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

September 2015

SWITCH

I. Ferengis in Redmond? Microsofts Aufbruch in eine neue Dimension des Datensammelns mit Windows 10

Die 59. Erwerbsregel der Ferengis – einer Spezies aus dem Start Trek Universum, deren Lebenssinn in der Anhäufung von Vermögen besteht – besagt: «Free advice is seldom cheap!». Ersetzt man «Ratschlag» durch «Betriebssystem», ist man beim neuen Windows 10. Nutzer der Vorgängerversionen Windows 7 oder 8 bekommen das Update auf das aktuelle Betriebssystem, ohne dafür Geld bezahlen zu müssen. Die neue Währung, die Microsoft statt dessen veranschlagt, heisst Nutzer- und Benutzungs-Daten. Deren Inkasso übernimmt das neue Betriebssystem nach seiner Installation voreingestellt, ungefragt, voll-automatisch und in umfassender Art und Weise:

Neben Namen, postalischer Adresse, Alter, Geschlecht und der Telefonnummer des Benutzers sammeln und verwerten die Fenstermacher aus Redmond unter anderem den jeweiligen Standort des Desktop- oder Laptop-Rechners, Websites, die in den Microsoft-Apps und -Diensten aufgerufen wurden, eingegebene Suchbegriffe, Kontakte zu anderen Personen, gekaufte Artikel etc. Um die Verlässlichkeit der Daten zu steigern, vergibt Windows 10 eine eindeutige

Identifikationsnummer für jeden Rechner, auf dem es installiert wird, und gibt diese zur Verwendung durch App-Entwickler und Werbenetzwerke frei – dies wohl aber nur gegen harte Währung.

Zwar verweist Microsoft inzwischen darauf, dass eine Anpassung der Datenschutzeinstellungen im Programm die Datensammelwut von Windows 10 stoppt, ohne dass dafür ein Benutzerkonto eröffnet werden müsste. Das aber ist zum einen mühsam. Zum anderen sind dann einige der neuen, primär dem Nutzungskomfort dienenden Funktionen des Betriebssystems nicht mehr verfügbar. Es bleibt abzuwarten, ob der sich abzeichnende Imageschaden für Microsoft die erwarteten Mehrwerte aus dem Datengeschäft schmälert oder gar komplett kompensiert. So wird über die Datensammelwut von Windows 10 heftiger diskutiert als über dessen Leistungsfähigkeit. Nicht nur russische Politiker sehen geltendes Recht verletzt, auch der oberste Schweizer Datenschützer prüft aktuell, ob und wie Windows 10 gegen Datenschutzrecht verstösst.

Microsoft demonstriert gegenüber Forderungen nach mehr Transparenz und Unmissverständlichkeit seiner Datenschutzerklärungen und Nutzungsbedingungen trotzige Gelassenheit und versucht seinerseits, mit der Zielvorgabe von einer Milliarde Windows-10-Installationen bis Ende 2018 zu beeindrucken. Zum 1. August haben die Redmonder noch nachgelegt und sich mit einem neuen Servicevertrag für zahlreiche Dienste von Office 365 über Skype bis hin zu Xbox Live und Software, die mit einem Microsoft-Konto verbunden ist (also auch Windows 10) das Recht eingeräumt, Konfigurationsänderungen vorzunehmen, wenn «gefälschte Spiele» oder «unerlaubte Hardware-Peripheriegeräte» erkannt werden - ohne aber näher zu definieren, was damit gemeint sei. In den Ferengi Rules of Acquisition steht übrigens als Regel 52: «Never ask when you can take!»

Nachzulesen unter:

https://www.verbraucherzentrale-rlp.de/windows-10--Ueberwachung-bis-zum-letzten-klick-1
http://www.heise.de/newsticker/meldung/Windows-10-Datensammelwut-beherrschen-2774941.html
http://www.zeit.de/digital/datenschutz/2015-08/privatsphaere-windows-10-einstellungen-deaktivieren
http://futurezone.at/netzpolitik/russischer-politiker-will-windows-10-verbieten/148.821.584
http://www.20min.ch/digital/dossier/microsoft/story/-Windows-10-koennte-in-der-Schweiz-verboten-werden--10890387
http://www.zdnet.com/article/microsofts-big-windows-10-goal-one-billion-or-bust/
http://www.welivesecurity.com/deutsch/2015/08/11/microsofts-neuester-wurf-windows-10-datenschutz-0
http://www.heise.de/newsticker/meldung/Windows-10-Pro-und-Contra-Nutzerdaten-nach-Redmond-2789194.html
https://en.wikipedia.org/wiki/Rules_of_Acquisition

II. Die digitale Revolution hackt ihre Macher: ICANN zum dritten Mal Opfer eines Hackerangriffs, Internet Provider 1blu gehackt und erpresst

Im letzten Security Report begann der zweite Post mit einem Satz, der hier gleich nochmal stehen könnte: «Es ist schon bittere Ironie…». Denn ausgerechnet die Internet Corporation for Assigned Names and Numbers ICANN hat Anfang August bekannt gegeben, dass sie zum dritten Mal Opfer eines Hackerangriffs geworden sei. Dabei seien Usernamen, e-mail-Adressen und Passwörter von Nutzern der Website icann.org gestohlen worden. Die Non-Profit-Organisation zeichnet für die Vergabe von IP-Adressen und Domain-Namen im Internet verantwortlich und ist nach eigenen Angaben der Sicherheit, Stabilität und Operabilität des Netzes verpflichtet.

Böse getroffen hat es offenbar auch den Berliner Internet System Provider «1blu». Nach einem erfolgreichen Angriff haben die Hacker/Erpresser nach Angaben von 1blu eine hohe Geldsumme gefordert (in Medienbereichten ist von einer Viertel Million Euro die Rede) und für den Fall der Nicht-Zahlung mit der Veröffentlichung vertraulicher Kundeninformationen gedroht. Offenbar wurden Zugangsdaten für das Kundenlogin, für E-Mail, FTP, MySQL und den Cloud-Speicher 1blu-Drive gestohlen. 1blu hat zwischenzeitlich die Login-Daten zurückgesetzt, alle Passwörter gelöscht und die Kunden aufgefordert, sich erneut anzumelden, zumal auch Zahlungsdaten in die Händer der Hacker gefallen sein könnten.

Nachzulesen unter:

https://www.icann.org/news/announcement-2015-08-05-en
http://www.theverge.com/2014/12/18/7414487/global-internet-authority-icann-hacked
http://motherboard.vice.com/read/icann-has-been-hacked-again
http://www.golem.de/news/hackerangriff-webhoster-1blu-wird-erpresst-1508-115740.html
https://www.1blu.de/sicherheit/kundenanschreiben
http://www.heise.de/security/meldung/Webhoster-1blu-gehackt-und-erpresst-2777957.html

III. Car Hacks, Autonomes Fahren und Telematik-Versicherungstarife: Gefahren für Sicherheit und Privatsphäre

Auch unter III. müssen wir uns erneut einem Thema widmen, das schon öfter im Security Report angesprochen wurde: Connected Cars. So wurden in den letzten Wochen drei Fälle bekannt, in denen entweder das komplette Fahrzeug oder existenzielle Einzelfunktionen wie etwa Gas und Bremse manipuliert werden konnten.

Die klaffendste Sicherheitslücke hatte ein Jeep Cherokee offenbart. Er konnte mit einem Zero-Day-Angriff auf das eingesetzte Infotainmentmodul «Uconnect» von einem 10 Meilen entfernten Laptop wireless manipuliert werden – vom Radio über die Scheibenwischer bis hin zur Motorsteuerung und den Bremsen.

Beim Model S von Tesla brauchten zwei Forscher privater Sicherheitsfirmen zunächst einen physischen Zugang, um über das zu Wartungszwecken hinter dem Fahrersitz angebrachte Netzwerkkabel Zugriff auf das Auto zu bekommen. Sie konnten das Auto starten und stehlen, aber auch einen Trojaner einschleusen, der eine Fernsteuerung des Fahrzeugs ermöglichte. Und sie fanden heraus, dass auch beim Tesla das Infotainmentsystem mit einer seit 4 Jahren bekannten Sicherheitslücke die Türen für Hacker einladend weit offen liess.

Dass Vernetzung von Autos in diesen Fällen aber auch ein Vorteil sein kann, belegt der unten genannte «Wired»-Artikel über den Tesla-Hack: «Unlike Fiat Chrysler, which recently had to issue a recall for 1.4 million cars and mail updates to users on a USB stick to fix vulnerabilities found in its cars, Tesla has the ability to quickly and remotely deliver software updates to its vehicles. Car owners only have to click „yes" when they see a prompt asking if they want to install the update.»

In einem dritten Fall hackten sich Forscher der University of California per SMS und der SIM-Karte des Dongles des US-Autoversicherers Metromile in eine 2013er Corvette. Diese Fälle zusammen genommen hat dann auch die amerikanische National Highway Traffic Safety Administration NHTSA aufgeschreckt. Denn existenziell bedrohliche Sicherheitslücken in Autos sind eben keine Einzelfälle, sondern gefährden eine stattliche Liste global verkaufter Automarken (siehe Artikel des INFOSEC-Institutes). Zudem sind sie oft seit Jahren bekannt.

Zusätzliche Brisanz bekommt das Thema Verletzbarkeit technischer Systeme in Fahrzeugen auch für die gesamte Entwicklung autonomer Land-, Wasser- und Luftfahrzeuge ohne Fahrzeugführer. Und die hat rasant an Fahrt aufgenommen. So testet Tesla das autonome Fahren gerade mit jenem Model S, von dem oben die Rede war (wenn auch mit installiertem Patch). Daimler hat vor kurzem die Behördenbewilligung für Tests autonomer Lastwagen auf deutschen Landstrassen- und Autobahnen erhalten. Und auch der Fahrdienst Uber forciert das Thema selbstfahrender Autos.

Daher haben sich verschiedene Autohersteller bereit erklärt, das seit längerem von der NHTSA geforderte Information Sharing and Analysis Center ISAC einzurichten. Unabhängig davon arbeitet der Automobilzulieferer Bosch an mehrstufigen Systemen, bei denen die Fahrzeugtechnik und die Systeme mit Internetverbindungen nicht unmittelbar verbunden sind. Die Zeit drängt tatsächlich, denn viele Versicherer möchten schnellstmöglich sogenannte «Telematik-Tarife» anbieten. Die «Pay-as-you-Drive»-Tarife belohnen Kunden für ein regelkonformes und unfallvermeidendes Fahrverhalten mit Prämienvergünstigungen. Im Gegenzug zeichnet ein im Fahrzeg installierter vernetzter Drive-Recorder das gesamte Fahrverhalten einschliesslich Geschwindigkeit, Beschleunigungs- und Bremsverhalten auf und meldet dieses an die Versicherung. Ob diese auch Daten zu gefahrenen Strecken und damit das Bewegungsprofil des Fahrzeugs auswertet, ist ungewiss. Der Metromile-Hack der Corvette zeigt aber, dass das Sicherheitsrisiko der Hard- und Software der Versicherer zusätzlich auf die Kostenseite der Rechnung «Prämienvergünstigung gegen Überwachung» muss.

Nachzulesen unter:

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already
http://futurezone.at/digital-life/forscher-hacken-corvette-mittels-sms/146.458.778
http://resources.infosecinstitute.com/the-nightmare-of-car-hacking
http://www.bankinfosecurity.com/blogs/car-hacking-spurs-automakers-to-share-threat-information-p-1922#
http://futurezone.at/digital-life/testfahrten-fuer-selbstfahrende-lkw-auf-autobahnen-kommen/148.285.509
http://www.spiegel.de/auto/aktuell/fahrdienst-vermittler-uber-setzt-auf-selbstfahrende-autos-a-1049884.html
http://www.welt.de/finanzen/versicherungen/article141298577/Diese-Kfz-Versicherung-weiss-wie-schnell-Sie-fahren.html
http://www.faz.net/aktuell/finanzen/meine-finanzen/ueberwachung-im-auto-telematik-tarife-im-kommenh-13732050.html

IV. Home, Smart Home: Wenn der Kühlschrank zum Verräter wird und das Handy den Bösen alle Türen öffnet

Dass ein Kühlschrank beim Blick in sein Inneres viel über die Lebens- oder zumindest Ess- und Trinkgewohnheiten seiner Besitzer verrät, ist eine Binsenweisheit, die so alt ist wie Alexander Twinnings Erstmodell. Dass ein smarter Kühlschrank aber auch Gmail-Login-Daten verrät, wenn man sich in das WLAN einhacken kann, mit dem er vernetzt ist, haben Hacker erst auf der letzten DEFCON-Konferenz mit einer Man-in-the-Middle-Attacke bewiesen. Samsung hat die Sicherheitslücke nach eigenen Angaben zwar inzwischen geschlossen, doch haben inzwischen die beiden Österreicher Strobl und Zillner gezeigt, dass nicht nur ein vernetzter Kühlschrank, sondern das gesamte smarte Zuhause geknackt werden kann, zumindest, wenn das Steuerungssystem auf ZigBee basiert. ZigBee ist Standard in den Smart-Home-Lösungen von Samsung, Philips, Osram und Motorola. Die beiden Sicherheitsforscher konnten per App Türen öffnen, die Heizung regeln sowie das Licht an- und ausschalten. Bereits vor Monaten, so Strobl und Zillner, hätten sie die Hersteller auf das Sicherheitsrisiko hingewiesen. Diese hätten darauf aber nur mit einem Schulterzucken reagiert. Es bleibt zu beobachten, ob die smarten Häuslebauer von ihren Kollegen der Fahrzeugbranche lernen oder lieber warten und nach Kosten und Imageschäden die Doppeldeutigkeit im Satz des großen Psychologen und Psychotherapeuten Carl R. Rogers erkennen (müssen): «Nichts ist so wertvoll, wie meine eigene Erfahrung.»

Nachzulesen unter:

http://www.digitaljournal.com/technology/hackers-steal-gmail-credentials-by-hijacking-samsung-smart-fridge/article/441913
http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar
http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge
http://futurezone.at/digital-life/oesterreicher-zeigen-wie-man-smart-homes-hackt/146.964.575
http://cognosec.com/zigbee_exploited_8F_Ca9.pdf

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