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

Februar 2015

SWITCH

I. Der Angriff nach dem Angriff – Privatsphäre und der Terror von Paris

Es spricht nicht für den Zustand der Welt, dass sich inzwischen ein Muster herausgebildet hat, demzufolge nach jedem neuen Terroranschlag nach einer umfangreichen Ausweitung von Überwachungsmassnahmen und einer immer rigoroseren Einschränkung der Privatsphäre gerufen wird. So forderte beispielsweise der britische Premierminister Cameron eine Woche nach dem Pariser Attentat die vollständige Überwachung jeder Art von Telekommunikation einschliesslich des Internets. Es dürfe, so der Premier, «keine Kommunikationsmittel geben, die wir nicht lesen können.» Auch die Innenminister der EU wollen die Massnahmen gegen den Terror verschärfen und dazu neben der Einführung neuer auch die Wiederbelebung von bereits ad acta gelegter Überwachungsmassnahmen wieder aufnehmen.

Im Kern der Debatte stehen aus IT-Privacy-Sicht die Frage der Vorratsdatenspeicherung sowie die, ob Sicherheitsbehörden IT-Anbieter dazu zwingen können, bei der Verschlüsselung von Daten eine Hintertür für Behördenzugriffe einzubauen und offen zu halten.

Dabei hatte der Informationsbeauftragte der britischen Regierung - Christopher Graham - angemahnt, dass die Verschlüsselung der Kommunikation von Privatnutzern als wichtiger Garant privater Sicherheitsinteressen nicht kompromittiert werden dürfe. Auch der US-amerikanische National Intelligence Council (NIC) bezeichnete in einem auf 2009 datierten Dokument, das im Rahmen der Snowden-Veröffentlichungen bekannt wurde, Verschlüsselung als die beste Verteidigung, um private Daten zu schützen.
Der Politiker-Forderung, diesen Schutz aufzuheben, begegnet der Präsident und CEO der Internet Association, mit dem Statement: «Just as governments have a duty to protect the public from threats, internet services have a duty to our users to ensure the security and privacy of their data. That´s why internet services have been increasing encryption security.»

Nachzulesen unter:

http://www.nzz.ch/international/europa/britische-konservative-fordern-totale-ueberwachung-des-internets-1.18461345

https://netzpolitik.org/2015/239-anti-terror-massnahmen-nach-911-sind-nicht-genug-eu-innenminister-wollen-freiheitsrechte-weiter-einschraenken

http://www.spiegel.de/netzwelt/netzpolitik/charlie-hebdo-streitgespraech-ueber-vorratsdatenspeicherung-a-1012141.html

http://www.bankinfosecurity.com/obama-sees-need-for-encryption-backdoor-a-7809

http://futurezone.at/digital-life/us-report-verschluesselung-ist-zentral-fuer-privatsphaere/108.451.938

http://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks

http://futurezone.at/netzpolitik/eu-innenminister-mit-massenueberwachung-gegen-den-terror/110.881.788

II. Schönes neues e-Banking

Seit geraumer Zeit laufen zu besten Sendezeiten im österreichischen Fernsehen Werbespots für «George», das nach eigenen Aussagen «modernste Banking Österreichs». Wer die Spots sieht und sich unter mygeorge.at einklickt, fragt sich unwillkürlich, ob da Google, Facebook, PayPal oder ein anderer der großen Netzplayer die Bankenlandschaft der Alpennachbarn disruptiv erneuern will. Es zeigen sich bunte Bilder, Links und Apps für alle Endgeräte. Das Verblüffende daran: Es ist eben kein IT-Spinoff in die Finanzwelt. Genau diesem wollen nämlich die Verantwortlichen der Ersten Bank und Sparkassen mit George

zuvorkommen und zeigen, dass e-Banking auf der Höhe der Zeit nicht nur ein modernes Design braucht, sondern von Grund auf so anzulegen ist, wie eine Social Network-Seite. Aktuelle Umfragewerte belegen, dass die Finanzinstitute bezüglich Usability, Design und Spassfaktor grosses Aufholpotenzial gegenüber Facebook, Amazon und Co. haben, im Gegenzug aber von 75 bis 81 % ihrer Kunden als sicher und vertrauenswürdig eingestuft werden – Werte, von denen Facebook (3%) und Google (1%) nur träumen können.

Deshalb erscheint es auch nicht verwunderlich, dass das erkennbare Bemühen, eine e-Banking-Plattform an Social Media anzugleichen, nicht von allen Kundinnen und Kunden begeistert aufgenommen wird. Die Kommentare zu einem Artikel über George auf der Technologie-Seite futurezone.at reichen denn auch von freudiger Zustimmung bis zur glatten Ablehnung, in der sich auch das eben angesprochene Vertrauensdefizit der grossen Netzwerke widerspiegelt.

Finanzinstitute schauen sich derzeit sehr genau an, wie sich Technologien aus der digitalen Welt ins Banking integrieren lassen. Der Druck kommt hier nicht nur von der Konkurrenz aus der Finanzwirtschaft, sondern vor allem auch von Technologieanbietern wie Apple, Ebay und Google.

Auf dem Weg zu einem moderenen e-Banking und der Suche nach neuen Einnahmequellen ist die Analyse von Zahlungsverkehrsdaten denn auch für Schweizer Bankkunden schon lange beschlossene Sache. Diese werden so zukünftig beim e-Banking beispielsweise von persönlichen Rabattangeboten profitieren können.

Nachzulesen unter:

http://futurezone.at/produkte/erste-bank-startet-online-banking-nach-google-vorbild/108.093.119

http://www.dailymail.co.uk/sciencetech/article-2773349/Could-credit-score-soon-based-FACEBOOK-FRIENDS-Expert-predicts-future-banking-rely-social-networks.html

http://www.computerworld.ch/marktanalysen/studien-analysen/artikel/banken-wollen-paypal-co-paroli-bieten-66423

http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Postfinance-baut-ein-Schnaeppchenportal-auf/story/13044454

II. Gone in less than 60 seconds – Vom Blechpiraten zum Automotive-Data-Hacker

«You can lock your car, but if he wants it... it´s gone in 60 seconds» – so stand es auf dem Originalplakat für den Film «Die Blechpiraten» zu lesen, der 2000 mit Nicolas Cage unter dem Titel «Gone in 60 Seconds» neu verfilmt wurde. 15 Jahre später sind Autodiebstähle zwar immer noch aktuell, dazugekommen sind aber Hacks auf Fahrzeug- und Strassenverkehrsdaten aller Art. Das zeigten u.a. auch Jimmy Schulz und Rüdiger Hannig auf dem 31. Chaos Communication Congress (31C3) Ende letzten Jahres in Hamburg. Hannig zitierte im Laufe des Vortrags den Vorstandsvorsitzenden des VW-Konzerns Martin Winterkorn mit den Worten «Your car´s data are mine». Besorgte Lenker eines Fahrzeugs aus dem Konzern, mögen sich fragen, ob der Lenker des Konzerns einfach nur neutral darauf hinweisen wollte, dass ein Auto inzwischen eine Datenmine ist. Oder ob er die Daten, die ein Fahrzeug über sich und seine Lenker abliefert, wirklich a priori als sein Eigentum betrachtet.

Fakt ist: Nicht nur Fahrzeuge aus Winterkorns Konzern sammeln Daten, die via offener, standardisierter Schnittstellen an Konzernzentralen, Vertragsgaragen, Zulieferer, Smartphone-Hersteller und Netzbetreiber übertragen und von diesen analysiert, gespeichert und ggfs. weitergegeben werden. Während die Generierung der Daten bislang im Fahrzeug in einem abgeschlossenen System erfolgt war, öffnen unverschlüsselt sendende Black Boxes, wie z.B. Fahrtenschreiber oder Versicherungsrecorder, diesen internen Datenbus und machen ihn damit für Hackerangriffe zugänglich (siehe Security Report vom Oktober 2014). Anschaulich erklärt ist dies auch in einem neuen Awareness-Video der Universität des Saarlands (siehe Vimeo-Link). Die Plattform hackernews.com sieht mehr als zwei Millionen US-amerikanischer Autos, die mit einem drahtlos funkenden Dongle ihrer Versicherung ausgerüstet sind, als akut hack-gefährdet. Aber auch beispielsweise elektronische Reifendruck-Kontrollsysteme können für Angriffe auf die Privatsphäre genutzt werden. An der TU Wien hat man daher zwischenzeitlich damit begonnen, Strategien zu entwickeln, mit denen sich Autos irgendwann selbstlernend gegen Hackerangriffe schützen sollen. EU-Digitalkommissar Günther Oettinger warnte derweil kürzlich die deutschen Autobauer: «Wir brauchen (gegenüber den USA und

Südkorea) eine digitale Aufholjagd. [...] Wer die Daten hat, hat die Macht. Und Autos und Autofahrer liefern besonders attraktive, wertvolle Daten.»

Nachzulesen unter:

http://vimeo.com/111822896

http://www.idgconnect.com/blog-abstract/8344/global-car-makers-join-data-race

http://blogs.strategyanalytics.com/AMCS/post/2014/11/03/Consumers-will-expect-greater-transparency-regarding-vehicle-data-extraction-interpretation-and-sharing.aspx

http://www1.wdr.de/fernsehen/ratgeber/servicezeit/sendungen/reifendruck106.html

http://www.heise.de/security/meldung/TU-Wien-will-Autos-vor-Hacking-Angriffen-schuetzen-2483552.html

http://thehackernews.com/2015/01/progressive-snapshot-device-hacking-car.html

http://www.heise.de/newsticker/meldung/EU-Kommissar-Oettinger-Deutsche-Autobauer-muessen-bei-Vernetzung-Tempo-erhoehen-2532487.html

III. Microsoft vs. Google und umgekehrt – eine biblische Sehschwäche?

Ohne die weltanschauliche Neutralität des Security-Reports verlassen zu wollen, drängt sich einem beim Blick auf die Auseinandersetzung zwischen Google und Microsoft um die Behebung von Sicherheitslücken doch das biblische Gleichnis von jenem Mann auf, der den Splitter im Auge seines Gegenübers moniert, ohne wahrzunehmen, dass er selbst von einem Balken im eigenen Auge in seiner (Welt-) Sicht stark eingeschränkt wird.

Zu den Fakten: 2012 hatte Microsofts damaliger CEO Steve Ballmer den höchst polarisierenden Politik-Berater Mark Penn nach Seattle geholt, der mit der ebenso polarisierenden PR-Kampagne «Scroogled» Googles Umgang mit Nutzerdaten anzuprangern versuchte. Was in der US-amerikanischen Politik vermeintlich zu funktionieren scheint, ging jedoch in der IT-Welt nach hinten los – was letztlich auch dazu führte, dass die Kampagne Anfang des Jahres stillschweigend eingestellt wurde.

Denn zum einen überzogen User wegen der eher unkomischen, teilweise auch plagiativen Sujets Microsoft massiv mit Spott und Häme. Zum anderen holte Google zum Gegenschlag aus. Unter dem Namen «Project Zero» startete der Suchmaschinen-Gigant im Juli 2014 eine Initiative, um nach eigenen Angaben das

Internet sicherer zu machen. Dabei spürt Google Sicherheitslücken in Software auf, informiert zunächst die jeweiligen Hersteller vertraulich und gibt ihnen 90 Tage Zeit, entsprechende Patches zu entwickeln. Ist bis zur Deadline kein Patch einsatzfähig, veröffentlicht Google die Sicherheitslücke.

Was auf den ersten Blick nach nobler Absicht aussieht, hat beim zweiten Hinsehen dennoch zwei Schönheitsfehler: Erstens ist die 90-Tage-Frist so gesetzt, dass nicht in jedem Fall ausreichend getestet werden kann, ob ein Patch wirklich mehr Sicherheit bringt. Und zum zweiten – und da kommt der Vergleich mit Splittern und Balken ins Spiel – verweist Google rigoros auf Fehler vorzugsweise in Microsoft-Software (inzwischen aber auch in Apples OS-X), stellt aber keine Security-Updates mehr zur Verfügung um Sicherheitslücken in eigener Software, wie z.B. Webview, einer Kernkomponente zur Darstellung von Websites unter Android 4.3 «Jelly Bean», zu schliessen. Was Sicherheitsexperte Graham Cluley in seinem Blog wie folgt kommentiert: «Just imagine if Microsoft researchers gave Google 90 days to fix a WebView vulnerability in Android 4.3, and then released proof-of-concept exploit code. I wonder how Google would feel then?»

Nachzulesen unter:

http://futurezone.at/digital-life/microsoft-stellt-umstrittene-anti-google-kampagne-ein/108.473.001

http://www.golem.de/news/windows-google-enthuellt-dritte-sicherheitsluecke-in-drei-wochen-1501-111748.html

http://www.zdnet.de/88215782/microsoft-kritisiert-google-wegen-offenlegung-von-weiterer-windows-8-1-luecke

http://www.macworld.co.uk/news/mac-software/googles-project-zero-publishes-three-os-x-zero-day-vulnerabilities-3595374

http://www.security-insider.de/themenbereiche/plattformsicherheit/mobilesecurity/articles/472142

http://grahamcluley.com/2015/01/google-discloses-microsoft-windows-vulnerability

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Phil Zimmermann, der Vater von PGP und ZRTP, plaudert in einem Interview mit netzpolitik.org über Verschlüsselung, Geheimdienst-Überwachung und Krypto-Kriege:

https://netzpolitik.org/2015/netzpolitik-podcast-126-phil-zimmermann-ueber-verschluesselung-geheimdienst-ueberwachung-und-krypto-kriege/

Die European Union Agency for Network and Information Security (ENISA) hat einen 73-seitigen Report zum Thema «Privacy and Data Protection by Design» veröffentlicht.

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

Eine weltweite Liste von Information Security Konferenzen 2015 gibt's auf Concise Courses Cybersecurity Blog:

http://www.concise-courses.com/security/conferences-of-2015/

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