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

Juli/August 2021

I. Perhaps 1984 WAS like *1984* – Apples grosser Sündenfall, oder: War alles nur geniale Werbung?

1949 erschien in London "Nineteen-Eighty-Four", George Orwells düstere Vision einer Zukunft, in der ein allmächtiger Staat alles und jeden in jedem Moment seines Lebens überwacht. Als Apple am 24. Januar 1984 den Macintosh einführte, geschah dies mit einem Werbespot, der in keiner Hall of Fame der Werbung fehlt. Die Botschaft: "On January 24th, Apple Computer will introduce Macintosh. And you'll see why 1984 won't be like *1984*!" Seither hat sich Apple immer als der "Good Guy" unter den Tech-Giganten als Hüter und letzte Verteidigungslinie der Privatsphäre seiner Userinnen und User positioniert. Jedenfalls bis zum 5. August 2021. Da veröffentlichte der Konzern aus Cupertino ein Whitepaper mit dem Titel "CSAM Detection", weil man aktiver gegen Verbreitung und Nutzung von Kinderpornographie (Child Sexual Abuse Material) tun wolle. Letzteres ist sicher ohne Wenn und Aber ein ebenso wichtiges wie gutes Anliegen. Zudem verpflichten weltweite Gesetze alle Anbieter von Speicherdiensten dazu, kinderpornographischen Content auf ihren Servern aufzuspüren und den Strafverfolgungsbehörden zu melden. Es wird wohl kaum jemand geben, der dies nicht gutheissen würde.

Was Apple aber jetzt mit IOS 15 und iPad OS15 ausrollt, ist schlichtweg DER grosse Sündenfall, der Apple vom selbsternannten Verteidiger der Privatsphäre zum Türöffner für die Überwachung der Menschen durch IT-Geräte und das Internet der Dinge mutieren lässt. Denn die Idee, die hinter dem iPhone- und iPad-Scanning steht, ist die, dass auf allen mobilen i-Devices des Konzerns im System de facto Wanzen implementiert werden, die permanent nach illegalen Inhalten scannen und diese melden.

Die Geschichte der Menschheit im Allgemeinen und der IT-Privacy im Besonderen lässt Kritiker befürchten, dass die Themen der Inhalte schon bald von der Kinderpornographie weg und zur Meldung jeder erdenklichen, von der gewünschten Norm abweichender Auffälligkeiten ausgeweitet werden könnten. Der Fantasie sind seitens der Technik dann keine Grenzen gesetzt. Wie hungrig Staaten nach Überwachungsdaten sind, zeigt ganz aktuell auch der Pegasus-Case, den wir unter Top II weiter unten nochmals explizit aufgreifen werden.

Der massiven Kritik, die u.a. auch von Edward Snowden via Twitter geäussert worden war, begegnet Apple mit dem Hinweis, dass ein komplexes Datenschutzverfahren die Privatsphäre auch weiterhin gewährleiste.

Daher wirkt es umso peinlicher, dass es den Kaliforniern noch immer nicht gelungen zu sein scheint, jene Sicherheitslücken zu schliessen, die es dem Staatstrojaner Pegasus ermöglichen, auch iPhones und iPads im gleichen Masse auszuspionieren wie die Geräte der Apple-Konkurrenz. Wenn dann auch noch Medien darüber berichten, dass der i-Konzern selbst zum Big Brother mutiert, der seine Mitarbeiter mit Bodycams überwacht, um der Weitergabe von Firmengeheimnissen vorzubeugen, bleibt einem nur die Schlusszeile aus dem gleichnamigen Song von Robbie Williams: "All that´s left in any case is advertising space."

Nachzulesen unter:

https://www.digitec.ch/de/page/apple-neuralhash-gegen-privatsphaere-die-buechse-der-pandora-wird-geoeffnet-20759
https://www.heise.de/meinung/Totalueberwachung-durch-die-Hintertuer-Apples-fataler-Suendenfall-6157251.html
https://www.tagesschau.de/ausland/apple-kritik-foto-funktion-kinderpornos-101.html
https://www.chip.de/news/Snowden-kritisiert-Apple-scharf_183756528.html
https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/
https://www.t-online.de/digital/sicherheit/id_90484688/pegasus-luecke-in-iphones-noch-immer-angreifbar.html
https://www.giga.de/news/apple-als-big-brother-mitarbeiter-sollen-body-cams-tragen/
https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life

II. Pegasus, oder: was IT-Anwender von den alten Griechen lernen können

In der Götterwelt der griechischen Mythologie war Pegasus das geflügelte Pferd, das neben anderen Heldentaten dem obersten Herrn im Götterhimmel - Zeus - mit Blitz und Donner zwei

mächtige Vernichtungswaffen geliefert hat. Im schmutzigen Alltag staatlicher und geheimdienstlicher Überwachung gibt ein Staatstrojaner namens Pegasus vielen Machthabern dieser Welt ein hochfunktionelles, kaum erkennbares und noch schwerer auszuschaltendes Ausspähwerkzeug an die Hand, das ihnen hilft, Zielpersonen auszuspionieren und bei Bedarf auch aufzuspüren.

Er stammt von der israelischen NSO-Group, deren Selbstverständnis nicht nur im Firmenslogan "Cyber Intelligence for Global Security and Stability", sondern auch in der an den US-amerikanischen Super-Geheimdienst NSA angelehnten Namensgebung zeigt. Da wirkt es geradezu naiv, wenn NSO beschwichtigt, dass Pegasus ausschliesslich zum Einsatz gegen Kriminelle und Terroristen gedacht sei. Dass dem nicht so ist, belegt zudem eine geleakte Liste, die Amnesty International und der Non-Profit Media-Organisation "Forbidden Stories" zugespielt worden war. Sie enthält mehr als 50.000 Telefonnummern von Geschäftsleuten, Politikern, Journalisten, Akademikern, Gewerkschaftern, religiösen Würdenträgern und Regierungsvertretern, darunter auch von Kabinettsmitgliedern und Staatspräsidenten. Zudem berichtete der Guardian davon, dass Pegasus von einem mexikanischen Kunden offenbar dazu genutzt wurde, den Reporter Cecilio Pineda Birto auszuspähen und aufzuspüren. Wenige Wochen nach der Infektion seines Smartphones mit dem NSO-Trojaner war Pineda ermordet aufgefunden worden – ohne eine Spur seines Telefons. NSO wies jede Mitverantwortung an Pinedas Ermordung zurück. Dennoch bleibt festzuhalten, dass der Reporter neben 24 weiteren mexikanischen Journalisten als Überwachungsziel ausgewählt worden war. Mit mehr als 15.000 überwachten Telefonen gilt Mexico als grösster Pegasus-Anwender. Mit jeweils 10.000 Pegasus-Einsätzen folgen Marokko und die Vereinten Arabischen Emirate auf Rang 2. Doppelt bitter, weil zum einen auch die Regierung eines EU-Landes auf der geleakten NSO-Kundenliste auftaucht und man zum anderen eigentlich schon gar nichts anderes erwartet hätte: Ungarns Geheimdienste spähen seit 2018 mutmasslich 300 Kritiker Viktor Orbans mit Pegasus-Hilfe systematisch aus.

Pegasus hat sich also vom dichterischen Mythos in ein Stück schmutzige – und in manchen Fällen tödliche - Spionagerealität entwickelt. Dabei scheint sich auch ein weiterer Mythos aufzulösen: der des vermeintlich werkseitig eingebauten Sicherheitsplus´ von iPhones und iPads. Denn die waren den Pegasus-Attacken in gleichem Masse schutzlos ausgesetzt wie Android-Geräte. Deshalb verwies Ende Juli Matthew Green, Kryptologe und Associate Professor für IT-Security an der Johns Hopkins University, darauf, dass Apples Kommunikationsdienst iMessage "wirklich böse" Angriffsvektoren böte. Die Klagen darüber, dass man die Lücken entweder nicht schliessen könne oder nicht wolle und stattdessen mit der NeuralHash CSAM-Detection (siehe Top1) die Initialzündung zur Totalüberwachung via Smartphone und Tablet liefere, werden lauter. Es scheint, als habe Pegasus Blitz und Donner auch nach Cupertino gebracht.

Nachzulesen unter:

https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus
https://www.dw.com/de/pegasus-skandal-kein-system-ist-sicher/a-58705194
https://www.heise.de/news/NSO-Skandal-100-Organisationen-fordern-Verkaufsstopp-fuer-Spyware-6149195.html
https://www.nzz.ch/international/pegasus-in-ungarn-ausspionierte-orban-kritiker-kein-dementi-ld.1636774?reduced=true
https://www.heise.de/news/Pegasus-Sicherheitsforscher-fordert-Apple-zu-besserer-iPhone-Absicherung-auf-6144134.html
https://www.heise.de/meinung/Kommentar-Apple-setzt-die-falschen-Prioritaeten-6158007.html

III. Grösster Hack der Kryptowährungsgeschichte - ein pädagogischer Zeigefinger oder einfach nur pure Hacker-Eitelkeit?

Fasziniertes Entsetzen durchzog die ersten Meldungen über einen Hackerangriff der Superlative: Mehr als 600 Millionen US-Dollar in verschiedenen Kryptowährungen hätten unbekannte Hacker bei einer Cyberattacke auf das Unternehmen Poly Network erbeutet. Das hatte die relativ unbekannte Firma, die Software anbietet, um den Austausch von Daten zwischen unterschiedlichen Blockchains, insbesondere aber zum Transfer und zur Konvertierung verschiedener Kryptowährungen zu ermöglichen, am 11. August per Twitter mitteilen müssen. Die Cyberkriminellen hatten eine gravierende Sicherheitslücke im Protokoll entdeckt und dazu genutzt, die Adressen von Zehntausenden Kunden durch die eigene zu ersetzen und so die Riesensumme auf ihre Konten umzuleiten: 273 Mio. USD in Ether aus der Ethereum Blockchain, 253 Mio. aus der Binance Smart Chain und ca. 85 Mio. aus dem Polygon-Network (die technischen Details finden sich im untenstehenden Link zu SlowMist).

Einige Stunden nach dem ersten Poly Network-Tweet hatte sich die Firma in einem zweiten direkt an die Hacker gewandt, diese aufgefordert, die Beute zurückzugeben und Kontakt aufzunehmen, um einer schweren Strafverfolgung zu entgehen. Derweilen hatten die Krypto-Securityforscher von Elliptic mitgeteilt, dass ein Grossteil der Beute wieder zurückgegeben worden wären. Elliptic-Co-Founder Tom Morrison erklärte dies damit, dass zum einen der Betrag zu gross sei, um ihn unauffällig waschen zu können. Zum anderen liefere die Transparenz der Blockchain-Technology einen weiteren Grund.

Tatsächlich hatte unmittelbar nach Bekanntwerden des Hacks die Kryptocommunity damit begonnen, Jagd auf den oder die Täter und seine Beute zu machen. So liess die Security-Firma SlowMist kurz nach dem zweiten Poly-Tweet verlauten, man habe Mailbox, IP und Aktivitätsspuren auf dem Smartphone des Hackers identifiziert. Dieser habe primär über die chinesische Kryptobörse Exchange Hoo verschiedene Währungskonvertierungen vorgenommen. Ausserdem werde man weitere Erkenntnisse über den Hacker mit Poly Network teilen, damit der Hack zu einem guten Ende komme.

Inzwischen hat der Hacker fast die komplette Beute zurückgegeben, nicht aber seine Identität preisgegeben. Im Gegenteil: In einer Nachricht bot er jenem Hacker, der ihn innerhalb eines Monats identifizieren könne, ein persönliches Geschenk an.

Auch erteilte er dem Ansinnen der Poly Network-Verantwortlichen eine Abfuhr, ihn mit 500.000 Dollar und Straffreiheit zu belohnen, weil er ihnen geholfen habe, eine gravierende Sicherheitslücke zu entdecken und zu schliessen. Poly Network bezeichnet den Hacker inzwischen als "Mr. White Hat", sieht also positive Absichten hinter seinem Angriff. Dass es ihm nicht um das Geld ginge, sondern darum, die Schwachstellen in der Poly Network Software blosszustellen, hatte der Unbekannte mit dem weissen Hut über der schwarzen Weste schon zuvor in einer dreiseitigen Frage-Antwort-Runde verkündet. Die hatte Tom Robinson via Twitter veröffentlicht. Dem diametral gegenüber steht ein früherer Tweet des Hackers, in dem er bedauert hatte, dass der Hack "ein Milliarden-Ding" hätte werden können, wenn er diverse "Shitcoins" rechtzeitig auf seine Konten transferiert hätte. Man darf also gespannt sein darauf, ob das Mysterium seine Aufklärung findet.

Nachzulesen unter:

https://www.tagesschau.de/wirtschaft/finanzen/krypto-waehrung-diebstahl-hacker-angriff-ethereum-binance-polygon-101.html
https://blockchainwelt.de/poly-network-hack-mindestens-611-millionen-usd-wurden-gestohlen
https://bitcoinist.com/biggest-heist-in-defi-how-a-hacker-stole-600-million-from-poly-network
https://www.btc-echo.de/news/poly-network-hacker-zahlt-fast-alles-zurueck-und-teasert-mit-seiner-124042
https://www.tagesanzeiger.ch/hacker-erbeuten-ueber-600-millionen-dollar-aus-spass-rueckzahlung-laeuft-417830762835
https://www.manager-magazin.de/finanzen/geldanlage/poly-network-krypto-hacker-gibt-beute-zurueck-und-zitiert-martin-heidegger-a-4f8b2e0c-1f81-4212-bf01-aef637f5422a
https://slowmist.medium.com/the-root-cause-of-poly-network-being-hacked-ec2ee1b0c68f
https://www.youtube.com/watch?v=MfW7jUqLZ7Q
https://www.youtube.com/watch?v=O6M2JuIsCrQ

IV. Im Bett mit Siri, Alexa und Uber - wie steht es um Privatsphäre und Datensicherheit in HomeOffice und Schlafzimmer?

Was viele Menschen als coronabedingte Ausnahmesituation während einer oder mehrerer Lockdownphasen erlebt haben, ist für andere schlicht und ergreifend Berufsalltag: Arbeiten von zuhause aus. Schon immer war Heimarbeit eine Alternative für viele Menschen. Mit dem Wechsel von der Industrie- zur Dienstleistungsgesellschaft verlagerten immer mehr Unternehmen Telekommunikationsleistungen wie Kundenservice oder Telefonmarketing an darauf spezialisierte Unternehmen, deren Angestellte diese Leistungen in ihren privaten Räumlichkeiten erbringen. Gerade in ärmeren Ländern steht den Angestellten dazu kein Büro zur Verfügung - oft müssen Küche, Kinder- oder Schlafzimmer reichen.

Das wäre kein Thema für diesen Security Report, solange dabei nicht auch Fragen der Privatsphäre und der Datensicherheit berührt wären. Spätestens mit dem Übergang vom reinen Telefonservice zur Übertragung audiovisueller Inhalte und der Zwei-Wege-Kommunikation smarter Geräte und Sprachassistenten stellen sich solche Fragen aber in zunehmendem Masse. So haben wir hier bereits vor Jahren darüber berichtet, dass "Hello Barbie" die Gespräche von Kindern mit ihrer smarten Puppe aufzeichnet und an den Hersteller Mattel schickt, der die Inhalte auswertet und den Eltern ein Wochenbulletin über ihr Kind zuschickt. Glücklicherweise haben Eltern die Möglichkeit, diese Funktion zu deaktivieren - eine Option, die Mitarbeitenden mancher Firmen nicht offensteht.

So berichtete NBC NEWS anfangs August darüber, dass BigTech-Konzerne wie Apple, Amazon und Uber Ihre Kundenservices an Teleperformance-Anbieter auslagern, die mit Kamera(s), Mikrofon(en) und KI-gesteuerter Überwachungssoftware Mitarbeitende am (Heim-)Arbeitsplatz überwachen. NBC verwies auf einen zugespielten Arbeitsvertrag einer kolumbianischen Angestellten des französischen Call Center-Anbieters Teleperformance, die im Serviceteam für Apple arbeitet. Darin sei festgelegt, dass die Firma die Frau bei der Heimarbeit mit oben genannten Mitteln überwachen könne und es dabei ganz egal sei, in welchem Raum dieser Arbeitsplatz eingerichtet sei. Während Apple die Meldung als falsch zurückwies, bezog eine Amazon-Sprecherin die Position, dass für Heimarbeit "keine zusätzliche" Überwachung verlangt worden sei. Dass bei Amazon überwacht wird, ist seit längerem bekannt: 4 HD-Kameras in der Fahrzeug-Kabine überwachen in den USA die Verkehrssituation, das Verhalten der Fahrerinnen und Fahrer im Auto sowie die Zustellung der Pakete.

Mit steigender Zahl vernetzter Überwachungsgeräte steigt aber auch das Risiko, dass die - oft schlecht verschlüsselten - Devices Hackern ein enorm grosses Einfallstor ins private Reich unbedarfter Userinnen und User öffnen. So berichtete die in Mississippi beheimatete Nachrichtenplattform WMC5, dass die Amazon-Ring-Kamera, mit denen ein Elternpaar das Kinderzimmer überwachen wollte, von Hackern genutzt worden war, um der achtjährigen Tochter Songs vorzuspielen und mit ihr zu sprechen. Zugeben mussten die Eltern allerdings auch, dass sie es versäumt hatten, die Zwei-Wege-Authentifizierung zu aktivieren, die Hackern den Zugriff auf das System erschwert hätte. Der IT-Blog Motherboard von vice.com griff den Fall ebenfalls auf und berichtete zudem von weiteren Ausspähangriffen via Amazon Ring in anderen Bundesstaaten. Motherboard warnte davor, dass eigene Recherchen im Darknet gezeigt hätten, dass sich dort in mehreren Foren Cyberkriminelle über die besten Wege austauschen würden, Ring-Kameras zu hacken.

Der Ring-Anbieter Amazon reagierte auf den Vorfall mit der dringenden Empfehlung an alle Nutzer, die Zwei-Wege-Authentifizierung zu aktivieren, anstelle eines Logins die Ring-Funktion "Shared Users" zu nutzen, starke Passwörter zu verwenden und diese regelmässig zu erneuern.

Das Thema "Sicherheit versus Privatsphäre" bleibt damit auch 72 Jahre nach dem Erscheinen von Orwells "1984" aktuell wie nie.

Nachzulesen unter:

https://www.nbcnews.com/tech/tech-news/big-tech-call-center-workers-face-pressure-accept-home-surveillance-n1276227
https://www.golem.de/news/apple-amazon-uber-callcenter-ueberwachen-angestellte-mit-kameras-im-homeoffice-2108-158804.html
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-05_de.pdf
https://futurezone.at/digital-life/hacker-spionieren-mit-kameras-von-amazon-ring-kinderzimmer-aus/400703223

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