SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

August 2016

SWITCH

I. Aus Freude am Sammeln: Das Thema informationelle Selbstbestimmung und Transparenz bei Fahrzeugdaten nimmt Fahrt auf

Vernetzte Autos, ihre Datensammlungen und die Frage, wem diese Daten eigentlich gehören und wer was damit machen darf, waren schon des öfteren Thema hier im Security Report. Nun hat der ADAC aktuell einen BMW i3, einen BMW 320d, eine Mercedes B-Klasse und einen Renault ZOE daraufhin untersucht, welche Daten sie sammeln. Das Ergebnis ist aus Privacy-Perspektive ernüchternd: Alle vier Fahrzeuge sammeln Daten in einem Umfang, der deutlich über das hinausgeht, was für eine On-Board Diagnose in der Werkstatt nötig wäre. So sendet z.B. der Mercedes alle zwei Minuten neben GPS-Position, Kilometerstand, Verbrauch und Reifendruck auch die Zahl der Gurtstraffungen, die Rückschlüsse auf das Fahrverhalten zulassen, an seinen Hersteller. Ähnliche Daten sind auch aus den beiden BMW auslesbar. Dagegen ist der Renault ein wahrer Alles-Sammler. Denn via Mobilfunkverbindung und Controller Area Network Bus kann Renault praktisch alle beliebigen Daten auslesen, für die sich der Hersteller interessiert. Mehr noch: Werden die Leasingraten für die Batterie nicht rechtzeitig und/oder vollständig bezahlt, kann Renault jederzeit den Ladevorgang unterbinden und so das Fahrzeug stilllegen.

Dafür lässt BMW mit dem Paradoxon aufhorchen, dass man nach eigenen Angaben keine Standortdaten von Kundenfahrzeugen speichere, dem Landgericht Köln nun aber eben solche Daten geliefert hat, aus denen ein komplettes Bewegungsprofil eines Drive-Now-Kunden erstellt wurde. Drive-Now ist ein CarSharing-JointVenture von BMW und Sixt und erklärte, dass lediglich Ort und Zeit der Fahrzeugübernahme und -abgabe gespeichert würden. Das Landgericht Köln gab indes bekannt, dass die Daten aus dem Bestand von BMW stammten, wo man zwar einräumte, dass mehrere Datenspeicher im Fahrzeug Daten sammelten, aus denen sich aber kein Bewegungsprofil ableiten liesse (was nach dem in Deutschland geltendem Datenschutzrecht als problematisch bis illegal zu werten wäre). Weitere Auskünfte verweigerte BMW mit dem Hinweis auf den Datenschutz (!).

So ganz geheuer scheint BMWs Freude am Sammeln auch der Polizei Nordrhein-Westfalens nicht zu sein. Die hat nach Angabe ihres Pressesprechers per Vertrag festgelegt, dass die in ihren neu geleasten BMW-Streifenfahrzeugen fest verbauten SIM-Karten (embedded SIM) von BMW beim Netzbetreiber abgemeldet werden.

Auf einen ganz anderen Problemkreis vernetzter und softwaregesteuerter Fahrzeuge verweist der Automotive Warranty & Recall Report 2016: Der weist nach, dass die immer komplexere IT-Steuerung die Fehleranfälligkeit und die Rückrufquoten für Fahrzeuge immens erhöht. Und das, obwohl die High-Tec-Oberflächen der meisten neuen Autos nach Meinung des Sicherheitsexperten David Kennedy auf Low-Tec-Standards aus den 1980er und teilweise sogar 1970er Jahren aufgesetzt sind und «…it was never designed with security in mind.»

Nachzulesen unter:

http://www.heise.de/newsticker/meldung/ADAC-Untersuchung-Autohersteller-sammeln-Daten-in-grossem-Stil-3227102.html
https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=8749&quer=daten
http://www.tagesschau.de/wirtschaft/adac-ueberwachung-auto-101.html
http://www.zeit.de/mobilitaet/2016-02/datenschutz-autos-adac-aufklaerung-transparenz
http://www.manager-magazin.de/unternehmen/autoindustrie/bmw-autobauer-liefert-gericht-kundendaten-fuer-bewegungsprofil-a-1104050.html
https://netzpolitik.org/2016/bmw-speichert-keine-standortdaten-gibt-aber-bewegungsprofil-an-gericht
https://netzpolitik.org/2016/neue-streifenwagen-in-nrw-uebermitteln-keine-daten-an-bmw
http://www.computerworld.ch/news/security/artikel/automobile-immer-mehr-rueckrufe-wegen-software-problemen-70306
http://www.techinsider.io/hacker-car-hacking-2016-6

II. Tor für mehr Sicherheit im Internet der Dinge? Neues vom Guardian Project und Riffle, einem Gemeinschaftsprojekt von MIT und EPFL

Fragen der Datensicherheit spielen bei der Vernetzung bislang unvernetzter Geräte (oder wie unter I beschrieben: bei Autos) wenn überhaupt, dann nur eine marginale Rolle. Darauf hatten wir schon im September 2014 im Security Report hingewiesen. Da Fortschritte nicht oder nur in sehr bescheidenem Umfang zu beobachten sind, hat sich The Guardian Project des Themas angenommen. Das global aktive Kollektiv aus Menschen unterschiedlichster Berufe hat sich zum Ziel gesetzt, Open Source Software und Security Apps bereit zu stellen. So auch Home Assistant, eine neue Open Source Plattform zur Steuerung aller vernetzten Geräte in einem Gebäude. Der Clou dabei: Home Assistant kann so konfiguriert werden, dass es die angeschlossenen Geräte über das Anonymisierungsnetzwerk Tor mit dem Internet verbindet. Damit wird das Hacken wie auch das Tracken dieser Geräte und ihrer Nutzung deutlich schwerer. Das als Proof-of-Concept angelegte Projekt ist noch nicht marktreif, doch hofft sein Initiatior, The Guardian Project Gründer Nathan Freitas: «Our goal is to show this can work and hopefully advocate towards commercial product vendors». Die implementierten Sicherheitsmechanismen der «Product Vendors» endet in vielen Fällen damit, dass sie vernetzte Geräte mit einem auf 0000 eingestellten 4-stelligen Sicherheitscode ausstatten.

Nicht zu verwechseln ist Freitas´ The Guardian Project mit Stan Lees Superhelden-Meet-National-Hockey-League-Comictruppe gleichen Namens (aber wohl mit deutlich kommerzielleren Ambitionen). Ebenso gehört Teddy The Guardian nicht zu Freitas´ The Guardian Project. Der putzige Teddy und andere Guardian-Plüschtiere sind mit einer Vielzahl an Sensoren ausgestattet, die über eine entsprechende App Eltern den Gesundheitszustand ihres Kindes melden.

Neues zum Thema Anonymisierungsnetzwerke gibt es auch aus Cambridge, Massachusetts und Lausanne zu berichten. Forscher des MIT und der EPFL arbeiten derzeit an einer Alternative zu Tor, die anders als Tor einen formellen Sicherheitsnachweis vorweisen kann. Dazu arbeitet Riffle mit einem Mixnet: Nachrichten aus unterschiedlichen Sendungen werden verschlüsselt und vermischt, bevor sie weitergeleitet werden. Jeder Server, der dieses Mix-Paket weiterleitet, muss nachweisen, dass er es nicht verändert hat. Das gehe zwar auf Kosten der Leistungsfähigkeit, erhöhe aber die Sicherheit gegenüber Tor deutlich, argumentieren

die Riffle-Entwickler. Sie betonen, dass sie mit ihrem Netzwerk Tor nicht ersetzen, aber eine Alternative dazu bieten wollen und verweisen darauf, dass Riffle derzeit noch in der Entwicklungsphase steckt.

Nachzulesen unter:

http://www.theverge.com/circuitbreaker/2016/7/22/12251714/tor-smart-hub-iot-security-guardian-project
https://theintercept.com/2016/07/20/tor-could-protect-your-smart-fridge-from-spies-and-hackers
https://blog.torproject.org/blog/quick-simple-guide-tor-and-internet-things-so-far
https://www.youtube.com/watch?v=m8CkvrCiikE
http://www.nhl.com/ice/page.htm?id=66928
http://teddytheguardian.com
http://futurezone.at/produkte/stofftiere-sammeln-daten-ueber-die-gesundheit-von-kindern/209.192.015
http://www.spiegel.de/netzwelt/web/riffle-neue-tor-alternative-soll-noch-mehr-sicherheit-bieten-a-1103766.html
https://techcrunch.com/2016/07/11/mits-anonymous-online-communications-protocol-riffle-could-beat-tor-at-its-own-game
http://www.ictjournal.ch/News/2016/07/13/Le-MIT-et-lEPFL-imaginent-un-reseau-danonymisation-plus-fort-que-Tor.aspx

III. Sommerhype 2013 im Real-Update: Macht SFG/FURTIM Blackout zum realen Horrorszenario?

2013 empfahlen wir im Switch Security-Blog Marc Elsbergs Roman „Blackout“ als spannende, aber unter Security-Aspekten auch sehr nachdenkenswerte Sommerlektüre. Dass das dort fiktive Szenario zum Teil real werden könnte, schien nicht ausgeschlossen, als Sicherheitsforscher des auf Endpoint-Security spezialisierten Unternehmens SentinelOne meldeten, sie hätten einen SCADA-Angriff auf einen europäischen Energiekonzern entdeckt. Die als SFG bezeichnete Schadsoftware sei quasi das Mutterschiff des Schädlings FURTIM und befalle Steuerungssysteme, die in der industriellen Automatisierung zum Einsatz kommen. Untersuchungen des Securityunternehmens Dalballa postulierten dagegen SFG und FURTIM seien eng verwandt und nicht auf bestimmte Anwendungen spezialisiert. Daraufhin veröffentlichte SentinelOne eine Klarstellung, in der betont wurde, dass aus der bereitgestellten Analyse der Malware falsche Interpretationen gezogen worden seien, wies aber darauf hin, dass mit SFG/FURTIM nicht zu spassen sei. Denn die Malware ist so ausgekügelt programmiert, dass sie in drei Stufen angreift und dabei auch Anti-Virus-Software und Firewalls umgeht, die statische und heuristische Techniken einsetzen. Damit sie selbst nicht entdeckt werden kann, kann die Malware Systeme mit biometrischer Zugangskontrolle und Sandbox-Umgebungen erkennen und sich bei Verfolgung selbst verschlüsseln. Die Komplexität und Raffinesse der Malware lässt die

Forscher vermuten, dass sie von einem staatlichen Auftraggeber bestellt und eingesetzt wurde. Viele Indizien deuten auf einen osteuropäischen Staat hin.

Die Frage, wie gut – oder eben leider auch wie schlecht – kritische Infrastruktur vor unbefugtem Zugriff oder gar Manipulation geschützt ist, bleibt also nach wie vor aktuell. So gelang es Golem.de und internetwache.org nach eigenen Angaben innerhalb weniger Wochen Zugriff auf Steuerungssysteme von Wasserwerken, Blockheizkraftwerken, Interfaces zur Gebäudeautomatisierung und sonstiger Industrial Control Systems (ICS) auf der ganzen Welt zu erlangen.

Nachzulesen unter:

https://securityblog.switch.ch/2013/07/31/sommerlekture-blackout
http://www.finanzen.net/nachricht/aktien/SentinelOne-entdeckt-staatlichen-SCADA-Angriff-auf-westeuropaeischen-Energiekonzern-4981504
http://www.theregister.co.uk/2016/07/18/firm_calls_bullshit_on_scada_malware
https://sentinelone.com/blogs/sfg-furtims-parent
http://www.golem.de/news/schwachstellen-aufgedeckt-der-leichtfertige-umgang-mit-kritischen-infrastrukturen-1607-122063.html
http://derstandard.at/2000041246620/Oesterreichische-und-deutsche-Kraftwerke-und-Smart-Homes-ueber-Internet-angreifbar

IV. Sommerhype 2016: Auch Cyberkriminelle profitieren von Pokémon Go

77 Millionen Suchergebnisse liefert Google derzeit zum Sommerhype des Jahres 2016. Pokémon Go (gestartet am 6. Juli 2016) ist die Augmented Reality Version des vor 20 Jahren erstmals veröffentlichten Nintendo-Konsolen-Blockbusters, aus dem seither ein ganzes Entertainment-Eco-System u.a. mit 18 Kinofilmen entstanden ist. Mit mehr als 200 Millionen verkauften Videospielen gilt das Pokémon-Universum als eine der erfolgreichsten Produktideen im Gaming-Geschäft überhaupt. Da kann es nicht verwundern, dass findige Trittbrettfahrer auf den Zug zum Erfolg aufspringen wollen. Und wie immer sind darunter auch nicht wenige böse Schwarzfahrer, die mit gefakten Apps, oder gar einer angeblich «offiziellen» Pokémon Go-Facebookseite unbedarfte Spieler zur Herausgabe von Geld und/oder Daten locken. Auf Giga.de wird nicht nur das Spiel erklärt, sondern auch ausdrücklich vor Phishing-Versuchen, Abofallen und anderem Cyber-Betrug gewarnt. Die Charakterisierung Augmented Reality nehmen inzwischen auch «Old-School»-Verbrecher als Chance, Pokémon Go-Spieler virtuell anzulocken, um sie dann ganz real auszurauben.

Nachzulesen unter:

http://futurezone.at/games/pokemon-go-betrug-mit-gewinnspielen-und-fake-apps/210.702.019
http://www.giga.de/spiele/pok-mon-go/specials/pokemon-go-gewinnspiel-fake-vorsicht-vor-phishing-und-abofallen
http://www.theverge.com/2016/7/10/12142434/pokemon-go-armed-robberies-missouri

V. Schafe statt Pokémons: Google Sheep View und die Faröer Inseln

Ein Jahr bevor Pokémon Go die Strassen eroberte, starteten die Niederländer Ding Ren und Michael Karabinos aus Anlass des Jahres des Schafes 2015 ihr Fotoprojekt «Google Sheep View». Darin sammlen sie statt Pokémons Schnappschüsse von Schafen, die sie auf Google Street View finden. Die Autoren erklären, dass das Projekt nicht mit Google verbunden ist.

Genau das aber will Daruta Dahl im Auftrag des Tourismusamts der Faröer Inseln erreichen: Weil Google Street View die abgelegenen Inseln nicht zeigt, hat sie das Projekt SheepView 360 gestartet und fünf mit 360-Grad-Kameras, einem Mobiltelefon und Solarpanels ausgestattete Schafe losgeschickt. Die sollen die Inseln werbewirksam abbilden und potenziellen Touristen die besten Orte der Insel näherbringen. Wer schon zuhause wissen möchte, wie saftig die Weiden zum Grasen auf Faröer sind, wird hier fündig: http://visitfaroeislands.com/sheepview360

Nachzulesen unter:

http://www.googlesheepview.com/about
https://www.theguardian.com/travel/2016/jul/12/sheep-view-360-faroe-islands-google-mapping-project
http://www.faz.net/aktuell/gesellschaft/tiere/google-sheep-view-auf-den-faroeern-14339363.html
http://futurezone.at/digital-life/sheepview360-kamera-schafe-scannen-faeroeer-inseln-ein/209.583.637

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.