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

Januar 2015

SWITCH

I. iBeacons – werden die Minisender 2015 «the next Big Thing»?

Auch wenn die mit dem energiesparenden Bluetooth Low Energy (BLE) sendenden Leuchtfeuer (wörtlich für Beacon) für sich genommen nur in Reichweiten von bis zu 30 Metern senden: IT- wie auch Handelsexperten erwarten von dem von Apple unter dem Markennamen iBeacon eingeführten Standard zur Navigation in geschlossenen Räumen nichts weniger als eine grosse Revolution auf dem Weg hin zu personalisierter Echtzeitkommunikation und Datenanalyse – sie sehen in den nächsten drei Jahren ein Marktwachstum auf bis zu vier Milliarden Dollar. Die neue Technologie ermöglicht es, Apps auf Mobilgeräten ab iOS 7 bzw. Android 4.3, Signale zu senden, um z.B. Kunden am Regal auf Sonderangebote hinzuweisen und sie danach zur kürzesten Schlange vor den Kassen zu lenken. In Museen könnte eine iBeacon-fähige App den Audio Guide ersetzen und in Sportstadien oder grossen Kulturarenen Besucher zu ihren Plätzen leiten und ihnen auf dem Weg dahin noch schnell ein Platzupgrade anbieten (in den USA bereits in 20 Baseballstadien Realität). Schulen, Universitäten und Bibliotheken könnten Suchende in Räume und zu anderen Objekten ihrer Suche führen.

Das alles kann natürlich nur funktionieren, wenn das System weiss, wo sich das Smartphone zusammen mit seinem Besitzer gerade befindet – wer Services via iBeacons nutzen will, bezahlt mit der Preisgabe seiner Daten über Laufwege, Verweildauer vor Regalen oder Exponaten, Einkaufsverhalten und Kunstkonsum usw. Gerade wegen dieser Tracking- und Profiling-Optionen sind viele Datenmineure in Goldgräberstimmung. Datenschützer fordern daher eine entsprechende Hinweispflicht. Problemfrei sind iBeacons aber auch für jene nicht, die sie einsetzen. Denn sie sind von Wettbewerbern oder Rewardjunkies leicht zu klonen: «…it is easy to trick reward systems that rely on you being somewhere. Like ‚get a free coffee if you enter our shop 100 times'».

Nachzulesen unter:

http://startups.co.uk/tech-trends-for-2015-the-ibeacon

http://www.sueddeutsche.de/digital/beacon-technologie-in-kaufhaeusern-rabatt-schlacht-auf-dem-smartphone-1.2047755

http://www.absatzwirtschaft.de/marketingentscheider-setzen-auf-die-nutzung-von-ibeacons-40829

http://www.huffingtonpost.com/rebecca-abrahams/what-ibeacon-may-mean-for_b_4964375.html

http://www.absatzwirtschaft.de/besteht-eine-hinweispflicht-auf-ibeacons-17558

http://airfy.svbtle.com/clone-a-beacon-ibeacon-and-the-proof-of-location-issue

II. «Locate. Track. Manipulate» – Handyüberwachung auf neuem Level

Der erste Teil dieser Kapitelüberschrift ist keine eigene Kreation, sondern der Titel eines Werbeprospekts des New Yorker Anbieters einer Handyüberwachungssoftware namens «Sky Lock». Diesen hatte die Washington Post kürzlich veröffentlicht, um zu zeigen, dass globale Trackingsysteme, von denen bislang angenommen wurde, sie stünden nur technologisch versierten Organisationen, wie etwa den Geheimdiensten NSA oder GCHQ zur Verfügung, inzwischen auf dem freien Markt von nahezu jedermann gekauft und missbräuchlich eingesetzt werden können. Kommentatoren befürchten, dass die «Geoslavery» – so bezeichnen die beiden Forscher für Geoinformationssysteme, Jerome E. Dobson und Peter F. Fisher die negativen Auswirkungen von Geodaten-Tracking – damit ein neues Niveau erreicht hat. Dass und wie die globale Handyüberwachung via Ortung über das internationale

Signalisierungsprotokoll SS7 funktioniert, wurde kürzlich von Tobias Engel auf dem Chaos Computer Congress vorgestellt.

Neben dem kreativen Nutzen des SS7-Protokolls machen auch Abhör- und Manipulationsversuche via Fake-Mobilfunk-Basisstationen von sich reden, die die führende norwegische Zeitung «Aftenposten» im Dezember aufdeckte. Diese IMSI-Catcher imitieren eine Mobilfunk-Basisstation, über die jede Mobilfunkaktivität in Reichweite manipuliert werden kann. Alleine im Zentrum von Oslo konnte Aftenposten sechs solcher Fake-Basisstation entdecken. Bereits im September hatte die Washington Post 18 IMSI-Catcher in und um Washington D.C. aufgespürt und darüber berichtet.

Nachzulesen unter:

http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

https://www.msu.edu/~kg/874/geoslavery.pdf

http://www.nzz.ch/international/europa/wie-die-totale-handy-ueberwachung-funktioniert-1.18456550

http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html

http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

III. Wie man mit einem 200mm-Teleobjektiv Fingerabdrücke stehlen kann

Jan Krissler kennt sich aus mit Fingerabdrücken. Der Hacker forscht an der TU Berlin über Sicherheitsverfahren und hatte schon 2008 gezeigt, wie leicht sich ein achtlos auf einem Wasserglas hinterlassener Fingerabdruck – im konkreten Fall der des damaligen deutschen Innenministers Schäuble – sichern, kopieren und missbrauchen lässt. Um zu beweisen, dass Fingerabdrücke als Sicherheitsmerkmal denkbar ungeeignet sind, hat er nun nachgelegt. Mittels der 400-Euro-Software «Verifinger» und eines Fotos der rechten Hand (im realen Sinne) Ursula von der Leyens, das mit einem von Pressefotografen standardmässig eingesetzten 200-mm-Teleobjektiv aus 3 Meter Entfernung geschossen war, hat er den Fingerabdruck von Schäubles Kollegin aus dem Verteidigungsministerium gefaket. Und weil er sowieso gerade in Regierungskreisen aktiv war, hat er aus einem 110-Pixel-Durchmesser-Foto der Iris von Kanzlerin Merkel gleich noch ein weiteres Biometrie-Fake erstellt.

Zwei Monate zuvor hatte Mastercard in Zusammenarbeit mit einer norwegischen Biometrie-Firma eine neue Kreditkarte vorgestellt, bei der die PIN durch den Fingerabdruck des Karteninhabers ersetzt wird. Nach Aussagen des Testpartners, der norwegischen Bank Sparenbanken DIN, soll die Technologie künftig bei allen Bezahlkarten der Bank eingesetzt werden. Ob die Bank nach dem aktuellen Auftritt Krisslers auf dem Jahreskongress des Chaos Computer Clubs 31C3 umdenkt und zu jeder dieser Karten ein Paar undurchsichtige Handschuhe mitliefern will, ist nicht bekannt …

Nachzulesen unter:

http://www.zeit.de/digital/datenschutz/2014-12/fingerabdruck-merkel-leyen-hack-ccc-31c3

http://www.nzz.ch/mehr/digital/jan-krissler-starbug-chaos-communication-congress-31c3-fingerabdruck-von-der-leyen-1.18452235

http://www.theregister.co.uk/2014/10/18/mastercard_adds_fingerprint_scanner_to_credit_card_for_pinless_transactions

IV. Drohnen: Brummendes Geschäft, rigidere Regeln und weniger Nutzen als erwartet

Folgt man der Consumer Electronics Association CEA, dann brummt das Geschäft mit den Drohnen. Am Rande der von ihr ausgerichteten Consumer Electronics Show CES in der zweiten Januarwoche in Las Vegas veröffentlichte die CEA Marktfoschungsdaten, denen zufolge die Umsätze mit Drohnen für den Konsumentenmarkt 2015 um 55% auf 130 Millionen USD und ca. 400.000 verkaufte Exemplare anwachsen werden. In den nächsten 5 Jahren will die Branche gemäss CEA-Daten Drohnen im Wert von mehr als einer Milliarde Dollar verkaufen. Dabei scheint der Dichtestress am Himmel schon heute den einen oder anderen Drohnenpiloten zu überfordern, wie das Beispiel eines Beinahezusammenstosses einer Drohne mit einem Airbus im vergangenen Sommer am Londoner Flughafen Heathrow zeigt. Eine Sicherheitsbedrohung ganz anderer Art sahen französische Behörden im Oktober in den Drohnenflügen über mehreren französischen Atomkraftwerken.

Auch in der Schweiz gibt es inzwischen neue Regeln für Drohnenflüge. So hat z.B. die Stadt Zürich, deren Stadtpolizei im Sommer eine 30.000-Franken-Drohne durch einen

Absturz aus ungeklärter Ursache verloren hatte (wir berichteten darüber im Oktober), Drohnenflüge über öffentlichem Grund komplett verboten, Flüge über Privatgrund brauchen die Einwilligung der Besitzer. Der Bund erlaubt Flüge über Menschenmengen nur noch gegen Bewilligung und errichtet bei Grossanlässen wie dem WEF oder der OSZE-Konferenz in Basel 2014 Flugverbotszonen.
Derweil hat er US-amerikanische Inspector General die Drohneneinsätze der U.S. Customs and Border Protection Agency als zu teuer und zu wenig effektiv gerügt. Dazu Tom Barry, ein Analyst am Center for International Policy: «I don't want to say drones have no place in border control, but expensive, military-grade drones have not proven effective in catching immigrants or stopping drug flows.»

Nachzulesen unter:

http://tech.firstpost.com/news-analysis/ces-2015-the-drone-revolution-begins-with-airdog-hexo-and-nixie-248607.html

http://www.tagesschau.de/ausland/drohnen-ueber-akw-in-frankreich-101.html

http://www.nzz.ch/zuerich/stadt-zuerich/drohnen-verbot-ueber-zuerich-1.18439947

http://www.steigerlegal.ch/2014/12/01/osze-drohnen-flugverbot-und-helikopter-bordschuetzen

http://yaleglobal.yale.edu/content/drone-patrols-us-border-ineffective-report-finds

V. Golden Globes im Zeichen des SONY-Hacks

«Dieser Abend steht im Zeichen aller Filme, mit denen Nordkorea kein Problem hat.» Mit diesen Worten verliehen die Moderatorinnen Tina Fey und Amy Poehler anlässlich der Golden Globe-Awards am 11. Januar dem Hack der Sony Pictures Server und der Server für das Sony Playstation Netzwerk nach der technischen, der kriminellen und der politischen auch noch eine kulturelle Facette. Seit dem Bekanntwerden am 24. November letzten Jahres wurde so intensiv über den Hack berichtet und über Täter und Motive spekuliert, dass an dieser Stelle lediglich auf eine aktuell aufdatierte Historie und auf die Kommentare von Bruce Schneier verwiesen werden soll. Zu (nicht ganz ernst gemeinten) Mitspekulieren sei der letzte Link empfohlen, der bei jedem Reload eine neue Variante über Täterschaft und Motive aufstellt.

Nachzulesen unter:

https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack
https://www.schneier.com/blog/archives/2014/12/did_north_korea.html
http://sony.attributed.to

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Die Talks vom letzten Chaos Computer Congress, inklusive denen zur Fingerabdruck-Fotografie und dem SS7-Hack sind online verfügbar:

http://media.ccc.de/browse/congress/2014/

Who's Attacking Whom? Brian Krebs hat ein paar schöne dynamische Visualisierungen von Internetangriffen zusammengestellt:

http://krebsonsecurity.com/2015/01/whos-attacking-whom-realtime-attack-trackers/

Was passiert, wenn Sie die Top-10-Anwendungen von – sagen wir download.com – installieren, haben die Jungs von howtogeek.com ausprobiert:

http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/

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