SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Mai 2015

SWITCH

I. «Grosser Lauschangriff» oder gelungene Güterabwägung zwischen Sicherheit und Freiheit? Zur Reform des Schweizerischen Nachrichtendienstgesetzes

Dass Nachrichtendienste befreundeter Staaten oft partnerschaftlicher miteinander umgehen als deren Regierungen, zeigt sich gerade am Beispiel der BND-Affäre: Nach und nach sickert durch, wie intensiv die Zusammenarbeit und der Austausch von gesammelten Daten und daraus gewonnenen Erkenntnissen zwischen dem deutschen und dem US-amerikanischen Geheimdienst NSA wirklich war und ist. Offenbar will auch die Schweiz am verborgenen Tauschhandel teilhaben – immerhin gilt sie nach Aussagen Edward Snowdens als Drehscheibe für Spionage aller Art und vieler Nationen. Ermöglicht würde dies durch die geplante Reform des NDG, welche gerade dem Ständerat vorgelegt wurde. Denn dieses erlaubt dem Nachrichtendienst des Bundes nicht nur die Weitergabe von Daten an ausländische Partnerdienste. Vielmehr schafft sie mit der Ermächtigung zur sogenannten Kabelaufklärung auch eine Legitimationsbasis zur Durchsuchung des grenzüberschreitenden Datenverkehrs via kabelgebundener Netze nach Stichworten. Weil aber der grösste Teil des

Datenverkehrs im Internet den Umweg über ausländische Server nimmt, würden auch Datenströme zwischen einem Schweizer Sender und einem Schweizer Empfänger Ziel eines «grossen Lauschangriffs». So bezeichnet jedenfalls Fredy Künzler, CEO des Schweizer ISPs Init7, das neue Reformvorhaben. Anders als der Schweizerische Datenschützer Hanspeter Thür, der darauf verweist, dass die aktuelle Vorlage ein Genehmigungsverfahren enthält, welches die flächendeckende und permanente Überwachung wie im Programm «Tempora» der NSA verhindern soll, lässt Künzler kein gutes Haar am Reformvorhaben. Denn das neue Gesetz sieht unter anderem auch vor, dass Anbieter von Datendiensten zur Kooperation mit dem Schweizer Nachrichtendienst verpflichtet sind. Während mit Ausnahme der Grünen alle Parteien Zustimmung zum neuen Gesetz signalisiert haben, formiert sich ausserhalb des Parlaments Widerstand von so unterschiedlichen Seiten wie dem Chaos Computer Club Schweiz, der Stiftung für Konsumentenschutz SKS oder dem Dachverband der Schweizerischen IT-Wirtschaft SWICO.

Nachzulesen unter:

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 wird Bond-Girl: Spielzeughersteller spionieren im Kinderzimmer

Es ist kein Geheimnis, dass Barbie-Puppen schon seit längerem sprechen und auf Knopfdruck Banalitäten von sich geben. Die neueste «Hello Barbie» aber kann noch viel mehr: Sie führt mit den Kindern «echte» Gespräche, stellt Fragen, lernt dazu, registriert die Antworten und leitet diese via WLAN direkt an den

Hersteller weiter, der die Daten sammelt und auswertet: Hello Barbie ist eine Spionin im Kinderzimmer. Deshalb ist es auch nicht verwunderlich, dass sie Seite an Seite mit dem Bundesnachrichtendienst einen der diesjährigen «BigBrotherAwards» des Vereins Digitalcourage erhalten hat.

Barbie ist aber nicht allein: Auch das New Yorker Startup Elemental Path hat – finanziert mit Crowdfunding-Geldern – mit dem CogniToys-Dino ein «Smart Toy» in der Pipeline. Dieser Schnüffeldino wird von IBMs KI-Technologie «Watson» gesteuert. Und natürlich meldet auch er die erfassten Daten an seinen Hersteller zurück.

Damit Eltern die Netzverbindung aktivieren und so den «Lauschangriff im Kinderzimmer» überhaupt erst möglich machen, verlassen sich die Hersteller nicht alleine darauf, dass Eltern Betreuungs- und Erziehungsarbeit an die sprechenden Spielzeuge delegieren wollen. Vielmehr appellieren sie an die Verantwortung der Eltern für die Sicherheit ihrer Kinder. Schliesslich könnten Mami und Papi via WLAN das Gespräch ihrer Kinder mithören und auf diese Weise erfahren, was ihre Kinder beschäftigt. Auch immer mehr Spielzeuge für die Grossen sind mit Daten sendenden Rückkanälen ausgestattet sind. Zum Beispiel Amazon Echo, das neue «allwissende» (und eben auch allhörende) digitale Info-, Entertainment- und Haushaltsorganisationssystem, das den Zentralcomputer auf Captain Kirks Enterprise in jeden Haushalt bringt – für 99 Dollar und nicht erst in einer fernen Zukunft.

Nachzulesen unter:

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. Nur wer mitmacht wird geschädigt: Aktuelle e-Banking Trojaner setzen auf Social Engineering

Mit Social Engineering werden Versuche bezeichnet, aus der Gutgläubigkeit, Hilfsbereitschaft oder Unsicherheit von Anwendern vertrauliche Daten zu gewinnen, wie etwa beim Phishing oder mit Hilfe fingierter Anrufe. In jüngster Zeit wurden via täuschend echt aussehender Mails mit bösartigem Anhang oder entsprechenden Links die beiden e-Banking-Trojaner «Emotet» und «Dyre» verbreitet. Auch wenn sich beide in der Art unterscheiden, wie sie den Angreifern Zugriff auf die e-Banking-Konten der Opfer verschaffen, so haben sie doch eine augenfällige Gemeinsamkeit: Beide brauchen die aktive Mitarbeit der Anwender. «Emotet» umgeht die Zwei-Wege-Authentifizierung via TAN oder mTan, indem die User beim Start des e-Banking zu einer Schulung aufgefordert werden, während der auch eine angebliche Testüberweisung erledigt werden muss. Diese wird dann aber real ausgeführt, und zwar zugunsten des Kontos eines Mittelsmannes der Hacker. «Dyre» täuscht technische Probleme vor und fordert dazu auf, eine Servicenummer anzurufen. Diese führt zu den Angreifern, die im Telefonat versuchen, Infos und Zugangsdaten zum Konto abzugreifen. Banken und IT-Security-Dienstleister fordern deshalb zu erhöhter Wachsamkeit auf.

Nachzulesen unter:

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. eHealth made in Switzerland – Das elektronische Patientendossier

Was für aktuelle Automodelle beim Werkstattbesuch gang und gäbe ist, soll auch in Arztpraxen und Spitälern der Schweiz für Patienten Alltag werden: Der digitale Sofort-Check, der dem Mechaniker, respektive Arzt ein umfassendes Bild über den gesamten bisherigen Gesundheitsverlauf liefert. Dadurch sollen die Kosten

für die Diagnose gesenkt und die Effektivität der Behandlung verbessert werden. Das Eidgenössische Departement des Inneren hat in zwei Szenarien für einen Zeitraum von 20 Jahren Einsparungen zwischen 3,5 und 4,1 Mrd. Franken errechnet – vorausgesetzt, alle Leistungserbringer, also Ärzte, Spitäler, Therapeuten etc. machen mit. Patientinnen und Patienten soll es freigestellt bleiben, ob ihre Gesundheitsdaten zentral gesammelt werden sollen. Auf kantonaler Ebene laufen bereits einige Modellprojekte, wie z.B. MonDossierMedical der Post im Kanton Genf oder das Modellprojekt Evita der Swisscom. Das Bundesgesetz über das elektronische Patientendossier soll nun für schweizweit einheitliche Standards sorgen und den Datenaustausch auch über die Kantonsgrenzen hinweg ermöglichen.

Dabei soll der Sicherheit der sensiblen Gesundheitsdaten oberste Priorität eingeräumt werden. Denn zum einen wecken Datensammlungen immer Begehrlichkeiten – im Falle von eHealth könnten Arbeitgeber, aber auch Versicherer oder Darlehensgeber starkes Interesse anmelden. Zum anderen bieten gerade die vorgesehenen vielfältigen Schnittstellen zu Gesundheitsapps Angriffsvektoren für Hacker. So schreibt z.B. computerworld.ch: «Via Schnittstellen zu den gängigsten Apps [aus dem Gesundheits- und Fitness-Bereich] sollten sich die [dort] bereits abgelegten Daten transferieren lassen.» Durch die zentrale Datenhaltung könnten sich Ärzte und andere Leistungserbringer besser über den Gesundheitszustand orientieren und allfällige Einflüsse von privaten Trainings auf den Therapieverlauf besser abschätzen. Gut möglich also, dass Ärzte zur Diagnose künftig statt in die Augen ihrer Patienten lieber auf die Daten von deren Smartwatch schauen.

Nachzulesen unter:

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. Flugangst 2.0 – US-Behörden warnen vor In-Flight-Hacking

Wer oft Langstreckenflüge zu bewältigen hat, wird das Angebot verschiedenster Airlines begrüssen, auch während der Flugzeit dank WLAN-HotSpots Internetzugang zu haben. Darauf, dass damit im Flugzeug aber auch ein Einfallstor für Hackerangriffe geöffnet werde, haben kürzlich FBI, TSA (Transport Security Administration) und das US Government Accountability Office GAO hingewiesen. Zwar sei ein Hack nicht einfach durchzuführen, aber eben auch alles andere als unmöglich. In einer gemeinsam herausgegebenen Warnung haben FBI und TSA deshalb die Airlines aufgefordert, der Sicherheit von On-Board-WiFi erhöhte Aufmerksamkeit zu widmen. Auslöser war der IT-Security-Forscher Chris Roberts, der auf einem United-Airlines-Flug den als Scherz gekennzeichneten Tweet «Bin gerade auf einer 737/800, lasst uns mal Box-IFE-ICE-SATCOM überprüfen? Sollen wir mit den EICAS-Nachrichten spielen? Wie wäre es mit ‚PASS OXYGEN ON'? :)» abgesetzt hatte, um auf Sicherheitslücken hinzuweisen. Nach der Landung verhaftete Ihn das FBI, beschlagnahmte sein Equipment und befragte ihn über 4 Stunden. Zudem verweigerte ihm United Airlines den Rückflug. Flugangst hat offenbar eine neue Facette – und die macht wohl nicht nur die Passagiere nervös.

Nachzulesen unter:

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

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Marcus Murray hat auf der RSA-Sicherheitskonferenz demonstriert, wie man mit einem JPEG unautorisierten Zugriff auf einen Microsoft-Webserver erlangen kann:

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

Computer Security Incident Response Teams (CSIRTs) müssen sich stetig weiterentwickeln, um mit den Herausforderungen Schritt zu halten. Auf der Global Conference on CyberSpace 2015 wurde dazu ein CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity - vorgestellt:

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

Im CISCO-Blog gibt es eine Analyse der Malware «Rombertik», die eine Reihe von Anti-Analyse-Mechanismen vereint:

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

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.