SWITCHcert Security Report

November 2015

SWITCH

I. No safe harbour in the Land of the Free – EU Court of Justice restricts data transfer to US

The judgment handed down by the EU Court of Justice in Luxembourg on 6 October 2015 caused ructions. The Court declared the Safe Harbor Agreement between the EU and the US on the transfer of personal data to be invalid, specifically because the judges believed that the US does not offer a «safe harbour» for EU citizens' personal data. Under Safe Harbor, over 4,400 US firms undertook to ensure adequate protection for European customers' data. However, these firms are required to supply data to the authorities on an unrestricted basis if this is deemed necessary for national security, the public interest or enforcing US law. The agreement does not guarantee EU citizens access to their data transferred to the US or the right to have them deleted, as a result of which the Court agreed with EU Advocate General Yves Bot's opinion that the US does not afford adequate data protection. Current EU law, meanwhile, states that personal data may only be transferred to third countries if such protection is assured. The judges in Luxembourg also bemoaned the fact that a rule generally allowing the authorities to access the content of electronic communications compromises the essence of the fundamental right to privacy enshrined in EU law.

Austrian lawyer Max Schrems, who was still a student at the time, initially lodged a complaint only against the transfer of his data from Facebook's servers in Ireland to those in the US following the publication of National Security Agency documents by Edward Snowden. Ireland's Data Protection Commissioner refused to take up the case, citing Safe Harbor. Following the Luxembourg judgment, current Irish Data Protection Commissioner Helen Dixon said that the complaint would now be looked into with due care and attention. Facebook has offered to cooperate fully.

Representatives of the US proved to be less receptive to the EU, accusing Bot and Schrems of making false assumptions because the NSA's PRISM surveillance scheme is legally approved and «subject to accordingly rigorous controls». Indeed, it may be feared (from the US point of view) that the judgment will unleash a flood of individual complaints against Internet firms that store their customers' personal data in the US. Beside the «AGFA» heavyweights (Apple, Google, Facebook and Amazon), this covers more than 5,000 companies for which the end of Safe Harbor would have a severe economic impact. German business paper Handelsblatt sees it as a threat to these companies' business models, while Swiss daily NZZ spots an opportunity for providers in Switzerland: «Companies operating exclusively at the national level could gain a competitive edge thanks to the Swissness label.»

Facebook and co. may still insist that they can maintain their data transfer and storage practices because their customers agree to their data being transferred to and stored in the US when they accept the terms and conditions. However, doggedly defending this position could ultimately lead to a reassessment of the extent to which these very terms and conditions, along with other standard contractual clauses, are in fact legal. At least, this is what tagesschau.de believes. The original breath of complaint from Max Schrems may well turn into a hurricane that not only lays waste to Safe Harbor, but also calls all transatlantic data transfer into question.

Read more here:

http://www.nzz.ch/international/eu-richter-staerken-online-datenschutz-1.18625282
http://www.zeit.de/digital/2015-10/facebook-eugh-erklaert-safe-harbor-abkommen-fuer-ungueltig
http://www.zeit.de/digital/datenschutz/2015-10/safe-harbor-facebook-irland-ermittlungen
http://www.nzz.ch/digital/usa-attackieren-eugh-generalanwalt-ld.2236
http://www.handelsblatt.com/my/technik/it-internet/folgen-des-safe-harbor-urteils-attacke-auf-google-und-co/12506476.html
http://www.nzz.ch/international/wie-die-firmen-mit-dem-verschaerften-datenschutz-umgehen-1.18625546
http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=de
http://www.golem.de/news/nach-malware-infektion-apple-raeumt-den-app-store-auf-1509-116473.html
http://www.nzz.ch/sperrbildschirm-siri-ios-9-austricksen-ld.2138

II. A different kind of virus – medical equipment hackable online on a grand scale

When we talk about doctors fighting viruses, we usually think of HIV, Ebola and bird flu. However, as digitalisation and networking in medicine and the equipment it uses increase, computer viruses and Trojans are becoming more of an issue. The Register and computerworld.ch, for example, reported at the end of September about a honeypot experiment by security researchers Scott Erven and Mark Collao. Over a period of six months, they simulated a magnetic resonance tomograph and a defibrillator. They were amazed to see tens of thousands of login attempts, more than 55,000 of which were successful. Shocked by the number of attackers, they extended their investigation to the real world and discovered over 68,000 vulnerable systems at an unnamed major healthcare provider in the US from which hackers could steal patient and hospital data with relative ease. Security researcher Bill Rios used the example of an infusion pump to show that even critical life-saving systems could be manipulated online, for instance to change drug doses or make stored units of blood unusable. ISC-Cert warned about security loopholes in medical equipment back in 2013, but little appears to have been done since then. Most systems are still running Windows XP, and manufacturers are either unaware of the security risks posed by badly protected systems or simply choose to ignore them.

Read more here:

http://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed
http://www.computerworld.ch/news/security/artikel/security-albtraum-medizinische-geraete-zu-tausenden-online-hackbar-68825/
http://www.zeit.de/digital/internet/2015-04/medizintechnik-krankenhaus-it-sicherheit
http://www.heise.de/ix/meldung/Gravierende-Luecken-in-medizinischen-Geraeten-2178432.html
http://www.t-online.de/computer/sicherheit/id_75604958/wegen-windows-xp-zehntausende-medizinische-geraete-angreifbar.html

III. Viruses, scanned – free anti-virus programs almost as good as those you pay for

In contrast to the previous story, this one is all about ICT viruses, or more specifically programs designed to identify and eliminate them – virus scanners and anti-virus software. These should ideally meet three criteria: offer effective protection against viruses and other malware, slow the machines on which they run down as little as possible and be easy to use. The range on offer is rather broad and diverse. The pages linked to below can help you choose, and they allow us to draw two fundamental conclusions. Firstly, using virus scanners is worthwhile, since the one that performed best in the test filtered out 98% of all zero-day attacks and actually protected against 100% of all known malware. One free program matched this score, but at the cost of noticeably slowing down the scanned system. The paid-for test winner, on the other hand, did its job without any loss of speed. See the links below for more test results.

As an alternative, Google subsidiary VirusTotal offers a free service that searches suspicious files and URLs for viruses, Trojans, worms and other malware using all available scanners. VirusTotal comes in the form of browser extensions or a desktop or mobile app and also spots false positives (when a virus scanner mistakenly identifies a harmless program as malware).

Read more here:

http://www.n-tv.de/technik/Die-besten-Virenwaechter-fuer-Windows-7-article16054561.html
http://www.antivirus-programme-test.de/?kw=test%20virenschutz%202015&match_kw=1&campaign=1&network_type=2&network=1&ad_group=2&ad_text=5&lp_pool_id=6&gclid=CIOn_9elo8gCFUnlwgodLNIFMQ
http://www.antivirus-programme-test.de/?kw=bester%20virenscanner&match_kw=1&campaign=2&network_type=2&network=1&ad_group=14&ad_text=54&lp_pool_id=6&_$ja=cgid:1992071274%257Ctsid:30607%257Ccid:57186354%257Clid:4726158094%257Cnw:search%257Ccrid:56103698994%257Cbku:1&gclid=CKbM2LXBzsgCFUv3wgod9QkD5w
https://www.virustotal.com/de/about

IV. Let's hear it, buddy! ETH Zurich research team simplifies two-factor authentication with sound recognition

Since a password on a device makes life very easy for hackers, some sensitive online logins – e.g. for e-banking – use two-factor authentication (2FA). The user signs on using one device, generally a computer, and must then enter another code provided by a second device, which could be a dongle or a mobile phone. Only then is the user properly logged in. Most 2FA procedures work in a sort of «master-slave» mode, with the mobile phone as the slave. The reverse, in which the mobile phone acts as the master, is not usually viable. Nevertheless, 2FA procedures increase login security compared with single-password procedures on one device. Unfortunately, many users do not bother with them because a 2FA routine is apparently too laborious for them. WIRED, for example, writes: «But there is one big problem with it: it's really annoying. … For far too many people, this is just too big of a hassle, so they leave themselves open to attack.»

To make things simpler, a research team at ETH Zurich has developed a 2FA procedure called Sound-Proof that dispenses with the second code. Instead, the built-in microphones in both devices record background noise, and the recordings are compared. If the sound profiles match, the system assumes that both devices are in the same place and thus that the user is authorised to log in. Sound-Proof does not need any additional software or plugins on the master device to do this, just an app on the mobile phone. Anyone wishing to delve deeper into this story can find the technical details in the paper the team submitted to the 2015 USENIX conference (see link below).

Criticism of Sound-Proof centres on the one hand on the fact that both devices must have their microphones turned on and be able to pick up background noise. On the other hand, hackers may well be nearby and able to cheat the system if a user is logging in from somewhere public such as a university computer room or a public Wi-Fi hotspot. However, Nikolaos Karapanos, Claudio Marforio, Claudio Soriente and Srdjan Capkun, the developers of Sound-Proof, believe that this scenario is fairly unlikely.

Read more here:

http://www.heise.de/security/meldung/Leichtere-Zwei-Faktor-Authentifizierung-per-Handy-2826973.html
http://www.wired.com/2015/08/noise-around-strengthen-passwords
http://futurezone.at/science/zwei-faktor-authentifizierung-sound-statt-code/147.290.001
https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-karapanos.pdf

V. Situation critical – researchers find vulnerabilities in 87% of all Android devices

Do Android devices have a security problem, or are they one? This may seem a rather impertinent question, but it is one we have to ask after a closer look at the findings of a recently published University of Cambridge study. Using an app they developed themselves called Device Analyzer, the British researchers scanned approximately 20,000 Android mobile phones and tablets and discovered that, since 2013, at least 87% – sometimes closer to 100% – of all Android devices have been affected by one or more of 11 known critical vulnerabilities.

They also bemoan the fact that security updates are supplied too late or at much too long intervals and even then have to be installed manually by users. What is much more serious, however, is the fact that consumers, authorities and companies alike have no idea when buying Android devices which of the security patches provided by Google each manufacturer has incorporated into its version of Android. The researchers therefore set up their own website, androidvulnerabilities.org (see link below) that ranks Android manufacturers in terms of security. The website will be kept up to date on an ongoing basis. Anyone wishing to play a part in these efforts can read all about the study on the website and install the app from the Google Play Store. The team guarantees that personal data are anonymised.

Read more here:

http://www.golem.de/news/cambridge-studie-87-prozent-der-android-geraete-sollen-unsicher-sein-1510-116884.html
http://www.zdnet.de/88249099/studie-87-prozent-aller-android-geraete-haben-mindestens-eine-kritische-sicherheitsluecke
http://www.theguardian.com/commentisfree/2015/oct/18/were-all-casualties-holy-war-android-security-apple-john-naughton
http://www.theregister.co.uk/2015/10/12/android_patching_survey
http://androidvulnerabilities.org/press/2015-10-08

The SWITCHcert Security Report was written by Dieter Brecheis and Michael Fuchs.

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.