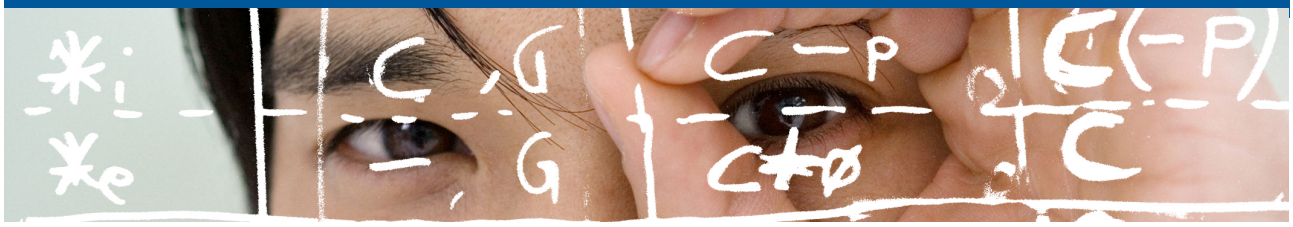
SWITCHcert Security Report

December 2013



SWITCH
Serving Swiss Universities

Start-ups promise digital self-defence help - but don't always deliver

Admittedly, you cannot really speak of a real "exodus" from commercial suppliers such as Google, Facebook, WhatsApp and Co. Yet since details of the NSA's spying operations have emerged, industry experts have been observing a decidedly increased interest in alternative ways of chatting, mailing and surfing the Net. Companies and private users are currently more than ever concerned with encryption and private communications.

Experts consider this to be one of the largest growth markets in the coming years, as economic journalist Steffan Heuer confirms: "This is comparable to the rise of antivirus software, which is unquestionably a standard requirement now." As a representative survey by the Bitkom inter-trade organisation shows, since July 2012 the number of people encrypting their mails with special software has indeed increased by 50 per cent. 91 per cent of all citizens still do without this option though - usually due to a lack of technical knowledge (61 per cent); because nobody else much uses this (56 per cent); or because it is considered too elaborate a measure to implement (25 per cent).

There are start-ups springing up literally everywhere lately, wanting to supply Internet users with their products as a means of "self-defence". For instance, a Swedish supplier called "Hemlis" ("secret") currently wants to take on WhatsApp and Co.: "Any communications across networks are monitored by the authorities and private organisations; and politics just won't change that. For this reason we have decided to develop a service which makes eavesdropping impossible", co-founder Peter Sunde explains. "Hemlis" uses encryption for all communications and does not store anything centrally. Judging by the increasing number of their users, so far Sunde's plan seems to work like a charm.

European search engine providers such as "Startpage" and "Ixquick" with servers outside American territories have also been benefiting from increased user numbers. The one black sheep of the industry however turns out to be the "DuckDuckGo" search engine: with now four rather than previously two million search enquiries per day, it is very explicitly riding the crest of this anti-NSA wave. Company boss Gabriel Weinberg promotes their services stating that they do not store any user data, scrupulously use encryption and do without any cookies and tracking software. Shame though that DuckDuckGo is a US company, runs its services on Amazon servers and hence is subject to NSA rules in any case.

"Die Zeit" journalist Patrick Beuth considers the fact that user enquiries have still doubled to currently four million a day over the last few months the expression of an "act of desperation" by people looking for a place to store their data safely away from surveillance.

However, whether there is such a place at all is doubted by just about anyone by now: A survey by the German Bitkom inter-trade organisation found that 80% of Internet users generally believe that their data are not safe on the Net. At the same time, for many companies investment into increased security measures has lately become a matter of the highest priority.

Further reading:
http://futurezone.at/digital-life/privatsphaere-ist-wieder-gefragt/41.877.492
http://www.zeit.de/digital/datenschutz/2014-01/duckduckgo-startpage-ixquick-nsa
http://techcrunch.com/2014/01/12/duckduckgos-popularity-exploded-in-2013-following-the-nsaprism-leaks/
http://www.bitkom.org/de/presse/78284_78077.aspx

The Cloud industry is realigning itself - and so are customers

As early as August - when it emerged that the NSA is extracting data from the servers of leading Cloud providers such as Google, Amazon and Microsoft, and completely legally at that - experts were forecasting dire prospects ahead for this industry: the "Information Technology & Innovation Foundation" for instance estimated that Cloud suppliers were facing some 35 billion dollars in damages over the next three years. Others expect them to get stung by up to 180 billion. Ever since, European competitors have been rubbing their hands in glee and started a security promotional campaign themselves.

Many suppliers and initiatives now see the heightened need for security as a godsend: in Germany for instance, there are plans for independent bodies to offer "data protection certification for Cloud Computing" from spring 2015 onwards.

The SAP software manufacturer located there has just announced that they are expediting their worldwide expansion of data processing centres that will all be subject to German law.

At home, Swisscom is pinning their hopes on advertising at this opportune time: they are planning to commence operations in a new centralised data processing centre running all of their Cloud business, supported by new services here. Their spokesperson Olaf Schulz considers Switzerland to be an even more attractive data storage and processing location for European customers these days, because their data is believed to be doubly protected over here: both by the Swiss data protection act and telecommunications law.

Better double-encrypted than sorry

Cloud providers wishing to gain their customers' trust for the long term cannot simply use an NSA-free zone for advertising purposes, as Bruno Crispo, a Trento university expert, warns: on the one hand because the British secret service also captures data on a massive scale, on the other because it will arguably be difficult to offer a Cloud exclusively based on European software and hardware. He recommends what the US providers Google, Amazon and Co. have already vowed to do: improving their own security standards and offering end-to-end encryption to users. Which means: users will be able to encrypt their data locally at their end before sending them to the respective Cloud service in encoded form later, with service providers not knowing the key.

Legal experts now explicitly recommend that companies wishing to benefit from the flexibility and efficiency of global Clouds concentrate on European providers. However, you should make sure you read the small print here, too. As Dr. Thomas Jansen, solicitor, explains, it is not simply the location of the Cloud provider which is of importance, but also its server locations: "Legally, there are great differences depending on whether providers store data or data security copies on IT systems in Germany, Switzerland, Malta, Canada, the USA, India or China. Often data is also stored in several locations at the same time. It is important to have explicit and binding contractual assurances in this regard, and vital to check all legal aspects." With Clouds where data is stored in low-wage countries, there is the added risk of "third parties sometimes being able to access data very quickly and easily by simply bribing employees." His recommendation: The fewer clear legal specifications there were for Cloud computing, the more important a thorough contract would be.

He also advised using services that offer end-to-end encryption, or alternatively encrypting your data inside your own organisation before transferring it to the Cloud.

Further reading:
http://www2.itif.org/2013-cloud-computing-costs.pdf
http://www.tagesanzeiger.ch/wissen/technik/Jetzt-bauen-die-Europaeer-eigene-Clouds/story/20482995?track
http://www.itmittelstand.de/home/a/rechtliche-grundlagen-fuer-die-cloud.html

Christmas trade on the Internet more profitable than ever - and so is card and identity theft fraud

The US "Target" store-chain - with its 1900 or so outlets is one of the largest chains in the country - has just fallen victim to a massive cyber attack. For two weeks from the end of November onwards, attackers were able to capture some 70 million customer credit and debit card datasets from the Target database.

The IT specialist and blogger Brian Krebs finally uncovered this incident: on behalf of a bank, he was investigating black market for payment cards and discovered the stolen Target data records. Card copies were offered in batches for up to 100 US-Dollars each. The heise.de IT news portal reports: also contained in these batches were card owners' postcodes - very handy for fraudsters "because banks' security mechanisms do not strike as quickly for purchases made around the area where the card owner lives". The Reuters news agency writes that the cards' encrypted PINs were also stolen, with security experts warning that the attackers now have everything required to duplicate these cards and withdraw money. At least four other retailers are said to have also been hit.

Times where retail sales are high are particularly ideal for such attacks, says Paul Kocher, a cryptography expert, because with customers flocking to buy in droves, fraud-warning systems are no longer able to distinguish between legal and fraudulent transactions.

Record online sales thanks to tablets and smartphones

Given their growing turnovers, retailers in the US do not really have to worry too much either though. As per Adobe's "Digital Index 2013", twice as many customers were doing their Christmas shopping on their mobile devices nowadays than the previous year: During the two most busy shopping days of Thanksgiving and Black Friday, a quarter of all purchases were made by mobile buyers using a tablet (15.6 per cent) or Smartphone (8.6 per cent). iOS device users in the USA therefore managed to spend a total 550 million US Dollars in purchase value - 417 million of which was generated on iPads, 126 million on iPhones and 42 million on Android tablets. These figures are based on an analysis of some 400 million visits to websites of around 2000 US retailers using Adobe's "Marketing Cloud" tool.

Retailers were prepared for this mobile shopping offensive though, promoting mobile access by offering free Wi-Fi in their branches, giving their online shops a fresh new look, and providing enhanced app offers and screen-optimised web pages (key word: Responsive Design) .

Further reading:
http://www.reuters.com/article/2013/12/25/us-target-databreach-idUSBRE9BN0L220131225
http://pressroom.target.com/news/target-confirms-unauthorized-access-to-

payment-card-data-in-u-s-stores
http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/
http://www.heise.de/newsticker/meldung/Target-Kartenraubzug-Weihnachten-fuer-Kriminelle-2071721.html
http://www.enhancedonlinenews.com/news/eon/20131129005409/en/Adobe/Thanksgiving/Black-Friday

News from the mobile payment market: Paypal is pinning its hopes on payment by verbal confirmation

There is currently tough competition between payment providers, retailers, credit card and mobile suppliers in search of a breakthrough in mobile payment methods. “Paypal” is currently attempting to position itself as a true problem solver. Company boss David Marcus promised at the “Le Web” Internet conference, from 2014 onwards: “Never queue again” - to everyone downloading Paypal's “Beacon” mobile-app. Retailers on the other hand would profit from increased customer loyalty. The “Beacon” or “sender/receiver” technology works as follows: once a customer enters a shop, their mobile will receive signals from radio modules set up by the retailers. Then the potential customer’s mobile phone will transmit their photograph, shopping history or current location to the retailer who can now proceed to provide individually tailored services. All that the customer eventually needs to do to pay, is a verbal confirmation - for instance upon leaving the store, as shown in their promo clip.

Anonymity was yesterday

Paypal president David Marcus considers the Beacon technology to be an important building block in the process of changing the retail sector and providing a whole new shopping experience. Users will be able to define those stores where they would like to pay automatically and those that will require specific authorisation. This would also fulfil data protection requirements. However, Security experts did not take such a rosy view of this Beacon technology: they believe that convenience will once again be achieved at the expense of data protection, not to mention a whole string of issues with regard to abuse and security which will need to be clarified. This starts with the question: “what will happen if a mobile is stolen?”, and ends with the issue of: “what

will be done with all the stored customer data?"

By the way, iBeacon is the name of a similar indoor navigation system Apple integrated into their latest mobile operating system iOS7 and has been testing in 250 US stores since December: using Bluetooth technology, customers are referred to special offers inside a store or steered towards products of interest to them.

According to Marcus, Beacon is already being tested all over Europe. Paypal has also recently started trialling payment by face recognition in Great Britain.

An app for every supermarket

Industry experts do not believe that the various technologies currently buzzing around consumers' ears will make a breakthrough this year: insufficient standards, little acceptance and too many isolated applications make it difficult for customers to actually recognise any added value. In Germany alone, there are some 30 different payment providers all doing their own (app) thing. You can hardly expect buyers to download tons of different apps onto their mobile. In this country, Swisscom has been tinkering with the "Tapit" app for cashless payment in Co-op stores, which is scheduled to launch in 2014. Meanwhile, their competitor Migros prefers throwing their lot in with cashless payment using nearfield communication technology.

Further reading:
http://youtu.be/g8h_i8qv1FY
http://techcrunch.com/2014/01/13/paypal-debuts-a-simpler-native-checkout-experience-for-merchants-and-expand-beacon-internationally/
http://www.spiegel.de/netzwelt/apps/beacon-paypal-kuendigt-gegenstueck-zu-apples-indoor-navigation-an-a-938220.html
http://t3n.de/news/drops-noch-gelutscht-uns-2014-520509/

30th Chaos Computer Club meeting totally under Snowden's spell

There is currently an atmosphere of departure and excitement and a combative spirit prevalent amongst Internet activists and hackers all over the world. There was no

way you could ignore this fact during the 30th congress of the Chaos Computer Club (CCC) in Hamburg. Over 8000 visitors - more than ever before - had travelled there. They spent four days discussing on how to proceed at all with the freedom on the Internet, after all the massive spying disclosures. Following the conference, one thing was clear: it won't be all that easy.

Right at the beginning, there were standing ovations for the keynote speaker Glenn Greenwald, appealing to the masses for digital liberation via a video conferencing connection. Greenwald was a reporter working for the British "Guardian" newspaper, and as a confidant of Edward Snowden, he is one of many who have helped the public realise the extent of the spying revelations. "The NSA wants to eliminate privacy on a global scale." This is why everybody would have to campaign to protect privacy.

As a side note, Greenwald admits, he almost missed the "Snowden story", because the PGP technology used by Edward Snowden to encrypt all his e-mails was too complicated for him. In the meantime, he had learned how to encrypt e-mails and data - a skill that has now become commonplace and important for all Internet users. Many people were by now aware of how important securing Internet communications is: "If any reporters or activists contact me today, they should be embarrassed if they don't encrypt their mails first."

While Greenwald implored all hackers to not make themselves available to work for any secret services, interestingly enough Wikileaks founder Julian Assange did exactly the opposite: also joining the conference via a video conference from the Ecuadorian embassy in London. Assange specifically appealed to system administrators to exploit their power and expert knowledge of networks. "Join the CIA!" These so-called "Sysadmins" should infiltrate secret services and corporations, collect information and then publicise it. "We are the last free generation."

By the end of the conference, one question preoccupied Greenwald, and Internet activists all over the world: "Is the Internet an instrument of liberation and democracy, or is it the worst instrument of oppression of all times?".

Further reading:
http://youtu.be/qqk4ItPjU5g
http://www.golem.de/news/glenn-greenwald-sie-muessen-angst-vor-uns-bekommen-1312-103605.html

http://www.faz.net/aktuell/feuilleton/debatten/abschied-von-der-utopie-die-digitale-kraenkung-des-menschen-12747258.html
http://www.faz.net/aktuell/feuilleton/chaos-communication-congress-ein-tor-zur-anonymitaet-12729573.html

Facebook never misses a thing. Even those things users deliberately wish to leave unpublished

To find out if and how often Facebook users type a comment or status update but then delete it again at the last second, the largest social network in the world has launched a study into "self-censorship on Facebook". To this end, data analyst Adam Kramer and postgraduate Sauvik Das have had a closer look at the meta data of unpublished entries of some four million English-speaking users. The result: 71 per cent of all Facebook users composed at least one entry over a period of 17 days that they then deleted again at the last second. With 51 per cent, this was a status update already typed out on their own profile page, with 44 per cent a comment on a friend's page. But why is Facebook interested in this at all? Because the network loses value due to content not shared, the analysts say. As the social network lives off the revelations of its users, it wants to reduce their self-censorship levels.

Something other companies, such as Google, store such data; in their case to "rescue" user entries in case of system failure. While Facebook does it out of pure self-interest, critics grumble. In addition, it says nowhere in their data protection terms that Facebook also stores data which users quite deliberately have chosen not to publish. It only says that they collect data if one "looks at things or interact in any other way." Kramer and Das indicate that Facebook even wants to take a step further: their next study is meant to research the contents of posts deleted before publication. Mark Zuckerberg wants to find out exactly what is being deleted and why.

Facebook has an estimated 1.19 billion users worldwide; in our country, there are some 3.3 million - an 8 per cent increase compared to 2012. However, the under-20s are still increasingly losing interest in Facebook.

Further reading:

http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350

http://www.spiegel.de/netzwelt/web/was-ein-forscher-mit-facebooks-datenschatz-anstellt-a-934893.html

http://www.pctipp.ch/news/web-dienste/artikel/schweizer-facebook-nutzer-werden-aelter-70315/

The Clipboard: Interesting presentations, articles and videos

The 30th Chaos Communication Congress (30C3) took place in Hamburg from the 27th to the 30th of December 2013. 140 Videos of talks and presentations from the 30C3 can be found on the new CCC-TV portal:

http://media.ccc.de/browse/congress/2013/index.html

Another security conference Hack-in-the-Box (HITB) as released a magazine in addition to there slides. You might find it an interesting read:

http://magazine.hackinthebox.org/hitb-magazine.html

Glenn Wilkinson held an interesting presentation on mobile device tracking at the SECURE 2013 conference in Poland; “The Machines that betrayed their Masters”:

http://www.youtube.com/watch?v=03iEaKPRb9A

SWITCH, Security, P.O. Box, CH-8021 Zürich, +41 44 268 15 40, cert@switch.ch, www.switch.ch/all/cert