SWITCHcert Security Report

June 2015

SWITCH

I. What do tax authorities and contact sites have in common? Neither can protect customer data

Three cases of large-scale data theft have made the headlines in recent days. Hackers took rich pickings from attacks on the contact site Adult Friend Finder, the US Internal Revenue Service and the Japanese Pension Service.

According to research by security blogger Bev Robb, a hacker in Thailand stole and published the dates of birth, e-mail and postal addresses and sexual preferences of 3.9 million Adult Friend Finder users on the Tor network as an act of revenge. It remains unclear whether the hacker is also in possession of credit card details. He may have removed them and saved them «for later use» before publishing the rest of the data.

Between February and mid-May, hackers attempted to access around 200,000 US taxpayers' accounts. They succeeded in getting hold of personal details such as dates of birth, addresses and social security numbers in roughly 100,000 cases. To do this, they gained access to a system called Get Transcript, which allows users to view all of their dealings with the tax authority. They cheated the multi-stage authentication process with the aid of data that were already in their possession. This led to the IRS temporarily suspending Get Transcript.

The number of Japanese Pension Service customers who had their identities stolen was more than ten times greater – about 1.25 million. Names, pension account numbers, dates of birth and addresses fell into cybercriminals' hands after a member of staff opened an e-mail that contained a virus.

What all three attacks have in common is the fact that neither private nor government organisations seem to be capable of reliably protecting sensitive customer data. This sobering conclusion casts a negative light on the plans for centrally collecting personal healthcare data (see Security Report, May 2015 and December 2014).

Read more here:

https://teksecurityblog.com/blog/2015/04/13/hacked-how-safe-is-your-data-on-adult-social-sites
http://www.heise.de/security/meldung/Sexboerse-Adult-Friend-Finder-gehackt-Nutzerdaten-im-Netz-verteilt-2663029.html
http://www.golem.de/news/hack-auf-datingplattform-sexuelle-vorlieben-von-millionen-menschen-veroeffentlicht-1505-114219.html
https://krebsonsecurity.com/2015/05/irs-crooks-stole-data-on-100k-taxpayers-via-get-transcript-feature
http://www.bankinfosecurity.com/irs-100000-taxpayer-accounts-breached-a-8261
http://www.spiegel.de/netzwelt/web/irs-online-angriff-auf-die-us-steuerbehoerde-a-1035706.html
http://www.zeit.de/news/2015-06/01/japan-japans-pensionskasse-gehackt-01124207

II. Good friends listen, and so does the BND – the scandal continues

All of the major powers in the Second World War ran huge information campaigns about eavesdropping. The US Office of War Information, for instance, warned: «The ENEMY is listening. He wants to know what you know. KEEP IT TO YOURSELF.» Now it is becoming ever clearer that one of that same country's modern-day intelligence services, the National Security Administration (NSA), wanted (and still wants) to know things even from allies' services like the German BND that the BND itself did not know (and still does not). To put this in rather simpler terms, BND President Gerhard Schindler has said that the NSA used the friendly BND for economic and other forms of espionage and «encouraged» it to spy on other friends such as Switzerland, Belgium and the EU. It is not currently possible to gauge the extent to which this is still going on. What

is clear, however, is the fact that the BND had noticed back in 2005 that the NSA's so-called selector lists of search terms included the names of companies, European institutions, high-ranking politicians and foreign firms. The German website ZEIT ONLINE also reports that, in addition to the selector data, the BND delivers some 1.3 billion items of metadata to NSA computers every month.

For its part, the BND claims that it informed the Chancellor's office about the data sharing in a confidential report as long ago as 2008, which was followed by another in 2010. Nothing happened, however, until Edward Snowden's leaks – probably because the German government (among others) felt too dependent on information from the US intelligence services in the face of new security threats.

Airbus has now brought spying charges. The Swiss and Belgians are also up in arms about what we might call «friendly spying» as a word-play on the rather cynical phrase «friendly fire». The US intelligence community is increasingly annoyed too – by the calls from German and European politicians to get to the bottom of the scandal.

Read more here:

https://netzpolitik.org/2015/internes-dokument-belegt-bnd-und-bundeskanzleramt-wussten-von-wirtschaftsspionage-der-usa-gegen-deutschland
http://www.spiegel.de/politik/deutschland/bnd-affaere-weitere-listen-mit-brisanten-suchbegriffen-a-1035018.html
http://www.zeit.de/digital/datenschutz/2015-05/bnd-affaere-selektoren-nsa-liste/komplettansicht
http://www.zeit.de/politik/deutschland/2015-05/bnd-nsa-milliarden-metadaten
http://www.golem.de/news/bnd-chef-schindler-wir-sind-abhaengig-von-der-nsa-1505-114201.html
http://www.handelsblatt.com/politik/deutschland/bnd-affaere-airbus-stellt-strafanzeige-wegen-nsa-spionage/11715836.html
http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890
http://www.heise.de/newsticker/meldung/Belgien-erwartet-Antworten-von-Deutschland-zu-BND-Spaehvorwuerfen-2671162.html
http://www.heise.de/newsticker/meldung/Der-grosse-Bruder-reagiert-genervt-2663846.html
http://www.sueddeutsche.de/politik/no-spy-abkommen-geschichte-eines-taeuschungsmanoevers-1.2494417
http://www.faz.net/aktuell/politik/ausland/amerika/entscheidung-im-senat-nsa-spaehprogramm-vor-dem-aus-13622851.html

III. A new kind of government Trojan – cyberattack on German parliament's secure network

The cyberattack on the German parliament's secure network could have almost become a mere footnote in the history of cybercrime, were it not so serious in terms of its execution and scope and so disastrous in terms of its impact. After a

majority of its members voted in favour of using government-sponsored Trojans, the Bundestag was itself the target of a Trojan attack at the beginning of May. In fact, the attack is still ongoing because it is so mysterious and sophisticated that even the Bundestag's security experts have been unable to halt or avert it so far. No one knows when it started, how long it will continue or indeed where the malware is sending data to from parliamentarians' computers. The members themselves thus believe that it is the work of a foreign intelligence service, and they are not alone in that view. If attempts to stop the malware fail, the Bundestag's entire IT infrastructure will have to be rebuilt.

Read more here:

http://www.zeit.de/digital/datenschutz/2015-05/hackerangriff-bundestag-sommerpause
http://transdata.info/schwerer-angriff-auf-das-bundestagsnetz-seit-mai-2015
http://www.heise.de/security/meldung/Cyber-Angriff-auf-Bundestag-bleibt-ausser-Kontrolle-2662336.html
http://www.nzz.ch/international/bei-hackerangriff-auf-bundestag-wurden-daten-gestohlen-1.18551627
http://www.spiegel.de/netzwelt/netzpolitik/bundestag-ermittler-vermuten-geheimdienst-hinter-cyberangriff-a-1034790.html

IV. Reset, then reload – Android smartphones keep data even after factory reset

The title of the classic sci-fi story by Philip K. Dick that inspired the film «Blade Runner» is a question that remains unanswered to this day: «Do Androids Dream of Electric Sheep?» Meanwhile, many ex-owners of smartphones running versions 2.3.x to 4.3 of the Android operating system might well be having nightmares after reading two studies by Laurent Simon and Ross Anderson of Cambridge University. The first of the two studies linked to below proves that, even after a factory reset is performed (i.e. the phone is reset to the state in which it left the factory), sensitive data such as login details, text messages, e-mails and photos can still be recovered. Simon and Anderson claim that they also achieved this with handsets on which Android full encryption had been used to safeguard data, although it took a lot more time and effort.

In their second study, they dash any hopes that the security loophole was due to a lack of care on the manufacturers' part and could be closed using so-called wiping tools. They conclude that ten of the most popular apps for wiping a device's memory fail to remove data such that it cannot be restored. A forensic

investigation by Steve Mellings, founder of the Asset Disposal & Information Security Alliance (ADISA), and Andrew Blyth, Professor at the University of South Wales, comes to a similar conclusion but draws a comparison with BlackBerry and Apple iOS devices: «In summary, the factory reset function, when performed on the sample of BlackBerry and Apple devices, erases the user data from the device such that using standard forensic tools and techniques it is impossible to recover the data … However, the story with the Android devices is very different. The research findings show that the factory reset function, when performed on certain Android devices, is not sufficient and that data can be recovered.»

Read more here:

http://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf
http://www.cl.cam.ac.uk/~rja14/Papers/mav_most15.pdf
http://www.heise.de/security/meldung/Daten-von-Millionen-zurueckgesetzten-Android-Smartphones-wiederherstellbar-2663267.html
http://www.informationsecuritybuzz.com/forensic-analysis-of-smartphone-factory-reset-function

The Clipboard: interesting presentations, articles and videos

In a research project, Sune Lehmann has taken a look at how well mobile users can be tracked using WiFi information, in some cases even when they have turned their device's WiFi off:

http://sunelehmann.com/2015/05/26/tracking-human-mobility-using-wifi-signals/

A new exploit kit attacks local routers from home PCs to reconfigure them for its own ends. The blog «Malware don't need Coffee» has an analysis:

http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html

http://www.heise.de/security/meldung/Exploit-Kit-greift-ueber-50-Router-Modelle-an-2665387.html

PGP inventor Phil Zimmermann has moved from the US to Switzerland. He tells The Guardian why he feels safer here:

http://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy

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