SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

März / April 2018

SWITCH

I. Die dunkle Seite der Datenmacht: Facebook, Cambridge Analytica und die drängende Frage, wer was wozu mit wessen Daten anstellt

Star Wars mal andersrum: Diesmal schlug das Imperium zurück, aber die Rebellen sind die Bösen. Seitdem die Tech-Giganten – allen voran Facebook, aber auch Google mit Google News und YouTube und Amazon mit Netflix und Amazon Prime – zu Medienunternehmen der zweiten Generation mutierten, sind viele klassische Medien in ihrem Bestand bedroht. Nun haben ein Whistleblower und klassischer investigativer Journalismus des Oberservers, der New York Times und des britischen TV-Senders Channel 4 Facebook in eine schwere Krise und Alexander Nix, den Chef der Datenanalysefirma Cambridge Analytica, von seinem Chefsessel gestürzt. Kern des Skandals ist der Fakt, dass die Daten von ca. 50 Millionen Facebook-Nutzern unerlaubt abgesaugt und zu Wahlkampfzwecken bei der letzten US-amerikanischen Präsidentschaftswahl und wohl auch bei der britischen Brexit-Abstimmung missbraucht wurden. Darum herum finden sich alle Zutaten für eine Jahrhundert-Story: Ein quantitativ wie qualitativ noch nie dagewesener Missbrauch von Daten, schwerwiegende und in dieser Form bislang für kaum möglich erachtete Manipulation demokratischer Wahlen durch inländische Manipulatoren und ihre Hintermänner und -frauen (allen voran Steve Bannon sowie Robert und Rebekah Mercer). Das Ganze

angereichert mit den prahlerischen Geständnissen von Alexander Nix, der angibt, neben virtuellen auch reale Erpressungen inszeniert zu haben, um Wahlen zu beeinflussen.

All diese Vorgänge sind alltagsrelevant, aber auch so haarsträubend, dubios und surreal, als hätte jemand die Drehbücher für House of Cards, Breaking Bad und Homeland mit dem Seldon-Plan aus Isaac Asimovs «Foundation»-Science Fiction Trilogie aus den Jahren 1942-1950 zu einer Horror-Serie der Big Data-Gesellschaft verschmolzen. Wohl auch deshalb vergeht kein Tag, an dem der Skandal in den Medien thematisiert wird. Der Guardian, heise.de, netzpolitik.org und die Zeit haben eigene, lesenswerte Dossiers dazu eingerichtet (s. Links unten).

Einmal mehr zeigt sich Facebook-Gründer und CEO Mark Zuckerberg zerknirscht darüber, dass sich sein Unternehmen dem Vorwurf ausgesetzt sieht, den Schutz der Mitgliederdaten zu wenig Aufmerksamkeit zu schenken. Hinzu kommt aber dieses mal erschwerend die Tatsache, dass erst dadurch der Missbrauch durch Cambridge Analytica ermöglicht wurde. Inzwischen wird Zuckerberg nicht nur mit Fragebogen der Europäischen Kommission konfrontiert, sondern auch mit Vorladungen zur Befragung durch einen britischen Parlamentsausschuss und den Justizausschuss des US-Senats. Vor dem sollen auch Google-Mitgründer Larry Page und Twitter-Chef Jack Dorsey aussagen. Das hat offenbar andere Tech-Giganten-Chefs wachgerüttelt. So hat etwa Brian Acton, Mitbegründer des 2014 von Facebook für 16 Milliarden US-Dollar gekauften Messengerdienstes WhatsApp, öffentlich zum Löschen des Facebook-Accounts aufgerufen (#deletefacebook). Zuvor hatte Tesla-Chef Elon Musk bereits die Facebook-Accounts seiner beiden Firmen Tesla und Space-X löschen lassen. Auch Prominente wie Jim Carrey verkaufen ihre Facebook-Aktien, löschen ihren Account und fordern ihre Fans auf, es ihnen nachzutun.

In Bedrängnis bringen könnte Facebook auch ein bekannter Kritiker des Sozialen Netzwerks: Max Schrems. Der betonte am 21. März 2018, dass er Facebook bereits 2011 in Irland angezeigt habe, dass die Daten millionenfach missbraucht würden und Facebook das seinerzeit als völlig legal bezeichnet habe. Interessieren dürfte diese Aussage zahlreiche Investoren und die amerikanische Handelsaufsicht FTC. Letztere hatte mit Facebook ein Datenschutz-Abkommen geschlossen und will nun prüfen, ob Facebook dieses Abkommen verletzt habe. Im Fall eines Verstosses drohen dem Sozialen Netzwerk Bussgelder in Höhe von 40.000 US-Dollar – pro Einzelfall! Bei 50

Millionen Einzelfällen steht demnach eine Bussgelddrohung in Höhe von 2000 Milliarden Dollar im Raum. Kein Wunder, dass bereits die ersten Investoren Facebook anklagen, falsche Angaben zur Sicherheit und zum Schutz der Daten gemacht zu haben. Neben den horrenden Bussgelddrohungen hängt über grossen Unternehmen, die ihre Marktmacht missbrauchen, in den USA nämlich auch immer das Damoklesschwert der Zerschlagung. Wohl auch deshalb plädierten Ende März Tim Cook von Apple und IBM-CEO Virginia Rometty für eine sinnvolle Regulierung und strengere Vorschriften für den Umgang mit persönlichen Daten. Noch weiter ging z.B. Salesforce-CEO Marc Benioff, selbst Internetmilliardär aus dem Silicon Valley, als er am WEF in Davos Facebooks Zerschlagung forderte. Es sieht so aus, als wüchse in den Chefetagen der Tech-Riesen das Gefühl, dass man die Geister, die man rief, nur noch mit drastischen Mitteln loswerden könne.

Nachzulesen unter:

https://www.theguardian.com/uk-news/cambridge-analytica
https://www.heise.de/thema/Facebook_Datenskandal
https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen
http://www.zeit.de/suche/index?q=Cambridge+Analytica+
https://www.nzz.ch/wirtschaft/die-rebellin-hinter-den-barrikaden-ld.1348569
http://www.spiegel.de/netzwelt/web/cambridge-analytica-firmenchef-alexander-nix-prahlt-mit-erpressungen-a-1198925.html
https://www.engadget.com/2018/03/21/mark-zuckerberg-apology-tour-2018
http://www.faz.net/aktuell/wirtschaft/diginomics/amerikanischer-senat-bestellt-facebook-chef-zuckerberg-ein-15514592.html
https://www.theverge.com/2018/3/20/17145200/brian-acton-delete-facebook-whatsapp
http://www.absatzwirtschaft.de/zusammen-mehr-als-5-millionen-abonnenten-trotzdem-loescht-musk-die-facebookseiten-von-spacex-und-tesla-128703
https://www.bild.de/unterhaltung/leute/jim-carrey/verkauft-seine-facebook-aktien-und-loescht-account-54730232.bild.html
https://futurezone.at/netzpolitik/max-schrems-facebook-wusste-von-illegaler-datenweitergabe/400008921
https://futurezone.at/netzpolitik/nutzerdaten-abgegriffen-facebook-droht-billionenstrafe/400007871
https://www.handelszeitung.ch/unternehmen/erste-investoren-verklagen-facebook
http://www.handelsblatt.com/unternehmen/it-medien/facebook-skandal-apple-chef-cook-fordert-mehr-datenschutzregeln/21111738.html
https://www.tagesanzeiger.ch/digital/daten/experten-fordern-die-zerschlagung-von-facebook/story/23677763

II. Neues in Sachen Staatstrojaner: Microsoft analysiert FinFisher

Dass Geheimdienste und Strafverfolgungsbehörden Rechner und Mobilgeräte mithilfe sogenannter Staatstrojaner infiltrieren, um Terroristen, Kriminelle oder auch nur Verdächtige auszuspionieren, ist keine Neuheit. Dass es dabei immer wieder zum Überschreiten legaler Grenzen und Missbrauchsfällen kommt, auch nicht. Auf der anderen Seite arbeiten IT-Sicherheitsfirmen und Betriebssystementwickler daran,

Sicherheitslücken zu schliessen, die es (Staats-) trojanern ermöglichen, sich auf Geräten einzunisten mit deren Hilfe Daten und Datenverkehr abgegriffen oder gar das ganze Gerät ferngesteuert werden kann.

FinFisher, der Staatstrojaner des gleichnamigen deutsch-britischen Zulieferunternehmens für Sicherheitsbehörden, spielt laut Sicherheitsforschern von Microsoft hinsichtlich seiner Tarnung, Komplexität, Raffinesse und Adaptionsfähigkeit «in einer ganz eigenen Liga». Anfang März gab Microsoft bekannt, FinFisher bis ins Detail auseinandergenommen und analysiert zu haben. Mit den gewonnenen Erkenntnissen sei die Advanced Threat Protection (ATP) der Microsoft-Software Defender sowie die von Windows 365 verbessert worden. Damit andere Entwickler und Security-Experten ihre Software optimieren und die Ausbreitung von Malware eindämmen können, stellten die Microsoft-Security-Fachleute ihre Erkenntnisse auf Microsofts Cloudblogs.

Nachzulesen unter:

https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

https://www.heise.de/security/meldung/Microsoft-vs-FinFisher-Windows-Defender-ist-gegen-den-Staatstrojaner-gewappnet-3988226.html

https://www.extremetech.com/computing/265074-microsofts-windows-defender-atp-good-enough-catch-law-enforcement-spyware

http://www.zdnet.com/article/microsoft-windows-defender-can-now-spot-finfisher-government-spyware

https://cyware.com/news/microsoft-windows-defender-can-now-spot-finfisher-government-spyware-baec1989

III. Russische APT28-Hacker monatelang im Datennetz der deutschen Bundesverwaltung

Die Meldung des deutschen Innenminsteriums am Abend des 28. Februar 2018 klang unspektakulär und nüchtern: «Wir können bestätigen, dass derzeit durch das BSI (Anm. d. Verf.: Bundesamt für Sicherheit in der Informationstechnik) und die Nachrichtendienste ein IT-Sicherheitsvorfall untersucht wird, der die Informationstechnik und Netze des Bundes betrifft.» Vorher hatte die deutsche Nachrichtenagentur dpa berichtet, dass sich Cyberspione der immer wieder mit der russischen Regierung in Verbindung gebrachten Hackergruppe ATP28 mittels erfolgreicher Angriffe auf das deutsche Aussen- und das Verteidigungsministerium Zugang zum kompletten Datennetz der Bundesregierung verschafft haben. Es sei ihnen gelungen, das Netz zu infiltrieren, Malware einzuschleusen und Daten zu stehlen –

offenbar während eines Zeitraums von einem Jahr. Wie tief die Hacker in die Systeme vorgedrungen sind und welchen Schaden sie anrichten konnten, sei aktuell Gegenstand intensiver Abklärungen. Im Gegensatz zur nüchternen Medienerklärung könnten sich die «als isoliert und unter Kontrolle gebrachten Angriffe» also als Super-GAU der deutschen Regierungsinformatik herausstellen. Zumal ATP 28 auch als verantwortlich für den Hack auf das bis dahin als sicher geltende Netz des deutschen Bundestags 2015 identifiziert worden ist. Die Nachrichtenlage zum Thema ist leider dürftig: Alle grossen Tageszeitungen berichteten meist nur einmalig über den Vorfall. Lediglich heise.de deckte das Thema länger als eine Woche ab.

Nachzulesen unter:

http://www.faz.net/aktuell/russische-hacker-dringen-in-deutsches-regierungsnetz-ein-15472050.html
http://www.zeit.de/digital/datenschutz/2018-02/hacker-dringen-in-deutsches-regierungsnetz-ein
http://www.netzwoche.ch/news/2018-03-01/hacker-greifen-deutsche-regierung-an
http://www.inside-it.ch/articles/50371
https://www.tagesanzeiger.ch/ausland/europa/deutsche-regierung-liess-hacker-monatelang-gewaehren/story/10128411
https://www.nzz.ch/international/der-hackerangriff-auf-die-deutsche-regierung-dauert-an-ld.1361876
https://www.heise.de/newsticker/meldung/Sicherheitskreise-Hacker-drangen-in-deutsches-Regierungsnetz-ein-3983510.html
https://www.heise.de/newsticker/meldung/Bundeshack-Angriff-laut-de-Maiziere-technisch-anspruchsvoll-und-lange-geplant-3984840.html
https://www.heise.de/newsticker/meldung/Kommentar-zum-Bundeshack-Schluss-mit-Schlangenoel-und-Monokultur-3985144.html
https://www.heise.de/security/meldung/Bundeshack-Daten-sollen-ueber-Outlook-ausgeleitet-worden-sein-3987759.html

IV. Besser Bitcoins auf dem Konto als Aliens auf dem Schirm – Cryptomining und die teils bizarren Folgen

Das Schürfen virtueller Währungen kostet nicht nur enorme Mengen an Energie, sondern setzt solche auch in immer kreativeren Formen frei. So schätzte der digiconomist am 27. März 2018 den Jahresenergieverbrauch für Cryptomining auf ca. 58 Terrawattstunden pro Jahr, was dem Jahresverbrauch der Schweiz schon sehr nahe kommt. Eine einzige Bitcoin-Transaktion verbraucht aktuell zudem mehr als viermal so viel Energie wie 100.000 Transaktion des Kreditkartenunternehmens VISA. Weil das Netzwerk zum grössten Teil mit Strom aus Kohlekraftwerken läuft, ist die CO_2-Bilanz schlichtweg eine Katastrophe.

Katastrophal wirkt sich das Cryptomining auch für die Forscher des SETI (Search for Extraterrestrial Intelligence) aus, die verzweifelt auf neue, leistungsfähige Grafikkarten

warten, um nach Signalen von Ausserirdischen zu lauschen. Da sich die Karten mit den neuesten GPUs (Graphics Processing Units) auch wunderbar zum Minen eignen, haben die Cryptominer den Markt schier leergekauft und die Forscher müssen warten. Unterdessen hat der in Miami beheimatete Zigarrenhersteller «Rich Cigars» angekündigt, sein Geschäft mit dem Rauch einzustellen und zukünftig auch auf das aggressive Schürfen von Kryptowährungen zu setzen – was der Pennystock-Aktie einen Sprung von 2000% bescherte.

Kryptomineure, die keine Lust auf hohe Stromrechnungen haben, schleusen Miningsoftware über Plattformen wie github oder die vielbesuchten Pornoseiten auf die Rechner unbedarfter User. Wie das Onlinemagazin gizmodo kürzlich berichtete, nutzen manche auch einfach die Tesla-Cloud. Das in diesem Rahmen zitierte Statement von Gaurav Kumar, CTO der Sicherheitsfirma RedLock, fasst den Trend zusammen: «The recent rise of cryptocurrencies is making it far more lucrative for cybercriminals to steal organizations' compute power rather than their data.»

Nachzulesen unter:

https://digiconomist.net/bitcoin-energy-consumption
https://futurezone.at/digital-life/bitcoin-mining-behindert-suche-nach-ausserirdischem-leben/400003853
https://futurezone.at/b2b/zigarrenhersteller-steigt-auf-bitcoin-mining-um/302.226.171
https://www.heise.de/security/meldung/Mining-Trojaner-lauern-auf-Github-4000476.html
https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247
https://motherboard.vice.com/en_us/article/9kzyv7/porn-sites-are-doing-the-most-cryptocurrency-coinhive-browser-mining

In eigener Sache: Neu im SWITCH-CERT Security Blog

A Day in the Life of nic.ch

https://securityblog.switch.ch/2018/03/20/a-day-in-the-life-of-nic-ch/

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.