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

April 2015

SWITCH

I. Shades of Grey, made in Germany: SAP und die NSA

Wer nach den Snowden-Leaks die Bösen jenseits des Atlantiks und die Guten diesseits verortete, muss wohl spätestens seit Anfang März in Betracht ziehen, dass auch die digitale Welt nicht binär tickt, sondern in vielen Graustufen abgeschattet ist. Unter dem Titel «SAP arbeitet für die NSA» berichtete Zeit online, dass die US-amerikanischen Geheimdienste zur Auswertung ihrer gigantischen Datenmengen auf die hoch leistungsfähige Datenbank-Technologie HANA des Walldorfer Software-Riesen zurückgreifen. Das ARD-Magazin Fakt mutmasste zudem, dass die jüngsten Akquisitionen des grössten deutschen Software-Herstellers und die Gründung der US-Tochter NS2 zu eben dem Zweck erfolgt seien, ins Geschäft mit den amerikanischen Diensten zu kommen. Dies wurde seitens SAP zwar relativiert. Darauf, dass SAP dennoch grosses Interesse an Geschäften in diesem Marktsegment hat, deuten neben Hinweisen in SAP-eigenen Veröffentlichungen auch Exklusivverträge zwischen SAP und amerikanischen Entwicklern von Überwachungs-, Auswertungs- und Analyse-Tools hin. Einer davon ist ebenfalls in deutscher Hand, gehört zum Firmenkonglomerat von Peter Thiel und trägt den bezeichnenden Namen

Palantir (bei Tolkien ein Überwachungs- und Kommunikationstool des bösen Weltenvernichters Sauron). Diese schon beinahe belustigende Selbstironie schlägt jedoch schnell um, wenn man sich bewusst macht, dass es offenbar als Geschäftsmodell gedacht ist, auf der einen Seite die Zusammenarbeit mit der NSA zu forcieren und auf der anderen den Schutz vor deren Ausspähmethoden anzubieten.

So lukrativ dieses Modell auf den ersten Blick aussieht, so gross sind allerdings auch seine Risiken. Denn inzwischen stellen kritische Stimmen die Frage, ob in der zivil genutzten SAP-Business-Software eventuell Hintertüren zum Ausspionieren der Anwender eingebaut sein könnten. SAP-CEO McDermott dementierte dies am Rande der CeBit energisch: »There are no back doors in SAP technology, period".

Nachzulesen unter:

http://www.zeit.de/digital/internet/2015-03/nsa-sap-uberwachung-technik

http://www.mdr.de/fakt/fakt_sap_ueberwachungssoftware100.html

http://de.news-sap.com/2011/05/25/vor-lauter-baumen-den-wald-doch-sehen-mit-sap-intelligence-analysis-for-public-sector-by-palantir

http://www.manager-magazin.de/unternehmen/it/palantir-und-die-dunkle-seite-der-macht-a-1013000.html

https://netzpolitik.org/2015/sap-produkte-im-wert-von-250-millionen-euro-beim-deutschen-militaer

http://recode.net/2015/03/17/sap-ceo-mcdermott-walks-a-fine-line-on-nsa-allegations

http://www.computerworld.ch/news/security/artikel/spionageskandal-ueberwacht-sap-schweizer-firmen-67485

http://www.handelsblatt.com/politik/deutschland/schroeder-stellt-buch-vor-basta-kann-er-immer-noch/9485784.html

II. David, Goliath und die Suche nach einem wirklich sicheren Hafen

Ein 27-jähriger Österreicher gegen das mit 1,4 Milliarden Mitgliedern grösste Social Network der Welt in den USA – alleine in dieser David-gegen-Goliath-Konstellation liegt Aufmerksamkeitspotential. Doch auch das Thema der Auseinandersetzung hat es in sich. Denn die Frage, die Max Schrems, den Salzburger Juristen, Datenschutzexperten und Gründer von europe-v-facebook.org motiviert, immer wieder gegen Facebook und seinen Umgang mit den Daten europäischer Bürger vorzugehen, betrifft letztlich alle.

Sie heisst: Dürfen US-amerikanische Unternehmen Daten europäischer Bürger auf Server in den USA ablegen, auf die die NSA im Rahmen ihres PRISM-Programms nach Genehmigung durch ein amerikanisches Geheimgericht zugreifen kann, obwohl gemäß der EU-Datenschutzrichtlinie diese Übertragung in die USA an und für sich untersagt ist, weil das Niveau des amerikanischen Datenschutzes nicht an das des europäischen heranreicht? Zwar hatte die EU-Kommission im Safe-Harbor-Abkommen aus dem Jahr 2000 US-Unternehmen – grob dargestellt – zugestanden, dass sie sich selbst bescheinigen, angemessenen Datenschutz zu leisten. Doch zweifeln selbst der EU-Kommissar für Digitalen Binnenmarkt, Andrus Ansip, und die deutsche Bundesdatenschutzbeauftragte Andrea Voßhoff daran, dass Safe Harbor wirklich Sicherheit für persönliche Daten bietet.

Inzwischen befasst sich der Europäische Gerichtshof mit der Klage Schrems´. Das könnte zwar dazu führen, dass der EuGH Safe Harbor für nichtig erklärt, wird aber die Überwachung der Daten ausländischer Bürger ohne oder mit allenfalls minimaler juristischer oder parlamentarischer Kontrolle durch amerikanische Regierungsbehörden nicht stoppen. Das Recht dazu hat sich die amerikanische Regierung u.a. mit der präsidialen Verfügung 12333 selbst eingeräumt. Sichere Häfen sind also noch lange nicht in Sicht.

Nachzulesen unter:

http://europe-v-facebook.org
http://www.zeit.de/digital/datenschutz/2015-03/eugh-facebook-safe-harbor-max-schrems
http://futurezone.at/netzpolitik/facebook-eugh-prueft-datenuebermittlung-in-die-usa/121.250.876
http://www.silicon.de/41610652/eugh-verhandelt-ueber-klage-gegen-facebook
http://www.tagesanzeiger.ch/leben/gesellschaft/Max-Schrems-gegen-Mark-Zuckerberg/story/13147716
http://www.handelsblatt.com/unternehmen/it-medien/eugh-klage-gegen-facebook-der-kampf-gegen-die-lebensluege-datenschutz/11548230.html

Mehr zum Thema als Buch und aktuell auf Twitter:

http://www.silicon.de/41599539/wie-facebook-tickt-und-nutzer-dafuer-kann
http://kaempfumdeinedaten.com
https://twitter.com/maxschrems

III. Wird der Apfel zum Straussenei?– Apple entfernt die Rubrik «Anti-Virus- und Anti-Malware-Programme» samt Apps aus iOS AppStore

Keine Viren in iOS, also auch keine Anti-Virus- und Anti-Malware-Apps mehr im iOS-AppStore. Das ist in Kurzform die Begründung dafür, dass Apple die entsprechende Rubrik samt allen Apps aus dem Store entfernt hat. Weil diese wie alle anderen Apps in einer Sandbox laufen und daher das iOS-Device an sich nicht schützen können, mag dieser Schritt nachvollziehbar erscheinen. Dabei wäre es aber durchaus sinnvoll, wenn z.B. virenbefallene Mail-Anhänge oder Malware und Viren, die sich via USB-Verbindung mit einem Mac oder MacBook unter OS X auf das iOS-Gerät schleichen, erkannt und aussortiert werden könnten. Zumal auf Macs aus Cupertino zunehmend mehr Malware- und Virusbefall zu beobachten ist. Ob sich das Problem mit der nach aussen demonstrierten Vogel-Strauss-Politik lösen lässt, darf bezweifelt werden.

Nachzulesen unter:

http://www.intego.com/mac-security-blog/where-did-virusbarrier-ios-go
http://www.gizmodo.de/2015/03/23/apple-entfernt-anti-virus-rubrik-aus-app-store.html
http://futurezone.at/apps/keine-viren-auf-ios-apple-entfernt-antiviren-apps/121.116.431
http://www.huffingtonpost.com/2012/04/24/mac-malware_n_1448561.html
http://www.sophos.com/en-us/press-office/press-releases/2012/04/one-in-every-five-mac-computers-harbors-malware.aspx

IV. Pleitegeier kennen keine Privatsphäre – RadioShack will Kundendaten versteigern

Der Spruch «If you're not paying for the product, you are the product.» wird gerne verwendet, um die mögliche Kehrseite von Gratis-Angeboten im Informationszeitalter zu beschreiben. Allerdings lässt sich der vielleicht suggerierte Umkehrschluss, nämlich dass wenn man bezahle, die Kundendaten nicht zu Geld gemacht würden, nicht halten. Den Beweis dafür liefert gerade die insolvente Unterhaltungselektronik-Kette RadioShack. Im Insolvenzverkauf möchte man nun auch Namen, Adressen, Telefonnummern und Daten zu den Käufen von 117 Millionen US-Kunden an den Meistbietenden versteigern – entgegen der eigenen Privacy Policy-Erklärung, die besagt «We will not sell or

rent your personally identifiable information to anyone at any time." Auch wenn die Generalstaatsanwälte von New York, Tennessee und Texas im Verkauf der Kundendaten eine Verletzung geltenden Rechts in ihren Bundesstaaten sehen und angekündigt haben, dagegen vorzugehen, gibt es vielleicht demnächst T-Shirts mit dem Spruch: «Even though you're paying for it, you are the product.»

Nachzulesen unter:

http://www.bloomberg.com/news/articles/2015-03-24/radioshack-s-bankruptcy-could-give-your-customer-data-to-the-highest-bidder

http://newyork.cbslocal.com/2015/03/25/report-radio-shack-to-sell-customers-personal-information-in-bankruptcy-sale
https://www.theverge.com/2015/3/24/8285319/radioshack-selling-customer-information-bankruptcy

V. Trau, schau, wem – Hacker faken Profile auf Datingplattform

Vollumfänglich bestätigt wurde vor Kurzem eine andere Ikone der Internetcommunity – der legendäre, am 5. Juli 1993 in «The New Yorker» veröffentlichte Peter-Steiner-Cartoon «On the Internet, nobody knows you´re a dog.» Im März berichtete das Online-Magazin «theverge.com» darüber, dass ein kalifornischer Programmierer die Dating-App Tinder so gehackt hätte, dass zwei heterosexuelle Männer miteinander in dem Glauben flirteten, sie würden mit der Frau auf dem ihnen fakeweise eingespielten Bild und Profil chatten.

Bei aller (Tragi)Komik verweist die Manipulation auf zwei ernsthaftere Probleme: Denn offenbar klafft in der Tinder-App ein scheunentorgrosses Sicherheitsleck, das in der Vergangenheit bereits mehrfach genutzt wurde und bis heute nicht geschlossen ist. Und zudem stellt sich die grundsätzliche Frage, ob und inwieweit Apps und Plattformen im Sinne der Informationssicherheit für die Authentizität ihrer User sorgen sollen und können - auch wenn Peter Steiners Internet-Hund damit wohl nicht allzu glücklich wäre.

Siehe:

http://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html

http://www.theverge.com/2015/3/25/8277743/tinder-hack-bros-swiping-bros

http://www.nzz.ch/mehr/digital/tinder-patrick-hack-dating-1.18510550

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Die Stanford University hat ein Projekt zum Thema «Secure Internet of Things» ins Leben gerufen. Auf der Projekt-Website gibt es Slides der abgehaltenen Seminare und Events:

http://iot.stanford.edu/

Talks und Slides der diesjährigen Security-Konferenz Troopers15 sind online abrufbar. Ein heisser Tipp ist die Keynote von Haroon Meer: «InfoSec - The hard thing about the hard thing»:

https://www.troopers.de/archives/troopers15/presentations/

https://www.youtube.com/playlist?list=PL1eoQr97VfJkfckz9nZFR7tZoBkjjj23f

https://www.youtube.com/watch?v=rarpym8JJXQ

Pierluigi Paganini hat einen «Buyers Guide to Stolen Data on the Deep Web» veröffentlicht. Trend auf dem Schwarzmarkt: Das möglichst vollständige Personenprofil:

http://blog.norsecorp.com/2015/04/07/a-buyers-guide-to-stolen-data-on-the-deep-web/

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