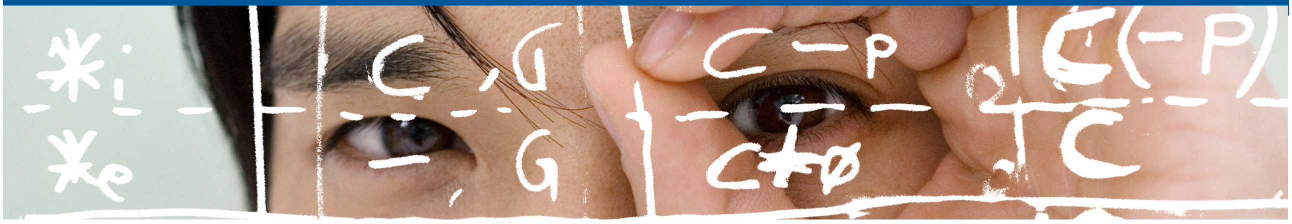
# SWITCHcert Security Report

February 2014



SWITCH
Serving Swiss Universities

## E-mail security service backfires for German government office

In the course of a widespread investigation of criminal botnets, German scientists and security services traced roughly 16 million compromised user names and passwords for various e-mail services. In an effort to act quickly on behalf of the affected users, the data was shared with the German Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik BSI). However, the government agency dragged its feet, eventually putting together an amateur effort that resulted in a PR disaster.

In January, the BSI recommended all affected users change their passwords. On a specially built website, users could check whether their accounts belonged to the 16 million compromised ones or not. The BSI also warned that if affected users didn't change their login information, their accounts might be subject to identity theft, account hijacking, eavesdropping on private and business communications or online fraud.

### Lacklustre communication

Scared by the government warnings, thousands of internet users wanted to check whether their accounts were compromised. However, most never found out, as the BSI website buckled under the onslaught of concerned visitors. BSI's recommendation to simply try a few times probably didn't help. However, the backlash reached a new level when Der Spiegel reported in late January that the BSI had known about the security issues since August 2013, when it informed roughly 600 German government officials about their compromised accounts. BSI president Michael Hange claimed that the public wasn't informed until months later because the office wanted to be "extremely well prepared" for the reactions to the news. But as net journalist Richard Gutjahr wrote on his blog, the BSI's website was so extremely well prepared it went down as soon as two separate visitors tried to check the database for their accounts.

Furthermore, BSI's mailing system only contacted users with a compromised account. Security experts say that simply not receiving an e-mail shouldn't be considered an all-clear signal. The message itself was also a textbook example of an untrustworthy e-mail, according to IT forum Heise Security, containing personal addressing, but no imprint. Finally, the BSI website features numerous security flaws vulnerable to attackers and copycats. BSI claims the site has seen roughly 12.5 million requests since late January, with 884,000 positive replies.

Find out more:
https://www.sicherheitstest.bsi.de/
http://www.br.de/presse/inhalt/pressemitteilungen/radiowelt-michael-hange-100.html
http://www.spiegel.de/netzwelt/web/online-konten-geknackt-mail-adressen-check-beim-bsi-in-der-kritik-a-944739.html
http://gutjahr.biz/2014/01/ich-glaub-es-hackt/

## Media alarmism over worldwide ATM failure

In April of this year, Microsoft will cease support for its hugely popular Windows XP operating system, with widespread consequences. However, one such consequence was recently blown out of proportion after a Bloomberg Businessweek interview with Robert Johnston, manager of Automatic Teller Machine (ATM) producer National Cash Register (NCR). Johnston warned that 95% of all ATMs on the planet still run on Windows XP, with predictable results – a global panic about ATM security.

Until April 2014, roughly 15% of all American ATMs would be converted to Windows 7, Johnston estimated. However this should have been taken care of for all 3 million ATMs worldwide long ago. Since most ATMs are older than Windows XP itself, the machines have to be completely replaced to cope with modern operating systems. XP-based machines are already six times more vulnerable to malware than computers running Windows 8. Aravinda Korala of Korala Associates Limited, a maker of ATM software, says: the situation is a bit different for ATMs, which experience much slower technical progress than PCs.

### Swiss bank customers on the safe side

The German banking industry isn't concerned about the ATM panic either. Since the machines aren't connected to the internet, the operating system isn't very relevant, said a spokeswoman to IT news portal Golem.de. Experts claim most German ATMs are still running Windows XP or 2000. In Switzerland, the situation is a bit better, with most ATMs running an embedded version of Windows XP, which will be supported by Microsoft until 2016. Newer NCR machines are already being delivered with Windows 7. Constanze Ehrt, PR manager for NCR, says the conversion from Windows XP to Windows 7 is up to the banks and operators. Machines built by American manufacturer Diebold are apparently already fully upgraded, according to Inside-IT research.

However, there are also methods of manipulating offline ATMs, as demonstrated by two researchers at a recent Chaos Computer Club meeting. After cutting a hole in the casing of the machine and accessing a free USB port (intended for a printer or webcam), a pre-loaded USB stick allowed the team to inject their own code into the machine, exploiting a Windows XP security flaw to secure control over money issuance. The banks behind the hacked ATMs only noticed after the machines lost money for multiple months.

Find out more:

http://blogs.technet.com/b/mmpc/archive/2014/01/15/microsoft-antimalware-support-for-windows-xp.aspx

http://www.inside-it.ch/articles/35103

http://youtu.be/0c08EYv4N5A

http://www.businessweek.com/articles/2014-01-16/atms-face-deadline-to-upgrade-from-windows-xp

http://www.golem.de/news/ncr-weltweit-95-prozent-aller-geldautomaten-mit-windows-xp-1401-103997.html

http://www.heise.de/ct/heft/2014-3-Signaturen-fuer-Virenscanner-unter-Windows-XP-nach-April-2014-2085393.html

http://www.20min.ch/digital/news/story/Windows-XP--Ein-Risiko-fuer-Geldautomaten--18642174

## Google Glass to ban facial recognition

Hands-free, eyes-free surfing was Google's big selling point when Glass was introduced in April 2012. Since then, not a lot has happened. The market introduction has been postponed multiple times, and only selected individuals have been able to test the device so far. Media and enthusiasts alike speculate that the real problem is actual application areas. Google seems to agree – in April 2013, the company released a Glass SDK so app developers could come up with creative uses for the innovative piece of hardware.

The resulting collection of ideas heavily featured facial recognition, even though Google had, after pressure from data privacy groups, already stated that facial recognition would not be allowed on Glass. Kay Overbeck, Google's spokesperson for Northern Europe, said as much in an interview with Die Zeit: "Fundamentally, we will not tolerate facial recognition apps on Google Glass. They will not be accepted as official 'Glassware'."

One such app, called NameTag, was created by FacialNetwork and would allow Glass wearers to immediately call up background information on people they're facing. According to the team behind the app, the quality of information would depend mostly on available cooperation partners, such as dating sites, social networks or even national crime registry databases. Developer Kevin Alan Tussy considers

NameTag the ultimate way to “better understand people”. The app will be published shortly, though Tussy won’t say how people can avoid being listed in the NameTag databases.

## Wearable computing ready for everyday use

American start-up Lambda Labs was inspired by Google Glass to create the Lambda Hat, an Android-based baseball cap that records its surroundings. Similar wearable computing products for everyday use have received an enormous boost from Google Glass’ hype. Juniper Networks expects worldwide sales of 15 million wearable computing devices in 2014, increasing to 70 million by 2017. While Google may be restrictive on the allowed apps, experts claim successful hacking of the device is inevitable – at which point Google will lose control over what apps users load onto their Glasses.

## Google Glass with corrective lenses

One interesting step Google has taken was to offer Glass with corrective lenses, which has gotten some users into hot water. One Glass wearer in Ohio was interrogated by police for three hours after wearing his Glasses at a local cinema. In San Diego, car driver Cecilia Abadie had to present herself before a judge after driving with her Glasses on. Since it could not be proven that the device was switched on at the time, she was cleared of all charges. In other US states, data glasses may be banned completely, a step already taken in Great Britain in August 2013. However, Google is already working on Smart Contact Lenses that will integrate Glass circuitry into contact lenses.

Google Glass is a gesture- and language-controlled set of glasses. The glasses connect to a smart phone via Bluetooth and can display information in the top right corner of the wearer’s field of view, such as navigation information, e-mails or appointment details. The device can also handle videoconferences, phone calls and taking photos and videos.

Find out more:
http://www.heise.de/tr/artikel/OK-Glass-find-a-Killer-App-2076138.html
http://www.androidnext.de/news/nametag-google-glass/
http://www.dispatch.com/content/stories/local/2014/01/21/google-glass-at-easton-theater.html

http://www.latimes.com/local/la-me-google-glass-20140117,0,5347315.story

http://www.zeit.de/digital/mobil/2014-02/google-glass-gesichtserkennung-kommt

http://www.juniperresearch.com/viewpressrelease.php?pr=347

http://www.computerwoche.de/a/google-glass-bereitet-den-weg,1237959

## NSA update: critics lining up

For the casual citizen, it's becoming quite hard to keep track of what exactly the American National Security Agency and British Government Communication Headquarters know about us. According to the discoveries of the past few months, their investigative capabilities cover just about every aspect of our daily life:

- Monetary transactions
- Personal and business computers
- Location and communication of cell phones
- Live tracking of internet traffic
- Corporate IT networks
- Bot nets
- Back doors in standardized software and hardware, such as routers, firewalls and hard drives

### Charges filed against British, German governments

Despite the remaining widespread ignorance about government spying on citizens, civil rights groups, politicians and net activists are beginning to organize a protest movement. At the European High Court for Human Rights in Strasbourg, the topic is a hot one: both British civil rights groups and the German Chaos Computer Club (CCC) have recently filed charges against their respective governments. The CCC hopes the court will assess whether the recently published internet activities of British security services violate basic human rights. Apparently the court has already demanded that British Prime Minister James Cameron make a public statement about the hundreds of thousands of cases of unfounded espionage of European citizens. The filers are hoping for new regulations curbing government wiretapping and mass investigations. Politicians and security services have always claimed they operated within the confines of law – a statement that the High Court will now investigate.

## Internet sabotage

In the USA, a leading group of 50 cryptography and security experts have signed an open letter condemning the baseless collection, storage and analysis of unheard-of amounts of user data conducted by the NSA. By designing back doors, sabotaging security standards and eavesdropping on communication between commercial data centres, the NSA may be facilitating digital crime. The experts hope the government will put an end to the development of mass wiretapping programs and the undermining of security standards. New technologies should be developed to improve online privacy and security and support technical innovation and free trade.

## No water, no data centre

In a slightly less common effort to put an end to government investigations, civil rights groups and politicians are trying to shut down water pipes leading to the NSA’s new computing centre in Utah. The website of the self-titled “protest coalition” claims the data centre requires 6.5 million litres of water each day just for cooling – making the water mains the Achilles heel of the NSA’s IT infrastructure.

## Government-corporate espionage

In a recent interview with German TV station NDR, whistleblower Edward Snowden reaffirmed previous statements that the NSA conducts corporate espionage: “If Siemens has information that serve the national interests of the USA, but don’t have anything to do with national security, they’ll still take that information.”

In January, president Obama promised more transparency and control for the NSA. American internet companies are now allowed to publish how often American government agencies request data from them, not that the generic information is very useful to the public.

Find out more:
http://www.ccc.de/de/updates/2014/gchq-egmr
http://www.nsa.gov/public_info/press_room/2014/civil_liberties_privacy_officer.shtml
http://online.wsj.com/news/article_email/SB10001424052702303519404579353173552039730-lMyQjAxMTA0MDMwMDEzNDAyWj

http://www.presseportal.de/pm/69086/2648795/-snowden-exklusiv-der-wortlaut-des-interviews-von-ndr-autor-hubert-seipel
http://www.tagesanzeiger.ch/ausland/amerika/Vizeadmiral-Michael-Rogers-soll-die-NSA-umkrempeln/story/23310173
http://offnow.org
http://www.nzz.ch/aktuell/digital/wie-die-nsa-iphones-attackierte-1.18213327

## The Clipboard: Interesting Presentations, Articles and Videos

Security services provider Kaspersky has discovered a cross-platform Java bot that exploits a dangerous security flaw in Java. The bot works Windows, Mac and Linux:

https://www.securelist.com/en/blog/8174/A_cross_platform_java_bot

Net security experts Arbornetworks have published their yearly security report. Important topics for this year: Bring Your Own Device and mobile networks, attacks on corporate IT infrastructure and IPv6.

http://www.arbornetworks.com/corporate/blog/5112-the-9th-annual-wisr-the-wisr-authors-weigh-in

Blogger Krebs-on-Security highlights a firmware bug in IP cameras built by Chinese camera giant Foscam, allowing anyone with an internet connection to access the cameras' streams:

http://krebsonsecurity.com/2014/01/bug-exposes-ip-cameras-baby-monitors/

The SWITCHcert Security Report; Original German version by Katja Locker and Frank Herberg in collaboration with SWITCH-CERT; released monthly.