„Update Verfügbar – ein Podcast des BSI“4

Transkription für Folge 18, 28.02.2022:
Die Mobilität der Zukunft – autonom, vernetzt, sicher

Moderation: Ute Lange, Michael Münz
Gast: Christian Wieschebrink, BSI
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Lange: Hallo und herzlich Willkommen zu einer neuen Ausgabe von „Update verfügbar“, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute Lange.

Münz: Ich bin Michael Münz. Heute haben wir bei uns im Podcast einen Gast zum Thema vernetztes Fahren. Dazu dann später mehr. Erst einmal zurück zu einem Thema, das uns in diesem Podcast in den letzten Wochen regelmäßig beschäftigt hat, nämlich Log4j. Lass uns darüber sprechen, was sich seitdem getan hat.

Lange: Es ist eigentlich nicht mehr so viel passiert, was allerdings nicht heißt, dass es eine totale Entwarnung gibt. Wir hatten letztes Mal mit Christoph Lobmeyer vom BSI darüber gesprochen, was sich dahinter verbirgt. Er hat uns erzählt, dass das BSI die entsprechende Gefahrenstufe für diese Sicherheitslücke in einem Programm von Rot auf Gelb heruntergestuft hat. Das heißt aber nicht, dass alle sich jetzt zurücklehnen sollten. Wir hatten das in der letzten Folge besprochen: Wer noch nicht die aktuellste Version installiert hat, sollte dringend Updates machen. Das Motto unseres Podcasts können wir nur nochmal unterstreichen: Wenn ein Update verfügbar ist, sollte das bitte sofort installiert werden. Michael, dann springen wir mal vom Thema Update zum Thema Backup. Du hast letztes Mal von deinen IT-Neujahrsvorsätzen gesprochen und wolltest eifrig und fleißig Backups von allen deinen Daten machen. Wie ist es dir damit ergangen?

Münz: Ich würde sagen, wie mit vielen Neujahrsvorsätzen: Ich habe erstmal alle meine alten externen Festplatten herausgekramt und war ganz stolz, wie viele Daten ich über die Jahre schon gesichert hatte – das war super. Dann habe ich aber festgestellt, dass ich auf diesen Festplatten von meinem neuen Rechner, der jetzt ein Mac ist, keine Daten auf die Festplatte aufspielen konnte. Ich musste erst einmal recherchieren und habe herausgefunden, dass es damit zu tun hat, dass mein alter Rechner ein Windows-Rechner war und auf dem Rechte aufgespielt sind, die ich mit

dem Mac nicht habe. Lange Rede kurzer Sinn: Ich bin für mehrere Stunden in meinem Kaninchenbau verschwunden und habe recherchiert – und dann habe ich mir irgendwann gedacht, „ich muss jetzt die neue Folge von Boba Fett gucken“, und habe alle Festplatten wieder in die Schublade getan. Aber jetzt ist mir zumindest bewusst, dass ich da noch eine Baustelle habe. Und das ist schon ein Anfang. Das Jahr hat noch 10 Monate.

Lange: Vielleicht gibt dir folgende Geschichte einer Freundin von uns die Motivation, das doch noch mal aufzunehmen. Bei der hat sich ihr Smartphone wegen eines Hardware-Problems zerlegt. Sie hat immer nur daran gedacht, Backups zu machen, sie aber nie durchgeführt. Vielleicht weil sie auch eine Folge von irgendeiner Lieblingsserie gucken musste oder anderweitige Interessen verfolgt hat. Jedenfalls war das Telefon hinüber, und sie stellte fest, dass viele ihrer Daten nicht auf der SIM-Karte gespeichert sind. Das heißt, sie hat einen ziemlich hohen Datenverlust erlitten, und ich soll dir ausrichten, du mögest dich bitte bei ihr melden, weil sie auch deine Telefonnummer nicht mehr hat. Vielleicht gehst du doch in deine Schubladen und machst die Backups schneller als geplant.

Münz: Das mache ich. Danke. Das war der nötige Tritt, den ich brauche.

Lange: Für alle, die jetzt denken, es gibt irgendwas, was sie verpasst haben: bei unterschiedlichen Herstellern funktioniert es unterschiedlich. Prüft einfach, auf welche Einstellungen ihr bei eurem Smartphone achten solltet, damit wichtige Daten wie Kontaktdaten, Telefonnummern, Fotoalben, App-Einstellung und Chatverläufe nicht verloren gehen, wenn man vielleicht einfach nur ein simples Hardware-Problem hat. Dafür braucht man keine Expertise. Vielleicht geht es schneller als bei dir, Michael.

Apropos digitale Kompetenz. Mir ist etwas ins Auge gefallen: Die Süddeutsche Zeitung hat mit einem Forschungsinstitut eine Umfrage bzw. einen Selbsttest dazu entwickelt, wie hoch wir unsere digitale Kompetenz selbst einschätzen. Dazu haben Sie ein paar Tausend Menschen befragt. Es gibt etwa 80 Fragen zu unterschiedlichen Themengebieten. Man kann herausfinden, wie fit man digital in der Welt unterwegs ist und in welchen Bereichen man sich verbessern könnte. Man kann seine Ergebnisse auch mit dem Durchschnitt der Befragten in Deutschland vergleichen. Ich fand es spannend, dass neben Themen wie dem Umgang mit Informationen und Daten, Kommunikation, also welche Messengerdienste nutze ich und wie nutze ich sie, auch das Thema Datensicherheit eine Rolle gespielt hat. Ich habe den Test gemacht. Ich glaube, du auch. Unsere Ergebnisse wollen wir unseren Hörerinnen und Hörer noch nicht verraten, packen aber den Link dazu in die Shownotes und laden euch ein, uns eure Ergebnisse zu schicken. Bei der nächsten Ausgabe können wir schauen, wie

digital die Zuhörerschaft von „Update Verfügbar“ ist. Natürlich haben wir das auch an die Kolleginnen und Kollegen im BSI gegeben und sind gespannt auf die Ergebnisse. Die müssten natürlich bei dem Test 100 Prozent schaffen. Wir sind sehr neugierig, wie das ausgeht.

Münz: Dann machen wir in der nächsten Folge ein Ranking zu den digitalen Kompetenzen und schauen, ob Hörerinnen und Hörer, wir oder die Expertinnen und Experten vom BSI besser abgeschnitten haben. Ich bin gespannt. Schickt uns auf jeden Fall eure Zahlen. Ich habe noch einen Link-Tipp und eine witzige Geschichte, die ich noch loswerden wollte, bevor wir zu unserem Experten wechseln: Ich habe vor ein paar Tagen ein Online Special gesehen zum Thema Hackerinnen und Hacker. Wir haben bei „Update Verfügbar“ schon über Hackerinnen und Hacker gesprochen und für mich ist immer noch nicht ganz klar, was das für Menschen sind und wer hinter den Hacking-Aktionen steckt. Ich denke dabei immer an Stock Fotos, die Agenturen verteilen, auf denen Männer mit Schirmmützen abgebildet sind, die vor einem Rechner sitzen und im Zweifelsfall auch noch Pizza essen. Aber ein Reporterteam vom Bayerischen Rundfunk hat sich auf die Suche nach einem Hackerteam gemacht und eine spannende Dokumentation ins Netz gestellt, die sich wie ein Krimi ansehen lässt. Es geht um eine Hackergruppe, die Snake heißt, angeblich eine der besten oder erfolgreichsten oder perfidesten Hackergruppen, die sich auch in Regierungsnetzwerke einhacken, unter anderem ins Auswärtige Amt. Da waren die über ein Jahr lang aktiv, bis sie Ende 2017 aufgefallen sind. Das BSI war an der Lösung des Falles damals auch beteiligt, wie ich gelesen habe. Sie sind allen Spuren nachgegangen, die die Hackerinnen und Hacker im Netz hinterlassen haben, bis hin zu Namen offensichtlich. Ob das jetzt die richtigen Namen waren oder nicht, sei erstmal dahingestellt. Ich habe zum ersten Mal eine bessere Vorstellung davon bekommen, was das für Menschen sind, die dahinterstecken könnten, was deren Motivation ist und wie sie arbeiten. Die Dokumentation kann ich wirklich nur empfehlen. Total spannend und visuell super aufbereitet. Fand ich total gut.

Lange: Fand ich auch. Du hattest mir die Dokumentation ja zugeschickt. Ich war begeistert. Auch wenn was ganz Ernstes dahintersteckt, hatte das einen gewissen Unterhaltungswert. Das ist vielleicht das falsche Wort, aber es war sehr gut recherchiert, und ich mochte die Aufmachung sehr gerne.

Münz: Es gibt eine andere Geschichte, die ich loswerden wollte, bevor wir das Thema wechseln. Wir hatten in einer vergangenen Folge am Ende des Jahres über Router gesprochen und gesagt, dass man mit modernen Routern die Nutzungszeit des WLANs einschränken oder bestimmte Netze für Gäste einrichten kann. Für Eltern, die den Internetkonsum ihrer Kinder kontrollieren wollen, ist das natürlich ein ganz probates Mittel, um zu schauen, dass die Kleinen nicht den ganzen Tag und die ganze

Nacht am Handy hängen. In Frankreich hat ein Familienvater einen anderen Weg gesucht, um die Internetnutzung seiner Kinder einzuschränken: Er hat einen Störsender aufgestellt, der aber dazu geführt hat, dass das Mobilfunknetz im Nachbarort in der Nachbargemeinde ausgefallen ist.

Lange: Damit ist er also weit über das Ziel hinausgeschossen.

Münz: Die zuständige Behörde in Frankreich hat sich auf die Suche nach diesem Störsender gemacht und das Haus des Familienvaters gefunden. Er hatte das Ding im Internet bestellt und aufgestellt. Das ist in Frankreich, genauso wie in Deutschland, nicht legal, deswegen muss er jetzt mit Strafen rechnen. Bevor man sich Sachen aus dem Internet bestellt und vielleicht den Pfad der Tugend verlässt, sollte man also lieber in die Router-Einstellungen schauen, ob es nicht andere Mittel und Wege gibt, um das tägliche Erziehungsthema „beschäftigt euch nicht so viel mit euren Smartphones“ zu lösen.

Lange: Das ist eine sehr extreme Methode. Damit wollen wir nicht zum Nachmachen motivieren, sondern eher auf unsere Folge zum Thema Router hinweisen, falls ihr sie noch nicht gehört habt.

Wir haben heute einen Gast eingeladen, wie Michael schon gesagt hat. Wir sind auf das Thema Vernetztes Fahren schon vor ein paar Monaten aufmerksam geworden. Bei der letzten Automesse in München hat das BSI viel zu diesem Thema informiert und einen Simulator abgebildet. Das war für uns der Moment, an dem wir wussten, dass wir darüber sprechen wollen, weil wir natürlich gerne wissen würden, was man mit einem Simulator beim vernetzten Fahren und beim Thema Datensicherheit anfangen will. Ich hatte die bisher immer nur in der Fahrschule oder in anderen Situationen erlebt. Und dann ist uns kürzlich noch eine Meldung ins Auge gefallen: Und zwar über einen deutschen Softwareentwickler, der behauptet hat, er habe etwa 20 Teslas gehackt. Das konnte er auch nachweisen. Z.B. konnte er die Fenster rauf- und runterheben, die Musik laut und leise stellen, aber er konnte die Autos offensichtlich auch starten. Das hat mich und dich, Michael, ein bisschen beunruhigt, weil wir gedacht haben, dass man anfangen kann, das Auto zu steuern, wenn der Besitzer im Auto ist. Deswegen haben wir einen Experten aus dem BSI eingeladen.

Münz: Meine größte Sorge war, dass wenn ich im Auto fahre, stellt jemand auf einmal Helene Fischer an oder so was in der Art. Das will ich auf keinen Fall. Ich hoffe, dass Christian Wieschebrink vom BSI uns vielleicht sagen kann, welche Vorkehrungen getroffen werden können, um sowas zu verhindern. Christian, schön, dass du da bist. Herzlich willkommen!

Wieschebrink: Hallo! Freut mich auch, bei euch zu sein.

Münz: Stell dich bitte kurz vor. Was machst du beim BSI und wie war dein Weg dorthin?

Wieschebrink: Meinen Namen hast du schon verraten. Ich arbeite seit 2004 beim BSI, bin da gleich nach meinem Mathestudium gelandet. Das sind nun schon 17 oder 18 Jahre, die ich beim BSI arbeite. Seit ungefähr 5-6 Jahren beschäftige ich mich mit dem Thema IT-Sicherheit und intelligente Transportsysteme im Auto.

Münz: Wir haben für dich eine Entweder-Oder-Frage mitgebracht, die du vorher nicht kanntest. Wir würden von dir gerne wissen, ob du lieber deinen Haustürschlüssel oder dein Handy verlieren würdest.

Wieschebrink: Gute Frage, aber ich glaube, dass mein Hausschlüssel mir doch wichtiger ist.

Münz: Ich vermute, weil der Hausschlüssel wahrscheinlich das Einzige ist, was du nicht mit dem Handy lösen kannst.

Wieschebrink: Ich achte ein bisschen darauf, nicht zu viele Daten auf meinem Handy zu speichern, wobei das natürlich immer wichtig ist. Ich achte, wenn ich morgens aus dem Haus gehe, auch immer darauf, dass das Handy auf jeden Fall mit dabei ist. Aber eine warme Wohnung ist mir dann im Winter doch wichtiger, als nicht mehr WhatsApp nutzen zu können.

Lange: Christian, Michael und ich sind eher Fahrradfahrende, Autofahren ist bei uns eine seltenere Sache. Deswegen haben uns die Informationen darüber, was beim vernetzten Fahren oder im Auto mit unseren Daten schon alles möglich ist, beeindruckt. Du beschäftigst dich damit beruflich. Fährst du selbst Auto? Und wenn du ein Auto hast, was kann das alles außer fahren?

Wieschebrink: Ich muss euch leider enttäuschen. Ich fahre auch nur selten Auto und habe kein eigenes. Autos nutze ich nur, wenn ich größere Sachen besorgen muss bzw. Freundinnen und Freunde oder Verwandte besuche, die nicht so gut mit dem Zug zu erreichen sind.

Lange: Dann stelle ich die Frage mal anders: Du beschäftigst dich mit modernen Fahrzeugen. Was können die alles außer fahren? Was passiert da hinter den Kulissen, was wir, wenn wir darin sitzen, vielleicht gar nicht mitbekommen? Vor allen Dingen mit Blick auf Daten.

Wieschebrink: Es ist so, dass jede Menge Daten im Auto anfallen und für diverse Dienstleistungen im Fahrzeug genutzt werden. Das hängt natürlich immer vom Modell ab, was man kauft, oder auch vom Hersteller. In der Tendenz werden immer

mehr Daten aus dem Fahrzeug heraus übertragen oder gelangen von außen ins Fahrzeug.

Lange: Kannst du ein paar Beispiele nennen. Welche Art von Daten?

Wieschebrink: Das einfachste bzw. naheliegendste Beispiel sind Fahrzeugzustandsdaten wie z.B. Mitteltemperatur oder Batterieladestand bei Elektrofahrzeugen oder der Zustand der Fahrzeugleuchten oder die Anzahl der Beschleunigung- und Bremsvorgänge im Fahrzeug. Diese Daten werden im Auto gespeichert und können z.B. bei einem Werkstattbesuch von Mechanikerinnen und Mechanikern ausgelesen werden. Die können dann feststellen, ob bestimmte Dinge im Auto zu reparieren sind. Das sind Daten, die aus einer Box im Fahrzeug über die sogenannte OBD2-Box ausgelesen werden. Viele Daten werden, wie schon angedeutet, auch per Internetverbindung über Mobilfunk übertragen. Diese Daten landen dann bei den Servern der Hersteller. Nicht alle Daten, die ich gerade genannt habe, aber einige von denen werden durchaus in Hintergrundsysteme übertragen.

Münz: Die Werkstatterfahrung, die du gerade erwähnt hast, war bei mir der erste Moment, an dem ich persönlich verstanden habe, dass sowas tatsächlich passiert. Der Werkstattmitarbeiter sagte, dass er mal nachsieht, was das Auto an Fehlern gemeldet hat, und da ist mir bewusst geworden, dass das Auto mithört, mitliest und mitschreibt, während ich das Auto fahre. Das hat vielleicht noch andere Konsequenzen. Ein Nachbar von mir z.B. erzählt, dass er schon seit einiger Zeit nach einer neuen Autoversicherung sucht, die günstig ist. Die hat er dann gefunden und sie ist so günstig, da sie ihren Preis auf Basis seiner Fahrdaten generiert. Wenn er brav und vorbildlich und gesetzeskonform fährt, wirkt sich das auf seine Rate aus, die er an seine Versicherung zahlt. Ich habe kürzlich gelesen, dass Tesla auch ins Autoversicherungsgeschäft in Deutschland einsteigen will. Da war ich natürlich ein bisschen erstaunt, wie viel da offensichtlich mitgeschrieben wird. Ich weiß, LKWs haben Fahrtenschreiber, solche Papierdinger. Und haben wir im Auto auch Fahrtenschreiber, ohne dass wir uns dessen bewusst sind?

Wieschebrink: Im Moment ist das noch nicht so, aber es gibt Pläne, so etwas einzuführen. Zwei Dinge werden kommen: Einmal der Unfalldatenspeicher, der wichtige Fahrzeugparameter, die kurz vor einem Unfall aufgezeichnet werden, abspeichert. Und es gibt dann, wenn zukünftig das autonome oder das automatisierte Fahren sich weiterverbreitet, eine Vorschrift, dass solche Daten in einem speziellen Speicher abgelegt werden müssen, um z.B. bei einem Unfall festzustellen, ob das automatische System aktiv war oder ob der Fahrer oder die Fahrerin selbst gesteuert hat.

Lange: Wir haben jetzt zwei Begriffe. Wir haben mit dem vernetzten Fahren angefangen. Jetzt hast du automatisiertes Fahren genannt. Gibt es da Unterschiede oder ist das dasselbe?

Wieschebrink: Das sind zwei verschiedene technologische Entwicklungen, die gerade in der Automobilindustrie stattfinden. Das Thema Vernetzung gibt es schon seit einer ganzen Weile. Es gibt Fahrzeugmodelle, in denen das schon implementiert ist und die man kaufen kann. Das Thema Automatisierung kommt aktuell auch auf die Straße. Vor ein paar Monaten ist das erste Fahrzeug in Deutschland genehmigt worden, das über eine Automatisierungsfunktionen nach der sogenannten SAE Stufe 3 funktioniert. Das heißt, das Fahrzeug darf in bestimmten Situationen selbst fahren und der Fahrer darf sich in dieser Zeit anderen Beschäftigungen widmen, z.B. Zeitung lesen. Er muss aber immer aufmerksam sein, dass er nach einer Übergabephase wieder die Fahrzeugsteuerung übernehmen kann.

Münz: Du hast ‚gerade genehmigt' gesagt. Wer genehmigt solche Sachen?

Wieschebrink: In Deutschland macht das das Kraftfahrt-Bundesamt, das KBA, in Flensburg. Das muss solche neuen Fahrzeugtypen genehmigen.

Münz: Seid ihr als BSI bei IT-Sicherheitsfragen mitbeteiligt oder gibt ihr die Ratschläge und Empfehlungen dazu?

Wieschebrink: Genau richtig. Das Thema IT-Sicherheit im Fahrzeug ist jetzt als neue Typ Genehmigungsanforderung dazugekommen. Es gibt dazu ein internationales Abkommen, in dem diese Typ Genehmigungsregeln vereinbart werden. Da gibt es seit vorletztem Jahr auch neue Vorschriften. Das KBA ist zuständig für die Prüfungen der Umsetzung, und wir haben eine Vereinbarung mit dem KBA, dass wir bei diesen Genehmigungsvorgängen unterstützen. Wir geben Hilfestellung bei den Verfahren, schauen, welche Prüfungen durchgeführt werden sollten, welche Anforderungen die Prüfer stellen und solche Dinge.

Münz: Wenn ich dich richtig verstanden habe, ist es ja offensichtlich so, dass es jetzt auch in Autos so eine Art Blackbox gibt, die alles mitschreibt, wie man es aus dem Flugverkehr kennt. Die wird dann z.B. nach einem Unfall gesucht und dann weiß man, was in den letzten Minuten vor einem Unglück passiert ist. Das heißt, dass Autos jetzt mit einem riesigen Datensatz durch die Gegend fahren und immer weiter mitschreiben. Wie ist denn geregelt, wer auf solche Daten überhaupt Zugriff hat?

Wieschebrink: So einen Unfalldatenspeicher gibt es momentan noch nicht, das wird erst kommen. Das ist nach einer EU-Vorschrift geregelt. Ich weiß jetzt das genaue Datum nicht, aber das wird in den nächsten Jahren eingeführt. Darin ist festgehalten, wer in diesem konkreten Fall darauf zugreifen darf. Bei den ganzen anderen Daten,

die im Auto anfallen und vielleicht an den Hersteller übertragen werden, ist das nicht so wirklich klar, wer dann Zugriff auf die Daten hat. Ich hatte das Beispiel Werkstatt genannt. Da muss natürlich der Mechaniker oder die Mechanikerin lokal drauf zugreifen können. Aber wenn die Daten in so einem Backend beim Hersteller landen, sollte es eigentlich so sein, dass vorher der Fahrer zugestimmt hat, dass diese Daten genutzt werden. So wird es nach Datenschutzgrundverordnung geregelt, aber meistens findet sich das im Kleingedruckten irgendwo im Vertrag oder in der Anleitung, und es ist vielen Menschen vielleicht gar nicht bewusst, dass solche Daten aus dem Fahrzeug heraus übertragen werden.

Lange: Gehen wir in die Perspektive derjenigen, die jetzt über ein neues Auto nachdenken: Welche Dinge sollte man wissen, die die neuen Autos schon haben, in denen unter Umständen Daten kompromittiert werden können oder worauf ich im Kleingedruckten besonders achten sollte? Wenn wir bei diesem Tesla-Beispiel bleiben: Das war ja nicht jemand, der in böser Absicht gehandelt hat, sondern das war ein junger Programmierer, der zufällig auf ein paar Sachen gestoßen ist, diese dann weiterverfolgt hat, und die bei der Firma ja auch sofort gemeldet hat. Er hat direkt darauf hingewiesen, über welchen Weg er Zugang bekommen hat und was er machen konnte. Der hatte sich auch bemüht, die Besitzer und Besitzerinnen dieser Autos zu kontaktieren, weil er über seine Recherche tatsächlich deren E-Mails rausfinden konnte. Es klang ein bisschen Science-Fiction-mäßig, aber in dem Fall war es jemand, der in guter Absicht auf etwas hingewiesen hat, was sofort korrigiert worden ist. Wenn ich mir jetzt ein neues Auto kaufe und diese Geschichte im Ohr habe, hinterfrage ich schon, ob ich es überhaupt will. Will ich nicht lieber wieder ein Modell, das ganz analog fährt, was es aber heute nicht mehr auf dem Markt gibt? Worauf können wir als Verbraucherinnen und Verbraucher achten bzw. welche Fragen sollten wir auch stellen?

Wieschebrink: Das ist ein guter Punkt. Zur Datenübertragung sollte man sich so gut es geht darüber informieren, welche Dienstleistungen in dem Fahrzeug angeboten werden. Es gibt eine ganze Palette, die, je nachdem welches Modell man hat, dann vom Hersteller zu buchen ist. Man sollte genau prüfen, welche Daten für solche Dienstleistung tatsächlich benötigt werden, wie beispielsweise für Updates von Navigationssystem. Manchmal werden solche Fahrdaten auch dafür verwendet, um Staus zu erkennen. Diese Stauinformationen werden teilweise auch wieder zurück übertragen und an andere Nutzerinnen und Nutzer. Man sollte nachprüfen, ob diese Daten übertragen werden und ob man das möchte. Das ist ähnlich wie beim Smartphone oder beim Handy. Da sollte man auch bei jeder App schauen, ob man der App die Berechtigung gibt, auf bestimmte Daten zuzugreifen und nutzen zu lassen.

Lange: Um auf einen aktuellen Fall aus der Presse zurückzukommen: Da war es wohl so, dass einige der Fahrzeugbesitzer und -Fahrzeugbesitzerinnen bestimmte Updates oder bestimmte Sicherheitseinstellungen nicht von sich aus korrigiert haben. Deswegen ist dein Hinweis an dieser Stelle ganz wichtig, und es wäre ratsam, dass man sich, genau wie beim Smartphone, selbst ein bisschen schlau macht. Denn auch hier gibt es Sicherheitseinstellungen, denen kann man zustimmen oder auch nicht.

Wieschebrink: Zu diesem konkreten Fall kann man sagen, dass das gar nicht Schuld des Herstellers war, dass diese Lücke aufgetreten ist. Hier lag das Problem in einer externen Software, welche die entsprechenden Nutzerinnen und Nutzer installiert haben. Über diese Software konnte man bestimmte Daten aus dem Fahrzeug auslesen und umgekehrt auch bestimmte Funktionen auslösen. Um sich an dem Auto anzumelden, muss man sich authentisieren, also man muss dem Auto ein Geheimnis mitteilen, das dann wiederum diesen Zugriff gestattet. Die Nutzerinnen und Nutzer haben dieses Geheimnis auf ihren Servern irgendwo im Internet offen gespeichert, und der Hacker, den du erwähnt hast, hat herausgefunden, dass man auf diese Token zugreifen kann.

Lange: Haben sie vielleicht noch das 1 2 3 4 5 6 7-Passwort genutzt? Darüber haben wir schon häufiger gesprochen.

Wieschebrink: Ja, so ganz im Detail habe ich mir das nicht angeguckt. Ein Kollege von mir hat sich das angeschaut und mir so berichtet.

Münz: Jetzt haben wir ein paar Mal das Thema Handy erwähnt, auch in diesem Zusammenhang. Ich fahre zwar nicht oft Auto, aber immer wenn ich in ein Auto einsteige, mache ich es mir erstmal komfortabel. Die Musik, die ich auf dem Handy habe, schicke ich an das Auto, meine Routenplanung mache ich über das Telefon und schaue mir die an. In anderen Folgen hatten wir immer wieder Hinweise darauf, dass man immer aufpassen soll, wenn man sich mit anderen Geräten und Netzwerken verbindet. Also das man hier aufpassen soll, welche Daten übertragen werden oder nicht, ob man sich irgendwas einschleppt, wenn man sich in fremde Netze einloggt oder sich mit anderen Geräten verbindet. Kannst du was dazu sagen, wie sicher so die Verbindung zwischen Mobiltelefon und Auto ist? Und besteht im Zweifelsfall sogar die Gefahr, dass ich mir aus dem Auto irgendwas mit nach Hause nehme, in mein Heimnetz, wo sich mein Telefon dann wieder einloggt.

Wieschebrink: Auf ganz abstrakter theoretischer Ebene kann das passieren. Das kann bei jeder Form von Datenverbindung passieren, dass Schadsoftware über diesen Weg auf das andere Gerät gelangt. Im Idealfall sollte sowas aber nicht passieren. Es gibt unterschiedliche Möglichkeiten, wie man ein Handy beispielsweise an das Fahrzeug ankoppeln kann. Man kann die Bluetooth-Verbindung nutzen oder Programme wie

Android Auto oder Apple CarPlay benutzen. Bei den letzten Beispielen, bei Apple CarPlay oder Android Auto ist es so, dass da nur das Display des Handys auf dem Display des Fahrzeugs im Informationssystem angezeigt wird. Das ist ein zusätzliches Anzeigegerät, dass dafür genutzt wird, bestimmte Apps auf dem Handy zu starten. So sollte im Idealfall kein weiterer Datenaustausch mit dem Fahrzeug stattfinden.

Münz: Okay, das beruhigt mich jetzt.

Wieschebrink: Das heißt jetzt nicht, dass man sich das bei der Entwicklung nicht genau anschauen sollte. Auf beiden Seiten: sowohl beim Hersteller als auch beim Anbieter des Betriebssystems auf dem Handy. Die Entwickler müssen darauf achten, dass da keine Sicherheitslücken auftreten oder dass sowas bekannt wird und entsprechend in der neuen Version gepatcht wird.

Lange: Wir haben nicht nur den Namen Update Verfügbar, wir sprechen auch häufig darüber, dass man ein Auge darauf haben sollte, wann Updates verfügbar sind und das man sie dann installiert, wenn sie angeboten werden. Wenn ich mir vorstelle, dass ich jetzt, wenn ich ein modernes Auto habe, dauernd darauf achten muss, dass ich alle neuen Updates ziehe, dann wirkt es so, als würde das ziemlich viel mit den Updates. Ist das meine Verantwortung bei so einem modernen Auto oder wird das anders geregelt? Oder ist das schon anders geregelt? Und worauf sollte ich achten, wenn ich jetzt so ein ganz modernes Fahrzeug ins Auge fasse?

Wieschebrink: Wie ich das sehe, wollen die Hersteller es künftig so machen, dass solche Updates automatisch runtergeladen werden, wobei man als Fahrzeughalter oder Fahrzeughalterin immer zustimmen muss, bevor ein Update ins Fahrzeug eingespielt wird. Ein Update bedeutet auch eine Veränderung des Geräts oder des Fahrzeugs, das man nutzt, und da ist immer der Vorbehalt da, dass erst zugestimmt werden muss bevor so eine Veränderung stattfindet. Im Idealfall sollte es so sein, dass der Hersteller mit dem notwendigen Update auf einen zukommt, sodass die Nutzerinnen und Nutzer sich nicht selbst irgendwo später die nötigen Updates raussuchen müssen. Solche Updates können tatsächlich nur eingespielt werden, wenn das Fahrzeug steht und keine Gefahr für andere Verkehrsteilnehmende entsteht, falls ein Update mal schiefgeht.

Lange: Passiert natürlich nie. Es ist immer fehlerfrei und funktioniert im ersten Angang.

Münz: Wie oft kam es schon vor, dass man nach einem Update gesehen hat, dass der Rechner dann doch lieber zurück geht auf den Ursprungszustand? Ich glaube, ich habe das schon in diesem Zusammenhang erzählt: Ich lege nebenbei noch als DJ auf und habe morgens um drei in einem vollen Club einen Update-Hinweis erhalten, der

nicht ganz passend war. Ich glaube, wenn man gerade auf der Autobahn mit 130 km/h fährt und dann den Hinweis bekommt, dass das Auto jetzt ein Update benötigt, ist natürlich eine ungünstige Situation.

Lange: Es ist beruhigend zu wissen, dass das zumindest ein Teil der Diskussion ist. Ich habe schon gesagt, dass ich nicht so viel in Autos sitze und wenn doch, dann meistens in älteren Modellen, deswegen kam mir das alles noch ein bisschen zukunftsvisionär vor. Aber vieles von dem ist heute schon möglich und vieles hat auch Vorteile. Ich weiß, dass bei mir im Bekanntenkreis Menschen davon schwärmen, dass ihr Auto ihnen bei längeren Fahrten Signale gibt, wenn der Abstand zum vorderen Fahrzeug zu eng wird oder wenn ein Fahrzeug im toten Winkel an ihnen vorbeifährt, sodass sie wissen, dass sie nicht in dem Moment überholen wollen. Es hat also viele Elemente, die einem das Fahren, das manchmal ein bisschen hektisch oder stressig sein kann, erleichtert. Ich sehe die Vorteile auch, aber ich hatte nach dieser Hacker-Geschichte mit dem Auto gedacht: Wenn der nicht nur meine Musik ändert, vielleicht auf eine Interpretin, die ich nicht mag, oder mir das Fenster runter macht im Winter, wenn es kalt ist, oder im Sommer wieder hoch, wenn ich eigentlich frische Luft will, ist es schon fast zu viel an Gefährdung. Aber das war in dem Fall ein Test, um darauf hinzuweisen, dass es noch offensichtlich viel Arbeit vor uns liegt. Wo geht denn die Reise hin, Christian? Was prognostiziert ihr oder woran arbeitet ihr vielleicht schon – worauf können wir uns einstellen?

Wieschebrink: Das Thema IT-Security im Auto ist unheimlich komplex. Es gibt vielleicht dieses halbe Dutzend an möglichen Verbindungen in die Außenwelt. Das Thema Fahrzeug zu Fahrzeug Kommunikation haben wir jetzt gar nicht angesprochen. Das ist eine zusätzliche Datenverbindung nach außen, die wir uns schon seit längerem angucken. Wir werden uns als BSI überlegen müssen, wie wir die Sicherheit des Fahrzeugs prüfen wollen und wie wir feststellen können, dass alles, was gemacht werden sollte, im Fahrzeug tatsächlich umgesetzt wird. Das ist noch die Baustelle bei uns. Wir werden uns überlegen müssen, mit welchen Prüfwerkzeugen oder Prüfmethoden wir als Behörde zusammen mit dem KBA rangehen wollen.

Lange: Ich hätte noch eine abschließende Frage zu dem Simulator, den ihr im letzten Jahr bei der Automesse dabeihattet. Uns interessiert, was ihr denn da simuliert habt. Bestimmt nicht wie ich korrekt rechts abbiege. Das war nicht euer Thema.

Wieschebrink: Wir haben versucht zu simulieren, wie ein Cyberangriff aussehen könnte, wenn er in Wirklichkeit stattfinden würde. Wir haben zwei Sachen implementiert. Das eine war ein simulierter Ransomware-Angriff. Wenn man mit dem Auto versucht, seine neuesten Kartendaten für das Navi herunterzuladen, gelangt eine Schadsoftware mit aufs Fahrzeug und blockiert das Fahrzeug. Beim nächsten Mal

lässt es sich nicht mehr starten. Erst nachdem man einen gewissen Betrag an Bitcoins an die Erpresserinnen und Erpresser überwiesen hat. Das andere war ein simulierter Lenkrad-Eingriff. Die fahrende Person fährt irgendwo auf der Landstraße oder Autobahn, will abbiegen und plötzlich wird die Servolenkung schwergängig. Das sind Szenarien, die demonstriert wurden. Das waren keine echten Angriffe, aber die, die von White-Hat-Hackern entdeckt wurden. Das sind also theoretische Möglichkeiten, die zeigen, welche Gefährdung es geben könnte und verdeutlichen worauf sich die Hersteller einstellen müssen, wenn sie solche neuen Fahrzeuge und Funktionen entwickeln.

Münz: Wir sind wieder zurück bei der oft zitierten Kaffeemaschine, die ihren Dienst verweigert, oder bei dem Backofen, der nicht mehr starten will. Offensichtlich muss man das Auto in diese Richtung mitdenken, die wir oft bei Peripheriegeräten zitieren: Updates installieren und immer darauf achten, dass keine Daten auf die Geräte gelangen, die dort nicht hingehören, sondern Software von seriösen Quellen herunterladen. Das sind Dinge, die scheinbar auch ein bisschen für Autos gelten, wenn ich das richtig verstanden habe.

Wieschebrink: Die Hauptverantwortung trägt der Hersteller, der dafür Sorge trägt, dass solche Software-Updates geprüft sind, bevor sie auf das Fahrzeug gelangen. Es ist in Zukunft vorstellbar, so ähnlich wie bei Smartphones, dass Drittanbieter Apps für das Fahrzeug anbieten. Da ist auch der Hersteller in der Verantwortung, zu prüfen, dass solche Apps sicher implementiert sind und keine Gefährdung für die Verkehrssicherheit darstellen.

Münz: Danke dir, Christian. Ich bin sehr gespannt, was mich an Neuerungen erwartet, wenn ich um Weihnachten herum das nächste Mal in das Mietauto steige. In der Regel muss ich mir immer zeigen lassen, wo der Schalthebel ist bei diesen neuen Autos. Den finde ich nie. Es ist noch offensichtlich viel Verwirrungspotenzial vorhanden. Danke für deine Hinweise. Es hat wirklich sehr geholfen, und ich glaube auch, dass unsere Hörerinnen und Hörer jetzt ein bisschen sensibilisierter sind für das, was in ihrem Auto passiert und was das Auto alles kann.

Lange: Vielen Dank! Es war wirklich sehr spannend, auch der Blick in die Zukunft. Vielen Dank, dass du dir Zeit dafür genommen hast. Zusätzliche Infos findet ihr in den Shownotes. Das BSI hat auch noch weitere Information zu dem Thema vernetztes Fahren auf seiner Webseite. Wir bereiten uns schon bald auf die nächste Folge vor, recherchieren aber noch ein bisschen und freuen uns schon darauf. Bis wir so weit sind, liked und folgt „Update Verfügbar“ auf euren Podcast Plattformen. So verpasst ihr keine Folge. Vielleicht habt ihr auch Lust in die ein oder andere ältere Folge noch einmal reinzuhören.

Münz: Wie immer gilt: ihr könnt uns gerne über die BSI Kanäle kontaktieren oder auf Facebook, Instagram, Twitter oder YouTube. Schickt uns ansonsten auch gerne eine E-Mail an bsi@bsi.bund.de.

Lange: Es gibt noch einen Geschwister-Podcast, den das BSI zusammen mit der Allianz für Cybersicherheit macht. Der heißt CYBERSNACS. Falls ihr da noch nicht reingehört habt, dort wird auch immer über spannende Themen gesprochen. Geht mal auf eure Plattformen und hört rein, und wir freuen uns von euch zu hören. Vor allen Dingen wollen wir wissen, wie ihr in diesem digitalen Test abgeschnitten habt. Wir werden dann mal schauen, wo wir uns befinden im Vergleich zu euch und freuen uns, wenn ihr das nächste Mal wieder reinhört. Bis dahin alles Gute und auf bald. Tschüss!

Münz: Vielen Dank auch an dich, Christian, und tschüss. Bis nächstes Mal.

Wieschebrink: Vielen Dank und tschüss!

Besuchen Sie uns auch auf:

https://www.bsi.bund.de/
https://www.facebook.com/bsi.fuer.buerger
https://twitter.com/BSI_Bund
https://www.instagram.com/bsi_bund/
https://social.bund.de/@bsi

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185-189, 53133 Bonn