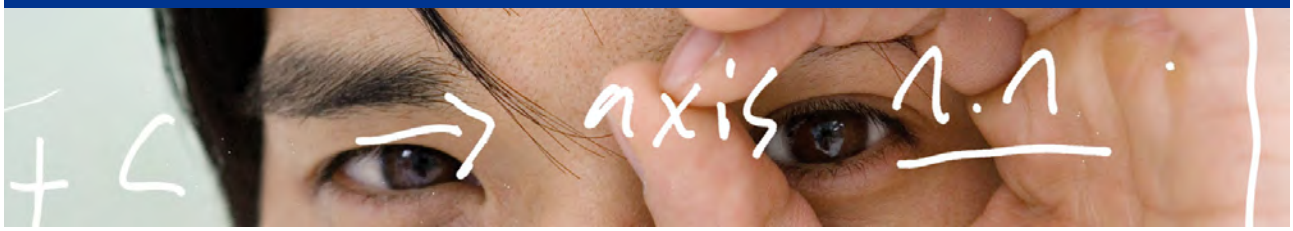
SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

April 2014



SWITCH

I. NSA und die Reaktion der grossen Player: Wer sagt die Wahrheit?

Wirtschaftliche Schadensbegrenzung – das ist momentan das Einzige, was Internetfirmen in den USA bewegt. Seit den Enthüllungen der vergangenen Monate wurden viele Konzerne «geoutet» als mehr oder weniger bereitwillige Komplizen der National Security Agency (NSA). Um vergraulte Geschäfts- und Privatkunden wieder für sich zu gewinnen und Vertrauen gutzumachen, geben jetzt vor allem die grossen Player Gas – als da wären Apple, Google, Facebook, AOL, Microsoft, Yahoo und IBM:
Er sei «verwirrt und frustriert», klagt Mark Zuckerberg den 1,2 Milliarden Facebook-Mitgliedern pathetisch sein Leid: Er habe sich persönlich bei Präsident Barack Obama über die heimlichen Spähaktionen der NSA beschwert. Die Regierung habe damit «Schaden für die Zukunft von uns allen angerichtet».

Eine Mischung aus Pathos und Praxisorientierung führt Google-Chef Larry Page ins Feld: Den Mailverkehr der Gmail-Nutzer werde man künftig doppelt verschlüsseln. Auf den eigenen Servern sowie per verschlüsselter https-Verbindung. Im Übrigen, liess Page jüngst die Netzgemeinde bei der TED-Konferenz in Vancouver wissen, sei er ernsthaft besorgt um Googles Hauptmission, den freien Informationszugang: «Ich

glaube nicht, dass wir in einer Demokratie leben, wenn wir unsere Nutzer vor der Regierung schützen müssen, aus Gründen, über die nie mit uns gesprochen wurde. Wir müssen wissen, was geschieht, welche Form von Überwachung die Regierung anwendet, wie und warum.» Den Unterschied zwischen guter und böser Überwachung zu erklären, dazu war Page allerdings nicht in der Lage.

IBM streitet derweil vehement ab, irgendetwas mit der NSA zu tun zu haben: Dafür hat IBMs Chef-Justiziar Robert Weber einen offenen Brief geschrieben, indem er versichert, man habe niemals Kundendaten oder Entschlüsselungscodes weitergegeben, geschweige denn irgendwelche Hintertürchen für Dritte in den eigenen Produkten eingebaut.

Ausgerechnet Yahoo – einer der wenigen «Big Player», der nicht freiwillig mit der US-Regierung kooperierte, sondern die gewünschten Informationen erst auf gerichtlicher Anordnung lieferte – hält sich bisher zurück mit grossen Ansagen.

Internetfirmen schnüffeln selbst in Kundendaten

Alles ohnehin nur Show, glaubt man den Aussagen des Leiters der NSA-Rechtsabteilung Rajesh De. Die Internetkonzerne hätten von der Spionage gewusst, sogar «volle Unterstützung» geleistet, gab Re gegenüber «Privacy and Civil Liberties Oversight Board» des US-Senats aus. Das beträfe den gezielten Zugriff auf Meta- und Kommunikationsdaten von Kunden ebenso wie das generelle Anzapfen des Internetverkehrs im Firmennetz, schreibt der britische «Guardian».

Eine gewisse Doppelmoral müssen sich die Konzerne auch nach den jüngsten Beobachtungen des IT-Forums «Heise» vorwerfen lassen: Die Spezialisten haben sich die Datenschutzbedingungen der US-Mailanbieter Microsoft, Apple, Google und Yahoo näher angesehen und festgestellt: Sie schimpfen über den Imageschaden durch die NSA-Spionage, nehmen sich aber allesamt das Recht heraus, nach Lust und Laune in den persönlichen Nachrichten und Daten ihrer Kunden rumzuschnüffeln oder diese an Dritte weiterzuleiten.

NSA fehlen noch 1,2 Milliarden Metadaten

Neuesten Gerüchten zufolge steht der NSA-Spionage-Zähler zurzeit auf rund sechs Milliarden Metadaten täglich. Bei einer Weltbevölkerung von knapp 7,2 Milliarden

keine schlechte Quote. Man darf davon ausgehen, dass die Mehrzahl der 7,2 Milliarden unverdächtig im Web surft oder telefoniert. Und man darf davon ausgehen, dass deren persönliche Kommunikationsdaten brüderlich geteilt werden unter den verbündeten «Big Five»-Geheimdiensten Grossbritannien, Kanada, Australien und Neuseeland. Abgesehen davon hat James Clapper, nationaler US-Geheimdienstchef, gerade zugegeben, dass man auch die eigenen Bürger ohne richterliche Erlaubnis überwacht habe. Dank einer Gesetzeslücke. Und wenn man schon legal Daten sammeln kann, dann könne es ja auch nicht so «verboten» sein, diese Daten zu durchsuchen. Immerhin war das Prozedere dann einwandfrei, wenn man tatsächlich etwas Verdächtiges gefunden habe, berichtet Clapper. Zumindest dem «systematischen Sammeln von Daten über die Telefongewohnheiten der Amerikaner» will Präsident Obama jetzt angeblich ein Ende bereiten. Das sollen künftig auch nicht mehr NSA-Mitarbeiter erledigen, sondern die, die an der Quelle sitzen: die US-Telefonanbieter.

Nachzulesen unter:

http://gmailblog.blogspot.de/2014/03/staying-at-forefront-of-email-security.html
http://www.politico.com/story/2014/03/barach-obama-tech-ceos-nsa-104881.html
http://asmarterplanet.com/blog/2014/03/open-letter-data.html
https://www.facebook.com/zuck/posts/10101301165605491?stream_ref=10
http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de
http://www.mobilegeeks.de/vertrauen-zerstoeren-dafuer-brauchen-wir-die-nsa-nicht/
http://www.nzz.ch/aktuell/international/auslandnachrichten/nsa-sammelwutsoll-gebremst-werden-1.18270453
http://futurezone.at/meinung/ueberwachen-koennen-wir-am-allerbesten/57.970.001
http://www.golem.de/news/geheimdienste-nsa-faengt-irakische-kommunikationsdaten-komplett-ab-1404-105521.html
http://www.wyden.senate.gov/download/?id=130BFF88-A3C0-4315-A23B-C4F96C499D9D&download=1

II. Europäischer Gerichtshof macht Weg frei für Websperren und Zensur

Europas Politiker zeigen sich zutiefst beunruhigt über die Entwicklungen in der Türkei. Dabei könnten die sich ruhig an die eigene Nase fassen: Just zu dem Zeitpunkt, an dem sich die ganze Welt über die Netzsperren der Türkei aufregt, hat der Europäische Gerichtshof (EuGH) in Luxemburg de facto sein «Ja» zur Einrichtung staatlicher Internetsperren gegeben. Internetaktivisten befürchten jetzt, das Urteil könnte staatlicher Internetzensur europaweit Tür und Tor öffnen.

Internetanbieter sind fortan verpflichtet, Inhalte im Netz zu sperren, wenn dadurch Urheberrechte in einem Mitgliedsland verletzt werden. Im konkreten Streitfall hatte sich der österreichische Provider «UPC Telekabel Wien» geweigert, die inzwischen stillgelegte Streaming-Seite «kino.to» auf Drängen des «Filmverleih Constantin» für alle Internetnutzer zu sperren.

Die Mär von der guten und der schlechten Zensur

Dabei greift man in vielen Ländern Europas schon längst zu solchen Sperren «auf Betreiben der Filmbranche», wie das Nachrichtenmagazin «Der Spiegel» schreibt. In Deutschland hatte man solche Filter gerade erst abgewandt und sich auf die Maxime «löschen statt sperren» geeinigt. In der Schweiz wünscht sich zumindest die Unterhaltungsindustrie auch eine solche Rechtslage, wie sie der EuGH geschaffen hat. Das behauptet der Zürcher Chaos Computer Club (CCCZH) mit Berufung auf eine Websperren-Wunschliste der «Swiss Anti-Piracy Federation». Die Sperrliste enthält diverse illegale Download-Seiten. Wer durch die CCCZH-Newseinträge der vergangenen Monate scrollt, bekommt schnell einen Eindruck davon: Die Zahl und Bandbreite derjenigen, die Webinhalte sperren, löschen und kontrollieren möchten, ist auch hierzulande recht gross. Das Problematische daran, findet der CCCZH: «Es gibt keine ‚gute' oder ‚schlechte' Zensur. [...] jede Form von Zensur führt zu Missbrauch.»

Ein typisches und aktuelles Beispiel dafür ist das Video einer US-Diplomatin, die mit deutlichen Worten auf die EU schimpft. Titel: «Fuck the EU». Besagtes Video ist so bekannt und beliebt – nur auf den Rechnern deutscher Staatsbediensteter ist es gesperrt. «Entweder gibt es Inhalte, die man nicht ansehen darf, weil sie illegal sind. Dann muss man sie löschen. Oder es gibt legale Inhalte. Dann gibt es keinen Grund, diese zu sperren», so ein Vertreter der Linksfraktion. Sie will nun von Bundeskanzlerin Angela Merkel wissen, warum hier gefiltert wird und wie dies technisch vor sich geht. Die Bundesregierung hat sich erstmal Bedenkzeit erbeten.

Weiterführende Infos:

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-03/cp140038de.pdf
http://www.anwalt24.de/beitraege-news/fachartikel/europaeischer-gerichtshof-provider-muessen-illegale-seiten-sperren-das-freie-internet-ist-gefaehrdet
https://www.ccczh.ch/News
http://www.heise.de/tp/artikel/41/41402/1.html

III. Zuckerberg setzt auf «Virtual Reality» als nächsten grossen Trend

Was will Mark Zuckerberg mit dem Virtual-Reality-Spezialisten «Oculus VR»? Und warum legt der Facebook-Chef dafür Wochen nach dem 19-Milliarden-Dollar-Kauf von WhatsApp direkt nochmal 2,3 Milliarden Dollar für das relativ unbekannte Start-up auf den Tisch? Oculus VR ist vor allem in Gaming-Kreisen ein Begriff – als Entwickler des 3D-Headsets «Oculus Rift». Bislang gibt es davon zwar nur den Prototypen der Computerbrille – der hält aber bereits grosse Teile der Gaming-Community in Atem. «Immersive Gaming» nennt sich das, was Oculus Rift Spielern erlaubt – das Eintauchen in die Spielwelt. Aber was hat das mit Facebook zu tun?

Geht es nach Mark Zuckerberg, wird das Headset *die* neue Kommunikationsplattform der Zukunft. «Das Unglaubliche an dieser Technologie ist, dass du das Gefühl hast, als wärst du tatsächlich an einem anderen Ort mit anderen Leuten», schreibt Zuckerberg auf seiner Facebook-Seite. Der 29-Jährige hält Virtual Reality für den nächsten grossen Trend nach mobilen Apps. Er will Oculus-Rift-Technologie für persönliche, nützliche und unterhaltsame Alltagsszenarien nutzen, «neue Welten für uns alle erschliessen».

Crowdfunding-Plattform «Kickstarter» machte Datenbrille erst möglich

Fans des Gaming-Headsets finden das alles andere als gut: Das Geld, mit dem «Oculus Rift» überhaupt erst entwickelt werden konnte, stammt nämlich teilweise von ihnen. 2012 konnten die Oculus-Macher gerade mal den zusammengeklebten Prototyp ihres Daten-Headsets vorweisen. Das Geld dazu sammelten sie über die Crowdfunding-Plattform «Kickstarter»: gut 2,5 Millionen US-Dollar Spenden. Dass sich ein von der Internet-Community «gesponsertes» Start-up jetzt von einem kommerziellen Anbieter aufkaufen lässt, hat den Zorn der Internetaktivisten erregt.

Oculus habe «die Chance, die sozialste Plattform aller Zeiten zu erschaffen und damit die Art und Weise zu verändern, wie wir arbeiten, spielen und kommunizieren», sagt Mark Zuckerberg. Als Beispiel nennt er virtuelle Kinobesuche zu zweit (und doch allein), virtuelle Klassenzimmer oder Arztbesuche. Fragt sich nur, wer ein vertrauliches Arztgespräch durch die Datenleitung seiner Internet-Brille schicken möchte.

Sicherheitslücken: Bloss nicht die Glass-Brille liegen lassen!

Zumal die Frage der Sicherheit bei Facebook traditionell eine untergeordnete Rolle spielt. Und auch Google, dessen Glass-Datenbrille direktes Konkurrenzprodukt ist, schenkt dem Thema erstaunlich wenig Beachtung: Gerade haben Professoren gezeigt, wie sich Angreifer aus wenigen Metern Entfernung in die Brille hacken können.

Seit einem Jahr sind Entwickler weltweit von Google aufgerufen, sich schicke Apps für die Brille auszudenken. Ausser streng formulierten Entwicklerrichtlinien hat der Konzern Cyberkriminellen allerdings wenig entgegenzusetzen, wie die kalifornischen Polytechnik-Studenten Mike Lady und Kim Paterson gerade bewiesen haben. Ihre Glass-App «Malnotes» soll theoretisch dabei helfen, Notizen zu machen. Tatsächlich enthält sie aber eine Malware, die bei deaktiviertem Brillendisplay aktiv wird, alle zehn Sekunden Fotos der Umgebung aufnimmt und an mögliche Angreifer sendet. Wer sich die App auf seine Brille geladen hat, merkt davon jedoch rein gar nichts. Auch nicht, wenn der Tischnachbar in einer unaufmerksamen Minute ein Schadprogramm auf dem Gerät installiert. Drum warnt Kim Paterson alle Google-Glass-Träger schon jetzt davor, ihre Brille unbeaufsichtigt liegen zu lassen.

Google verteidigte sich mit dem Hinweis darauf, die Virtual-Reality-Brille sei noch kein Mainstream-Gerät und der gefundene Fehler «keine grosse Sache». Umso schlimmer, schimpfen Datenschützer. Zudem seien die besten Datenschutzrichtlinien wertlos, wenn im Gerät selbst keine Sicherheitsvorkehrungen integriert sind. Angesichts dessen, dass die Virtual-Reality-Brille bei Datenschützern schon vor dem Verkaufsstart sehr umstritten ist und in den USA vielerorts schon eine «No Glass»-Politik gilt, in jedem Fall kein gutes Signal. Immerhin hat die «Malnotes»-Affäre auch ihr Gutes: Kim Paterson beendet ihr Studium im Frühjahr und nimmt danach eine Stelle bei Google an...

Mehr zum Thema:

http://www.oculusvr.com/blog/oculus-joins-facebook/
https://www.facebook.com/zuck/posts/10101319050523971
http://www.nytimes.com/2014/03/26/technology/facebook-to-buy-oculus-vr-maker-of-virtual-reality-headset.html
http://www.forbes.com/sites/andygreenberg/2014/03/18/researchers-google-glass-spyware-sees-what-you-see/
https://www.kickstarter.com/projects/hellobragi/the-dash-wireless-smart-in-ear-headphones

IV. Türkische Regierung verbannt YouTube und Twitter

Die «Ahs» und «Ohs» auf dem internationalen Parkett waren gross, als der türkische Ministerpräsident Ende März seinen Landsleuten den Internetzugriff verboten hatte:

erst auf den Kurznachrichtendienst Twitter, danach auch auf Googles Videodienst YouTube. Beide, so polterte Recep Tayyip Erdogan, seien eine Gefahr. Zudem hätten sich beide Plattformen geweigert, von türkischen Gerichten wegen «anhaltender Beleidigungen» beanstandete Beiträge zu löschen. Eine Überraschung ist die Zensurmassnahme nicht: Erdogan ist ein ausgewiesener Gegner der Meinungsfreiheit im Internet, hat den Internetzugang im Land seit 2011 schon mehrfach eingeschränkt.

YouTube und Twitter werden in der Türkei vielfach als Sprachrohr für Bürgerrechtler und Oppositionelle genutzt. Zu Beginn der Sperre konnten diese sich noch mit einfachen Tricks zur Umgehung der Sperre behelfen: Beispielsweise indem sie Googles freien DNS-Dienst nutzten. Mittlerweile funktioniert das jedoch nicht mehr: Seit Ende März leiten Internet-Provider und Mobilfunkanbieter offenbar den Zugriff auf IP-Adressen von Googles DNS-Servern auf eigene DNS-Server um. Von diesen werden dann manipulierte IP-Adressen für YouTube und Twitter zurückgegeben, so dass der Benutzer auf einer Fake-Seite landet.

Heute Twitter, morgen das World Wide Web

Wer jetzt aus der Türkei über einen freien DNS-Server die Twitter- oder YouTube-IP aufruft, wird auf eine von der türkischen Regierung betriebene Website umgeleitet. Auf die Art, warnen Sicherheitsexperten der US-Firma «Renesys», liesse sich das komplette Surf-Verhalten der türkischen Bevölkerung überwachen, ihre Rechner heimlich manipulierten oder kapern. Eine «neue und bedrohliche Wendung», deren Ausmass erst später messbar sein werde: «Wenn Twitter und YouTube heute blockiert werden können, wie steht es dann morgen um Gmail oder Dropbox?» Renesys spricht dabei vor allem von möglichen ökonomischen Schäden für die Türkei als Land, das innerhalb einer Internet-abhängigen Welt ökonomisch wachsen will. Das Vertrauen in die türkische Internetinfrastruktur für Firmen wie Bürger in- und ausserhalb der Türkei dürfte jedenfalls dahin sein.

Näheres dazu unter:

http://www.nzz.ch/aktuell/international/auslandnachrichten/die-tuerkische-regierung-blockiert-youtube-1.18272248
https://blog.twitter.com/2014/victory-for-free-expression-in-turkish-court
http://www.heise.de/mac-and-i/meldung/Bericht-Belgischer-Richter-zog-Web-Sperre-gegen-Apple-in-Betracht-2133804.html

http://www.renesys.com/2014/03/turkish-internet-censorship/
http://www.spiegel.de/netzwelt/web/erdogan-laesst-surfer-in-die-irre-klicken-a-961757.html
http://googleonlinesecurity.blogspot.de/2014/03/googles-public-dns-intercepted-in-turkey.html

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Warum haben Web-Applikationen so viele Schwachstellen und sind derart schlecht auf mögliche Sicherheitsrisiken getestet? Jeff Williams, Spezialist im Bereich Softwareentwicklung und –Security, geht den Ursachen auf den Grund und hat drei Vorschläge, wie sich die Situation verbessern lässt:

http://www.darkreading.com/application-security/flying-naked-why-most-web-apps-leave-you-defenseless-/d/d-id/1127875

Ein Jahr nach «APT1» gibt Kevin Mandia ein Update darüber, was seither passiert ist und was Organisationen tun sollten, um ihr Security-Gap zu verringern:

http://www.fireeye.com/blog/corporate/2014/04/apt1-the-state-of-the-hack-one-year-later.html

Forscher der Sicherheitsfirma «ReVuln» zeigen, wie man aktuelle Philips SmartTVs kompromittieren und sensitive Daten abziehen kann. Einmal mehr wird das niedrige Sicherheitsniveau im Internet-of-Things demonstriert:

http://securityaffairs.co/wordpress/23523/hacking/philips-smarttv-susceptible-serious-hack-according-revuln-experts.html

Dieser SWITCHcert Security Report wurde von Katja Locker und Frank Herberg verfasst.