SWITCHcert Security Report

May 2015

SWITCH

I. «Massive snooping attack» or successfully treading the fine line between security and freedom? On the reform of Switzerland's intelligence services legislation

The recent affair involving Germany's BND proves that intelligence services of friendly states are often more willing to cooperate with each other than their respective governments. Details are gradually emerging of just how intensive the collaboration and exchange of collected data and analysis between the BND and the US National Security Agency (NSA) really was – and is. It seems that Switzerland also wants to join in this clandestine trade – indeed, Edward Snowden claims that it serves as a hub for all kinds of espionage involving many nations. This would be further aided by the planned reform of the Federal Act on Responsibilities in the Area of the Civilian Intelligence Services, which was recently brought before the Council of States. The new legislation would not only allow the Federal Intelligence Service (FIS) to forward data to foreign partner services, it would in fact also make it legal to intercept data transported between countries via cable networks and search it for keywords. Since the majority of Internet data traffic passes through servers outside Switzerland, however, data flowing between a Swiss sender and a Swiss recipient would be subject to a «massive snooping attack». These are the words of Fredy Künzler, CEO of Swiss ISP Init7. While Federal Data Protection and Information Commissioner

Hanspeter Thür points out that the current draft provides for an approval procedure intended to prevent permanent blanket monitoring as practised by the NSA's Tempora programme, Künzler has nothing good to say about the reform plan. The new Act would also compel providers of data services to cooperate with the FIS. All political parties apart from the Greens have signalled that they will support the revised Act, but resistance is building on various fronts outside parliament, for instance from the Chaos Computer Club Switzerland, the Swiss Consumer Protection Foundation and the Swiss IT industry association Swico.

Read more here:

http://www.nzz.ch/schweiz/wenn-auslaendische-geheimdienste-mitlesen-1.18524735

http://www.computerworld.ch/news/security/artikel/snowden-schweiz-ist-spionage-drehscheibe-67689/

http://www.vbs.admin.ch/internet/vbs/de/home/themen/ndb/uebersicht.html

http://www.vbs.admin.ch/internet/vbs/de/home/themen/ndb/dokumente.html

https://www.digitale-gesellschaft.ch/2015/03/12/offener-brief-zum-neuen-nachrichtendienstgesetz-schuetzen-wir-freiheit-und-privatsphaere-vor-der-massenueberwachung

https://www.woz.ch/-5775

http://www.srf.ch/news/schweiz/session/gruene-kaempfen-vergebens-das-nachrichtendienstgesetz-ist-durch

http://www.swico.ch/aktuell-medien/aktuell/neuer-entwurf-nachrichtendienstgesetz-problematisch/2303?referer=archiv

II. Barbie turns Bond girl – toy manufacturers spying on children's bedrooms

It is no secret that Barbie dolls have had the power of speech for some time. They can blurt out banal sayings at the touch of a button. The latest Hello Barbie edition, however, can do a lot more. It can hold a «real» conversation with children, ask questions, learn, register responses and forward them via Wi-Fi straight to the manufacturer, which records and analyses them. Hello Barbie is a spy in the child's bedroom. It therefore comes as no surprise that the doll, along with the BND, has won one of this year's BigBrotherAwards from the Digitalcourage lobbying group.

However, Barbie is not alone. New York-based startup Elemental Path is using crowdfunding to develop its CogniToys dinosaur smart toy. The toy works with

IBM's Watson artificial intelligence technology and – naturally – sends the data it records back to the manufacturer.

When it comes to activating network connections and allowing this kind of snooping to happen in the first place, the toy firms are not simply expecting parents to delegate child care to a talking doll. Instead, they are appealing to parents' sense of responsibility for their children's safety. After all, Mom and Dad could use a Wi-Fi connection to listen to what their children are saying and find out what is on their minds. At the same time, more and more grown-up toys are being sold with data feedback features. One example is Amazon Echo, the new «all-knowing» (and indeed all-hearing) digital information, entertainment and household organisation system that brings Captain Kirk's computer from the starship Enterprise into your home – for just USD 199 and right now, not in the distant future.

Read more here:

http://www.faz.net/aktuell/feuilleton/familie/hello-barbie-cognitoy-dino-sprechen-mit-kindern-13488930.html

http://www.sueddeutsche.de/digital/spielzeug-lauschangriff-im-kinderzimmer-1.2440374

http://mom.brigitte.de/haben-wollen/sprechende-barbie-1233657

http://mashable.com/2015/02/16/smart-dino-toy-powered-by-ibm-watson

http://recode.net/2015/02/17/cognitoys-for-kids-uses-ibms-watson-to-talk-like-a-buddy

https://digitalcourage.de/blog/2015/bigbrotherawards-die-preistraeger

http://www.zeit.de/digital/internet/2014-11/amazon-echo-lautsprecher-spracheingaben

https://www.youtube.com/watch?v=KkOCeAtKHIc

III. Only those who get involved get hurt – latest e-banking Trojans harness social engineering

Social engineering means attempting to exploit users' gullibility, helpfulness or insecurity in order to get at confidential data, for example through phishing or with fake phone calls. Some uncannily authentic-looking e-mails with malicious attachments or links to the e-banking Trojans Emotet and Dyre have been doing the rounds of late. The two Trojans differ in how they give hackers access to victims' e-banking accounts, but they have one striking feature in common: both require active help from the users they target. Emotet circumvents two-way authentication via TAN or mTAN by prompting users when they start e-banking to take a tutorial in which they have to make a supposedly fictitious payment for test purposes. This payment is then executed for real, with the money being transferred to a middleman's account. Dyre, on the other hand, fakes technical problems and prompts users to to call a helpline, which is really the hackers attempting to collect information and account access details over the phone. Banks and IT security providers are thus warning their clients to be especially vigilant.

Read more here:

https://www.ebankingbutsecure.ch/de/securitynews/445-e-banking-trojaner-setzen-vermehrt-auf-social-engineering

http://blog.botfrei.de/2015/04/neue-version-des-banking-trojaner-emotet-erreichen-unsere-rechner

http://www.itespresso.de/2015/04/10/kaspersky-banktrojaner-emotet-noch-im-deutschsprachigen-raum-aktiv/

http://www.viruslist.com/de/analysis?pubid=200883880

http://www.zdnet.com/article/dyre-wolf-attacks-your-corporate-bank-account-door

IV. E-health made in Switzerland – electronic patient records

It is already standard procedure when you take your car in for a service, but it will soon become commonplace in Swiss practices and hospitals too: an instant digital check-up that gives the mechanic (or doctor) a detailed picture of the vehicle's (or patient's) history. The aim is to reduce the cost of diagnosis and improve the efficacy of the treatment. The Federal Department of Home Affairs

has calculated two scenarios with savings of between CHF 3.5 billion and CHF 4.1 billion over 20 years, assuming that all doctors, hospitals, therapists etc. sign up. The intention is to give patients the choice as to whether or not their health data are stored centrally. Some pilot projects are already under way at the cantonal level, including Swiss Post's MonDossierMedical.ch in Geneva and Swisscom's Evita. The Federal Act on Patient Records will introduce national standards and allow data to be forwarded between cantons.

Ensuring the security of sensitive healthcare data will be a top priority. Any large collection of data arouses interest, and in the case of e-health this may come from employers, insurers or lenders. At the same time, the wide range of healthcare app interfaces envisaged offers a multitude of attack vectors for hackers. The magazine website computerworld.ch, for example, writes: «Interfaces to the leading [health and fitness] apps will be used to transfer data already stored by these apps.» Central data storage means that doctors and other service providers will have a clearer picture of an individual's health and be better placed to gauge how their personal exercise regime might influence their treatment. It is thus conceivable that doctors will in future spend more time examining data from patients' smartwatches than their eyes.

Read more here:

http://www.computerworld.ch/businesspraxis/artikel/startschuss-fuer-schweizer-ehealth-67588

http://www.srf.ch/gesundheit/gesundheitswesen/das-teilen-von-daten-ist-ein-grundanliegen-unserer-gesellschaft

http://www.srf.ch/play/radio/input/audio/ehealth-der-patient-auf-dem-chip?id=6033df48-a1ac-4ece-8f9e-fc80663c77c7

http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10359

http://www.parlament.ch/d/mm/2015/Seiten/mm-sgk-n-2015-02-20.aspx

V. Fear of flying 2.0 – US authorities warn of in-flight hacking

Anyone who regularly flies long-distance will welcome various airlines' offers of Internet access via Wi-Fi hotspots on board their aircraft. However, the FBI, the Transport Security Administration (TSA) and the Government Accountablity Office (GAO) in the US have all pointed out that this opens the door to in-flight hacking. While they admit that such hacking is not easy, they say that it is far from impossible. A joint warning from the FBI and TSA asks the airlines to pay greater attention to the security of their on-board Wi-Fi. The warning was prompted by IT security researcher Chris Roberts sending the following tongue-in-cheek tweet from his United Airlines flight: «Find myself on a 737/800, let's see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? 'PASS OXYGEN ON' Anyone ? :)» His intention was to highlight vulnerabilities. On landing, however, the FBI arrested him, impounded his equipment and questioned him for more than four hours. Moreover, United refused to let him on the return flight. Fear of flying has clearly taken on a whole new dimension, and it is not just passengers who are nervous.

Read more here:

http://www.theguardian.com/technology/2015/apr/15/wi-fi-on-planes-in-flight-hacking-us-government

http://www.wired.com/2015/04/fbi-tsa-warn-airlines-tampering-onboard-wifi

http://futurezone.at/digital-life/us-hacker-darf-nach-tweet-nicht-an-bord-von-flugzeug/126.115.105

http://gizmodo.com/fbi-and-tsa-warn-airlines-to-watch-out-for-wi-fi-hacks-1699386773

The Clipboard: interesting presentations, articles and videos

Marcus Murray demonstrated at the RSA Conference how it is possible to gain unauthorised access to a Microsoft web server using a JPEG:

https://www.rsaconference.com/events/us15/agenda/sessions/1513/the-little-jpeg-that-could-hack-your-organization

Computer security incident response teams (CSIRTs) must evolve continuously to meet the constantly changing challenges they face. At the Global Conference on CyberSpace 2015, a CSIRT Maturity Kit – a step-by-step guide towards enhancing CSIRT maturity – was presented:

https://www.gccs2015.com/csirt-maturity

Cisco's blog puts the spotlight on a piece of malware called Rombertik that includes a number of mechanisms for evading analysis tools.

http://blogs.cisco.com/security/talos/rombertik

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