Anfrage überhaupt reagiert. **Von der Ortbarkeit sind deshalb auch Halterinnen und Halter brandneuer Fahrzeuge mit UWB betroffen.** Solange die Entscheidung, ob geantwortet wird, nicht auf dem Telefon selbst getroffen wird, bleibt das Problem bestehen.

Zum Selbsttest: Was ein Fremder im Vorbeifahren über ein Fahrzeug erfährt

Wer beurteilen möchte, wie sichtbar das eigene Fahrzeug tatsächlich ist, braucht dafür kein Sicherheitslabor und muss auch nichts kaufen. Mit der Android-App **Tesla Radar** lässt sich nachvollziehen, welche Bluetooth-Informationen ein vorbeifahrendes oder geparktes Tesla-Fahrzeug ungefragt in seine Umgebung sendet — und was davon für jede Person mit einem Smartphone in Reichweite lesbar ist.

Am aufschlussreichsten ist dabei der Fahrzeugname: Tesla-Fahrzeuge tragen einen frei wählbaren Bluetooth-Namen, den viele Halterinnen und Halter auf ihren eigenen Vor- oder Nachnamen setzen. Dieser Name wird permanent ausgestrahlt. Wer die App laufen lässt, sieht binnen weniger Minuten im Straßenverkehr, wie viele Fahrzeuge sich damit faktisch namentlich zu erkennen geben — und wie zuverlässig sich ein einzelnes Fahrzeug so über Tage hinweg wiedererkennen ließe.

Tesla Radar stammt aus demselben Forschungsumfeld wie TeslaKee, ist aber ein reines Beobachtungswerkzeug: Es sendet nichts, greift auf kein Fahrzeug zu und kann nichts steuern. Die App ist kostenlos; ein optionaler Supporter-Beitrag unterstützt die Weiterentwicklung, schaltet aber keine wesentlichen Funktionen frei — für den hier beschriebenen Selbsttest wird er nicht benötigt (<https://play.google.com/store/apps/details?id=com.toothr.teslaradar>). **Der Punkt dieses Hinweises ist nicht der Vertrieb einer weiteren App, sondern eine Erkenntnis, die man schwer wieder vergisst:** Das eigene Auto und das eigene Telefon reden bereits heute mit jedem, der zuhört. Die Frage ist allein, wie viel sie preisgeben.

Die Lösung: TeslaKee prüft erst, dann antwortet es

TeslaKee tritt **nicht** an die Stelle der offiziellen Tesla-App. Es setzt gezielt an der einen Stelle an, die Tesla unsicher umgesetzt hat: **dem Bluetooth-Teil, also dem digitalen Schlüssel im Telefon.** Genau dort schaltet TeslaKee eine **Policy-Engine** vor jede Antwort:

Fahrzeug → Authentifizierungsanfrage → [Policy-Engine] → Antwort ODER Schweigen

Passt der Kontext des Geräts nicht zu einer plausiblen Annäherung an das eigene Auto, **schweigt die App.** Das weitergeleitete Signal des Angreifers läuft ins Leere, das Fahrzeug bleibt verschlossen — und der BlueBait-Köder des Stalkers bekommt schlicht keine Antwort, aus der sich eine Anwesenheit ableiten ließe. **Ein und derselbe Mechanismus schützt damit Fahrzeug und Privatsphäre.**

Ergänzung statt Ersatz

Alles, was die offizielle Tesla-App über das Internet leistet, bleibt dort, wo es hingehört: Navigationsziele senden, Software-Updates, Supercharger-Planung, Servicetermine, der Blick aufs Fahrzeug aus hunderten Kilometern Entfernung. Diese Funktionen setzen eine Verbindung zu Teslas Servern voraus und werden von TeslaKee weder ersetzt noch beeinträchtigt — **beide Apps lassen sich parallel betreiben**.

TeslaKee übernimmt den Nahbereich: alles, was über Bluetooth in unmittelbarer Fahrzeugnähe passiert. Das ist genau der Teil, in dem die beschriebenen Schwachstellen liegen — und zugleich der Teil, den man im Alltag am häufigsten benutzt. Für den Parallelbetrieb wird der offiziellen App lediglich der Bluetooth-Zugriff entzogen (Android-Berechtigung „Geräte in der Nähe“); ihr Schlüssel bleibt im Fahrzeug hinterlegt, damit sämtliche Cloud-Funktionen erhalten bleiben. Eine bebilderte Anleitung dafür liefert TeslaKee mit.

Die Policies: Regeln, die die Fahrerin selbst festlegt

TeslaKee bringt einen Baukasten prüfbarer Kontextregeln mit. Jede lässt sich einzeln aktivieren und als **Pflichtregel** (muss immer erfüllt sein) oder **optionale Regel** (zählt auf ein einstellbares Quorum ein) konfigurieren:

Policy	Prüfung
Bewegungserkennung	Hat sich das Telefon zuletzt tatsächlich bewegt — oder liegt es seit einer Stunde auf der Küchentheke?
GPS-Geofence	Befindet sich das Telefon in einer selbst definierten Zone (Zuhause, Arbeit, Stammparkplatz)?
Letzter Parkplatz	Passiver Zugang nur dort, wo das Fahrzeug zuletzt tatsächlich abgestellt wurde — inklusive Abgleich der damals sichtbaren Mobilfunkzellen
Vertrauenswürdiges WLAN	Ist das Telefon in einem bekannten Netz (SSID + BSSID) eingebucht?
Zeitfenster	Passiver Zugang nur zu Zeiten, in denen das Auto realistisch genutzt wird — pro Wochentag einstellbar
Signalstärke (RSSI)	Ist das Fahrzeugsignal stark genug für echte Nähe?
Schrittzähler-Gate	Ist die Person kürzlich tatsächlich gegangen?
Höhensperre	Stimmt die barometrische Höhe mit jener beim Abstellen überein — Parkdeck-Ebene statt Erdgeschoss?
Bildschirmstatus	Wurde das Gerät kürzlich entsperrt, ist die Besitzerin also aktiv?
Erlaubte Mobilfunkzellen	Ist das Gerät in einer vertrauten Funkzelle?

Für legitime Ausnahmen — Fahrzeugübergabe, Werkstattbesuch, Urlaubsparkplatz — gibt es eine **zeitlich befristete manuelle Übersteuerung** (15/30/60 Minuten), auch direkt aus der Schnelleinstellungs-Kachel des Android-Systems. Ein integrierter **Policy-Test** zeigt live im

Sekundentakt, welche Regel gerade greift und warum. Sicherheit, die man nicht nachvollziehen kann, wird abgeschaltet — deshalb macht TeslaKee jede Entscheidung sichtbar.

Häufige Steueraufgaben direkt in der App — ohne Umweg über die Cloud

TeslaKee ist nicht nur ein Türöffner. Die im Alltag am häufigsten gebrauchten Funktionen sind direkt in der App erreichbar und werden **lokal über Bluetooth** an das Fahrzeug übertragen — ohne Tesla-Account, ohne Internetverbindung, ohne Server dazwischen. Das funktioniert auch in der Tiefgarage ohne Empfang:

- **Ver- und Entriegeln**, Kofferraum und Frunk öffnen
- **Fenster lüften und schließen** — auf Wunsch automatisch beim Verriegeln
- **Ladeanschluss** öffnen und schließen, **Ladelimit** und **Ladezeitplan** setzen (Start- oder Abfahrtszeit)
- **Klimatisierung** samt Sitzheizung, Innen- und Außentemperatur, Hunde- und Camp-Modus
- **Mediensteuerung** — Titel, Wiedergabe, Lautstärke
- **Live-Fahrzeugstatus** — Schließzustand, Öffnungen, Gang, Schlafzustand
- **Auto-Sperre beim Weggehen**, sobald das Bluetooth-Signal abfällt
- **NFC-Kartenemulation (Android)**: Das Telefon ersetzt die Keycard an der B-Säule — als verlässliche Rückfalloption, wenn Bluetooth bewusst blockiert oder nicht verfügbar ist

Auto-Sentry-Modus: Wachsamkeit dort, wo sie gebraucht wird

Der Sentry-Modus von Tesla überwacht das abgestellte Fahrzeug per Kamera — kostet aber Reichweite und protokolliert in der eigenen Garage vor allem die eigene Familie. Deshalb bleibt er bei vielen Fahrern schlicht dauerhaft aus. Genau dann fehlt er, wenn es darauf ankommt.

TeslaKee automatisiert die Entscheidung anhand des Parkorts:

- Wird das Fahrzeug **außerhalb aller vertrauten Zonen** abgeschlossen — Innenstadt, Bahnhofsparkplatz, Hotel, fremdes Land —, **aktiviert TeslaKee den Sentry-Modus automatisch**.
- Wird es **innerhalb einer vertrauten Zone** abgeschlossen — eigene Garage, Firmenparkplatz —, **schaltet TeslaKee ihn wieder ab** und spart Energie. Diese Abschaltung ist bewusst separat schaltbar: In der falschen Situation zu aktivieren ist harmlos, in der falschen Situation zu deaktivieren nicht.

Dabei werden **dieselben Geofences** verwendet, die ohnehin für den passiven Zugang definiert sind — es ist nichts zusätzlich einzurichten. Die Umschaltung erfolgt exakt im Moment des Verriegelns, dem letzten Zeitpunkt, zu dem das Fahrzeug noch erreichbar ist. **Ein schlafendes Fahrzeug wird dafür nie geweckt**, um keine Reichweite zu verbrauchen. Anschließend liest die App den tatsächlichen Zustand zurück — gemeldet wird nur, was das Fahrzeug bestätigt hat.

Ohne Internet, ohne Cloud: Es gibt keinen Server, der ausfallen oder erbeutet werden kann

Der vielleicht wichtigste Unterschied ist einer, den man im Betrieb gar nicht bemerkt: **TeslaKee kommt vollständig ohne Internetverbindung aus.** Es gibt **keinen Tesla-Account, keine Anmeldung, kein Benutzerkonto, keinen Server des Anbieters** — die App spricht ausschließlich direkt per Bluetooth mit dem Fahrzeug.

Keine der vertraulichen Zugangsinformationen verlässt jemals den gesicherten Bereich im Smartphone. Der private Schlüssel wird im StrongBox-Sicherheitschip des Geräts erzeugt und ist von dort **technisch nicht auslesbar** — auch nicht durch die App selbst, auch nicht auf einem kompromittierten Telefon, auch nicht durch den Hersteller. Sämtliche kryptografischen Operationen finden innerhalb dieses Chips statt.

Das hat drei praktische Folgen:

- **Kein zentrales Angriffsziel.** Wo keine Zugangsdaten auf einem Server liegen, kann auch keine Datenbank mit Fahrzeugzugängen gestohlen werden. Ein Einbruch beim Anbieter hätte für Nutzerinnen und Nutzer keine Konsequenzen — es gibt dort schlicht nichts zu holen.
- **Kein Fahrprofil, nirgends.** GPS-Positionen, Geofences und Parkorte werden ausschließlich auf dem Gerät ausgewertet und nicht übertragen. Der Anbieter weiß nicht, wo ein Fahrzeug steht, wann es benutzt wurde oder wem es gehört. Es findet **kein Tracking und keine Analyse des Nutzungsverhaltens** statt; Protokolle bleiben lokal und löschen sich automatisch.
- **Funktioniert, wo es darauf ankommt.** Tiefgarage, Parkdeck, Funkloch, Ausland ohne Datenroaming, Serverstörung beim Hersteller: Nichts davon berührt TeslaKee. Bluetooth genügt.

Ergänzend gilt: **Ein Schlüssel lässt sich ausschließlich mit physischem Zugang anlernen** — mit der NFC-Keycard direkt am Fahrzeug. Zusätzlich überwacht TeslaKee die Schlüsselliste des Fahrzeugs und meldet, wenn ein fremder Schlüssel hinzukommt — ein bekanntes Diebstahlmuster.

Zur Einordnung: keine neuen Angriffstechniken

Beide hier beschriebenen Schwachstellen sind **seit 2022 öffentlich dokumentiert**. Sie wurden im Rahmen von Projekt TEMPA (trifinite.org) untersucht und erstmals auf der Sicherheitskonferenz **CanSecWest 2022 in Vancouver** öffentlich vorgestellt; seither sind sie samt Demonstrationsvideo frei zugänglich. **Bis heute — mehr als vier Jahre später — ist die Lücke in Millionen Fahrzeugen unverändert offen.** Mit dieser Mitteilung werden **keine bislang unbekannten Details und keine neuen Angriffswerkzeuge veröffentlicht** — es wird nichts offengelegt, was einem Angreifer heute nicht ohnehin zur Verfügung stünde.

Neu ist ausschließlich die Gegenmaßnahme. Das Ziel dieser Mitteilung ist entsprechend nicht die Beschreibung eines Problems, sondern der Hinweis, dass es für Fahrzeuge ohne UWB nun eine praktikable Lösung gibt.

Zitat

„Die Verschlüsselung von Tesla ist in Ordnung — das Problem ist, dass das Telefon jede Frage beantwortet, ohne sich zu fragen, wer da eigentlich fragt. Ein Auto, das aufgeht, weil jemand mein Signal aus dem Supermarkt auf den Parkplatz verlängert hat, ist die eine Hälfte. Die andere Hälfte ist, dass ein zwanzig Euro teures Bastelgerät am Straßenrand mitschreiben kann, wann ich vorbeigegangen bin — dafür muss mein Auto nicht einmal in der Nähe sein. Gegen den Diebstahl hilft UWB tatsächlich, aber nur bei neuen Fahrzeugen mit passendem Telefon. Gegen das Mitschreiben hilft es überhaupt nicht: Das Telefon antwortet dem gefälschten Beacon weiterhin, auch im nagelneuen Auto. Deshalb muss die Entscheidung, ob überhaupt geantwortet wird, auf das Telefon — und genau das macht TeslaKee.“ — *DI (FH) Martin Herfurt, IT-Sicherheitsberater bei IT-Wachdienst.com, Lehrbeauftragter an der Fachhochschule Salzburg und Sicherheitsforscher im Projekt TEMPA (trifinite.org)*

Verfügbarkeit und Preis

TeslaKee ist **ab sofort für alle Interessierten öffentlich verfügbar** — für **Android ab Version 10**, vorausgesetzt wird ein Gerät mit StrongBox-Sicherheitschip (verbreitet ab Baujahr 2019). Parallel läuft weiterhin ein internes Testprogramm, dessen Rückmeldungen in die Weiterentwicklung einfließen. Kompatibel sind Tesla Model 3, Y, S und X mit Bluetooth-PhoneKey. Für die einmalige Schlüsselanmeldung wird die NFC-Keycard des Fahrzeugs benötigt.

- **Kostenlos:** manuelles Ver- und Entriegeln, Fahrzeugstatus, Schnellaktionen
- **Premium (2,99 € / Monat oder 29,99 € / Jahr):** Policy-Engine und passiver Zugang, Auto-Sentry-Modus, Hintergrundbetrieb, Mediensteuerung, Protokollierung

Der Bezug erfolgt über Google Play sowie über alternative Vertriebswege: <https://play.google.com/store/apps/details?id=com.teslakee.teslakee>

iPhone-Version in Arbeit

An einer **TeslaKee-App für das iPhone** wird bereits gearbeitet. Sie setzt dieselbe Policy-Engine um und legt die Schlüssel in der **Secure Enclave** des Geräts ab — dem Apple-Gegenstück zum StrongBox-Chip. Damit steht der Schutz vor Relay-Diebstahl und BlueBait-Ortung künftig auch iPhone-Fahrerinnen und -Fahrern zur Verfügung, die von der UWB-Lücke besonders betroffen sind: Ihr Telefon bringt die Technik zwar mit, nützt ihnen bei einem älteren Fahrzeug ohne UWB aber nichts.

Ein Veröffentlichungstermin steht noch nicht fest. Interessierte können sich unter presse@it-wachdienst.com für Informationen zum Start der Beta vormerken lassen.

Über das Unternehmen

Die **toothR new media GmbH** ist ein **österreichisches IT-Sicherheitsunternehmen mit Sitz im Wissenspark Urstein bei Salzburg** — direkt neben dem Campus der Fachhochschule Salzburg.

Die Nähe ist keine zufällige: **Martin Herfurt, IT-Sicherheitsberater des Unternehmens, ist zugleich Lehrbeauftragter an der Fachhochschule Salzburg** und gibt dort weiter, woran im Unternehmen praktisch gearbeitet wird. Darüber hinaus organisiert er die Salzburger IT-Sicherheitskonferenz **HXZ.ONE**, die am 24. März 2027 zum dritten Mal stattfindet.

Unter der Marke **IT-Wachdienst.com** berät das Unternehmen **kleine und mittlere Unternehmen** in Fragen der IT-Sicherheit: von der Absicherung drahtloser Infrastruktur über Sicherheitsüberprüfungen und Schwachstellenanalysen bis zur Begleitung von Sicherheitsvorfällen. Der fachliche Schwerpunkt liegt auf drahtlosen Technologien — Bluetooth, NFC und Funkschließsystemen — sowie auf der Absicherung vernetzter Fahrzeuge. Gerade KMU verfügen selten über eigene Sicherheitsabteilungen, stehen aber vor denselben Bedrohungen wie Konzerne.

Aus derselben Forschungsarbeit stammt auch **Tesla Radar**, eine Android-App, mit der sich sichtbar machen lässt, welche Bluetooth-Informationen Fahrzeuge in ihre Umgebung senden. Sie dient der Aufklärung und ist kostenlos nutzbar; ein optionaler Supporter-Beitrag finanziert die Weiterentwicklung, ohne den Funktionsumfang wesentlich zu erweitern.

TeslaKee ist das erste kostenpflichtige Endkundenprodukt des Hauses. Es entstand direkt aus mehrjähriger Analyse des Tesla-BLE-PhoneKey-Protokolls im Rahmen von Projekt TEMPA (trifinite.org) und folgt demselben Grundsatz wie die Beratungsarbeit: erkannte Schwachstellen nicht nur beschreiben, sondern schließen.

Pressekontakt

toothR new media GmbH · Marke IT-Wachdienst.com DI (FH) Martin Herfurt, IT-Sicherheitsberater Urstein Süd 15 5412 Puch bei Hallein, Österreich

Mobil: +43 676 3787909 Presse und Anfragen: presse@it-wachdienst.com Web: <https://it-wachdienst.com> · <https://teslakee.com>

Bildmaterial, Screenshots, das Video der Relay-Angriffs-Demonstration sowie Interviewtermine mit Martin Herfurt stellen wir auf Anfrage zur Verfügung. Für Fachredaktionen bieten wir eine technische Live-Demonstration des Relay-Angriffs und der Abwehr durch die Policy-Engine an.

Terminhinweis für Redaktionen: Die von Martin Herfurt organisierte Salzburger IT-Sicherheitskonferenz **HXZ.ONE** findet am **24. März 2027 im Jazzit Musik Club Salzburg** zum dritten Mal statt: <https://3.hxz.one/> — Programm und Akkreditierung auf Anfrage.

Hinweis: Die toothR new media GmbH (Marke IT-Wachdienst.com) ist ein unabhängiges Unternehmen und steht in keiner Verbindung zu Tesla, Inc.; es ist von Tesla weder autorisiert noch gesponsert. „Tesla“ sowie alle zugehörigen Marken, Logos und Handelsnamen sind Eigentum von Tesla, Inc. TeslaKee kommuniziert über das öffentlich zugängliche Bluetooth-Low-Energy-PhoneKey-Protokoll. Änderungen an Fahrzeugfirmware oder Protokoll durch Tesla können die Funktion beeinflussen.