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

August 2015

SWITCH

I. What a Hack – Staatstrojaner «Galileo» für knapp eine halbe Million Franken nach Angriff auf Hacking Team unbrauchbar

Es ist schon bittere Ironie: Da investieren Schweizer Kantonsbehörden mit dem Segen des zuständigen Regierungsrats und unter allerstrengster Geheimhaltung 486.500 Euro in eine Überwachungssoftware namens «Galileo» inklusive «Rundum-Sorglos-Paket» – und dann wird das Unternehmen, das die teuren Staatstrojaner und andere Überwachungstechnologie verkauft und sich Hacking Team nennt, selbst gehackt. Alles kommt ans Licht und der ganze Effort war umsonst (wenn auch angesichts des Kaufpreises alles andere als gratis). Dabei sollte der Trojaner die Kommunikation von Verdächtigen auf allen gängigen PC-Systemen und Smartphone-Plattformen überwachen. Zudem weisen verschiedene Kommentatoren darauf hin, dass die mehr als eine Million Zeilen Code, aus denen «Galileo» besteht, weitaus mehr können, als dies im aktuellen Schweizer Recht – wenn denn überhaupt – zugelassen ist. So schreibt z.B. der Landbote: «Praktisch gesehen heisst das, dass die Behörden mit Galileo eine Überwachungssoftware einsetzen will, von der sie gar nicht genau wissen kann, was diese eigentlich tut. Auch ob die Programme angreifbare Schwachstellen haben oder ob ein Hersteller sogar absichtlich eine Hintertüre eingebaut hat, um seinerseits die

Überwacher zu belauschen, bleibt offen.» Letzteres wird zwar von Hacking Team verneint, doch befähigt der Quellcode von «Galileo» nach Meinung des britischen Sicherheitsforschers Joseph Greenwood, der die veröffentlichten gehackten Daten zumindest zum Teil ausgewertet hat, seine Entwickler sehr wohl dazu, die Server ihrer Kunden «funktionsunfähig» zu machen.

Dass die Behörden davor die Augen verschlossen und dafür vor den virtuellen Verkaufsregalen des italienischen Überwachungsanbieters weit aufgemacht hat – gemäss Sonntagsblick sollen sie sich auch noch für andere Technologien, wie z.B. Handy-Mikrophone zum Abhören oder Fernüberwachungs-Technologie für Smartphones und Computer interessiert haben – lässt sich allenfalls damit entschuldigen, dass sie sich als Hacking Team Kunde in illustrer Gesellschaft wähnte. Denn auch das FBI hat mit «Galileo» nicht nur Kinderpornografie-User, sondern offenbar auch nicht-kriminelle Tor-Netzwerk-User überwacht. Dass daneben auch Mittelsmänner der chilenischen Regierung, des russischen Geheimdienstes FSB und repressive Staaten wie Äthiopen, Ägypten oder der Sudan auf Hacking Teams Kundenliste stehen und im Falle des Sudans sogar ein internationales Handelsembargo unterlaufen wurde, hat die Beschaffer offensichtlich nicht gestört.

Nachzulesen unter:

http://www.nzz.ch/zuerich/aktuell/der-seltsame-aufschrei-um-die-trojaner-1.18578045
https://www.digitale-gesellschaft.ch/2015/07/11/einmal-trojaner-federal-fuer-die-zuercher-kantonspolizei/#more-6211
http://www.landbote.ch/ueberregional/standard/Eine-teure-Blackbox-fuer-die-Polizei-/story/31582953
http://www.srf.ch/wissen/digital/der-staatstrojaner-steht-vor-den-toren
http://arstechnica.com/security/2015/07/massive-leak-reveals-hacking-teams-most-private-moments-in-messy-detail/
http://arstechnica.com/security/2015/07/hacking-team-may-not-have-had-a-backdoor-but-it-could-kill-client-installs
http://www.1815.ch/news/schweiz/politik/staatstrojaner-und-frankenstaerke-die-grossen-themen-am-sonntag-20150712061324/
http://www.zeit.de/digital/datenschutz/2015-07/hacking-team-trojaner-kunden-hack

II. Himmelhoher Datenstapel: Die Cyberattacke auf die US-Personalverwaltung sprengt alle bislang bekannten Dimensionen

«If you printed out the 14 million SF86 forms (federal background investigation form) lost in the OPM breach, the stack would be approximately 185 miles high.» Das twitterte Gavin Millard, ein technischer Direktor bei Tenable Network Security am 27. Juni 2015 zu «einem der grössten Diebstähle von Regierungsdaten, die es jemals gab» (Zitat: Wall Street Journal). Anfang Juni wurde bekannt, dass Hacker, deren Spuren nach China führen, die Datenspeicher der US-Personalverwaltung OPM angegriffen und Daten von aktiven und ehemaligen Regierungsmitarbeitern gestohlen hatten.

Anfang Juli musste die Behörde einräumen, dass der Schaden weit grösser ist als bisher angenommen und sich wohl zur bislang grössten Cyberattacke seit Bestehen der amerikanischen Regierung entwickelt. Die Angreifer verschafften sich neben Adressen, Sozialversicherungsnummern, Geburts- und Gesundheitsdaten, Informationen zu Finanzen, manchmal auch zu sexuellen Vorlieben und ausserehelichen Affären sowie zu krimineller Vergangenheit auch rund 1,1 Millionen Fingerabdrücke – und dies nicht nur von Regierungsmitarbeitern, sondern auch von Menschen, die sich um einen Job bei der Regierung beworben haben. In zwei Angriffen wurden hochsensible Daten von insgesamt mehr als 25 Millionen Menschen gestohlen. Die Aufklärung, wie die Attacke überhaupt stattfinden konnte und abgelaufen ist, wird durch die Tatsache erschwert, dass sich schon in einem frühen Stadium der Ermittlungen die Log-Mechanismen innerhalb der angegriffenen IT-Struktur als schwach bis unzureichend herausstellten. Mit dem Rücktritt der OPM-Chefin Katherine Archuleta sind die Probleme also noch lange nicht aus der Welt geschafft.

Nachzulesen unter:

http://www.databreachtoday.com/analysis-opm-breach-so-bad-a-8359#
http://www.golem.de/news/cyberangriff-hacker-dringen-in-personalbehoerde-der-us-regierung-ein-1506-114498.html
http://www.tagesanzeiger.ch/ausland/amerika/Steckt-China-hinter-der-Cyberattacke-auf-die-USA/story/11715202
http://www.zeit.de/digital/2015-07/usa-behoerde-hacker-china
http://www.inforisktoday.com/opm-struggles-to-notify-breach-victims-a-8411
http://www.golem.de/news/nach-hackerangriff-opm-chefin-katherine-archuleta-tritt-zurueck-1507-115175.html

III. Doping-tests waren gestern: Mit dem Datendiebstahl beim Team Sky ist die Tour de France im digitalen Zeitalter angekommen

Dass Tour de France-Sieger unter dem Generalverdacht stehen, gedopt zu haben, gehört schon beinahe zu den vielen Traditionen der Grande Boucle. Dass die berühmteste aller grossen Radrundfahrten aber auch Plattform für zeitgemässe Innovation sein kann, zeigt der Hackerangriff auf das Team Sky des Tourgewinners Chris Froome. Dessen Leistungsdaten, wie Geschwindigkeit, Trittfrequenz oder Puls während einer Etappe wurden gestohlen und als (inzwischen nicht mehr aufrufbares) Video auf dem britischen Eurosport-Kanal übertragen. Die Motive der Hacker sind nicht klar. Sollte damit ein Versuch gestartet werden, Froome zu diskreditieren? Oder sollte damit die Frage aufgeworfen werden, wie Hobbysportler ihre Fitness- und Lifetracker-Daten sichern können, wenn das nicht einmal einem professionellem Team wie Sky gelingt? In Zeiten der Selbstvermessung und des «quantified self», in denen neuerdings sogar eine Mischung aus Toy und Tracker das eigene Liebesleben aufzeichnet, analysiert und speichert, keine ganz unberechtigte Frage …

Nachzulesen unter:

https://netzpolitik.org/2015/tour-de-france-team-sky-offenbar-gehackt
http://www.theguardian.com/sport/blog/2015/jul/14/chris-froome-team-sky-hacking-tour-de-france
http://www.zeit.de/digital/datenschutz/2015-06/datensicherheit-fitness-tracker-vergleich
http://www.primelife.co/lovely-wearable-fuer-sex

IV. IMSI-Catcher: Don´t let them catch you – if you can!

Hätte Leonardo di Caprio als Hochstapler in «Catch me if you can» ein Mobiltelefon besessen, wäre die Film-Komödie wohl deutlich kürzer ausgefallen. Denn mithilfe eines IMSI (für International Mobile Subscriber Identity)-Catchers lassen sich Handys einfach orten und ein Bewegungsprofil ihrer Nutzer erstellen – ohne dass dies die Nutzer erkennen könnten. Dazu simulieren IMSI-Catcher ein Mobilfunknetzwerk, indem sie sich gegenüber dem Telefon als Basisstation und gegenüber dem regulären Netzwerk als Mobiltelefon ausgeben. Deshalb identifizieren sie bei ihrem Einsatz z. B. in der Verfolgung Verdächtiger zwangsläufig nicht nur dessen Mobiltelefon, sondern auch alle anderen, die sich im Empfangskreis des Catchers befinden und dort

einbuchen. Und weil sie schon mal alle haben, zwingen die IMSI-Catcher die Telefone, ihre Verschlüsselungen abzuschalten und leiten von den eingefangenen Smartphones zwar alle verwendeten Daten ins richtige Netz weiter (schliesslich soll ja nicht auffallen, dass da jemand mittelefoniert), ziehen dabei aber erst einmal eine Kopie dieser Daten und analysieren sie. Behörden rechtfertigen den IMSI-Catcher-Einsatz, für den in der Schweiz derzeit keine rechtlichen Grundlagen existieren, mit dessen Effizienz, zum Beispiel bei der Suche nach Vermissten und Kriminellen. Wem aber die Kollateralschäden dabei zu hoch sind, oder wer (nicht zu Unrecht) befürchtet, dass bei Preisen von knapp 1.500.- € für einen Handyfänger auch Cyberkriminelle solche Werkzeuge einsetzen, der muss entweder sein Handy zu Hause lassen oder abschalten. Wer das auch nicht möchte oder kann, dem sei der Artikel in Link 4 (digitale-gesellschaft.ch) oder der Einsatz eines IMSI-Catcher-Catchers empfohlen.

Nachzulesen unter:

https://de.wikipedia.org/wiki/IMSI-Catcher
http://www.blick.ch/news/schweiz/zentralschweiz/am-gitschen-im-kanton-uri-wingsuit-flieger-stuerzt-in-den-tod-id3961344.html
http://www.zeit.de/digital/mobil/2014-09/mobilfunk-imsi-catcher-handy
https://www.digitale-gesellschaft.ch/2015/06/22/imsi-catcher-erkennen-und-dokumentieren
http://www.heise.de/ct/artikel/Digitale-Selbstverteidigung-mit-dem-IMSI-Catcher-Catcher-2303215.html

V. Träumen Androiden von elektrischen Pferden? Eine neue Variante des mTan-Trojaners ZeuS hat es auf Android-Nutzer abgesehen

1982 verfilmte Ridley Scott in seinem Kultfilm «Blade Runner» Philip K. Dicks Science Fiction-Roman «Träumen Androiden von elektrischen Schafen?». Gute dreissig Jahre später entwickeln sich digitale trojanische Pferde zum Albtraum vieler Android-Nutzer. Denn nach 2013 infiziert ein Trojaner erneut Android-Smartphones, um mobile- oder SMS-Anmeldecodes fürs Internet- oder Mobilbanking – mTANs – abzugreifen und an die Angreifer zu senden. Besonders perfide dabei ist, dass sich die neue ZeuS-Variante in einem EV-SSL-Zertifikat versteckt, das in perfekt gefakten Phishing-Mails an e-Banking Kunden verschickt wird. Die technische Analyse zeigt Link 3 (anubis.iseclab.org).

Zwischenzeitlich warnt auch eine Schweizer Kantonalbank vor ZeuS. Da der Trojaner nur selten erkannt wird, wird dringend empfohlen, die grundlegenden Sicherheitstipps für das e- und Mobil-Banking zu beachten.

Die 4 wichtigsten:

- Installieren Sie nur Apps, die Sie wirklich benötigen und die von einer vertrauenswürdigen Quelle stammen.
- Halten Sie Ihr Smartphone und die darauf installierten Apps stets aktuell.
- Aktivieren Sie die Code-Sperre Ihres Geräts.
- Speichern Sie Ihre Zugangsdaten wie PIN und TAN nicht auf Ihrem mobilen Gerät ab.

Nachzulesen unter:

http://www.heise.de/security/meldung/mTAN-Trojaner-hat-es-erneut-auf-Android-Nutzer-abgesehen-2721682.html
http://www.computerbase.de/2015-06/malware-mtan-trojaner-infiziert-android-smartphones
https://anubis.iseclab.org/?action=result&task_id=16277ab1d21cbec147997aec147fe4783&format=html
https://www.appkb.ch/metanavi/news.htm&detailid=335&isElement=inetnews&rss=1&gContrast=2
https://www.ebas.ch/de/securitynews/437-mobile-banking-wird-immer-beliebter

VI. VPN: Wie IPv6, DNS & Co. aus Virtual Private Networks weiterhin Very Problematic Networks machen können

Bereits 2013 haben wir im SWITCH Security Blog darauf hingewiesen, dass in so genannten Dual Stack Umgebungen Datenpackete an VPN Tunnels „vorbei laufen“ können, wenn gleichzeitig IPv6 Tunnels implementiert sind. Letztere werden oft automoatisch und ohne Wissen der Nutzer installiert.

Nun haben britische und italienische Forscher das Angebot 14 kommerzieller VPN-Dienste untersucht und gravierende Mängel festgestellt (ausführlich beschrieben in unten genanntem Link 3 eecs.qmul.ac.uk). Dual Stack-Technik, Mängel bei der Handhabung von DNS-Abfragen und nicht angepasste IPv6-Routing Tabellen führten dazu, dass der Datenverkehr in öffentlichen WLANs nicht durch sichere VPN-Tunnels lief, sondern über das öffentliche Netz. Die Folge: Die als sicher geglaubte Verbindung ermöglicht DNS-Angriffe und die Manipulation von Routing-Tabellen. Anonymität und Privatsphäre der Nutzer sind in solchen Umgebungen nicht mehr

geschützt. Schlimmer noch: Der Datenverkehr kann ausgeleitet und mitgeschnitten werden. Anbieter wie PureVPN setzen zur Vermeidung von DNS-Angriffen auf den Betrieb eigener DNS-Server, gehen von IPv6- wieder auf IPv4-Verbindungen zurück und raten Usern, die PureVPN unter Windows manuell eingerichtet haben, dort IPv6 komplett abzuschalten. Vom IPv6-Leck besonders betroffen sind offenbar Android-Geräte, aber auch Apples IOS ist zumindest in Versionen vor 8.4 nicht ausreichend gegen VPN-Hijacking durch Masque Attacks gesichert, wie Pierluigi Paganini in seinem Blog securityaffairs berichtet. Er rät dringend zum Systemupdate.

Nachzulesen unter:

http://securityblog.switch.ch/2013/08/28/ipv6-vpn-traffic-leakage-in-dualstack-umgebungen
http://www.golem.de/news/security-viele-vpn-dienste-sind-unsicher-1507-115006.html
http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf
http://www.heise.de/security/meldung/Privatsphaere-und-Anonymitaet-bei-vielen-VPN-Diensten-nicht-gewaehrleistet-2731928.html?wt_mc=rss.security.beitrag.atom
http://www.golem.de/news/vpn-schwachstellen-purevpn-veroeffentlicht-patch-fuer-seine-windows-software-1507-115026.html
http://securityaffairs.co/wordpress/38219/hacking/apple-partially-fix-masque-attack.html

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Ob End-to-End Verschlüsselung im Web 2.0 mittlerweile Realität oder nach wie vor ein Mythos ist, hat das Security-Team bei heise.de am Beispiel WhatsApp untersucht. Das Fazit findet sich hier:

http://www.heise.de/security/artikel/Der-WhatsApp-Verschluesselung-auf-die-Finger-geschaut-2629020.html

Mit Hilfe von WebRTC lassen sich lokale IP-Adressen von Clients identifizieren, die ansonsten verschleiert sind. Die New York Times macht sich das offenbar zunutze:

https://webrtchacks.com/dear-ny-times

Die Electronic Frontier Foundation feierte diesen Monat ihr 25-jähriges Jubiläum. CSOonline hat die Jahre nochmals revue passieren lassen:

http://www.csoonline.com/article/2949096/security-leadership/electronic-frontier-foundation-celebrates-25-years-of-defending-online-privacy.html

Interaktive Weltkarten, die Internettraffic zeigen, gibt es ja mittlerweile einige. Norse, kalifornischer Anbieter von Sicherheitslösungen, steuert eine besonders schöne bei, um die immensen Dimensionen von Hackerangriffen auf der ganzen Welt in einer bildlichen Darstellung in Echtzeit sichtbar und bewusst zu machen:

http://map.norsecorp.com

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.