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

Januar/Februar 2020

I. Wenn die Hintertür zur Falltür wird: Crypto-Leaks treffen die Schweiz, das Crypto-Valley, aber auch das ganze Eco-System

Die Operation Rubicon gilt nach Aussagen des amerikanischen Geheimdienstes CIA als "grösster Spionagecoup des Jahrhunderts": Im CIA-Bericht "Minerva", der im Rahmen der Veröffentlichungen der Crypto-Leaks nach einer gemeinsamen Recherche der Washington Post und des ZDF zusammen mit der Schweizerischen Rundschau anfangs der zweiten Februar-Woche publik geworden war, rühmt sich der amerikanische Geheimdienst: "It was the intelligence coup of the century. Foreign governments were paying good money to the U.S. and West Germany for the privilege of having their most secret communications read by at least two (and possibly as many as five or six) foreign countries."

Mehr als 50 Jahre lang hat die über eine anonyme Liechtensteiner Stiftung bis 1992 von beiden Diensten, danach nur von der CIA gehaltene Crypto AG aus Zug Chiffriermaschinen und Algorithmen zur Ver- und Entschlüsselung mit besten Schweizer Zutaten geliefert: Präzision, Vertraulichkeit, Sicherheit und Neutralität. Als "Mehrwert" gab's dazu auf Geheiss der ausländischen Besitzer aber noch etwas ganz und gar Unschweizerisches dazu:

eine eingebaute Hintertür, die die letzten drei Features ins Gegenteil verkehrt hat. In ihrem unnachahmlichen Zynismus (siehe auch obenstehendes Zitat) hat die CIA denn auch die Operation von "Thesaurus" in Operation "Rubicon" umbenannt. Zur Erinnerung: am 10. Januar des Jahres 49 v. Chr. hatte sich Julius Cäsar über die vom Senat erlassene Anweisung hinweggesetzt, sein Heer zu entlassen und den Fluss unbewaffnet zu überqueren, der die Grenze zwischen den von Cäsar eroberten Provinzen im Norden und dem damaligen Kerngebiet des römischen Reichs markierte – de facto eine Kriegserklärung an den Römischen Senat. Seither steht die Metapher "Überschreiten des Rubicon" für das Überqueren roter Linien unter Inkaufnahme hoher und höchster Risiken.

Die sind auch CIA und BND eingegangen, weil sie durch die Hintertür der Zuger Kryptomaschinen und -algorithmen nicht nur feindliche, sondern auch befreundete Staaten mit Technik aus dem Crypto-Valley ausspionierten. Beide Dienste rechtfertigen dies damit, dass auf diesem Weg viel globales Unheil hat verhindert werden können. Die Kollateralschäden sind indes beträchtlich: Nicht nur die Schweiz diskutiert, wie weit es denn her sei mit Neutralität und Vertrauenswürdigkeit der Alpenrepublik. Der Kanton Zug, in dem seit Mitte der 2010er Jahre mit Stolz der Brand "Crypto-Valley" entwickelt und vermarktet wurde, muss wohl eine neue Marke erfinden. Und Krypto-Technologie und -Industrie haben schwer am Reputationsschaden zu tragen.

Das Misstrauen von Userinnen und Usern trifft auch alle Tech-Konzerne, die ihr Geld mit Kommunikationstechnologie verdienen. Sie alle hätten die Möglichkeit, Hintertüren in ihre Algorithmen einzubauen, mit denen Geheimdienste Nutzerinnen und Nutzer ausspionieren können (und es in einzelnen Fällen – NSA, Cambridge Analytica etc. – nachgewiesenermassen auch getan haben und wohl immer noch oder immer wieder tun). Darauf verweist der amerikanische Verschlüsselungs- und IT-Spezialist Bruce Schneier in einem Interview mit der NZZ (Link unten). Schneier betont darin, dass Verschlüsselung wichtig und nützlich sei, verweist aber darauf, dass sie dennoch nicht vollständig schützt: "Wenn ein Staat Hintertüren für die Spionage einbauen will, wird er das auch tun."

Bleibt als einzige Hoffnung, dass manche Schweizer Täler so eng schliessen, dass nichts aus ihnen durch die Hintertür heraus kann. Vielleicht entstehen hier die nächsten wahren Schweizer Crypto-Valleys.

Nachzulesen unter:

https://www.srf.ch/play/tv/sendung/10vor10?id=c38cc259-b5cd-4ac1-b901-e3fddd901a3d
https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage
https://www.heise.de/newsticker/meldung/Cryptoleaks-CIA-und-BND-steckten-jahrzehntelang-hinter-Verschluesselungsfirma-4658033.html
https://www.nzz.ch/schweiz/der-it-spezialist-bruce-schneier-zur-crypto-affaere-ld.1540118
https://www.inside-it.ch/de/post/crypto-ag-bundesrat-veranlasst-eine-untersuchung-20200211

II. I, Robot, ZigBee und das IoT

Was unterscheidet die Robotik vom Internet der Dinge? Die Robotik kennt – zumindest literarisch – drei einfache Gesetze, die Roboter im menschlichen Umfeld absolut gebrauchssicher machen sollen: The Three Laws of Robotics. Formuliert von Isaac Asimov in seiner 1942 erschienenen Kurzgeschichte "Runaround" wurden sie zur fixen Leitlinie in allen Büchern des Asimovschen Roboter-Science-Fiction-Universums, das mit "I, Robot" seinen Anfang nahm. Sie lauten:

1.) Ein Roboter darf kein menschliches Wesen (wissentlich[3]) verletzen oder durch Untätigkeit (wissentlich[3]) zulassen, dass einem menschlichen Wesen Schaden zugefügt wird.

2.) Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren.

3.) Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert.

Das Internet of Things (IoT) lässt solche einfachen Sicherheitsregeln bislang vermissen. Insbesondere das ZigBee-Protokoll für die Verlinkung von Smart Home-Geräten gibt ab und an zu reden. Bereits zur Black Hat Konferenz 2015 wurde ein Artikel veröffentlicht, der mehrere, teils systemimmanente Sicherheitsrisiken von ZigBee-basierten Smart-Home-Netzen offenlegte. Um deren Sicherheitsstandard zu erhöhen, schlug der Autor des Black-Hat-Vortrags vor, die einzelnen Devices in ZigBee-Netzwerken mit Anti-Manipulationsmassnahmen auszustatten. Nun wurde bekannt, dass eine Sicherheitslücke im Zigbee-Protokoll Angreifern über smarte Philips-HUE-Lampen einen Weg ins Netzwerk des Smart-Home-Besitzers öffnet.

Das Bedrohungspotenzial wird als "hoch" eingestuft, auch wenn der Angriff ohne Mitarbeit des Opfers nicht funktioniert, und der Hersteller inzwischen ein Sicherheitspatch bereitgestellt hat.

Daher treibt die Frage, wie Smart-Home-Netze sicherer gemacht werden, Hersteller, vor allem aber Behörden um. Nun berichtet heise online, dass das britische Ministerium für Digitales, Kultur, Medien und Sport zusammen mit dem National Cyber Centre drei einfache Regeln (Asimov lässt grüssen) formuliert hat, die kurzfristig Gesetz werden könnten, falls das Parlament das so beschliessen würde:

1.) "Alle für Endkunden gedachte Passwörter mit dem Internet verbundener Geräte müssen einzigartig sein".

2.) "Alle Hersteller müssen eine öffentlich zugängliche Stelle einrichten, an die sich alle Nutzer und Sicherheitsforscher wenden können, wenn sie eine Lücke in einem IoT-System entdecken, damit auf sie in angemessener Zeit reagiert werden kann."

3.) "Alle Hersteller müssen bereits beim Verkauf im Laden oder online ihren Kunden gegenüber angeben, wie lange sie für ein von ihnen verkauftes Device Sicherheitsupdates anbieten wollen."

Dieser "Code of Practice for Consumer IoT Security" ist zwar etwas umfangreicher als Asimovs "Three Laws of Robotics", könnte aber wie diese zu einer der tragenden Säulen der Sicherheit im Internet of Things werden.

Nachzulesen unter:

https://de.wikipedia.org/wiki/Robotergesetze
https://www.smarthomeprofis.de/wie-sicher-ist-zigbee
https://www.heise.de/security/meldung/Sicherheitspatch-Philips-Hue-Lampe-als-Sprungbrett-in-Netzwerke-4655060.html
https://www.heise.de/tr/artikel/Gesetzliche-Regelungen-fuer-das-smarte-Heim-4651370.html
https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

III. Sicher ist sicher! Sicher?

Angesichts dessen, wie sehr auf der einen Seite unser Alltag von der Sicherheit und Integrität digitaler Systeme, Netze, Hard- und Software abhängt, und wie sehr diese auf der anderen Seite Bedrohungen und Angriffen krimineller Hacker, staatlicher Geheimdienste und anderer finsterer Gesellen ausgesetzt sind, ist der Einsatz von Security-Produkten und -Systemen verständlich bis unerlässlich. Naturgemäss erhöhen solche Produkte aber auch immer die Komplexität von IT-Systemen. Und je komplexer sich ein System zeigt, desto grösser wird seine Angriffsfläche. Letztlich verhält es sich wie mit Verschlüsselungssystemen im oben beschrieben Fall: Sie sind für die Sicherheit unentbehrlich, tragen aber eigene Risiken in sich und bieten nicht immer hundertprozentigen Schutz. Jüngstes Beispiel: die Sicherheitssoftware-Pakete aus dem Haus Symantec. In den Suites "Symantec Endpoint Protection (SEP)", "Symantec Endpoint Protection Small Business Edition (SEP SBE)" und "Symantec Endpoint Protection Manager (SEPM)" klaffen Sicherheitslücken, die die Angriffsrisiko-Einstufung "hoch" rechtfertigen. Gemäss einer Symantec-Mitteilung sind nur die Versionen SEP und SEP SBE 14.2 RU2 MP1 (14.2.5569.2100) und SEPM 14.2 RU2 MP1 abgesichert. Bei allen ungepatchten Vorgängern könnten Angreifer DDOS-Attacken starten oder gar eigenen Code auf kompromittierten Geräten ausführen. In einer Version sei laut Symantec auch ein DLL-

Injection-Angriff denkbar. Der Hersteller rät darum dringend, die Software-Pakete mit den bereitgestellten Sicherheitsupdates zu aktualisieren.

Ebenfalls ungeschützt vor DDOS-Attacken sind User, die die Sicherheitsmanagement-Software FortiSIEM des Herstellers Fortinet bis einschliesslich zur Version 5.2.6 einsetzen. In diesen Versionen war/ist nämlich ein statischer und zu aller Malaise auch noch unverschlüsselter SSH-Key im Programmcode integriert, den, so Fortinet, Angreifer extrahieren könnten, um sich damit ohne weitere Authentifizierung erneut mit dem System zu verbinden und Angriffe auszuführen. Deshalb rät Fortinet allen Kunden, schnellstmöglich auf FortiSIEM 5.2.7 und aufwärts upzudaten. Wer das integrierte Revers-Tunnel-Feature des Programms nicht nutzt, sollte es zudem deaktivieren (Details dazu im zweiten Link unten).

Von Security-Software verraten und verkauft – und das in des Wortes wahrstem Sinn – sind Nutzerinnen und Nutzer der Antiviren-Software des Herstellers Avast. Der hat nämlich Browser-Daten der Nutzer seiner Software über sein Tochterunternehmen Jumpshot im grossen Stil an Drittunternehmen verkauft. Auf der Kundenliste sollen unter anderem Google, Yelp, Microsoft, McKinsey, Pepsi, Condé Nast und viele andere mehr stehen. Und das seit mindestens Oktober 2018. Damals hatte der Adblock-Plus-Gründer Wladimir Palant die Daten-Weitergabe entdeckt und bekannt gemacht, woraufhin Mozilla und Google in ihren Browsern Avast-AdOns blockiert hatten.

Schon im letzten Security-Report hatten wir darüber berichtet, dass ein Mitarbeiter der Security-Firma Trend Micro Daten von 68.000 Kunden gestohlen und verkauft hatte. Verglichen damit liegt der Avast-Fall in einem ganz anderen Universum. Denn zum ersten hat hier kein fehlbarer Mitarbeiter auf eigene Rechnung gehandelt. Vielmehr war der Verkauf von Kundendaten fixer Bestandteil des Geschäftsmodells. Zum zweiten sind die 68.000 betroffenen Trend Micro Kunden echte Peanuts gegenüber den laut unternehmenseigenen Aussagen 435 Millionen monatlichen Aktivnutzer von Avast-Software. Und zum dritten zeugt es schon von Schamlosigkeit, wenn sich das Avast-Tochterunternehmen Jumpshot im Unternehmensprofil rühmt, das einzige Unternehmen zu sein, dass die wertvollsten geschlossenen Systeme (walled gardens) im Internet aufschliessen und das komplette Surfverhalten der User registrieren zu können. Nicht mehr aufschliessen lässt sich unterdessen die Website www.jumpshot.com für Interessierte. Wer darauf klickt, findet weder Logo noch Informationen, sondern nur noch eine komplett leere weisse Seite mit der Textzeile: "Jumpshot has ceased operations. Thank you."

Nachzulesen unter:

https://www.heise.de/security/meldung/Sicherheitsupdates-Symantec-Endpoint-Protection-vielfaeltig-angreifbar-4659864.html
https://www.heise.de/security/meldung/Fortinet-entfernt-SSH-Backdoor-aus-Security-Management-Loesung-FortiSIEM-4647473.html

https://www.heise.de/newsticker/meldung/Avast-Antivirus-verkauft-massenhaft-Browser-Daten-seiner-Nutzer-4646926.html
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH-Security-Report-2019-06-de.pdf
https://www.prnewswire.com/news-releases/jumpshot-strikes-strategic-partnership-deal-with-ascential-to-provide-marketers-with-deeper-visibility-into-the-entire-online-customer-journey-300888439.html?tc=eml_cleartime

IV. Viren, mal anders: China bringt die "Close Contact Detector" App auf Smartphones

Wenn wir hier im Security Report von Viren berichten, dann geht es im Normalfall immer um die digitale Variante, die Geräte aller Art befällt und kompromittiert. Wenn wir nun erstmals über ein medizinisches Virus berichten, dann deshalb, weil der Versuch der chinesische Regierung, die Verbreitung des Virus Sars-CoV-2 – besser bekannt als "Corona-Virus", offenlegt, wie subtil, umfassend und flächendeckend die Überwachungsmaschinerie im bevölkerungsreichsten Staat der Erde funktioniert. Am 11. Februar berichtete die BBC, dass die chinesische Regierung vor dem Hintergrund der offenbar doch pandemisch wachsenden Fälle gemeldeter Coronavirus-Infektionen eine App lanciert hat, die ihre User warnen soll, wenn sie mit Personen in Kontakt gekommen sind, die als infiziert gemeldet oder verdächtig sind. Der Download erfolgt via QR-Code-Reader, wie er in den Apps des Bezahldienstes Alipay oder der Social Media Plattform WeChat integriert ist. Die App registriert (und sendet) die Nummer des Smartphones, auf die sie geladen wurde. Name und Ausweisnummer müssen die User noch selbst eingeben. Dann bekommen sie mitgeteilt, ob eine Infektionsrisiko für sie besteht. Ist dies der Fall, werden sie aufgefordert, zuhause zu bleiben und die lokalen Gesundheitsbehörden zu informieren.

Damit die App funktioniert, kombiniert sie offenbar die Daten registrierter oder verdächtiger Virenträger mit deren und den Bewegungsprofilen des Anfragenden. Basis ihrer Effizienz ist offenkundig ein engmaschiges Überwachungsnetz, dessen elaborierteste Form am deutlichsten im so genannten "Uigurischen Autonomen Gebiet Xinjiang" erkennbar ist und von BuzzFeed als "real gewordener Polizeistaat des 21. Jahrhunderts" bezeichnet wurde. Die Kommunikationsplattform persoenlich.com schreibt dazu: "Im Kampf gegen die Ausbreitung von Sars-CoV-2 fährt China seine ganze Überwachungstechnologie auf." Und das wirft Fragen auf: Ist das ein Akt strategischer Planung, um die Verbreitung des Coronavirus so effektiv wie möglich einzudämmen? Ist es panische Verzweiflung einer überforderten Regierung? Ist es blanker Zynismus eines totalitären Regimes oder "something in between"? Damit steht zu befürchten, dass die neue App, auch wenn sie mit den besten Absichten gestartet worden sein sollte, den Verschwörungstheoretikern Wasser auf ihre ohnehin heisslaufenden Mühlen liefern wird.

Nachzulesen unter:

https://www.bbc.com/news/technology-51439401
https://futurezone.at/netzpolitik/app-warnt-wenn-man-kontakt-mit-coronavirus-infizierten-hatte/400751361
https://9to5mac.com/2020/02/11/coronavirus-app
https://www.engadget.com/2020/02/12/china-close-contact-detection-app-coronavirus
https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here
https://www.persoenlich.com/digital/china-kampft-mit-daten-gegen-virus
https://www.engadget.com/2018/02/22/china-xinjiang-surveillance-tech-spread
https://insideparadeplatz.ch/2020/01/29/stammt-corona-virus-aus-wuhan-waffenlabor

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

Der SWITCH Security Report greift aktuelle Themen aus dem Bereich der Cybersecurity auf und wendet sich an interessierte Internetnutzerinnen und -nutzer, um sie für die aktuellen Gefahren zu sensibilisieren. Eine Haftung für die Richtigkeit kann trotz sorgfältiger Prüfung nicht übernommen werden.