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

Januar 2016

SWITCH

I. Bringt PrivaTegrity das Ende der Kryptokriege? David Chaums neues Verschlüsselungssystem zwischen komplett anonymer Kommunikation und der Möglichkeit, kriminelle Machenschaften auszuschliessen

David Chaum gilt als der Vater der Anonymität und Privatsphäre im Internet. In der als «Kryptokriege» beschriebenen Auseinandersetzung zwischen Unternehmen, Regierungen und Strafverfolgungsbehörden auf der einen und den Verfechtern radikaler, uneingeschränkter Freiheit und absoluter Anonymität auf der anderen Seite entwickelte Chaum zahlreiche Verschlüsselungssysteme und -programme, die quasi die Grundstruktur für die Anonymität im Internet, so wie wir es heute kennen, bilden. Nun hat er an der Real World Crypto Conference der Universität Standford ein neues Kommunikationsnetzwerk angekündigt, das den Kryptokriegen ein Ende setzen soll, indem es beide Interessenlagen zusammenbringen soll: «You have to perfect the traceability of the evil people and the untraceability of the honest people».

PrivaTegrity soll Usern deshalb eine vollständig anonyme Kommunikation ermöglichen, die nach Aussagen Chaums weder von Geheimdiensten noch von Hackern zu knacken und damit sicherer sei als z.B. im TOR-Netzwerk. Obwohl das

High Performance Scalable Mixing als Kern von PrivaTegrity über neun Server plus einen von diesen und den transferierten Codes getrennten «Management-Server» läuft (bei TOR über drei freiwillig zur Verfügung gestellten), soll die Kommunikation via SmartPhone App und mindestens so schnell funktonieren wie bei Tor. Chaum und sein Team entwickeln das Netzwerk zunächst für Android.

Damit PrivaTegrity jedoch kein sicherer Hafen für Terroristen und Kriminelle wird, ist eine Hintertür vorgesehen. Sie steht allerdings nicht für staatlichen Stellen offen. Vielmehr sollen die neun Server-Administratoren in einer Art «Backdoor Security Council» entscheiden, ob und wann ein User seine Anonymität verlieren soll, weil seine Kommunikation auf kriminelle oder terroristische Machenschaften schliessen lässt. Daher sollen die meisten der PrivaTegrity Server auch ausserhalb der USA in Ländern mit einer demokratisch legitimierten Regierung installiert werden. Chaum nennt als Beispiele Kanada, Island oder die Schweiz.

Nachzulesen unter:

http://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars
http://www.gulli.com/news/26982-verschluesselungssystem-privategrity-soll-komplett-anonyme-kommunikation-bieten-2016-01-11
https://www.hackread.com/new-anonymous-communication-network-privategrity-launched
https://de.wikipedia.org/wiki/David_Chaum
https://de.wikipedia.org/wiki/Crypto_Wars

II. Boss hört mit – und zwar zurecht. Kontrollierte Überwachung privater Kommunikation am Arbeitsplatz verstösst nicht gegen Menschenrechte

Der Europäische Gerichtshof für Menschenrechte EGMR hat Anfang des Jahres ein weit reichendes Urteil gefällt. Demnach verletzten Arbeitgeber, die dienst-liche Rechner und Smartphones ihrer Angestellten überwachen, weder deren Privatsphäre noch geltende Menschenrechte, wenn sie dies unter Beachtung strenger Vorgaben tun. Und zwar auch dann nicht, wenn der Inhalt der Kommunikation privater oder gar intimer Natur ist. Gemäss dem EGMR-Urteil muss sichergestellt sein, dass Arbeitnehmende ihre vertraglichen Pflichten während der Arbeitszeit erfüllen, und die Arbeitgeber haben ein Recht, dies zu kontrollieren. Der Artikel 8 der Europäischen Menschenrechtskonvention, auf deren Grundlage der EGMR eingerichtet wurde,

schützt die Privatsphäre von Arbeitnehmenden umfassend. Denn Arbeitgeber müssen die Kontrollen verhältnismässig und sachbezogen durchführen und vorher eine klar definierte Politik und Regeln für die Nutzung von e-Mail und Messengerdiensten ausgearbeitet und ihren Angestellten zur Kenntnis gebracht haben.

Im aktuellen Fall waren diese Bedingungen nach Ansicht der Richter gegeben. Ein rumänischer Ingenieur hatte geklagt, weil er entlassen wurde, nachdem ihm sein Arbeitgeber umfangreiche private Nutzung von Chatdiensten als Zeichen für mangelnde Leistungserfüllung vorgeworfen und zum Beweis 45 Seiten Chat-Protokolle vorgelegt hatte. Die Richter gaben nun dem Arbeitgeber recht. Besondere Aktualität bekommt das Urteil angesichts der Tatsache, dass Mitarbeiter-Chats sich zunehmender Beliebtheit erfreuen. Bindend ist das Urteil für alle Staaten, die die Europäische Menschenrechtskonvention unterzeichnet haben, also auch für die Schweiz.

Nachzulesen unter:

http://www.handelsblatt.com/finanzen/steuern-recht/recht/europa-urteil-arbeitgeber-duerfen-chatprotokolle-ausspaehen/12834104.html
http://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/schutz-privatsphaere-arbeitsplatz
http://www.bbc.com/news/technology-35301148
http://www.mittelstand-die-macher.de/recht-finanzen/it-internetrecht/urteil-chatten-am-arbeitsplatz-ist-ein-kuendigungsgrund-19865
http://www.karriere.at/blog/buerokommunikation.html

III. Gestern noch Science Fiction – heute im Einsatz. Prognosesoftware und –systeme sollen Verbrechen entdecken, bevor sie begangen werden

Agatha, Arthur und Dashiell sehen in drogeninduzierten Fähigkeiten Morde der Zukunft samt Namen der Täter voraus und helfen der «Precrime» genannten Spezialeinheit der Washingtoner Polizei dabei die Zahl der Morde in der amerikanischen Bundeshauptstadt sechs Jahre lang auf Null zu halten – soweit die Science Fiction im 2002 verfilmten Thriller «Minority Report», dessen Drehbuch auf der gleichnamigen Kurzgeschichte von Philip K. Dick – der auch die Vorlagen für Blade Runner und Total Recall schuf – aus dem Jahre 1956 basiert. 60 Jahre später arbeitet «Precobs» – Precrime Observation System – für die Polizei im nordbadischen

Karlsruhe und der baden-württembergischen Landeshauptstadt Stuttgart. Aber auch in Bayern und den Kantonen Zürich, Baselland und Aargau nutzt die Polizei die Software, um vor allem Einbruchsdelikte vorherzusagen. Ausgangsüberlegung ist dabei die Near-Repeat-Theorie, nach der sich Delikte dort häufen, wo schon einmal welche begangen wurden. Aus den Angaben über Tathergang, gebrauchte Werkzeuge, Tatzeiten etc. versucht die Software ein Muster abzuleiten und entsprechend dieses Musters die nächsten Deliktwahrscheinlichkeiten voraus zu berechnen. Von der drogeninduzierten Visionalisierung und der umfassenden Verknüpfung mit persönlichen Daten aus anderen Quellen samt Iriserkenung aller Bürger wie in Minority Report sei die Software weit entfernt. Dennoch warnen Datenschützer, dass eine solche Verknüpfung mit Daten aus Social Media-Profilen, polizeilichem Führungszeugnis und anderen Datenquellen sowie Bewegungsmustern aus Connected Driving-Profilen und i-Beacons (allesamt in Minority Report dargestellt) dann eben doch zu totaler Überwachung und schlimmstenfalls falschen Verdächtigungen gläserner Bürger führen könnte. Zumal die Wirksamkeit der digitalen Kommissare bis anhin nicht einwandfrei erwiesen sei und die Polizei der englischen Grafschaft Kent als einer der Pioniere des «Predictive Policing» nach Einführung des Systems sogar steigende Verbrechenszahlen berichten musste.

Eine Referenz an gut gemachte Science Fiction hat auch eine Arbeitsgruppe der Internet Engineering Task Force (IETF) ins Spiel gebracht. Ray Bradburys Roman Fahrenheit 451 diente als Inspiration für den HTTP Status Code 451: «Unavailable for Legal reasons», der Usern deutlicher als die Codes 400: «Bad request», 403: «Forbidden» oder 404: «Not Found» zeigen soll, dass eine angeforderte Internet-Ressource aus rechtlichen Gründen nicht zugänglich ist.

Besonders häufig, oder eben gar nicht, dürfte der Code 451 in China erscheinen, wo die Regierung mit einer «Great Firewall» mehr als 6.000 Domains und unzählige Suchbegriffe seit Jahren sperrt, um auch im Netz die Deutungshoheit zu behalten.

Nachzulesen unter:

http://www.nzz.ch/international/deutschland-und-oesterreich/kommissar-kristallkugel-1.18667054
http://www.tagesanzeiger.ch/zuerich/stadt/Minority-Report-in-Zuerich/story/12692897
http://orf.at/stories/2261957/2261958
https://bigdatablog.de/2015/08/03/predictive-policing-big-data-in-der-polizeiarbeit
http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report
http://www.bbc.com/news/uk-england-kent-32529731
http://www.zeit.de/digital/internet/2015-12/fehlermeldung-451-statuscode-zensur
http://www.theregister.co.uk/2015/12/21/censorship_451_error_code_approved_by_ietf
http://www.nzz.ch/international/asien-und-pazifik/ein-schutzwall-gegen-westliches-gedankengut-1.18666754
http://www.nytimes.com/2015/08/18/opinion/murong-xuecun-scaling-chinas-great-firewall.html?_r=0
http://www.faz.net/aktuell/wirtschaft/fruehaufsteher/zensur-im-internet-china-zieht-die-great-firewall-hoeher-13386343.html

IV. Durchlöcherter Jahresstart – Meldungen über Sicherheitslücken lesen sich wie das Who-is-Who der Netzwerkausrüster

Für Juniper Networks, Fortinet, Cisco, AVM und UPC (und deren Kunden) hat das Jahr mit unerfreulichen Meldungen über Sicherheitslücken und Hintertüren begonnen. So musste sich Juniper Networks der Frage stellen, warum man den Zufallszahlengenerator Dual_EC_DRGB erst jetzt aus dem Betriebssystem ScreenOS für die Netscreen Firewalls entfernt habe. Seit Jahren ist bekannt, dass Dual_EC eine Hintertür für die amerikanische NSA eingebaut hat, andere Spuren zeigen Richtung GCHQ, den britischen Geheimdienst. Auch zur Frage, warum Juniper den als langsam und von schlechter Qualität bekannten DUAL_EC überhaupt eingesetzt hatte, macht das Unternehmen keine Angaben.

Mit ähnlichen Vorwürfen muss sich auch Fortinet auseinandersetzen, nachdem Sicherheitsforscher entdeckt haben, dass in älteren Versionen des Betriebssystems FortiOS ein SSH-Zugang mit fest eingestelltem Passwort voll umfängliche Administratorrechte für Fortinet Firewalls ermöglicht. Zwar hat Fortinet bekanntgegeben, dass es sich bei der Sicherheitslücke nicht um eine Hintertür handele und bereits Mitte Juli 2014 ein Patch bereitgestellt worden sei, dennoch sei das Risiko eines Angriffs bei allen FortiOS-Versionen von 4.3.0 bis und mit 5.07 «hoch».

Gleich vier als «hoch» bis «kritisch» eingestufte Sicherheitslücken hat Cisco in seinem Hard- und Softwareangebot ausgemacht. Zwar seien bisher keine Angriffe registriert worden, doch fordert der Netzwerkausrüster seine Kunden auf, die bereitstehenden

Sicherheitsupdates umgehend einzuspielen. Kritisch sei eine Lücke in der Identity Services Engine (ISE) in den Versionen 1.1 oder später, 1.2.0 vor Patch 17, 1.2.1 vor Patch acht, 1.3 vor Patch fünf und 1.4 vor Patch vier. Ebenfalls als kritisch stuft Cisco die Lücke in den Wireless-Controllern 2500 Series, 5500 Series und 8500 Series ein, wenn auf diesen Ciscos Wireless-LAN-Controller-Software (WLC) ab den Versionen 7.6.120.0, 8.0 oder 8.1 läuft. Hoch ist die Gefährdung nach Ciscos Angaben für die AccessPoints Aironet 1830e, 1830i, 1850e oder 1850i – hier sollte ein Firmware-Update durchgeführt werden. Eine zweite Lücke in Ciscos ISE bis zur Version 2.0 wird als mittel eingestuft, sollte aber dennoch schnell geschlossen werden. Weiters warnt das Unternehmen nach wie vor vor den Sicherheitslücken in OpenSSL, die im Dezember bekannt geworden waren. Eine Liste der betroffenen Geräte findet sich unter dem unten stehenden «tools.cisco…»-Link.

Schlechte Nachrichten auch für Fritzbox-User: Die Fritzboxen 3272/7272, 3370/3390/3490, 7312/7412, 7320/7330 (SL), 736x (SL) und 7490 mit einer Firmware älter als 6.30 weisen Lücken auf, die es Angreifern ermöglichen, auf Kosten des Fritzbox-Inhabers zu telefonieren, den Datenverkehr, der über den Router läuft, abzugreifen oder Geräte im lokalen Netz anzugreifen. Hersteller AVM empfiehlt dringend ein Update der Firmware und hat diese entsprechend bereitgestellt. Eine Sicherheitsempfehlung für seine Router hat auch UPC veröffentlicht, nachdem das UPC Recovery Tool auf Twitter veröffentlicht worden ist. Es ermöglicht, die werkseitig gelieferten WLAN Passwörter von UPC Homeroutern herauszufinden und die Router zu hacken.

Es sieht danach aus, dass auch im Neuen Jahr Sicherheitsexperten wieder viel zu tun haben werden.

Nachzulesen unter:

http://www.computerworld.ch/news/security/artikel/juniper-firewalls-muessen-gepatcht-werden-69351
http://www.heise.de/security/meldung/Juniper-entfernt-NSA-Zufallsgenerator-aus-Netzwerkgeraete-Betriebssystem-3067616.html
http://www.heise.de/newsticker/meldung/Festeingestelltes-Wartungs-Passwort-gefaehrdet-Fortinet-Appliances-3069680.html
http://www.darknet.org.uk/2016/01/fortinet-ssh-backdoor-found-firewalls
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151204-openssl
http://www.heise.de/security/meldung/AVM-Router-Fritzbox-Luecke-erlaubt-Telefonate-auf-fremde-Kosten-3065588.html
http://avm.de/ratgeber/sicherheit/tipps-fuer-zusaetzliche-sicherheit/uebersicht-fritzbox-modelle-und-sicherheitsupdate

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Der Datenschutzbeauftragte des Kantons Zürich hat neu einen Kanal auf Youtube, ein Awareness-Video ist schon online:

https://www.youtube.com/channel/UCghVVLU_hOTbClYaKQk8hTw

auf seiner Homepage gibt es ausserdem ein «Lernprogramm Datenschutz»:

https://review.datenschutz.ch/datenschutz/index.php?jss=1

159 Videos von den Vorträgen des diesjährigen Chaos Communication Congress 32C3 sind online:

https://media.ccc.de/c/32c3

Bitte sagen Sie uns Ihre Meinung! – Leserbefragung

SWITCH führt eine Leserbefragung über den Security Report durch. Tragen Sie mit Ihrer Meinung zu dessen Weiterentwicklung bei. Mit Ihrer Teilnahme können wir den Security Report besser auf Ihre Bedürfnisse zuschneiden und für Sie noch attraktiver gestalten. Alle Angaben und Antworten werden von uns in anonymisierter Form ausgewertet.

Bitte füllen Sie den Fragebogen bis spätestens Freitag, 31. Januar 2016 aus. Sie werden dazu etwa 8 bis 10 Minuten Zeit benötigen.

Mit diesen Links gelangen Sie direkt zum Fragebogen:
Deutsch: http://swit.ch/befragung-secrep
Englisch: http://swit.ch/survey-secrep

Falls Sie beim Ausfüllen Fragen haben, zögern Sie bitte nicht, uns zu kontaktieren: roland.eugster@switch.ch.
Wir danken Ihnen herzlich für Ihre Teilnahme!

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis, Frank Herberg und Michael Fuchs 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.