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

Dezember 2014

SWITCH

I. Kein «Land of the Free» in Sicht: NSA darf weiter Daten sammeln, BND listet Wünsche für 300 Mio. Euro auf

Lange Gesichter im US-Senat: Zwar hatte eine breite Koalition aus Demokraten, einigen freiheitlich gesinnten Republikanern, Bürgerrechtsorganisationen und Technologieunternehmen wie Apple, Google, Microsoft und Yahoo sowie Präsident Barack Obama selbst einen Gesetzentwurf unterstützt, der es der US-amerikanischen National Security Agency untersagt hätte, weiterhin massenhaft Telefonverbindungsdaten zu sammeln. Dennoch fehlten dem sogenannten «USA Freedom Act» Ende November letztlich zwei Stimmen zur notwendigen Mehrheit. Vor allem unter Hinweis auf neue terroristische Bedrohungen, etwa durch die Gruppe «Islamischer Staat» sprachen sich die Gegner des USA Freedom Act dagegen aus, dass Verbindungsdaten inneramerikanischer Telefonate nicht mehr bei der NSA, sondern bei den Telefongesellschaften gespeichert werden sollten und vom Geheimdienst per Gerichtsbeschluss hätten angefordert werden müssen. Dabei galt der USA Freedom Act als kleinstmöglicher gemeinsamer Nenner einer Reform, die als Reaktion auf die Snowden-Enthüllungen die Befugnisse der Geheimdienste neu regeln wollte.

Von solchen Reformbestrebungen völlig unbeeindruckt zeigt sich auch der deutsche Auslandsgeheimdienst BND. Noch während er sich vor dem Untersuchungsausschuss zur NSA-Affäre verteidigte, legte er den Mitgliedern des Haushaltsausschusses – passend zur Vorweihnachtszeit – seine Wunschliste vor. Ihr Wert: 300 Mio. EUR (zusätzlich zum normalen Etat von knapp 560 Mio. EUR). Ihr Ziel: den Bundesnachrichtendienst «im Cyberbereich auf Augenhöhe mit den Partnern» (O-Ton BND) bringen. In einem Artikel vom 13.11.2014 hatte Zeit online (Quellenangabe siehe unten) alle Vorhaben und Projekte im Rahmen des als «Strategische Initiative Technik» bezeichneten Konzepts beschrieben: Die Liste reicht von Staatstrojanern bis zur Echtzeitanalyse von Streamingdaten und zu einem Projekt mit dem technokratischen Titel «Schutz vor Identitätsaufklärung durch Bildmanipulation / -verfremdung». Dahinter verbirgt sich nichts anderes als ein automatisiertes Programm zur Umgehung der Gesichtserkennung durch biometrische Überwachungssysteme. Zumindest der Sinn für Selbstironie scheint dem BND nicht abhanden gekommen zu sein.

Nachzulesen unter:

http://www.nzz.ch/international/amerika/nsa-darf-weiter-ungebremst-daten-sammeln-1.18428311

https://netzpolitik.org/2014/usa-freedom-act-sogar-das-kleinstmoegliche-geheimdienst-refoermchen-faellt-durch

https://www.eff.org/deeplinks/2014/11/usa-freedom-act-week-whats-come-and-what-you-need-know

http://www.zeit.de/digital/internet/2014-11/bnd-bundesnachrichtendienst-ueberwachung-ausbau

https://netzpolitik.org/2014/kein-steuergeld-fuer-grundrechtsbruch-morgen-frueh-vorm-reichstag-gegen-etat-erhoehung-fuer-bnd-demonstrieren

http://www.golem.de/news/geheimdienst-bnd-moechte-sich-vor-gesichtserkennung-schuetzen-1411-110631.html

II. Zensur-Kultur in Grossbritannien

«Aus unserer Sicht stellt es (das Prinzip, mit Netzsperren illegale Inhalte aus dem Netz zu filtern, Anm. d. Red.) einen Rückschritt in der Bekämpfung illegaler Internetinhalte dar. Der Aufbau einer Infrastruktur zur Sperrung und Filterung von Internetinhalten ist aus unserer Sicht nicht nur kontraproduktiv für die Bekämpfung illegaler Inhalte und deren Löschung, sondern auch Einflugschneise für eine Zensur-Kultur, die die Grundprinzipien der Transparenz und Rechtsstaatlichkeit untergräbt.» Mit diesen

Worten kritisiert der deutsche Internetprovider-Verband die stetige Ausweitung der Netzsperren in Grossbritannien. Die als «Pornofilter» bezeichnete Sperre wurde unlängst um einen Button zur Meldung terroristischer oder extremistischer Propaganda erweitert. Das System blockiert derzeit 23.000 Webseiten in Grossbritannien, darunter auch Seiten mit Themen wie Nacktheit, Sexualerziehung, Dating, Glücksspiel, Gewaltdarstellungen, extremistische und terroristische politische Inhalte, Webseiten zu Magersucht und Essstörung, Suizid-Webseiten, Alkohol, Rauchen, Webforen, esoterisches Material und Umgehungstools für Netzsperren. Von den Sperren zumindest zeitweise betroffen waren auch Open-Source-Webseiten wie Linuxtracker, die Seiten des Nachrichtenaggregators Reddit oder das Onlinemagazin Torrentfreak, weil sie angeblich direktes Filesharing ermöglichen. Für Kritiker ein Zeichen dafür, dass unter dem Vorwand von Jugendschutz und Terrorabwehr jede Form missliebiger Netzinhalte zensiert werden sollen.

Nachzulesen unter:

http://www.theguardian.com/technology/2014/nov/14/isps-filter-extremist-material-internet

http://www.golem.de/news/ofcom-briten-schalten-den-pornofilter-ab-1407-108079.html

https://www.eco.de/2014/news/eco-britische-netzsperren-sind-rueckschritt-in-der-bekaempfung-illegaler-internetinhalte.html

http://www.bbc.com/news/technology-30052211

III. PR der Neuen Zeit: Wie Parteien, Unternehmen und Verbände Online-Foren zur Meinungsbildung manipulieren

«Wir machen Meinung» verspricht die österreichische PR-Agentur «Modern Mind Marketing» ihren Kunden. Wie die Agentur das tut, enthüllte vor kurzem das österreichische Magazin «Datum»: Man installiere zehntausende Fake-Accounts und beauftrage freiberuflich engagierte Poster damit, über diese Accounts (natürlich nicht aus den eigenen Büroräumen heraus sonst liessen sich die IP-Adressen ja zuordnen) Kommentare in Online-Foren zu stellen, um Auftraggeber in besserem Licht erscheinen zu lassen, Kritiker zu diskreditieren oder zumindest deren Kritik zurückzuweisen etc. Was dem russischen Geheimdienst in der Ukraine-Krise vorgeworfen worden ist, machten sich dem Datums-Bericht zufolge auch prominente Auftraggeber wie z.B. die Österreichische Volkspartei ÖVP, die staatliche

Eisenbahngesellschaft ÖBB, die Bank Austria, TUI Österreich, der Pharmakonzern Bayer Austria, aber auch nicht-deutschsprachige Kunden wie das britische Unternehmen Paysafecard zunutze. Nun ist die Existenz der manipulierenden Trolle zwar spätestens seit dem Bekanntwerden von Trollüberfällen auf Wikipedia 2013 nichts Neues mehr, doch hat das Ausmass der Manipulationen doch für einige Aufregung gesorgt. Der österreichische PR-Ethik-Rat verurteilte denn auch die Aktion aufs Schärfste.

Dass man mit meinungsbildenden Postings auch anders Geld verdienen kann, beweist ein Broadway Hotel im britischen Seebad Blackpool, das in seinen Buchungsbedingungen darauf hinweist, dass das Posting einer schlechten Bewertung mit einer Gebühr von 100 Pfund – umgerechnet etwa 150 Schweizer Franken – berechnet werde.

Nachzulesen unter:

http://www.datum.at/artikel/die-netzfluesterer

http://www.heise.de/newsticker/meldung/Putins-Trolle-schwemmen-die-Online-Foren-2221297.html

http://futurezone.at/digital-life/so-manipulieren-firmentrolle-online-foren/95.363.385

http://www.lunzer-kommunikation.at/imageschaden-fuer-die-imagemacher.html

http://futurezone.at/digital-life/auf-tripadvisor-schlecht-bewertet-hotel-verlangt-gebuehr/97.967.200

IV. Regin und die Detekt-ive: Neue Software findet bekannte Staatstrojaner – Symantec entdeckt einen bisher unbekannten

Nein, das ist kein Druck- oder Rechtschreibfehler in der Überschrift – «Detekt» ist der Name eines neuen Scanners, der Windows-Computer auf staatlich eingesetzte Schadsoftware durchsucht. Entwickelt wurde Detekt von einem der weltweit führenden Experten im Umgang mit Staatstrojanern, Claudio Guarnieri. Die Veröffentlichung der Open-Source-Software unterstützen 4 Menschenrechts-organisationen, der Quellcode ist auf GitHub publiziert. Die Liste der Malware, die Detekt erkennen kann, liest sich wie das Who Is Who der Staatstrojaner: BlackShades RAT, DarkComet RAT, FinFisher FinSpy, Gh0st RA, HackingTeam RCS, ShadowTech RAT, XtremeRAT und njRAT.

In Zukunft muss wohl auch «Regin» dazugerechnet werden. Der von ihren Entdeckern bei Symantec auf diesen Namen getaufte Backdoor-Trojaner ist wohl seit 2008 im Einsatz, seit 2013 aber in einer neuen, weit komplexeren Form, die von Experten als «most sophisticated» bezeichnet und diesbezüglich mit StuxNet, Flame oder Duqu verglichen wird. In dieser Version verschleiert der Trojaner auf allen erdenklichen Wegen sowohl seine Existenz auf befallenen Rechnern als auch, dass Daten entwendet werden. Ende November berichtete die Plattform «The Intercept», dass Regin von NSA und GCHQ, also dem amerikanischen und dem britischen Geheimdienst eingesetzt wurde, um u.a. die EU auszuspionieren. Hauptziele sind aber offenbar Unternehmen (hauptsächlich Infrastrukturbetreiber), Behörden aber auch Privatpersonen in Saudi-Arabien und Russland.

Nachzulesen unter:

https://netzpolitik.org/2014/detekt-anti-viren-scanner-fuer-staatstrojaner-veroeffentlicht

https://github.com/botherder/detekt

https://digitalegesellschaft.de/2014/11/software-gegen-staatstrojaner-veroeffentlicht

http://www.inside-it.ch/articles/38402

https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq

http://www.pcwelt.de/news/Regin___neuer_Super-Trojaner_spionierte_viele_Jahre_unentdeckt-Stuxnet-_und_Duqu-Nachfolger-9005597.html

http://www.spiegel.de/netzwelt/netzpolitik/trojaner-regin-ist-ein-werkzeug-von-nsa-und-gchq-a-1004950.html

V. Studium Generali oder: Prämienvergünstigung gegen Datenlieferung

Im Security-Report von Oktober hatten wir unter Verweis auf das Angebot vergünstigter Prämien einer Autoversicherung bei Einbau eines «Crash-Recorder» es noch als Möglichkeit angedeutet, dass Versicherungen gegen Lieferung von Gesundheits-, Fitness- oder Lifestyledaten aus dem Smart Home oder von Wearables Prämienrabatte gewähren könnten. Nun hat die Versicherung «Generali» angekündigt, ebendies in den nächsten 12 bis 18 Monaten in die Realität umzusetzen. Versicherte sollen via App nachweisen, dass sie Vorsorgetermine einhalten, sich fit halten und Sport treiben. Im Gegenzug könnten sie mit Prämienrabatten, Gutscheinen und Geschenken rechnen. Die Angaben sollen laut Generali stichprobenweise

überprüft werden. Ob und wann sich die Markteinführung der ersten bluetoothfähigen Zahnbürste mit Zahnputz-App im August 2014 auf die Höhe von Krankenkassenprämien oder Taschengeldzahlungen auswirken wird, ist derzeit noch völlig offen.

Nachzulesen unter:

http://www.zeit.de/digital/2014-11/versicherung-generali-fitness-daten-sammeln

http://www.sueddeutsche.de/kultur/juli-zeh-ueber-das-generali-modell-wir-werden-manipulierbar-und-unfrei-1.2232147

http://www.faz.net/aktuell/technik-motor/umwelt-technik/zahnbuerste-oral-b-pro-7000-bluetooth-fuer-weisse-zaehne-13079480.html

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Xavier Mertens schlägt im SANS InfoSec-Forum einen einfachen Weg vor, wie man mit Arpwatch, Nmap und OSSEC neue Geräte im Netz automatisiert auf ihr Schadpotenzial hin untersuchen kann:

https://isc.sans.edu/forums/diary/Guest+diary+Detecting+Suspicious+Devices+On-The-Fly/18993/

Google Hijacking Study - Google berichtete im November über den aktuellen Stand von Account Hijacking und was man dagegen tun kann:

http://googleonlinesecurity.blogspot.ch/2014/11/behind-enemy-lines-in-our-war-against.html

http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf

ICMP- respektive ICMPv6-Redirects sind als Angriffsvektor eigentlich ein alter Hut. Zimperium Mobile Security Labs berichteten nun, dass eine weiterentwickelte Form davon im Mobile-Bereich derzeit breite Anwendung findet:

http://blog.zimperium.com/doubledirect-zimperium-discovers-full-duplex-icmp-redirect-attacks-in-the-wild/

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