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

November 2015

SWITCH

I. Kein sicherer Hafen im Land of the Free: Der Europäische Gerichtshof beschränkt die Übermittlung von Daten in die USA

Das Urteil des Europäischen Gerichtshofs EuGH in Luxemburg glich einem Paukenschlag. Am 6. Oktober 2015 erklärte der EuGH die Safe-Harbor-Vereinbarung, in der die EU und die USA den Austausch personenbezogener Daten geregelt hatten, für ungültig. Eben deshalb, weil es in den Vereinigten Staaten nach Ansicht der Richter keinen sicheren Hafen für personenbezogene Daten von EU-Bürgern gäbe. Zwar hätten in der Safe-Harbor-Regelung mehr als 4.400 US-amerikanische Unternehmen zugesichert, die Daten europäischer Kunden adäquat zu schützen. Doch seien diese Firmen dazu verpflichtet, den Behörden Daten ohne Einschränkung auszuliefern, wenn die nationale Sicherheit, das öffentliche Interesse oder die Durchsetzung amerikanischer Gesetze dies erforderten. Da europäische Bürger zudem weder Zugang zu ihren in die USA übermittelten Daten hätten, noch deren Löschung beantragen könnten, schloss sich das Gericht der Meinung des Europäischen Generalanwalts Yves Bot an, dass in den Vereinigten Staaten von Amerika kein adäquater Datenschutz gewährleistet sei. Geltendes EU-Recht besagt aber, dass personenbezogene Daten nur dann in Drittländer übermittelt werden dürfen, wenn

dieser Schutz gegeben ist. Die Luxemburger Richter bemängelten weiter, dass eine Regelung, die es Behörden generell erlaubt, auf den Inhalt elektronischer Kommunikationsmittel zuzugreifen, dem Wesensgehalt des europäischen Grundrechts auf Achtung der Privatsphäre widerspreche.

Dabei hatte der österreichische Jurist Max Schrems (seinerzeit noch als Student) nach Veröffentlichung der Snowden-Dokumente im Zuge der NSA-Affäre zunächst nur Beschwerde gegen die Übermittlung seiner Daten von irischen auf US-amerikanische Facebook-Server eingereicht, worauf die irische Datenschutzbehörde mit Verweis auf das Safe-Harbor-Abkommen nicht eingetreten war. Nach dem nun gesprochenen Luxemburger Urteil erklärte die irische Datenschutzbeauftragte Helen Dixon, dass die Beschwerde nun mit der nötigen Sorgfalt geprüft werde. Dazu hat auch Facebook volle Kooperation angeboten.

Weniger konsensual zeigten sich die Vertreter der Vereinigten Staaten bei der Europäischen Union, die Bot und Schrems vorwarfen, von falschen Annahmen ausgegangen zu sein, da das NSA-Überwachungsprogramm PRISM gesetzlich genehmigt sei und «entsprechend strengen Kontrollen unterliege.» Tatsächlich steht (aus amerikanischer Sicht) zu befürchten, dass das Urteil eine Flut individueller Klagen gegen Internet-Unternehmen auslösen könnte, die die personenbezogenen Daten ihrer Kunden in den USA speichern – neben den AGFA-Riesen Apple, Google, Facebook und Amazon sind das mehr als 5.000 Firmen, für die das Ende von Safe-Harbor wohl auch gravierende wirtschaftliche Folgen hätte. So sieht das Handelsblatt deren Geschäftsmodelle generell in Frage gestellt, während die NZZ eine Chance für Schweizer Anbieter wittert: «Ausschliesslich national operierende Unternehmen könnten dank dem Swissness-Label Wettbewerbsvorteile erringen.»

Noch können Facebook und Co darauf verweisen, dass sie ihre Datentransfer- und speicher-Praxis beibehalten können, weil ihre Kunden mit der Zustimmung zu den Allgmeinen Geschäfts- und Nutzungsbedingungen die Übermittlung und Speicherung ihrer Daten in die USA akzeptiert haben. Ein starres Beharren auf dieser Position könnte aber letztlich dazu führen, dass die Zulässigkeit von AGBs und anderer Standardvertragsklauseln selbst auf den Prüfstand kommt. Dies berichtet zumindest tagesschau.de. Es könnte sein, dass aus dem anfänglichen Beschwerdelüftlein des Max Schrems ein Hurrikan werden könnte, der nicht nur den sicheren Hafen verwüstet, sondern den gesamten transatlantischen Datenverkehr in Frage stellt.

Nachzulesen unter:

http://www.nzz.ch/international/eu-richter-staerken-online-datenschutz-1.18625282
http://www.zeit.de/digital/2015-10/facebook-eugh-erklaert-safe-harbor-abkommen-fuer-ungueltig
http://www.zeit.de/digital/datenschutz/2015-10/safe-harbor-facebook-irland-ermittlungen
http://www.nzz.ch/digital/usa-attackieren-eugh-generalanwalt-ld.2236
http://www.handelsblatt.com/my/technik/it-internet/folgen-des-safe-harbor-urteils-attacke-auf-google-und-co/12506476.html
http://www.nzz.ch/international/wie-die-firmen-mit-dem-verschaerften-datenschutz-umgehen-1.18625546
http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=de
http://www.golem.de/news/nach-malware-infektion-apple-raeumt-den-app-store-auf-1509-116473.html
http://www.nzz.ch/sperrbildschirm-siri-ios-9-austricksen-ld.2138

II. Viren mal anders: Medizinische Geräte sind in grossem Stil online hackbar

Wenn vom Kampf der Ärzte gegen Viren und Bakterien die Rede ist, denkt man an HIV, Ebola und Vogelgrippe. Mit zunehmender Digitalisierung und Vernetzung der Medizin und ihrer Gerätschaften rücken nun vermehrt Viren und Trojaner in den Fokus. So berichteten The Register und computerworld.ch Ende September von einem Honeypot-Experiment der Sicherheitsforscher Erven und Collao. Über einen Zeitraum von sechs Monaten simulierten sie einen Magnetresonanz-Tomografen und einen Defribillator und mussten erstaunt mehrere Zehntausend Log-Ins registrieren, von denen über 55.000 erfolgreich waren. Aufgeschreckt von der Vielzahl der Angreifer dehnten sie ihre Untersuchungen in reales Umfeld aus und entdeckten alleine bei einem ungenannten grossen amerikanischen Healthcare-Anbieter mehr als 68.000 verwundbare Systeme, aus denen Hacker relativ einfach nicht nur Daten der Patienten und Informationen über das Spital stehlen könnten. Der Sicherheitsforscher Bill Rios hat am Beispiel einer Infusionspumpe gezeigt, dass sich auch lebenswichtige Systeme online manipulieren lassen, um z.B. Medikamentendosierungen zu verändern oder Blutkonserven unbrauchbar zu machen. Obwohl das ISC-Cert bereits 2013 vor Sicherheitslücken in medizinischen Geräten gewarnt hatte, ist seitdem offenbar wenig geschehen. Zum einen laufen die meisten Systeme noch unter Windows XP, zum anderen sind sich die Hersteller der Sicherheitsrisiken durch schlecht geschützte Systeme nicht bewusst oder ignorieren diese schlicht und einfach.

Nachzulesen unter:

http://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed
http://www.computerworld.ch/news/security/artikel/security-albtraum-medizinische-geraete-zu-tausenden-online-hackbar-68825/
http://www.zeit.de/digital/internet/2015-04/medizintechnik-krankenhaus-it-sicherheit
http://www.heise.de/ix/meldung/Gravierende-Luecken-in-medizinischen-Geraeten-2178432.html
http://www.t-online.de/computer/sicherheit/id_75604958/wegen-windows-xp-zehntausende-medizinische-geraete-angreifbar.html

III. Viren, gescannt: Gratis Anti-Virus-Programme fast so gut wie bezahlte

Anders als unter Punkt II geht es hier wieder ausschliesslich um ICT-Viren, bzw. um Programme, die diese erkennen und unschädlich machen – Virenscanner bzw. Anti-Virus-Programme. Diese sollten im Idealfall drei Kriterien erfüllen: Erstens einen wirksamen Schutz vor Viren und anderer Malware bieten, zweitens die Geschwindigkeit der Geräte, auf denen sie eingesetzt werden, so wenig wie möglich beeinträchtigen und drittens einfach zu benutzen sein. Das Angebot ist ziemlich gross und vielfältig. Entscheidungshilfen findet man auf den unten zitierten Seiten, die zwei grundlegende Erkentnisse zulassen: Der Einsatz von Virenscanner lohnt sich, denn der Testsieger filtert 98% aller Zero-Day-Attacken heraus. Bei bekannter Malware betrug die Schutzwirkung volle 100% – Zahlen, die auch ein Gratis-Programm erreicht, allerdings um den Preis einer spürbaren Verlangsamung des zu scannenden Systems. Der Bezahlsoftware-Testsieger erledigt seinen Job dagegen ohne Geschwindigkeitsverlust. Weitere Tests finden sich unter den nachstehend genannten Links.

Alternativ dazu bietet die Google-Tochter VirusTotal einen kostenlosen Dienst, um mit allen verfügbaren Scannern verdächtige Dateien und URLs auf Viren, Trojaner, Würmer und andere Malware zu untersuchen. VirusTotal ist in Form von Browser-Extensions, als Desktop- oder Mobilgeräte-App konzipiert und erlaubt auch das Aufspüren von False Positives, also Fehlalarmen, die von Virenscannern verursacht werden.

Nachzulesen unter:

http://www.n-tv.de/technik/Die-besten-Virenwaechter-fuer-Windows-7-article16054561.html
http://www.antivirus-programme-test.de/?kw=test%20virenschutz%202015&match_kw=1&campaign=1&network_type=2&network=1&ad_group=2&ad_text=5&lp_pool_id=6&gclid=ClOn_9elo8gCFUnlwgodLNIFMQ
http://www.antivirus-programme-test.de/?kw=bester%20virenscanner&match_kw=1&campaign=2&network_type=2&network=1&ad_group=14&ad_text=54&lp_pool_id=6&_$ja=cgid:1992071274%257Ctsid:30607%257Ccid:57186354%257Clid:4726158094%257Cnw:search%257Ccrid:56103698994%257Cbku:1&gclid=CKbM2LXBzsgCFUv3wgod9QkD5w
https://www.virustotal.com/de/about

IV. Lass hören, Buddy! Forscherteam der ETH Zürich vereinfacht Zwei-Faktor-Authentifizierung dank Sound-Erkennung

Weil ein Passwort auf einem Gerät Hackern die Arbeit sehr leicht macht, wird für einige sensible Online-Log-Ins, wie z.B. fürs e-Banking, eine sogenannte Zwei-Faktoren-Authentifizierung (2FA) angeboten. Dazu meldet sich ein Benutzer mit dem einen Gerät – zumeist dem Desk- oder Laptop-Rechner an und muss danach einen weiteren Code eingeben, der ihm via zweitem Gerät, z.B. Dongle oder Handy, zugestellt wird. Erst danach ist der Benutzer eingeloggt. Die meisten 2FA-Verfahren arbeiten dabei in einer Art «Master-Slave-Modus» mit dem Handy auf der Sklavenseite. Ein Reverse-Modus, bei dem das Handy die Masterrolle übernimmt, ist meist nicht machbar. Unabhängig davon steigern 2FA-Verfahren die Sicherheit bei Log-Ins gegenüber single-password-Verfahren auf einem Gerät erheblich. Dennoch verzichten vielen Nutzer darauf, weil ihnen eine 2FA-Routine offenbar zu aufwendig ist. So schreibt etwa WIRED: «But there is one big problem with it: it's really annoying. … For far too many people, this is just too big of a hassle, so they leave themselves open to attack.»

Zur Vereinfachung hat nun ein Forscherteam der ETH Zürich mit «Sound-Proof» ein 2FA-Verfahren entwickelt, beim dem die Eingabe eines zweiten Codes entfällt. Statt dessen zeichnen die im Erst- wie im Zweitgerät eingebauten Mikrophone automatisch die Umgebungsgeräusche auf und gleichen sie gegeneinander ab. Sind die empfangenen Soundprofile deckungsgleich, schliesst das System daraus, dass sich beide Geräte an einem gemeinsamen Ort befinden, und folgert daraus, dass bei diesen Bedingungen der Nutzer zum Log-In berechtigt ist. Dazu benötigt «Sound-Proof» keine Zusatzsoftware oder PlugIns auf dem Mastergerät, aber eine App auf dem

Handy: wer tiefer ins Thema einsteigen möchte, findet die detaillierte technische Dokumentation im Paper, das das Forscherteam zur Usenix-Konferenz 2015 eingereicht hatte unter dem zuunterst stehenden Link.

Kritik an «Sound-Proof» zielt zum einen darauf ab, dass bei den eingesetzten Geräten die Mikrofon-Aufzeichnung eingeschaltet und Hintergrundgeräusche erkennbar sein müssen. Zum anderen könnten sich gerade bei Log-Ins in öffentlichen Räumen, wie z.B. an einer Uni oder in einem öffentlichen WLAN-Bereich, Angreifer im gleichen Raum befinden und das System ad absurdum führen. Nikolaos Karapanos, Claudio Marforio, Claudio Soriente und Srdjan Capkun, die Entwickler von Sound-Proof, halten ein solches Setting aber für eher unwahrscheinlich.

Nachzulesen unter:

http://www.heise.de/security/meldung/Leichtere-Zwei-Faktor-Authentifizierung-per-Handy-2826973.html
http://www.wired.com/2015/08/noise-around-strengthen-passwords
http://futurezone.at/science/zwei-faktor-authentifizierung-sound-statt-code/147.290.001
https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-karapanos.pdf

V. Kritisch: Forscher finden Sicherheitslecks in 87% aller Android-Geräte

Haben Android-Geräte ein Sicherheitsproblem oder sind sie eines? Auch wenn diese Frage sicher sehr ketzerisch formuliert ist, so drängt sie sich dennoch auf, wenn man die Ergebnisse einer jüngst veröffentlichten Studie der University of Cambridge näher analysiert. Mit der eigenentwickelten App «Device Analyzer» haben die britischen Forscher ca. 20.000 Android-Handies und –Tablets untersucht und dabei festgestellt, dass seit 2013 mindestens 87% – teilweise gegen 100% – aller Android-Geräte mindestens eines von elf bekannten und als kritisch eingestuften Sicherheitslecks an Bord haben.

Die Forscher rügen zudem, dass Sicherheitsupdates zu spät beziehungsweise in viel zu grossen zeitlichen Abständen bereitgestellt und dann von den Mobile-Device-Nutzern erst noch per manuellem Update installiert werden müssen. Weit gravierender sei allerdings, dass weder Verbraucher noch Behörden oder Unternehmen bei der Anschaffung von Android-Geräten wissen, welche Hersteller welche von Google bereit gestellten Sicherheitspatches in ihre Android-Versionen integriert haben und welche

nicht. Deshalb haben sie auf der eigens eingerichteten Website androidvulnerabilities.org (Link unten) ein Sicherheits-Ranking der Android-Gerätehersteller veröffentlicht, das laufend aktualisiert werden soll. Wer dazu selbst einen Beitrag leisten und an der Studie teilnehmen möchte, kann sich auf der Website informieren und die App via Google Play Store auf seinem Android-Gerät installieren. Die Forscher sichern übrigens zu, dass persönliche Daten anonymisiert werden.

Nachzulesen unter:

http://www.golem.de/news/cambridge-studie-87-prozent-der-android-geraete-sollen-unsicher-sein-1510-116884.html
http://www.zdnet.de/88249099/studie-87-prozent-aller-android-geraete-haben-mindestens-eine-kritische-sicherheitsluecke
http://www.theguardian.com/commentisfree/2015/oct/18/were-all-casualties-holy-war-android-security-apple-john-naughton
http://www.theregister.co.uk/2015/10/12/android_patching_survey
http://androidvulnerabilities.org/press/2015-10-08

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.