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

März 2016

SWITCH

I. Tor-Schluss-Panik für eine Handvoll Dollars – Eine Universität hilft, Tor-Nutzer auszuspionieren

Als Andrew Carnegie, der zu seiner Zeit reichste Mann der USA, Teile seines in der Stahlindustrie gemachten Vermögens für den Aufbau der Carnegie Technical Schools spendete, um damit eine Berufsschule für die Töchter und Söhne der Pittsburgher Arbeiter zu schaffen, hätte er sich wohl kaum träumen lassen, dass sich diese Schule in nur einem Jahrhundert unter dem Namen Carnegie-Mellon-University (CMU) zu einer der teuersten Unis der westlichen Welt entwickeln würde. An deren renommierter School of Computer Science haben unter anderem Andreas von Bechtolsheim (Mitbegründer von Sun Microsystems), Charles Geschke (Mitbegründer von Adobe) und James Gosling, der Erfinder von Java, studiert. Diesen Hintergrund muss man im Bewusstsein haben, um zu verstehen, welche Wellen in der IT-Community die Nachricht geschlagen hat, dass ausgerechnet das Software Engineering Institute SEI eben dieser CMU dem FBI gegen eine Zahlung von mindestens einer Million US-Dollar geholfen haben soll, Tor-User zu deanonymisieren, um Drogenhändler der Handelsplattform Silk Road 2.0 zu identifizieren und dingfest zu machen. Das postete jedenfalls das

Tor-Projekt am 11. November im eigenen Blog. Ein Sprecher der Universität wies umgehend die Anschuldigungen mit der Forderung an das Tor-Projekt zurück, handfeste Beweise vorzulegen, um die Behauptungen zu stützen und beteuerte, dass ihm nichts von einer Bezahlung durch das FBI bekannt sei.

Mittlerweile hat der Prozess gegen einen gewissen Brian Farrell etwas mehr Licht ins Dunkel gebracht. Farrell nutzte nach Überzeugung der Anklage das Tor-Netzwerk, um auf dem illegalen Online-Marktplatz Silk Road Drogen zu handeln und konnte durch die Deanonymisierung identifiziert werden. Auf Antrag von Farrells Verteidiger wurde nun offen gelegt, wie das FBI zu seinen Erkenntnissen gelangt war: Das SEI der CMU betrieb tatsächlich Forschungen zur Deanonymisierung von Tor-Nutzern. Wie das FBI Kenntnis vom Forschungsprojekt erlangt hatte, bleibt zwar weiterhin ungeklärt. Dagegen ist deutlich geworden, dass das Forschungsprojekt nicht vom FBI in Auftrag gegeben und bezahlt worden ist, sondern vom Pentagon, also dem US-Verteidigungsministerium, das sich aber ebenso wie die Universität bezüglich der Auftragssumme in eisernes – angesichts der Historie des Gründervaters wohl eher stählernes – Schweigen hüllt.

Betroffenheit und Enttäuschung bei den Tor-Projektverantwortlichen löste die Stellungnahme des Richters zu ihrem Vorwurf aus, die Forschungsarbeiten untergrüben die Privatsphäre aller Tor-Nutzer. Richter Richard Jones widersprach dem mit dem Argument, dass Tor-Nutzer ihre öffentliche IP-Adresse freiwillig mit dem ersten Tor-Node teilen würden und deshalb nicht erwarten könnten, im Tor-Netzwerk eine Privatsphäre vorzufinden (reasonable expectation of privacy). Die Tor-Macher ihrerseits warfen dem Richter daraufhin vor, Sinn und Konzept des anonymen Surfens im Tor-Netzwerk nicht verstanden zu haben und versicherten, die von den SEI-Forschern aufgerissenen Lücken inzwischen geschlossen zu haben.

Nachzulesen unter:

https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
https://www.wired.de/collection/latest/die-carnegie-mellon-university-hat-angeblich-fuer-geld-das-tor-netz-gehackt
http://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds
http://www.golem.de/news/silk-road-verfahren-tor-nutzer-koennen-keine-privatsphaere-erwarten-1602-119388.html
https://de.wikipedia.org/wiki/Carnegie_Mellon_University
http://www.zeit.de/digital/datenschutz/2016-02/darknet-pentagon-bezahlt-forscher-angriff-auf-tor
https://blog.torproject.org/blog/statement-tor-project-re-courts-february-23-order-us-v-farrell

II. Crypto Wars 3.0: Bekommt das FBI die Lizenz zum Stöbern oder kann sich Apple erfolgreich gegen das Entsperren sperren?

Für Juristen und Ethiker ist das Prinzip, nach dem ein rechtlich geschütztes höherwertiges Gut im Falle eines Konfliktes dem geringerwertigen vorzuziehen ist, eine «Güterabwägung». Für Tim Cook und Apple ist es derzeit ein Dilemma. Denn was so einleuchtend einfach klingt, wird extrem problematisch, wenn zwei Seiten für sich in Anspruch nehmen, das höherwertige Gut zu verteidigen. Dann stellt sich die Frage: «Welches ist das höherwertige, welches das geringerwertige Gut?» nicht nur im unter I. beschriebenen Tor-Fall, sondern auch in der aktuellen Auseinandersetzung zwischen dem FBI und Apple. Und es hätte nicht einmal Donald Trumps Aufruf zum Apple-Boykott bedurft, um daraus einen medialen Hype zu machen, der uns vermutlich noch eine Zeit lang begleiten dürfte.

Deshalb hier kurz noch einmal die Faktenlage: In einem Urteil vom 16. Februar 2016 ordnete Richterin Shery Pym an, dass Apple das iPhone 5c von Syed Riszwan Farook entsperren müsse. Der hatte gemeinsam mit seiner Frau im Dezember 2015 im kalifornischen San Bernardino 14 Menschen getötet. Im Polizeieinsatz wurde das Paar erschossen, doch weil die Ermittler des FBI untersuchen wollen, ob Farook mit der Terrororganisation Islamischer Staat oder anderen militanten Gruppen in Verbindung stand, fordern sie von Apple ein Update für iOS, das ihnen ermöglichen soll, die Verschlüsselung zumindest dieses einen Smartphones aufzuheben.

Cook und Apple befürchten allerdings, damit einen Präzedenzfall zu schaffen, der einen Dammbruch nach sich ziehen würde. Tatsächlich hat das FBI Apple in eine perfide Zwickmühle manövriert: Der Fall ist in den USA hochemotional, der bislang nicht nachgewiesene, dennoch kolportierte Terrorverdacht erhöht den politischen, medialen und öffentlichen Druck, die Informationen auf dem Smartphone einzusehen. Das aber kann vom Attentäter selbst nicht mehr entsperrt werden, weil ihn die Polizei erschossen hat. Bleibt also nur der Weg über Apple. Der iPhone-Hersteller sieht sich indes einem gespaltenen Publikum gegenüber: Nicht nur der republikanische Präsidentschaftskandidat und blondierte Politpolterer Trump, sondern auch andere Politiker, IT-Grössen wie Bill Gates und 51% (!) der Teilnehmer einer eiligst durchgeführten Umfrage des

PEW Research Centers U.S. Politics & Policy plädieren dafür, das iPhone des Attentäters zu entsperren.

Demgegenüber befürchten die meisten grossen IT-Unternehmen und Politiker wie der demokratische Senator Ron Wyden, dass eine Software zum Entsperren von iPhones die Online-Sicherheit für ‚Millionen Amerikaner' gefährden könnte. Inzwischen häufen sich Berichte darüber, dass nicht nur das FBI, sondern auch weitere Strafermittler in den ganzen USA in anderen Fällen Anträge auf Entsperrung beschlagnahmter Smartphones einreichen. Ein New Yorker Staatsanwalt alleine würde gerne mehr als 170 iOS-Geräte entschlüsselt sehen.

Inzwischen hat Apple formell Einspruch gegen die Anordnung von Richterin Pym eingelegt, die mit dem «All Writs Act», einem aus dem 18. Jahrhundert stammenden Gesetz, begründet ist. Mit der Argumentation, dass die Anordnung die in der Verfassung garantierte Redefreiheit aushebele und der Kongress eine Gesetzgebung für solche und ähnliche Fälle schon beraten, aber nicht angenommen habe, will Apple notfalls bis zum Obersten Gericht ziehen. Aktuell bekommt der Konzern aus Cupertino dafür Schützenhilfe durch ein Urteil eines New Yorker Richters. Dieser hatte am 29. Februar den bereits Monate zurückliegenden Antrag der Strafverfolgungsbehörden auf Entsperrung eines iPhones in einem Drogendelikt mit der Begründung abgewiesen, dass der All Writs Act keine angemessene Grundlage für ein solches Begehren sei. Man muss also davon ausgehen, dass der Fall noch lange nicht zu den Akten gelegt werden kann.

Nachzulesen unter:

http://www.faz.net/aktuell/wirtschaft/macht-im-internet/donald-trump-ruft-zum-apple-boykott-auf-14080844.html
http://www.heise.de/newsticker/meldung/US-Gericht-Apple-soll-bei-Entsperren-von-iPhone-nach-Anschlag-helfen-3107411.html
http://www.ft.com/intl/cms/s/2/3559f46e-d9c5-11e5-98fd-06d75973fe09.html#axzz41ZdlaHHP
http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/2
http://derstandard.at/2000031344911/Donald-Trump-Was-bildet-sich-Apple-eigentlich-ein
http://www.heise.de/security/meldung/Streit-ueber-iPhone-Entsperrung-FBI-will-von-Apple-angeblich-in-weiteren-Faellen-Unterstuetzung-3115360.html
https://www.washingtonpost.com/news/post-nation/wp/2016/02/26/a-locked-iphone-may-be-the-only-thing-standing-between-police-and-this-womans-killer/?tid=sm_tw
http://www.heise.de/ct/artikel/Crypto-Wars-3-0-Hintergruende-zu-dem-Fall-Apple-vs-FBI-3116395.html
http://www.zdnet.com/article/fbi-director-iphone-unlock-case-will-be-instructive-to-other-courts/
http://www.nzz.ch/international/amerika/apple-fbi-iphone-1.18701470
http://www.nzz.ch/international/apple-muss-fbi-bei-drogenfall-nicht-beim-iphone-knacken-helfen-1.18704079

III. Tödliche Viren im Krankenhaus: Erpressungstrojaner Locky legt auf seinem «Siegeszug» komplette Kliniken lahm (und nicht nur die)

Als in diesem Februar von Viren und zeitweise von mehr als 5.000 Neuinfektionen pro Stunde die Rede war, ging es nicht um eine akute Grippewelle, sondern um einen Comupterschädling, der sich seit seiner Entdeckung mit rasender Geschwindigkeit ausgebreitet und dabei weder Krankenhäuser noch das Fraunhofer-Institut Bayreuth verschont hat: Der Kryptolocker «Locky» wird vom britischen Sicherheitsexperten Kevin Beaumont als «kriminelles Meisterstück» bezeichnet, weil er zum einen in vielen Sprachen sein Unwesen treibt, sich zum anderen nicht nur in E-Mail-Anhängen in Form von Word- oder Excel-Files versteckt, sondern sich auch via Drive-By-Infektionen (mehr dazu hier https://www.switch.ch/saferinternet) von legitimen Webseiten weiterverbreitet und sogar Laufwerke erreichen kann, die zum Zeitpunkt der Infektion nicht mit dem lokalen Laufwerk gemapped waren.

Inzwischen zeigen Infektionen, die via Javascript-Anhänge und sogar als Fax getarnt vonstatten gehen, wie breit angelegt die Locky-Angriffswelle tatsächlich ist.

Dramatische Auswirkungen hat das Virus besonders dort, wo Ärzte und medizinisches Personal gegen Real-World-Viren kämpfen. So wurden Mitte Februar nicht nur die IT-Systeme des Lukaskrankenhauses im westdeutschen Neuss komplett ausser Gefecht gesetzt, sondern alleine in Nordrhein-Westfalen noch mindestens zwei weitere Kliniken Opfer der Cyber-Erpresser. Kurz darauf wurde bekannt, dass die IT des Hollywood Presbyterian Medical Centers in Los Angeles am 5. Februar von einem Kryptolocker ins Cyber-Out befördert wurde und erst 12 Tage später wieder funktionierte, nachdem die Klinik den Erpressern 40 Bitcoins (ca. 16.000.- CHF) ins Darknet geschickt hatte.

Nachzulesen unter:

http://www.golem.de/news/krypto-trojaner-locky-mehr-als-5-000-infektionen-pro-stunde-in-deutschland-1602-119247.html
http://www.idigitaltimes.com/new-locky-ransomware-virus-spreading-alarming-rate-can-malware-be-removed-and-files-512956
http://www.golem.de/news/ransomware-locky-kommt-jetzt-auch-ueber-javascript-1602-119331.html
http://www.heise.de/security/meldung/Neue-Virenwelle-Krypto-Trojaner-Locky-tarnt-sich-als-Fax-3117249.html
http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html

http://www.rp-online.de/nrw/staedte/neuss/hackerangriff-auf-lukas-krankenhaus-in-neuss-virus-noch-nicht-gebannt-aid-1.5767907
http://www.heise.de/newsticker/meldung/Ransomware-Neben-deutschen-Krankenhaeusern-auch-US-Klinik-von-Virus-lahmgelegt-3103733.html
http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

IV. Algorithmus, übernehmen Sie! Big Data und Automated Law Enforcement

Wenn das eigene Auto eine Geschwindigkeitsübertretung feststellt, die Busse berechnet und automatisch vom Konto des Fahrers an die Polizei überweist oder bei krassen Übertretungen sich selbst abschaltet, dann klingt das zunächst nach eher schlechter Science Fiction. In Tat und Wahrheit werden solche Automated Law Enforcement Modelle nicht nur in Juristen- und Polizeikreisen diskutiert, sondern zumindest in ersten Ansätzen installiert. Sensoren und GPS im Auto erfassen heute schon jede Bewegung sogenannter Connected Cars. Automatische Erfassungssysteme für Kennzeichen und Verkehrsüberwachungskameras sind nicht nur an Grenzübergängen, sondern auch entlang der Autobahnen in vielen Ländern Europas und in der Schweiz installiert und im Dienst. Und Baumaschinenverleiher stellen schon seit einiger Zeit ihre Bagger, Radlader und Kräne per Fernsteuerung ab, wenn der Baggerführer nach der Arbeitszeit legale oder nicht-legale Überstunden machen will, die nicht im Mietvertrag vorgesehen sind. Von diesem aktuellen Stadium bis zur automatischen Strafverfolgung braucht es eigentlich nur noch ein Go! der Verantwortlichen.

Bereits seit 2011 sammelt die Kantonspolizei Thurgau Erfahrungen mit Kontrollschild-Scannern. Inzwischen sind mindestens acht weitere Kantone bekannt, die jedes Fahrzeugkennzeichen scannen, das über die Autobahn bewegt wird, um gestohlene oder zur Fahndung ausgeschriebene Fahrzeuge herauszufiltern. Ergibt der Abgleich keinen Treffer, werden die Daten wieder gelöscht.

Dänemark wird im Lauf des Jahres 2016 an jedem Grenzübergang systematisch und lückenlos alle Fahrzeugkennzeichen erfassen und abgleichen, die Daten aber mindestens 1 Monat speichern. Da deutsche und dänische Polizisten gemeinsam Streife fahren, befürchten Datenschützer, dass das deutsche Verbot der «anlassfreien Aufzeichnung von Autokennzeichen» auf dem kurzen Dienstweg

umfahren wird. Auch weiter westlich entwickelt sich Automated Law Enforcement zum wichtigen Thema. So warnt der Autor Jonny Evans auf Computerworld.com, vor Connected Cars, weil diese a) gehackt werden könnten. b) Connected Cars könnten Serviceleistungen auch gegen den Willen des Fahrers erzwingen oder Garantieleistungen durch die Dokumentation von Fehlverhalten zu ungunsten des Besitzers beeinträchtigen. c) Auch Evans weist auf die Gefahr hin, dass der lange Arm des Gesetzes vor allem in Connected Cars hineinreicht. d) Neben dem Kommissar sieht Evans aber auch Spitzel mitreisen, die im Auftrag von Versicherungen Fehlverhalten des Versicherten aufspüren und weitermelden, damit diese Gründe zur Leistungsverweigerung im Schadensfall bzw. zur Anpassung der Kosten für die Police (der Versicherung, nicht der Ordnungshüter) geliefert bekämen. e) Und schliesslich warnt Evans davor, dass mit dem Auto auch persönliche Daten beim Verkauf den Besitzer wechselten und niemand weiss, wie diese vor dem Verkauf zu löschen seien. Und John Bowman, der Kommunikationsdirektor der amerikanischen National Motorists Association kommentiert die Entwicklung von Automated Law Enforcement-Technologien in den USA mit den Worten: «If people don't push back against it … , I just think people will be surprised when they wake up one day and realize they have no privacy left.»

Nachzulesen unter:

http://www.faz.net/aktuell/feuilleton/big-data-algorithmen-ermitteln-14054010.html
http://www.tagblatt.ch/nachrichten/schweiz/schweiz-sda/Polizei-scannt-Autonummern;art253650,4410588
http://www.shz.de/regionales/schleswig-holstein/politik/kennzeichen-scanner-an-grenzuebergaengen-machen-aerger-id9381871.html
http://www.computerworld.com/article/2945367/internet/just-say-no-to-connected-cars.html
http://www.autoblog.com/2014/09/23/connected-car-traffic-enforcement-featured/

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