SWITCHcert Security Report

February 2015

SWITCH

I. Attacks in the wake of the attack – privacy after the horror of Paris

The fact that a pattern has emerged whereby each new terror attack brings calls for a sharp increase in surveillance and ever greater restrictions on privacy says nothing good about the state the world is in. UK Prime Minister David Cameron, for instance, said a week after the Paris attack that he wanted blanket monitoring of all forms of communication, including the Internet: «There should be no means of communication that we cannot read. » The EU interior ministers also want to step up the war on terror by rolling out new forms of surveillance and reviving old ones.

From an IT privacy standpoint, the debate centres on data warehousing and whether intelligence agencies can force IT providers to build a «back door» into data encryption mechanisms that they can open whenever they want.

UK Information Commissioner Christopher Graham had previously said that the encryption of private users' communications was an important safeguard of personal security that must not be compromised. The US National Intelligence Council (NIC) pointed out in a document dating back to 2009 and publicised in connection with Edward Snowden's revelations that encryption was the best form of defence for private data.

The President and CEO of the Internet Association countered political calls to remove this defence with the following statement: «Just as governments have a duty to protect the public from threats, Internet services have a duty to our users to ensure the security and privacy of their data. That's why Internet services have been increasing encryption security.»

Read more here:

http://www.nzz.ch/international/europa/britische-konservative-fordern-totale-ueberwachung-des-internets-1.18461345

https://netzpolitik.org/2015/239-anti-terror-massnahmen-nach-911-sind-nicht-genug-eu-innenminister-wollen-freiheitsrechte-weiter-einschraenken

http://www.spiegel.de/netzwelt/netzpolitik/charlie-hebdo-streitgespraech-ueber-vorratsdatenspeicherung-a-1012141.html

http://www.bankinfosecurity.com/obama-sees-need-for-encryption-backdoor-a-7809

http://futurezone.at/digital-life/us-report-verschluesselung-ist-zentral-fuer-privatsphaere/108.451.938

http://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks

http://futurezone.at/netzpolitik/eu-innenminister-mit-massenueberwachung-gegen-den-terror/110.881.788

II. A brave new world of e-banking

For some time now, advertisements have been running in prime-time slots on Austrian TV for George, which claims to be «Austria's most modern banking». Anyone seeing the ads and calling up mygeorge.at might be forgiven for wondering whether Google, Facebook, PayPal or some other online heavyweight is out to make waves in our neighbour's banking sector. There are glossy pictures, links and apps for every kind of device. Here is the twist: this is no financial spin-off from an Internet firm, but that is exactly what the people at Erste Bank and Sparkassen want it to look like. They want to show that state-of-the-art e-banking not only needs a contemporary look and feel, it should be designed from the ground up to resemble a social network. Recent survey figures confirm that financial institutions have a lot of catching up to do in terms of usability, design and the fun factor compared with Facebook, Amazon and the rest – the upside is that 75-81% of their customers consider them to be safe and trustworthy, a result Facebook (3%) and Google (1%) can only dream of.

It is no wonder, then, that not all customers are impressed by this obvious effort to create an e-banking platform in the image of social media. The comments in response to an article about George on the tech site futurezone.at range from keen approval to flat-out rejection, reflecting the aforementioned trust deficit of the big networks.

Financial institutions are currently looking very carefully at ways to integrate digital technologies into banking. They are under pressure not only from their competitors in the financial sector, but also first and foremost from tech giants such as Apple, eBay and Google.

It has thus been clear for quite a while that details of payment flows – including those of Swiss bank customers – will be analysed in the search for modern e-banking solutions and new sources of income. As a result, e-banking customers will in future benefit from personalised discount offers, for example.

Read more here:

http://futurezone.at/produkte/erste-bank-startet-online-banking-nach-google-vorbild/108.093.119

http://www.dailymail.co.uk/sciencetech/article-2773349/Could-credit-score-soon-based-FACEBOOK-FRIENDS-Expert-predicts-future-banking-rely-social-networks.html

http://www.computerworld.ch/marktanalysen/studien-analysen/artikel/banken-wollen-paypal-co-paroli-bieten-66423

http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Postfinance-baut-ein-Schnaeppchenportal-auf/story/13044454

III. Gone in less than 60 seconds – from car theft to automotive data hacking

«You can lock your car, but if he wants it...it's gone in 60 seconds» – this is the tagline from the original movie poster for «Gone in 60 seconds», which was remade in 2000 with Nicolas Cage. Some 15 years later, car theft is as much of a problem as ever, but it has now been joined by all manner of hacking into vehicle and traffic data. Jimmy Schulz and Rüdiger Hannig made this clear at the 31st Chaos Communication Congress (31C3) at the end of last year in Hamburg. Hannig's presentation quoted Volkswagen CEO Martin Winterkorn: «Your car's data are mine.» Concerned drivers of models from the VW Group line-up might think it would have been less contentious for him to state more neutrally that

today's cars are data mines. Does he really believe that the data a car produces about itself and its driver automatically belong to him?

The truth is that Winterkorn's company is not the only one making cars that gather data and share them via open, standardised interfaces with head office, affiliated garages, parts suppliers, smartphone manufacturers and network operators, which analyse them and in some cases forward them further. The data themselves used to be generated within a closed system inside the vehicle, but «black boxes» such as tachographs and insurance companies' telematic recorders now transmit unencrypted data to the outside world, making them vulnerable to hacking (see Security Report, October 2014). This is also illustrated to good effect in a new awareness video from Saarland University (see Vimeo link; in German). According to hackernews.com, over two million US cars fitted with wireless dongles from insurance companies are especially at risk. At the same time, electronic tyre pressure sensors and other systems can pose a threat to drivers' privacy. With this in mind, researchers at the Vienna University of Technology have already begun working on strategies for making cars learn to protect themselves against hackers. Günther Oettinger, the EU's Commissioner for the Digital Economy and Society, recently warned German carmakers: «Digitally speaking, we're playing catch-up with the US and South Korea. [...] If you have the data, you have the power, and cars and their drivers supply particularly attractive, valuable data.»

Read more here:

http://vimeo.com/111822896

http://www.idgconnect.com/blog-abstract/8344/global-car-makers-join-data-race

http://blogs.strategyanalytics.com/AMCS/post/2014/11/03/Consumers-will-expect-greater-transparency-regarding-vehicle-data-extraction-interpretation-and-sharing.aspx

http://www1.wdr.de/fernsehen/ratgeber/servicezeit/sendungen/reifendruck106.html

http://www.heise.de/security/meldung/TU-Wien-will-Autos-vor-Hacking-Angriffen-schuetzen-2483552.html

http://thehackernews.com/2015/01/progressive-snapshot-device-hacking-car.html

http://www.heise.de/newsticker/meldung/EU-Kommissar-Oettinger-Deutsche-Autobauer-muessen-bei-Vernetzung-Tempo-erhoehen-2532487.html

IV. Microsoft versus Google and vice versa – biblical short-sightedness?

Without wishing to cast aside the Security Report's unbiased worldview, we cannot help but notice the similarity between Google and Microsoft's fight over fixing security loopholes and the biblical tale of the man who pointed out the speck in his brother's eye while failing to acknowledge that a plank in his own eye was severely impairing his ability to see.

Back in 2012, Microsoft's then CEO Steve Ballmer brought the highly polarising political adviser Mark Penn to Seattle. Penn launched the typically partisan «Scroogled» PR campaign, which attempted to poke fun at Google's handling of user data. What apparently seems to work in the US political arena fell completely flat in the world of IT, ultimately resulting in the campaign being quietly ended at the start of the year.

Microsoft was derided for its unfunny jokes, some of which were actually copied from other sources. Meanwhile, Google hit back. The search giant started its own initiative, dubbed «Project Zero», in July 2014, supposedly aimed at making the Internet a safer place. Google finds security issues in software, informs the manufacturer confidentially at first and gives them 90 days to bring out a patch. If a viable patch does not appear in time, Google publishes the security issue.

This may seem like a noble intent at first glance, but look closer and there are two problems with it. Firstly, the 90-day deadline does not always allow enough time to test that a patch really does improve security. Secondly (and this is where the speck and the plank come in), Google is rigorously pointing out bugs in Microsoft software above all (although it has now started targeting Apple's OS X as well), but it is no longer providing security updates for its own programs. This includes WebView, a key component for viewing websites in Android 4.3 Jelly Bean. Security expert Graham Cluley had this to say on the matter in his blog: «Just imagine if Microsoft researchers gave Google 90 days to fix a WebView vulnerability in Android 4.3, and then released proof-of-concept exploit code. I wonder how Google would feel then?»

Read more here:

http://futurezone.at/digital-life/microsoft-stellt-umstrittene-anti-google-kampagne-ein/108.473.001

http://www.golem.de/news/windows-google-enthuellt-dritte-sicherheitsluecke-in-drei-wochen-1501-111748.html

http://www.zdnet.de/88215782/microsoft-kritisiert-google-wegen-offenlegung-von-weiterer-windows-8-1-luecke

http://www.macworld.co.uk/news/mac-software/googles-project-zero-publishes-three-os-x-zero-day-vulnerabilities-3595374

http://www.security-insider.de/themenbereiche/plattformsicherheit/mobilesecurity/articles/472142

http://grahamcluley.com/2015/01/google-discloses-microsoft-windows-vulnerability

The Clipboard: Interesting Presentations, Articles and Videos

In an interview with netzpolitik.org, Phil Zimmermann, the father of PGP and ZRTP, chats about encryption, secret service snooping and crypto-wars:

https://netzpolitik.org/2015/netzpolitik-podcast-126-phil-zimmermann-ueber-verschluesselung-geheimdienst-ueberwachung-und-krypto-kriege/

The European Union Agency for Network and Information Security (ENISA) has published a 73-page report entitled «Privacy and Data Protection by Design».

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

A global list of information security conferences in 2015 can be found on the Concise Courses Cybersecurity Blog:

http://www.concise-courses.com/security/conferences-of-2015/

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