VW Datenpanne: Zahlreiche Standortdaten im Internet zugänglich

Dass Autos heutzutage mit einer eigenen Software ausgestattet und mit Apps verknüpft sind, ist mittlerweile der Normalfall. Diese Anwendungen ermöglichen oft erst die Ausschöpfung der vollen Funktionen des Fahrzeugs. Zudem können damit Daten über das Fahrzeug und dessen Nutzung gesammelt werden, was von den Automobilunternehmen umfassend genutzt wird, nicht zuletzt für die Weiterentwicklung der Fahrzeuge und ihrer Funktionen. Dass Softwarehersteller hierbei besonders auf die Sicherheit dieser Daten achten müssen, verdeutlichte jüngst eine Datenpanne bei Volkswagen.

800.000 Fahrzeugdaten online zugänglich

„Kurios bis bedenklich" ordnete der Chaos Computer Club (CCC) seine Entdeckung ein, die er zu einem wortwörtlich bewegenden Abschluss des Jahres 2024 mit der (Datenschutz)Welt teilte: Bewegungsdaten von ca. 800.000 Fahrzeugen waren über mehrere Monate im Internet zugänglich. Die Daten lagen in einem Cloud-Speicher, der mit den nötigen Programmen und IT-Wissen relativ leicht aufzufinden war. Betroffen waren gewisse Modelle von Elektrofahrzeugen der Marken VW, Skoda, Audi und Seat. Einsehbar waren Daten über den Batterieladestand, den Inspektionsstatus oder darüber, ob der Motor gerade eingeschaltet war.

Doch das ist bei Weitem nicht alles: Bei 460.000 Fahrzeugen – und damit mehr als der Hälfte – waren die exakten Positionen der Abstellorte der Fahrzeuge mit Uhrzeiten einsehbar. Die Standorte wurden durch Längen- und Breitengrade angegeben und waren bei VW- und Seat-Modellen bis auf zehn Zentimeter (!) genau. Die Standorte der anderen Pkws waren bis auf zehn Kilometer genau, was deutlich weniger Aussagekraft hat, an sich jedoch nicht weniger problematisch ist. Denn bei den meisten Fahrzeugdaten konnte über die ebenfalls einsehbaren Zugangsdaten der Nutzer der VW-App eine Verknüpfung zu Namen und Kontaktdaten der Fahrer oder Eigentümer hergestellt werden. So ließen die in dem Cloud-Speicher

belegenden Datensätze Einblicke in den Alltag und die Bewegungsmuster etlicher Menschen zu.

Die meisten Daten betreffen Fahrzeuge in Deutschland. Aber auch Daten von Fahrzeugen in Norwegen, Schweden, Großbritannien und den Niederlanden tauchten in dem Cloud-Speicher auf.

Zügige Reaktion vermeidet unter Umständen schwere Folgen

Verantwortlich für diese Veröffentlichung war die VW-Tochtergesellschaft Cariad, zuständig für die Software-Entwicklung der VW-Group, die jedoch nicht selbst auf ihren Fehler aufmerksam wurde. Ein anonymer Hinweisgeber wandte sich an den CCC und den Spiegel.

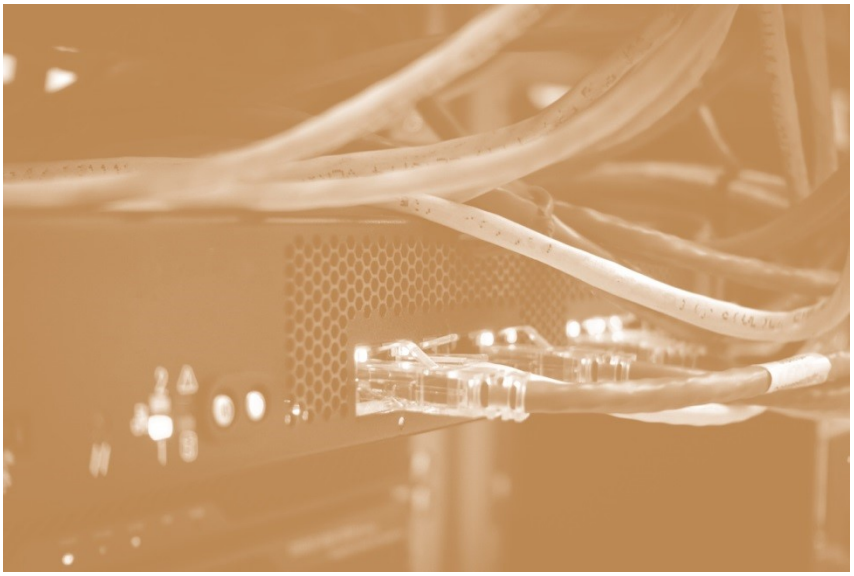
Den erheblichen Gefahren, die aus einer solchen „Fehlkonfiguration", wie Cariad sie nannte, folgen können, sollten sich Softwareentwickler besonders bewusst sein. Das zeigt diese Sicherheitslücke ganz besonders: Sie betraf Fahrzeug- und Bewegungsdaten zahlreicher Politiker, Polizeibeamter und Nachrichtendienstmitarbeiter. In solchen Fällen sind genaue Aufenthaltsorte oft sehr sensible Informationen. Aber auch für Privatpersonen kann es durchaus gefährlich werden, wenn einsehbar ist, wann sie zu Hause sind oder wann nicht. Mit Blick auf Einbrüche und Erpressungen bieten diese sensiblen Angaben eine wahre Datenschatzgrube für Kriminelle! Auch glaubwürdige Phishingmails par excellence hätten mithilfe dieser Informationen erstellt werden können, um an Kreditkarten und Zahlungsinformationen von Kunden zu gelangen.

Cariad hat zügig reagiert und die Verantwortung übernommen. Die Sicherheitslücke wurde geschlossen. Auch für betroffene Personen gab es Entwarnung: Das Unternehmen informierte darüber, dass es unwahrscheinlich sei, dass irgendjemand außer den Sicherheitsexperten, die das Datenleck untersucht hatten, tatsächlich auf die Daten zugegriffen habe. Auch der CCC habe lediglich auf Daten zugreifen können, die keine Rückschlüsse auf einzelne Personen zuließen.

Dennoch gilt: Solche Vorkommnisse sollten im Vorfeld vermieden werden, denn Vorsicht ist besser als Nachsicht – ganz besonders, wenn es um die IT- und Datensicherheit geht.

Verschärfung der IT-Sicherheit

Die IT-Sicherheit wird derzeit auch regulatorisch für viele zunehmend verschärft: Die NIS-2-Richtlinie ist zeitnah in nationales Recht umzusetzen und verpflichtet rund 30.000 Unternehmen in Deutschland zu einer verschärften IT-Sicherheit. Ende 2024 wurde zudem der Cyber Resilience Act, eine EU-Verordnung, verkündet, die ab 2027 zu umfassenden IT-Sicherheitsvorgaben für digitale Produkte von der Software bis zum IoT-Gerät verpflichtet. Unter diesen neuen Rechtsakten ist eine Panne wie bei VW dann neben dem Datenschutzrecht auch nach diesen Rechtsakten strafbewehrt und abzustellen.



Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49 221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49 221 65065-200
simon.kohm@loschelder.de

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-465
rebecca.mossner@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de