SWITCHcert Security Report

April 2015

SWITCH

I. Shades of grey, made in Germany – SAP and the NSA

Anyone believing, after Edward Snowden's leaks, that the bad guys are on the other side of the Atlantic and the good guys on this side would have been forced to admit since the start of March at the latest that the digital world is not quite so black and white. In fact, it comes in many shades of grey. Germany's ZEIT ONLINE ran a report with the headline «SAP working for the NSA», claiming that the US intelligence services are using the Walldorf-based software giant's HANA high-performance database technology to analyse the vast quantities of data they collect. The current-affairs show FAKT on ARD also alleged that the latest acquisitions made by Germany's biggest software manufacturer as well as the incorporation of its US subsidiary NS2 were aimed at facilitating business with the Stateside intelligence services. SAP tried to play this down, but statements in its own publications and exclusive contracts signed with US developers of surveillance, evaluation and analysis tools do point to a significant interest in this field of business. One of the developers in question is German-owned, belonging to Peter Thiel's conglomerate. The company's name, Palantir, is rather telling as it comes from a kind of crystal ball used by the evil destroyer Sauron in JRR Tolkein's books to observe and control others. This self-deprecation seems almost hilarious until you discover that the firm's business model is to work with

the NSA on the one hand while offering protection against its spying methods on the other.

As lucrative as this might at first seem, it entails major risks. Critics are already asking whether SAP's business software for civilian use might have back doors built in for spying on users. SAP CEO Bill McDermott categorically denied this at the CeBIT technology show: «There are no back doors in SAP technology, period.»

Read more here:

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 and the search for a truly safe haven

A 27-year-old Austrian versus the biggest social network in the US with 1.4 billion members. This David-and-Goliath situation alone is enough to attract attention, but the cause of the dispute is even more intriguing. In fact, Max Schrems, a Salzburg-based lawyer, data protection expert and founder of europe-v-facebook.org, repeatedly takes action against Facebook and its handling of European citizens' data for a reason that affects all of us.

It is the question of whether US companies can store these data on servers in the US that can be accessed by the NSA as part of its PRISM programme with the approval of a secret US court, despite the fact that the EU's Data Protection Directive expressly forbids their transmission to the US, where data protection standards do not match those in Europe. It is true that the European Commission, roughly speaking, gave US firms permission to have themselves certified as offering adequate data protection under the Safe Harbor Agreement of 2000. However, even Andrus Ansip, the EU Commissioner for the Digital Single Market,

and Andrea Vosshoff, Germany's Federal Commissioner for Data Protection and Freedom of Information, doubt that Safe Harbor really offers security for personal data.

The European Court of Justice is now dealing with the case brought by Schrems. The Court may declare Safe Harbor null and void, but this will not stop the US authorities from collecting data on foreign nationals with little or no legal or parliamentary control. The US government gave itself this power, for example, with Executive Order 12333 «United States Intelligence Activities». Truly safe havens (or «harbors») are therefore not on the horizon.

Read more here:

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

Take a look at Schrem's book and keep up to date with his Twitter feed:

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

III. Apple with its head in the sand? Entire anti-virus and anti-malware category of apps removed from iOS App Store

There are no viruses in iOS, so there is no need for anti-virus and anti-malware apps in the iOS App Store. This is essentially Apple's reasoning behind its decision to remove the entire category and all the apps that were in it from the store. The decision is understandable in that these apps, like all others, run inside a sandbox and are thus unable to protect iOS devices per se. However, it would certainly make sense, for example, to be able to identify and filter out infected e-mail attachments, malware and viruses transferred to an iOS device via USB from a Mac or MacBook running OS X. This seems especially desirable in view of the increasing quantity of malware and viruses affecting the desktops and laptops from Cupertino. It is doubtful that Apple can solve the problem with ostrich tactics (putting its head in the sandbox, so to speak).

Read more here:

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. Bankrupts have no respect for privacy – RadioShack to auction customer data

«If you're not paying for the product, you are the product» is a popular way of expressing the downside of free offers in the information age. However, it would be wrong to assume that the opposite – your data will not be monetised if you are paying for a service – holds true. Insolvent US electronics retailer RadioShack is proving this point at the moment. As part of its bankruptcy auction, it intends to sell off names, addresses, phone numbers and other details concerning purchases by 117 million US customers to the highest bidder – in violation of its own privacy policy, which states, «We will not sell or rent your personally identifiable information to anyone at any time.» Attorney Generals from New York, Tennessee and Texas claim that the sale of customer data violates their state laws

and intend to contest it before the courts. Nevertheless, we might soon be seeing a new t-shirt slogan: «Even though you're paying for it, you are the product.»

Read more here:

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. Look before you leap – hackers fake profiles on dating app

Another iconic image from the Internet community has been totally confirmed recently, namely the legendary Peter Steiner cartoon that appeared in The New Yorker on 5 July 1993 with the caption «On the Internet, nobody knows you're a dog.» The online magazine theverge.com reported in March that a Californian programmer had hacked the dating app Tinder in such a way that two heterosexual men flirted with each other in the belief that they were chatting up the beautiful woman depicted in a fake picture on a fake profile.

As tragicomic as this is, it highlights two rather serious problems. Firstly, there is obviously a gaping security hole in the Tinder app, which has been used more than once in the past and yet still not closed. Secondly, there is the fundamental question of the extent to which apps and websites can and should ensure information security to protect their users' identities – even if Steiner's dog would be less than happy about this.

See:

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

The Clipboard: Interesting Presentations, Articles and Videos

Stanford University has launched its Secure Internet of Things Project. The project website contains seminar presentations and event details:

http://iot.stanford.edu/

Talks and presentations from this year's Troopers15 security conference are available online. The keynote speech by Haroon Meer «InfoSec – The hard thing about the hard thing» is a hot tip:

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

https://www.youtube.com/playlist?list=PL1eoQr97VfJkfckz9nZFR7tZoBkjij23f

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

Pierluigi Paganini has published «A Buyers Guide to Stolen Data on the Deep Web». The latest trend on the black market is «Fullz» – as complete a personality profile a possible:

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

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.