Date: 11.07.2019

AUTOMOBIL REVUE

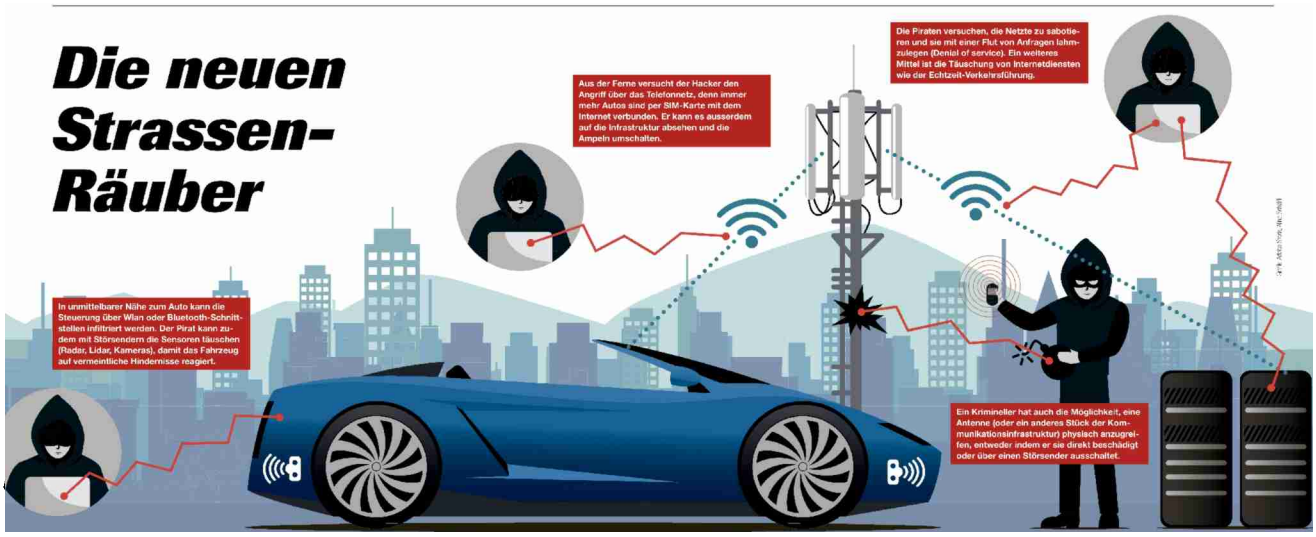
Automobil Revue
3172 Niederwangen
031 330 14 00
https://www.automobilrevue.ch/

Genre de média: Médias imprimés
Type de média: Magazines spéc. et de loisir
Tirage: 11'568
Parution: 48x/année

Page: 2
Surface: 172'757 mm²

Ordre: 1072864
N° de thème: 377.006

Référence: 74135325
Coupure Page: 1/3



CYBERSICHERHEIT Die Verbreitung der autonomen Autos wird zweifellos von einer neuen Sicherheitsgefahr begleitet werden, dem Hacking. Was könnte die Existenz autonomer Autos gefährden?

Lorenzo Quolantoni

Das autonome Fahren beflügelt schon seit Jahrzehnten die Fantasie der Autowelt, es birgt die Hoffnung, nach entspannter Fahrt frisch am Zielort anzukommen. Die Hersteller treiben die Entwicklung seit Jahren voran, angespornt vom potenziellen Gewinn etwa gegenüber anderen Marken und dem Aufbau von Dienstleistungen wie den Robo-Taxis.

Neue Mobilitätslösungen werden immer dringlicher, denn bis 2050 sollen gemäss einer Vorhersage der Vereinten Nationen vom vergangenen Jahr 68 Prozent der Bevölkerung in Städten wohnen (heute 55%). Dieses Szenario lässt mehr Verkehrsstaus erwarten, obwohl bereits heute die Situation in den Grossstädten alles andere als flüssig aussieht: Nennen wir nur das Beispiel Tokio, wo die Durchschnittsgeschwindigkeit eines Autos gemäss dem Zulieferer Bosch nur 15 km/h beträgt.

Kein Erfolg ohne Sicherheit

Aber diese tolle Profitmaschine hat einen Haken, noch bevor sie überhaupt in die Wirklichkeit umgesetzt wurde: Die Sicherheit ist noch nicht gewährleistet. Falls die fahrerlosen Autos nicht belegen können, dass sie viel sicherer unterwegs sind als die Menschen, werden sie Mühe haben, von der Öffentlichkeit anerkannt zu werden. Der Vorstandsvorsitzende des VW-Konzerns formulierte das Dilemma vergangenen November so: «Ein Verhältnis von eins zu zehn ist ungenügend. Wir beklagen pro Jahr etwa 3200 Tote auf den deutschen Strassen. Es wäre ein Desaster, wenn 320 Menschen in autonomen Autos umkommen würden.»

Um dieser Gefahr vorzubeugen, betreiben die Hersteller ihre eigenen Entwicklungen der autonomen Autos, die in allen Situationen sicher und zuverlässig arbeiten müssen. Allerdings könnten all ihre Anstrengungen markante Rückschläge erfahren, wenn sich Informatikpiraten in die Systeme dieser Fahrzeuge einschleichen. Die amerikanische Zeitschrift «Wired» hatte unzählige Alarmglocken in der Industrie zum Läuten gebracht, als ihre zwei Hacker – Chris Valasek und Charlie Miller – aus der Ferne die Kontrolle über einen Jeep Cherokee übernahmen. Die beiden Informatiker hatten eine Schwäche in der Infotainmentanlage ausgebeutet,

Date: 11.07.2019

AUTOMOBIL REVUE

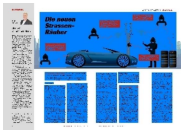
Automobil Revue
3172 Niederwangen
031 330 14 00
https://www.automobilrevue.ch/

Genre de média: Médias imprimés
Type de média: Magazines spéc. et de loisir
Tirage: 11'568
Parution: 48x/année

Page: 2
Surface: 172'757 mm²

Ordre: 1072864
N° de thème: 377.006

Référence: 74135325
Coupure Page: 2/3



übernahmen die Steuerung und hatten volle Kontrolle über Gas und Bremse des Fahrzeugs. Im Jahr 2016 war es eine Gruppe chinesischer Forscher, die über den Internetbrowser und das Stereosystem einen Tesla Model S kaperte. Sie gewann die Kontrolle über einige harmlose Funktionen wie die Verstellung der Rücksitze. Aber auch äusserst kritische Systeme wie die Bremsen konnte sie steuern.

Rollende Computer

Daran ist nichts Überraschendes: Das Automobil wird, genauso wie alle vernetzten Systeme, anfällig, wenn es ans Internet angebunden wird. «Die Autos haben sich zu rollenden Computern entwickelt», meint Thierry Hayoz, 5G-Fachmann bei der Swisscom. «Um eine sichere Funktion von A bis Z garantieren zu können, müssen alle drei Elemente eines Fahrzeugs abgedeckt werden: Technik, Datenübermittlung und Apps.»

Sehen wir uns zunächst das erste Glied in der Kette an, das Fahrzeug selbst. Die Informatikpiraten können in unmittelbarer Nähe Schwächen in der Bluetooth-Schnittstelle (handfreies Telefonieren) oder das Wlan ausbeuten, um in die Systeme des Autos einzudringen. Die Hacker können dann die verschiedenen Sensoren täuschen, auf denen das autonome Fahren aufbaut: Distanzmessung, Kameras, Lidar, Radar und GPS. Ihr Ziel ist, dem Auto eine falsche Realität vorzugaukeln und dadurch Fehlreaktionen auszulösen. Forscher der Universitäten von South Carolina (USA) und Zhejiang (China) vermochten 2016 mit Störsendern, Geräuschen und Lichtprojektoren die Messinstrumente eines Tesla Model S zu täuschen. Die Luxuslimousine nahm dadurch Hindernisse wahr, die gar nicht existierten und reagierte völlig unberechenbar.

Falsche Antennenrelais

Für diese Art des Angriffs müssen sich die Hacker dem Fahrzeug nähern. Wollen sie ihre Attacke aus der heimischen Stube führen, versuchen sie sich über die Mobilfunkantennen einzuklinken, über die moderne Fahrzeuge per SIM-Karte die Verbindung mit dem Internet sicherstellen. «Es gibt heute Mikrozellen, die sich als Leitantennen tarnen», erklärt Dimitri Konstantas, Professor am Institut für Informatik an der Universität Genf. «Die autonomen Autos können sich an diese anschliessen – im Glauben, über ein traditionelles Netz zu gehen. Von diesem Moment an hat der Hacker die Kontrolle über die Datenübermittlung zum Auto und von ihm weg.» Im schlimmsten Fall können die Übeltäter die Kontrolle über die sicherheitsrelevanten Systeme wie Bremsen, Gas und Lenkung übernehmen, wie im Fall des Cherokee von 2015.

Der zweite Angriffspunkt ist das Netzwerk. Wie beim Auto können physische Vorstösse aus der Nähe auf die Antenne oder via Funkwellen über Störsender lanciert werden. Diese Art von Attacke relativiert Thierry Hayoz: «Es gilt zu beachten, dass ein Auto gleichzeitig immer mit mehreren Antennen verbunden ist, um beim Fahren die konstante Datenübermittlung sicherzustellen. Wenn eine Antenne ausfällt, kann die Dienstleistung dank umliegender Antennen weitergeführt werden.»

Überladene Netze

Die Netzwerke können auch virtuell angegriffen werden, zum Beispiel durch eine Übermenge an Anfragen, was die Verbindung blockiert. Diese als Denial of Service oder Verweigerung des Dienstes bekannten Attacken unterbrechen die Übermittlung der für die autonome Funktion des Fahrzeugs nötigen Daten von den Sendestellen. «Wir nehmen diese Herausforderung sehr ernst, zumal 5G mit einer Bandbreitenvergrösserung einhergeht», erklärt Thierry Hayoz. «Wir suchen nach Anomalien im mobilen Netz, damit wir im Fall einer Cyberattacke die Datenübermittlung aufrechterhalten können. Wir sind in der Lage, die Geräte zu isolieren, welche den Angriff auslösen.»

Entführen der Dienstleistungen

Als dritte Möglichkeit können Cyberangreifer Dienstleistungen stören, die den vernetzten Fahrzeugen geboten werden, etwa die Verkehrsführung in Echtzeit. Ein entsprechendes Beispiel betrifft einen Piraten, der den autonomen Autos falsche Informationen zum Verkehr durchgibt mit dem Ziel, alle Fahrzeuge an ein und dieselbe Stelle hinzulotsen.

All diese Bedrohungen könnten sich mit ihren beträchtlichen Schadenpotenzial ernsthaft auf die Einführung der autonomen Fahrzeuge auswirken. Das meint Cybersicherheits-Expertin und Professorin an der Universität Lausanne Solange Ghernaouti. «Spektakuläre oder breit abgestützte Angriffe können tatsächlich ernsthafte Folgen haben. Ich glaube, man könnte Vergleiche mit dem Flugverbot für die Boeing 737 Max und deren fehlerhaftem Flugleitsystem ziehen.» Die Hersteller sind

Date: 11.07.2019

AUTOMOBIL REVUE

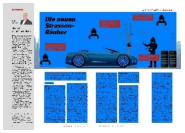
Automobil Revue
3172 Niederwangen
031 330 14 00
https://www.automobilrevue.ch/

Genre de média: Médias imprimés
Type de média: Magazines spéc. et de loisir
Tirage: 11'568
Parution: 48x/année

Page: 2
Surface: 172'757 mm²

Ordre: 1072864
N° de thème: 377.006

Référence: 74135325
Coupure Page: 3/3



sich der Gefahr durchaus bewusst und übernehmen die Initiative. So etwa der amerikanische Pionier Tesla mit der Ausschreibung einer Hacking-Challenge zum Model 3 im Juni: Die Kalifornier boten allen Programmierern, die eine Informatikschwäche bei ihrer Limousine aufdeckten, eine ordentliche Summe Geld.

Aber das sind nur die ersten kleinen Schritte in einem voraussichtlich endlosen Krieg. «Das Hacking ist einfach, es ist ein Katz-und-Maus-Spiel: Sobald man Abwehrmassnahmen eingerichtet hat, sucht der Hacker entsprechend nach neuen Schwachpunkten im System. Man stopft also ein Leck, worauf der Gegner andere strategische Stellen anbohrt. Es ist ein ewiges Seilziehen», meint Dimitri Konstantas. Ausser, dass man nie weiss, was von einem Update zum anderen alles passieren kann. ●

5G IST EINE NOTWENIDKEIT

Die Verbreitung des autonomen Fahrens ist ohne den Ausbau des neuen 5G-Netzwerks nicht machbar. Der Vorteil liegt nicht nur in der viel grösseren Übermittlungskapazität (bis zu 10 Gb/s). «5G übertrifft 4G vor allem bei der Datensendegeschwindigkeit (die Ansprechzeit des Netzes – Red.)», erklärt Thierry Hayoz von der Swisscom. «Über die ganze Datenkette, einschliesslich der Verbindung zu unseren Servern, sprechen wir von einer Latenz von zehn Millisekunden. Das ist vier- bis zehnmal schneller als das, was heute mit 4G machbar ist. Ein vernetztes Auto ist abhängig von der kürzest möglichen Verbindungszeit, um Entscheidungen so nahe an der Echtzeit wie nur möglich treffen zu können.» Der zweite Vorteil dieser Technologie betreffe die Möglichkeit, das Netz je nach Wichtigkeit einer App nach Prioritätsstufen aufzuteilen, meint Thierry Hayoz weiter: «Manche vernetzte Geräte, wie etwa ein Kühlschrank, müssen keine permanente Verbindung haben, wie das bei autonomen Fahrzeugen der Fall ist. Diese brauchen den konstanten Datenaustausch mit hoher Kapazität. Sollte das Netz zur Überlastung neigen, können wir es fragmentieren und Prioritäten setzen.» Die Swisscom hat bekanntermassen bereits im Jahr 2015 in Zürich die Anforderungen von autonomen Fahrzeugen mit Tests eines fahrerlosen Prototyps geprüft.