SWITCHcert Security Report

March 2014

I. Between Ignorance and Panic – Facebook Buys WhatsApp

In February, Facebook founder Mark Zuckerberg paid a cool 19 billion USD for the messaging service WhatsApp and its developer team – a big price for the social network's biggest competitor in the messaging game.

The future of Facebook-owned WhatsApp is murky right now. Blogger and IT journalist Michael Seeman thinks the deal is more about the future of Facebook than WhatsApp itself – he even considers it possible that Facebook might just shut it down.

The WhatsApp founders were never really interested in advertising or user data. The service was paid for by a yearly fee of 1$. Zuckerberg promises this business model will remain intact, despite skepticism from, ironically, Facebook users. «90 out of 100 users in my WhatsApp list share their lives on Facebook», remarked a user of the Futurezone internet forum, later pointing out that «Facebook already has the data anyway. So who cares?»

Data Protection vs. Laziness

Data privacy experts care very much about the multi-billion-dollar deal. Facebook and WhatsApp have been under criticism for years for their lax data protection standards. The Independent Data Protection Center of Schleswig-Holstein for example claims both services give their operators access to both communications meta-data and content.

Zürich’s data protection officer Bruno Baeriswyl knows why so few Swiss care about the mega-deal. «For starters, very few people know what profiles they have and what happens to them. Additionally, you barely notice the negative effects of excessive data collection in everyday life so far.»

However, says Baeriswyl, there are companies that offer comparable services to WhatsApp with improved security and encryption. Long-term, Baeriswyl expects companies with higher security standards to have a better chance at succeeding in a crowded market. But in the end, each user has to decide for himself whether he goes for the easy or the safe option. In the words of Twitter user and Open Source activist Dennis Ploeger: «The success of a WhatsApp alternative won’t be decided by the best encryption protocol, but by whether Chantal from the other class has it.»

Swedish Police Stumbles Over WhatsApp Group

According to a recent Der Spiegel article, even police forces are now using WhatsApp – albeit with difficulties. Due to a mistyped phone number, a Swedish police officer accidentally invited IT consultant Jan Svärdhagen into an investigations group chat. As Svärdhagen told IT magazine ComputerSweden, he was allowed access to information about ongoing investigations, photos of suspects and excerpts from police files. The officer in question apologized for the mistake, pointing out that the force relied on WhatsApp for quick data exchange because the Blackberries intended for this purpose were never distributed.

Find out more:

http://www.br.de/presse/inhalt/pressemitteilungen/radiowelt-michael-hange-100.html

http://www.srf.ch/wissen/digital/facebook-und-whatsapp-damit-die-sonne-im-reich-niemals-untergeht

http://futurezone.at/produkte/whatsapp-alternative-threema-verdreifacht-user-anzahl/52.561.981

http://www.shz.de/nachrichten/newsticker-nord/datenschuetzer-weichert-warnt-vor-kombination-facebookwhatsapp-id5791121.html

http://mspr0.de/?p=3974

http://www.handelsblatt.com/unternehmen/it-medien/instant-messenger-whatsapp-alternative-threemawaechst-rasant/9519942.html

http://de.statista.com/infografik/1931/anzahl-der-aktiven-nutzer-von-whatsapp/

http://www.20min.ch/schweiz/news/story/13345327

http://computersweden.idg.se/2.2683/1.547026/polisens-chatt-miss–hemlig-spaninfo-pa-drift-i-%20WhatsApp

II. Google, Apple and Co. In Future Cars

The increasing usage of powerful computers and fast internet connections in modern cars is fuelling a new kind of digital showdown – the race for the domination over the automobile operating system. At the Geneva Automobile Salon, the trends were evident – large touch screens, internet on the go and smart phone connectivity. The most modern vehicles also feature 360° camera coverage, accessible via in-car monitors.

«More intelligent, safer, more fun»

Mobile device giant Apple is currently partnering with Ferrari, Mercedes and Volvo to develop CarPlay, a «more intelligent, safer and more fun way of using an iPhone in a car». The goal is to embed Apple's iOS operating system deep within the car's command console, with voice-activated assistant Siri and the Apple touch screen playing especially important roles. Google's «Open Automotive Alliance» on the other hand is joining forces with Audi, General Motors, Honda and Hyundai. Here, too, the goal is to integrate a mobile OS (Android) into automobiles. Audi head of development, Prof. Ulrich Hackenberg, depicts the future: «The vehicle will be closely networked, will be fed with information on current traffic status, will communicate with other vehicles and infrastructure. And the vehicles will be able to make decisions – to offer them to the driver or take action themselves.» Networked vehicles will work together in moments of danger – for example, to alert each other of a non-networked vehicle approaching.

A partnership between BMW and software company SAP aims to bring the SAP HANA Cloud Platform to automobiles, allowing information provided by third parties to be provided in-car depending on route and location (Location Based Services). Two prototypes have been developed, one helping with finding parking spaces, the other providing route-based advertising and coupons to the driver via his smart phone.

Still looking for a potential partner is the team behind smart phone app «Smart Trailer Parking». The parking helper for towing vehicles connects directly to the vehicle's steering and drive train and theoretically even allows drivers to leave their vehicle and control the parking procedure from outside via smart phone.

The potential behind networked vehicles was recently demonstrated by Volvo at a pilot project at the Mobile World Congress: automobile owners were able to use their vehicles as delivery locations for online orders. Industry estimates say missed deliveries cost over one billion Euros a year. Klas Bendrik, Group Chief Information

Officer of Volvo Car Group, says: «It’s all about finding solutions that are intuitive, easy to use and offer our customers advantages in everyday life.»

The Downside of Laziness behind the Wheel

With all due respect for the advantages of such services, users should be wary of the cold hard truth behind these projects, said journalist Daniel Hüfner to technology news portal t3. So far, the car is one of the last refuges from the omnipresent World Wide Web. «In our cars, we don’t Google, order on Amazon or check in on Foursquare.» A billion people operate automobiles each day on Earth – a massive untapped market that hasn’t gone unnoticed in the advertising and technology industries.

Networking of traffic and engine data, say data privacy activists, could make cars just as susceptible to hacking attacks as smart phones. There are also legal and insurance concerns- «Even the new VW Passat determines when its driver needs a coffee break, and prompts him with a dash board warning light. If someone ignores the suggestion, keeps driving and has an accident, his innocence might be questioned if his vehicle data is downloaded. Movement profiles, aggressive driving behavior – lots of information is silently collected by cars and could be used against their drivers» writes Niklas Maag in the Frankfurter Allgemeine Zeitung.

Buying Used?

Roger Löhrer, head mobility expert for TCS, told Swiss Radio and Television: «Basically, all data can be stored. Modern data could be used to infer driving conditions and behavior.» Airbag control systems, for example, could provide feedback on accidents. Openings and closing of doors are also logged with date and time. Currently, this data is only stored locally and could only be retrieved by a licensed dealer. If this should change – say, if insurance companies downloaded the data via internet – drivers would have to opt for older car models. Swiss data privacy expert Hanspeter Thür insists: «It must be transparent, which data is being collected, and the vehicle’s owner must know what happens with it.» But current EU plans might make this difficult – starting in 2015, new cars must be equipped with the emergency call system eCall. The SIM card-based device automatically contacts emergency services in case of an accident – the driver has no control over what data is transmitted.

Find out more:

http://futurezone.at/digital-life/audi-das-auto-der-zukunft-entscheidet-selbst/51.788.826

http://www.newsxs.com/de/go/4748896/2845/

http://t3n.de/news/smartes-autofahren-startups-526202/

http://www.multivu.com/mnr/65010-volvo-pilots-roam-delivery-service

http://www.faz.net/aktuell/feuilleton/vernetztes-fahren-das-geschaeft-mit-den-intimen-daten-aus-dem-auto-12773929.html#null

http://www.srf.ch/konsum/themen/umwelt-und-verkehr/der-glaeserne-fahrer-datensammelwahn-im-auto

III. The Corporate War on Ad Blockers

A yellow bar, appearing similar to a browser warning, has been gracing Gmx and Web.de for the past month, to the chagrin of users and data privacy advocates alike. Clicking on the bar leads users to browsersicherheit.info, a site that looks deceptively similar to Google Chrome's settings page. Here, the user is informed that his system is infected by malware and that it should be scanned immediately.

As it turned out, the scareware popup was really intended to scare users to remove ad blockers installed on their computers. Browsersicherheit.info, a website operated by United Internet, provides users with a list of «dangerous malware», mainly ad blockers for Chrome, Firefox, Safari and others.

Internet companies often rely on advertising income to support their operations. Ad blockers like Ghostery or Adblock Plus (50 million users worldwide) pose a serious threat to ad-based companies. In early February, the first announcements regarding United Internet's moves against ad blockers were made. The organization defends its aggressive methods by pointing out they're really contributing to online security – after all, third party software is often the first venue of attack for real malware. «Not all users realize what add-ons they're installing and what risks they're taking by modifying websites browser-side», said Jörg Fries-Lammers, spokesman for 1&1 Internet AG, which also belongs to United Internet.

Of course, the teams behind ad blocking add-ons aren't monks either. Blogger Sascha Pellenberger claims that market leader Adblock Plus reportedly received over 30 million USD from Amazon, Google, Ebay and Yahoo to un-filter their respective ads. Pallenberger, who has experience uncovering murky connections between advertisers and ad blockers (see Security Report June 2013), contends that a mafia-like structure is behind Adblock Plus, powered by high-profile advertisers.

Find out more:

http://www.nzz.ch/aktuell/digital/gmx-webde-united-internet-11-adblocker-werbung-warnung-browser-1.18252530 http://labs.bromium.com/2014/02/21/the-wild-wild-web-youtube-ads-serving-malware/

http://www.mobilegeeks.de/adblock-plus-zahltag-30-mio-von-amazon-ebay-google-und-yahoo/

http://blogs.wsj.de/wsj-tech/2014/02/27/gmx-und-web-de-werbeblocker/

IV. The Fall of Bitcoin Exchange Mt Gox

If rumors are to be believed, a numbers mix-up led to the crash of Bitcoin trading platform Mt Gox. 850,000 Bitcoins are presumed lost, according to CEO Mark Karpeles, leaving the platform roughly 57 million CHF in debt to its users.

A web document claims the crash was caused by an error in Mt Gox' homebrew transaction system. Since January, more and more Bitcoin transactions got hung up in Mt Gox' system, forcing the operators to suspend services three weeks later. Financial experts consider the untimely end a just punishment for the string of security issues surrounding Mt Gox. Questionable security standards implemented by the Japanese company had threatened the Bitcoin exchange rate as early as 2011, caused multiple panic sells and crashed global Bitcoin trading. As late as August 2013, 60% of all worldwide Bitcoin transactions were run through Mt Gox, dropping to 20% by early 2014.

Apart from Mt Gox' issues, Bitcoin trading has seen a meteoric rise. Bitcoin was developed in 2009 as a crypto currency alternative. Coins are mined by users as part of complex algorithms and are primarily used for online transactions. Bitcoin trading enjoys zero regulatory or national oversight. Online exchanges provide dynamic exchange rates for real-world currencies.

However, Bitcoin exchanges are not required to carry deposit insurance – which means the majority of Mt Gox' users will never see their money again. According to American media, Karpeles may face a wave of civil lawsuits.

It is currently unclear how the demise of Mt Gox will affect Bitcoin trading as a whole. Financial authorities and politicians consider the black-market nature of Bitcoin a threat and are quick to deride it as «overvalued play money». Most real-world banks steadfastly boycott the acceptance of Bitcoin as an official currency, including the European Banking Authority and the Swiss National Bank. According to Neue Zürcher Zeitung, «digital currencies aren't safe anyway, as wallets can be hacked, passwords can be stolen or lost.» Luzius Meisser, president of the Bitcoin Association Switzerland, disagrees: «This debacle wouldn't have happened if we had a free market.»

According to the Bitcoin Foundation, the operators of Mt Gox are to blame for the issues surrounding their platform. «The regulator processes weren't followed. Users should have kept their coins on their laptops or smart phones», said foundation director Jon Matonis. Japan's government also should have taken influence. Recommended alternatives to Mt Gox are bitcoin.de, bitstamp.net, kraken.com or localbitcoins.com.

Find out more:

http://www.wired.com/wiredenterprise/2014/02/bitcoins-mt-gox-implodes/

http://online.wsj.com/news/article_email/SB10001424052702303801304579410010379087576-lMyQjAxMTA0MDIwNzEyNDcyWj

http://de.scribd.com/doc/209050732/MtGox-Situation-Crisis-Strategy-Draft

http://futurezone.at/digital-life/chef-von-bitcoin-boerse-mt-gox-dementiert-flucht/53.476.152

http://www.heise.de/tr/blog/artikel/Warum-Bitcoin-ruhig-sterben-darf-2125380.html

http://www.nzz.ch/finanzen/devisen-und-rohstoffe/devisen/bitcoins-disqualifizieren-sich-als-waehrung-1.18207689

The Clipboard: Interesting Presentations, Articles and Videos

Poul-Henning Kamp, a well-known FreeBSD kernel developer and tool author, presented his version of a fictional NSA operation, code-named ORCHESTRA, at FOSDEM 2014 in Brussels, and later delivered a status update on the intelligence gathering program in front of a fictional audience at NATO Headquarters:

https://fosdem.org/2014/schedule/event/nsa_operation_orchestra/

http://ftp.osuosl.org/pub/fosdem/2014/Janson/Sunday/NSA_operation_ORCHESTRA_Annual_Status_Report.webm

Could images of picturesque sunsets be emptying your bank accounts? Jerome Segura, Senior Security Researcher at Malwarebytes, explains how Zeus and Zbot Trojans exploit steganography in images:

http://blog.malwarebytes.org/security-threat/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/

«La Quadrature du Net« is a Non-Profit Organization dedicated to internet rights and freedoms. Since 2013, the group has collated and published all available info on NSA surveillance programs. The «NSA Observer« database is freely accessible and currently lists 539 separate NSA programs, attack vectors and divisions:

https://nsa-observer.laquadrature.net/

The SWITCHcert Security Report - Original German version by Katja Locker and Frank Herberg - released monthly.