SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

Juli/August 2019

I. Angriffe auf PGP-Keyserver: Ist Pretty Good noch gut genug?

Wer seine E-Mails nicht als Postkarten verschicken will, die von jedem auf dem Weg vom Sender zum Empfänger gelesen werden können, setzt neben ein paar Insellösungen in der Regel auf S/MIME oder PGP. Und auf letzteres Verfahren gab es in der letzten Zeit ein paar fiese Angriffe. PGP beruht auf einem Public-Key-Verfahren, in dem jeder Teilnehmer ein zusammengehörendes Paar aus einem geheimen und einem öffentlichen Schlüssel besitzt (asymmetrische Verschlüsselung). Der öffentliche Schlüssel liegt in der Regel auf einem sogenannten Keyserver – quasi einer Art "Telefonbuch". Und damit der Nutzer des öffentlichen Schlüssels auch (mehr oder weniger) sicher sein kann, dass der Schlüssel zu der Person gehört, die er anschreiben möchte, gibt es das Web-of-Trust: Man signiert sich gegenseitig die öffentlichen Schlüssel, um zu bestätigen, wem sie gehören.

Wohlwollend liesse sich das PGP-Verschlüsselungssystem samt seinem SKS Keyserver Netzwerk mit den Worten eines seiner Initianten, Robert J. Hansen, als "grosses, verlässliches und zensurresistentes verteiltes Filesystem" beschreiben, "in dem jedermann Einträge schreiben kann." Aber es hat auch gravierende Nachteile, auf die auch Leute wie Hansen selbst hinweisen:

- Dem System ist das Paradox inhärent, dass zur Herstellung eines sicheren privaten Kommunikationskanals wenigstens zum Teil öffentlich zugängliche Daten verwendet werden.
- Aus Angst vor Zensur hatten die Gründer das Netzwerk so angelegt, dass einmal angelegte Zertifikate nie mehr gelöscht werden können.
- Dies betrifft auch die sogenannten certificate signatures, also die Anhänge zu den Zertifikaten, die u.a. die Echtheit dieser Zertifikate bestätigen sollen. Sind sie einmal an ein Zertifikat angehängt, bleiben sie dort und können zu riesigen Appendizes führen, deren Datenmengen letztlich die Server blockieren können.
- Es gibt keinen standardisierten und verlässlichen Modus, der prüft, wer diese certificate signatures verfasst hat und ob sie korrekt sind.

Diese Schwachstelle haben Hacker in der letzten Juniwoche dazu benutzt, das PGP Keyserver-Netzwerk zu kompromittieren. Dazu haben sie die Sicherheitszertifikate von Hansen und die eines weiteren Mitglieds des inneren Zirkles in der OpenPGP-Community, Daniel Kahn Gillmor, mit einer sogenannten "Certificate Spamming Attack" angegriffen. Dabei wurden den Schlüssel immer neue signatures mit SPAM-Informationen angehängt. Hanson berichtet auf Github, dass alleine sein öffentlicher Schlüssel einen Ballast von mehr als 150.000 solcher Signaturen angehängt sind, die bei jeder Nutzung dieses Schlüssels mitgesendet werden und letztlich dazu führen, dass die Software überlastet ist und das System kollabiert. In seinem Beitrag zeigt er relativ nüchtern auf, wie es zu diesem Hack kommen konnte und warnt davor, das Netzwerk weiter zu benutzen.

Das vor einigen Wochen gestartete OpenPGP-Keyserver-Projekt mit einem neuen Server und einem aktualisierten Release der GnuPG-Software vordergründig einen möglichen Workaround. Nach dem Upload eines neuen Schlüssels schickt der Server eine E-Mail an alle enthaltenen Mailadressen. Diese enthalten einen Link über den der Empfänger den Key erst freigeben muss. Außerdem kann man auf seine Mail-Adresse registrierte Schlüssel auch wieder löschen. (Weitere Details im letzten der untenstehenden Links). Signaturen werden mit diesem Verfahren jedoch ignoriert und damit fehlt letztlich auf den Keyservern die Vertrauensbasis, auf der PGP bisher aufgesetzt hatte.

Wir folgen daher der Empfehlung des Heise-Autors Jürgen Schmidt, für ein Mehr an Sicherheit "Key-Signing-Parties" durchzuführen, bei denen man sich von Angesicht zu Angesicht die Schlüssel nach Verifikation der Identität gegenseitig signiert. Dies ist unter CERTs schon seit vielen Jahren gang und gäbe.

Nachzulesen unter:

https://www.it-daily.net/it-sicherheit/datenschutz/21858-e-mail-verschluesselung-mit-pgp-ist-nicht-sicher
https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f
https://dkg.fifthhorseman.net/blog/openpgp-certificate-flooding.html
https://www.zdnet.de/88364171/spam-attacken-gefaehrden-pgp-infrastruktur
https://www.heise.de/security/artikel/PGP-Der-langsame-Tod-des-Web-of-Trust-4467052.html
https://latacora.singles/2019/07/16/the-pgp-problem.html
https://www.heise.de/security/meldung/PGP-E-Mail-Verschluesselung-akut-angreifbar-4048489.html
https://www.heise.de/security/meldung/Angriff-auf-PGP-Keyserver-demonstriert-hoffnugslose-Situation-4458354.html

II. Wir müssen reden! Übers Zuhören von Sprachassistentinnen und -assistenten.

Im Jahr 2000 veröffentlichten Allan und Barbara Pease ihren Bestseller "Warum Männer nicht zuhören und Frauen schlecht einparken". Knapp 20 Jahre später stellt sich dem politisch korrekt denkenden Menschen nun die Frage: Ist die Tatsache, dass Alexa, Cortana und Siri weibliche Vornamen tragen, aber durchgängig in männlicher Form als Sprachassistenten bezeichnet werden, nur gendersprachliche Schludrigkeit oder bewusste Täuschung der Anbieter? Denn schliesslich wissen wir ja seit Pease & Pease, dass Männer eben nicht zuhören. Genau das aber tun mehr oder weniger alle digitalen Sprachassistenten. Und zwar auch dann, wenn ihre Besitzer das gar nicht wollen, und in Dimensionen, die jüngst für mediale Schlagzeilen gesorgt und das Eingreifen der Datenschützer ausgelöst haben. Der Vorwurf: "Die Nutzung von automatischen Sprachassistenten von Anbietern wie Google, Apple und Amazon erweist sich als hoch risikoreich für die Privat- und Intimsphäre von Betroffenen." Zu diesem Schluss kam der Hamburgische Beauftrage für Datenschutz und Informationssicherheit, nachdem bekannt geworden war, dass die drei Anbieter Sprachaufnahmen ihrer "digitalen Aussenstellen" millionenfach in Textfiles umwandeln, speichern und auswerten liessen – wohlgemerkt, ohne die Belauschten zu informieren. Anfang Juli 2019 hatte Amazon zugegeben, genau dies zu tun und die Daten auf unbefristete Zeit zu speichern, um damit nach Unternehmensangaben die KI hinter Alexa zu trainieren. Kurze Zeit später hatte ein Whistleblower einer Vertragsfirma von Google dem flämischen Rundfunk VRT etwa eintausend Aufzeichnungen zugespielt, die belegen, dass Google Home und die Google Assistant Smartphone App alles aufzeichnen, was ihnen Nutzerinnen und Nutzer nach dem Aktivierungsbefehl "Ok Google" anvertrauen. Ende Juli hatte dann der Guardian berichtet, dass auch Mitarbeitende von Apple-Subunternehmen Siri-Aufzeichnungen sammeln und auswerten – ungeachtet der Sensibilität der dabei erfassten Inhalte. Denn die digitalen Inhouse- und Mobilspione schalten sich in 10 bis 15 % aller Fälle auch dann ein, wenn ihre Nutzerinnen und Nutzer das gar nicht beabsichtigt haben. Grund dafür ist, dass Mikrofone und/oder Spracherkennung eben doch nicht so zuverlässig funktionieren, wie die Anbieter dies versprechen.

Aufgrund medialen und juristischen Drucks hat Google die Aufzeichnung für drei Monate ausgesetzt. Apple will künftig die explizite Zustimmung der Nutzerinnen und Nutzer einholen und Amazon bietet mit dem jüngsten Software-Update eine OptOut-Möglichkeit an.

Dennoch bleibt die Frage, wie es um den Schutz der Privatsphäre bei anderen Anbietern und deren Assistenzsystemen oder bei smarten mikrofonbestückten Geräten (SmartHome-Steuerungen, Smart-TVs, Smart-Spielsachen) bestellt ist. Etwa vier Wochen nach den Alexa-Enthüllungen berichtete Motherboard, dass Mitarbeitende von Microsoft-Vertragsfirmen sowohl die Kommunikation von Skypenden als auch die von Cortana-Nutzenden überwachen und mitschneiden. Natürlich ebenfalls nur zum Zweck, den Service weiter zu verbessern. Darüber, dass die smarte WLAN-Puppe "Hello Barbie" Gespräche an die Marketingabteilung des Herstellers Mattel schickt, hatten wir hier bereits im Mai 2015 berichtet.

Unbekannt ist bislang, ob die Hersteller von Fahrzeugen, die mit eigenen Sprachassistenten ausgestattet sind, die Gespräche, die im Fahrzeug stattfinden, ebenfalls aufzeichnen. Zumindest Tesla hat solche Vorwürfe im Zusammenhang mit der Beschaffung von Fahrzeugen durch die Basler Polizei 2018 zurückgewiesen. Dagegen ist bekannt und unbestritten, dass Hersteller bislang ohne Zustimmung der Käufer Fahrzeugdaten sammeln und auswerten. Man darf also gespannt sein. Mit recht grosser Wahrscheinlichkeit kann man jedoch vermuten, dass digitale Einparkassistenten männliche Vornamen bekommen werden. Denn wenn Männer nach Pease und Pease auch nicht zuhören – einparken können sie.

Nachzulesen unter:

https://steigerlegal.ch/2019/08/05/google-assistant-datenschutz
https://www.handelsblatt.com/technik/it-internet/apple-google-amazon-sprachassistenten-und-datenschutz-wer-zuhoeren-will-muss-fragen/24865836.html?ticket=ST-7871286-JAKLMphM455YvRS5bcBC-ap1
https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings
https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms
https://www.sueddeutsche.de/digital/alexa-siri-google-datenschutz-1.4552480
https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/microsoft-hoert-bei-skype-mit/story/16596840
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-05.pdf
https://www.srf.ch/news/regional/basel-baselland/datenschutzprobleme-basler-polizei-auto-weiss-zuviel
https://www.zeit.de/wirtschaft/2017-09/datenschutz-autohersteller-apps-datenverschluesselung-stiftung-warentest

III. Breaking Binance: Die grösste Bitcoin-Börse der Welt wurde gehackt und wird erpresst

Mehr als 700 Kunden der Bitcoin-Börse Binance fanden am 7. August ihre KYC (Know-Your-Customer-)Daten – Porträtfoto, Kopie der Anmeldung bei Binance sowie von Reisepass, Ausweis oder Führerschein – in einer eigens dafür eingerichteten öffentlichen

Gruppe des Messengerdienstes Telegram gepostet. Wie blockchain-hero.com wenige Stunden nach den ersten Posts berichtete, wurden die Daten, die zum grössten Teil von asiatischen Kunden der Bitcoin-Börse stammen, offenbar aus der Datenbank eines Vertragspartners gestohlen, der für Binance die Anmeldungen verifiziert. Sie beziehen sich soweit bekannt auf Anmeldungen, die zwischen Februar und März 2018 erfolgt sind. In dieser Zeit hatte es schon einmal ein Datenleck bei Binance gegeben. Ob die geposteten Daten bei diesem oder einem neuen Angriff gestohlen worden waren, liess Binance-CEO Changpeng Zhao offen, als er unmittelbar nach Bekanntwerden des Leaks auf Twitter warnte.

Kurze Zeit später veröffentlichte die Finanzplattform in ihrem Blog einen Beitrag, aus dem hervorgeht, dass ein unbekannter Hacker damit gedroht habe, weitere 10.000 Anmeldefotos mit KYC-Daten zu posten, falls ihm nicht 300 Bitcoins überlassen würden. Binance hat einerseits die Strafverfolgungsbehörden eingeschaltet, andererseits eine Belohnung von bis zu 25 Bitcoins für sachdienliche Hinweise zur Identifikation des Täters und zur Ermöglichung einer legalen strafrechtlichen Verfolgung ausgelobt. Denn wie blockchain-hero berichtet, hatte der Hacker angeblich zuvor versucht, die Daten im Darknet zu verkaufen. Weil ihm dies offenbar nicht gelungen war, scheint er nun auf diesem Weg zu Geld kommen zu wollen.

Offensichtlich nimmt sich der Cyberkriminelle Kim Yong-un zum Vorbild, dessen Staatshacker bei mehr als 35 Cyberangriffen auf Finanzinstitutionen und Kryptoplattformen bisher bis zu zwei Milliarden US-Dollar für das nordkoreanische Atom- und Rüstungsprogramm gestohlen haben sollen. Die Zahlen stammen aus einem offiziellen Bericht unabhängiger Experten für den Nordkorea-Sanktionsausschuss der Vereinten Nationen.

Unbekannt sind bis heute dagegen die Hacker, die am 11. Juli 2019 die japanische Bitcoin-Börse BITPoint gehackt und ihrem Betreiber sowie etwa 50.000 Kunden aus deren Hot Wallets mehr als 28 Millionen US-Dollar in verschiedenen Kryptowährungen gestohlen haben. Zwei Drittel davon waren Kundengelder, ein Drittel gehörte der Börse selbst. In einer Pressemitteilung gab BITPoint kurz darauf bekannt, dass zwischenzeitlich mehr als 2,3 Millionen US-Dollar auf einer Offshore-Plattform ausfindig gemacht werden konnten. Tags darauf folgte die Mitteilung, dass alle Betroffenen eins zu eins in Kryptowährung für ihren Verlust entschädigt würden.

Innerhalb weniger Wochen wurde damit bereits die zweite asiatische Kryptobörse Opfer eines grossen Hackerangriffs. Am 26. Juni hatten Cyberkriminelle Bitrue, eine Bitcoin-Börse aus Singapur um 9,3 Millionen US-Dollar in XRP (Ripple) und ADA (Cardano) erleichtert.

Verglichen mit dem grössten virtuellen Bankraub in der Geschichte der Kryptowährungen sind diese Zahlen jedoch nur "Peanuts": Im Januar 2018 hatten bis heute Unbekannte ein unzureichend gesichertes Hot Wallet dazu genutzt, etwa 260.000 Kunden der japanischen

Handelsplattform Coincheck NEW-Tokens (für New Economy Movement-Tokens) im Wert von 440 Millionen Dollar zu stehlen. Coincheck wurde inzwischen vom Onlinebroker Monex übernommen, hat die Betroffenen weitgehend entschädigt und ist seit dem 11. Januar 2019 wieder mit einer offiziellen Lizenz der japanischen Finanzaufsichtsbehörde aktiv.

Nachzulesen unter:

https://blockchain-hero.com/eilmeldung-binance-kyc-datenleak
https://www.btc-echo.de/breaking-massiver-datenleak-bei-bitcoin-boerse-binance
https://www.binance.com/en/blog/365766157488967680/Statement-on-False-KYC-Leak
https://www.btc-echo.de/gehackte-bitcoin-boerse-bitpoints-verspricht-entschaedigungen-fuer-kunden
https://www.heise.de/newsticker/meldung/Malware-Attacken-ueber-Avalanche-Botnet-Drahtzieher-vor-Gericht-4423942.html
https://de.cointelegraph.com/news/japanese-regulators-grant-cryptocurrency-exchange-license-to-coincheck

In eigener Sache: Neu im SWITCHcert Security Blog

Attacks on DNS continue, targets are also in Switzerland
https://securityblog.switch.ch/2019/07/10/attacks-on-dns-infrastructure-continue/

SWITCH Public DNS Resolver with DoT/DoH support
https://securityblog.switch.ch/2019/08/07/switch-public-dns-resolver/

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