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

September / Oktober 2017

SWITCH

I. Angriff der Digitaldelfine: Alexa, Siri & Co. lassen sich mit Ultraschall hacken

Dass sowohl die amerikanische Marine in San Diego als auch die russische in Sewastopol Delfine dazu ausbilden, Waffen, Minen und feindliche Taucher zu orten und ggfs. auch anzugreifen, ist seit den frühen 2000er-Jahren bekannt. Dass mit sogenannten Dolphin Attacks auch digitale Sprachassistenten wie Alexa (Amazon), Siri (Apple), Cortana (Microsoft), Google Now, S Voice (Samsung) oder Hi Voice (Huawei) manipuliert werden können, haben Forscher der Zhejiang University nachgewiesen – wenn auch unter Laborbedingungen. In ihrem Versuch modulierten sie Sprachbefehle in den für menschliche Ohren nicht mehr hörbaren Ultraschallbereich jenseits von 20.000 Hz und schickten diese «inaudible voice commands» an Geräte, auf denen eines der oben genannten Sprachassistenz-Systeme installiert und aktiviert war. So konnten sie FaceTime-Anrufe auf einem iPhone starten und ein Android-Handy in den Flugmodus schalten. Das klingt zunächst nach nichts Weltbewegendem. Mit der Manipulation des Navigationssystems eines Audi bekamen die Angriffsversuche der Forscher aber eine andere Dimension. Zudem werden viele der angreifbaren Geräte als Steuerzentrale für weitere Geräte, IoT-

Devices oder Netzwerke genutzt, wie z.B. Connected Cars, Smart Homes, Zutrittssysteme uvm.

Die chinesischen Forscher befürchten, dass Dolphin-attackierte Geräte in mehrfacher Weise Schaden verursachen könnten:

- Das Gerät wird zum Besuch einer Malware-Website aufgefordert und wird Opfer einer Drive-by-Attacke, die Malware auf dem Gerät installiert.
- Das Gerät wird aufgefordert, einen Video- oder Telefonanruf an eine Adresse zu starten, an der Ton- oder Bildnachrichten aufgezeichnet werden, um den Besitzer des Geräts auszuspionieren.
- Das Gerät wird aufgefordert, Fake-Informationen via Textmessage, E-Mail oder Online-Posts zu verbreiten oder im Kalender des Besitzers Fake-Termine einzutragen.
- Das Gerät wird aufgefordert, in den Flugmodus zu schalten und damit seinen Besitzer unbemerkt von jeder kabellosen Kommunikation abzuschneiden.
- Dem Gerät werden Befehle übermittelt, die den Angriff verschleiern sollen.

Zur Abhilfe schlagen die Forscher sowohl hard- als auch softwareseitige Massnahmen vor: von der Verbesserung der Mikrofone bis zum Einsatz von Software, die solche Dolphin Attacks erkennt und ausfiltert.

Nachzulesen unter:

https://arxiv.org/pdf/1708.09537.pdf
https://www.youtube.com/watch?v=XBbHDQH47tk
https://thehackernews.com/2017/09/ai-digital-voice-assistants.html
https://hothardware.com/news/siri-alexa-ai-vulnerable-ultrasonic-dolphin-attack-hijacking-commands
http://t3n.de/news/forscher-hack-siri-alexa-ultraschall-855527

II. Anti-Antivirus-Programm: US-Regierung verbannt Kaspersky-Software von Behördenrechnern

Das 20. Jubiläumsjahr der Firmengründung hatte sich Jewgeni Walentinowitsch – oder kürzer: Eugene – Kaspersky sicher anders vorgestellt. Denn der Bann, mit dem die US-Regierung Kaspersky-Software zur Mitte des Jahres belegte, kratzt am wichtigsten Kapital einer IT-Security-Firma: dem Vertrauen der User. Auch wenn seit 1997 immer wieder über die Verbindungen des Absolventen einer Hochschule des russischen Geheimdienstes KGB spekuliert wird, gilt Kaspersky als anerkannter

Security-Experte. Seiner Software vertrauen aktuell etwa 400 Millionen User auf der ganzen Welt, um sich vor Spionage, Hacking und Datenmissbrauch zu schützen. Darunter sind auch so bekannte Namen wie das deutsche Bundeskriminalamt und eine stattliche Anzahl von US-Behörden. Doch die sahen sich Mitte September mit der Aufforderung der US-Regierung konfrontiert, binnen 60 Tagen Pläne vorzulegen, wie die Nutzung von Kaspersky-Programmen gestoppt werden könne, die dann innerhalb von weiteren 90 Tagen umzusetzen seien. Bereits im Juli 2017 hatte die US-Beschaffungsbehörde GSA das in Moskau domizilierte Unternehmen von der Liste zugelassener Anbieter für Internetsicherheitsprodukte gestrichen. Eugene Kaspersky wies seinerzeit geäusserte Spionagevorwürfe mit den Worten zurück: «Das Unternehmen hat niemals und wird niemals irgendeiner Regierung auf der Welt dabei helfen, Cyberspionage zu betreiben.»

Hintergrund der Auseinandersetzung sind Befürchtungen des FBI und der amerikanischen Heimatschutzbehörde, dass russische Geheimdienste und Regierungseinrichtungen via Kaspersky-Software ihre US-amerikanischen Pendants ausspionierten. In mehreren Interviews und auf seinem Twitterkanal betonte und betont Kaspersky immer wieder, dass es keinerlei Beweise für die Anschuldigungen gegen sein Unternehmen gäbe und die Vorwürfe der US-Regierung haltlos und unbegründet seien: «Wir werden unseren Kunden niemals schaden. Wir schützen sie vor Malware - sei sie nun russische oder amerikanische oder von irgendeiner anderen Nation.» Schützenhilfe bekommt der Security-Experte vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI), das die gute und vertrauensvolle Zusammenarbeit mit Kaspersky Lab hervorhebt und darauf verweist, dass Kaspersky als erstes zahlreiche Cyber-Spionage-Kampagnen russischen Ursprungs veröffentlicht und detailliert beschrieben habe.

Die Entwicklung der Auseinandersetzung und eine detaillierte Herleitung ihrer Ursachen hat Vesselin Bontchev auf medium.com fundiert dargestellt. Darin bedauert er, dass die gesamte Aktion eigentlich nur Verlierer produzieren kann: De US-Behörden würden mit dem Verdikt auf eine der besten Virenschutz-Software verzichten müssen. Kaspersky selbst wird im US-Markt, der für 25% seiner Wertschöpfung verantwortlich ist, viel Geld verlieren. Und schliesslich befürchtet Bontchev, dass alle User an Sicherheit einbüssen würden, weil aus seiner Sicht unethische Kampagnen verschiedener Kaspersky-Wettbewerber (Symantec, Bitdefender, McAfee, Avira und andere) die Zusammenarbeit der Cybersecurity-Spezialisten gefährde.

Inzwischen vermeldete Bloomberg, dass eine Anhörung des Ausschusses für Wissenschaft, Weltraum und Technik im amerikanischen Repräsentantenhaus am 27. September kurzfristig abgesagt und durch ein geheimes Treffen zum gleichen Thema ersetzt wurde. Bei der Anhörung hätte Kaspersky zu den Vorwürfen Stellung nehmen sollen – und auch wollen. Ein Ersatzdatum ist ebensowenig bekannt wie die weitere Entwicklung.

Nachzulesen unter:

https://www.reuters.com/article/us-kasperskylab-russia-usa/russia-doesnt-rule-out-retaliation-if-u-s-bans-kaspersky-products-idUSKBN19K1KV
https://www.reuters.com/article/us-usa-kasperskylab/trump-administration-limits-government-use-of-kaspersky-lab-software-idUSKBN19W2W2
https://www.cyberscoop.com/fbi-kaspersky-private-sector-briefings-yarovaya-laws
https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152_story.html?utm_term=.f88d7b7b5e55
https://www.usatoday.com/story/tech/news/2017/09/14/confusion-hits-consumer-market-over-u-s-ban-kaspersky-software/666211001
http://www.spiegel.de/netzwelt/netzpolitik/kaspersky-firmenchef-eugene-kaspersky-verteidigt-sich-gegen-anschuldigungen-a-1167916.html
http://www.zeit.de/digital/2017-09/spionageverdacht-usa-russland-kaspersky-software
http://www.focus.de/digital/computer/unternehmen-bsi-lobt-nach-us-vorwuerfen-vertrauensvolle-zusammenarbeit-mit-kaspersky_id_7593541.html
https://medium.com/@bontchev/understanding-the-us-government-kaspersky-lab-controversy-f0ed6cd3b52
https://www.bloomberg.com/news/articles/2017-09-26/house-panel-is-said-to-receive-classified-briefing-on-kaspersky

III. «Kolossal-epochaler» Hack bei Equifax

Equifax ist der grösste Wirtschaftsauskunftsdienst der USA. Auf den Servern des in Atlanta im US-Bundesstaat Georgia beheimateten Traditionsunternehmens (gegründet 1899 als Retail Credit Company) sind Sozialversicherungs-, Kreditkarten- und Führerscheinnummern, Geburts- und Adress- sowie weitere Daten von Abermillionen Kunden aus den USA, Kanada und Grossbritannien gespeichert. 143 Millionen von ihnen müssen nun davon ausgehen, dass ihre Daten in falsche Hände bzw. auf falsche Server gelangt sind. Denn Equifax wurde Opfer des bisher grössten Diebstahls von Sozialversicherungsnummern überhaupt, auch wenn sich die Zahl angesichts ~~500 Millionen~~ drei Milliarden* gehackter Yahoo-Accounts relativiert – für eine Wirtschaftsauskunftei ist dieser Hack dennoch der Super-GAU. Denn neben dem Verlust des Kundenvertrauens musste Equifax auch hinnehmen, dass die Zertifizierungsstelle nach Bekanntwerden des Hacks und seiner Umstände das SSL

Root Zertifikat widerrief. Diese Umstände und Begleiterscheinungen toppen dann auch den als «kolossal» oder «epochal» bezeichneten Hack und lassen interessierten Beobachtern die Haare zu Berge stehen.

So musste die Firma am 7. September eingestehen, dass die Hacker schon von Mai an ungestört Daten stehlen konnten, bis der virtelle Einbruch am 29. Juli schliesslich entdeckt wurde. Dabei nutzten sie eine Sicherheitslücke in Apache Struts aus, für die seit März ein Patch bereit stand. Equifax hatte diesen aber schlichtweg nicht installiert. Dabei wurde Equifax bereits im März Opfer eines Datenhacks, hatte diesen aber offenbar aus Angst um den Vertrauensverlust verheimlicht, bis Bloomberg zugespielte Insider-Informationen darüber veröffentlichte. Zwar bemühte sich Equifax eilfertig zu erklären, dass beide Hacks nichts miteinander zu tun hätten, sah sich aber mit dem Vorwurf konfrontiert, dass Muster und Angreifer in beiden Fällen identisch gewesen seien.

Weitere Brisanz bekommt das Bekanntwerden dieses früheren Hacks dadurch, dass leitende Mitarbeiter der Firma Anteile am Unternehmen im Gesamtumfang von 1,8 Millionen Dollar verkauft hatten und nach dem zweiten Hack ganze sechs Wochen verstreichen liessen, ehe sie die Öffentlichkeit informierten. Deshalb hat die Staatsanwaltschaft inzwischen ein Ermittlungsverfahren wegen Verdachts auf Insiderhandel eröffnet.

Am 21. September berichtete der Multimedianachrichten- und Radioproduzent npr in seinen Breaking News, dass Kunden, die von Equifax aufgefordert wurden, durch Eingabe ihrer Sozialversicherungsnummer zu prüfen, ob ihr Account unter den gehackten sei, auf eine Fakeseite geleitet wurden, die ihre Daten – dann zum zweiten, oder gar zum dritten Mal abfischen konnte. Es scheint, als habe Equifax eine spezielle Interpretation für das Wort Traditionsunternehmen gefunden.

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/Equifax-soll-frueheren-Hack-verheimlicht-haben-3835052.html
http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html
https://www.washingtonpost.com/opinions/the-equifax-disaster-points-to-a-much-bigger-problem/2017/09/21/4bd683da-9ee3-11e7-9083-fbfddf6804c2_story.html?utm_term=.602d6b1a0fda
https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed
http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site
https://www.golem.de/news/kreditrating-equifax-krisenreaktion-ist-ein-desaster-1709-129967.html
https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/chefs-verkaufen-aktien-bevor-gigantischer-hack-publik-wird/story/15298299
* https://www.golem.de/news/yahoo-mail-alle-yahoo-kunden-im-jahr-2013-gehackt-1710-130405.html

IV. Science Fiction 4.0 – Wie man Computer mit Spucke hackt

Welche neuartigen Sicherheitsrisiken entstehen, wenn biomolekulare Information auf binäre Informationsverarbeitung trifft? Diese Ausgangsfrage führte zwei Forscher an der Universität von Washington zum wohl futuristischsten Hack des Jahres – der Kaperung eines Computers mithilfe malwareverseuchter DNA. Ziel von Tadayoshi Kohno und Luiz Ceze war es dabei, darauf hinzuweisen, dass mit einer immer weiteren Entwicklung der Gentechnologie auch die Risiken steigen, dass Geräte zur DNA-Sequenzierung gehackt werden könnten. Davon betroffen sind unter anderem Hochschulen, kommerzielle Forschungseinrichtungen und Labore der Life Science Industrie oder der Polizei.

Der Hack selbst fand in drei Stufen statt: Zunächst schrieben die Forscher bösartigen Binärcode, der sich via Exploit auf den Rechner schleichen sollte. Diesen Code übersetzten sie in eine DNA-Sequenz, die sie für 89 Dollar synthetisieren liessen. Auf dem Zielsequenzierer lasen sie die kompromittierte DNA wieder aus und analysierten die ausgelesenen Daten mit üblicher Software. Ergebnis: Der via DNA eingeschleuste Exploit brachte den Rechner dazu, Kontakt zum Command-and-Control-Server aufzunehmen, vor dem im Ernstfall ein Hacker gesessen hätte. Dieser hätte nun via befallenem Rechner Zugriff aufs Netzwerk gehabt, in das der Rechner eingebunden war. Auch wenn Kohno und Ceze selbst darauf verweisen, dass ein solcher Angriff wohl auf Jahre hinaus nicht zur realen Bedrohung werden wird, konnten sie doch nachweisen, dass DNA-Analysesoftware dem allgemeinen Sicherheitsstandard nicht genügt, und einen Weckruf absetzen, dem Gehör zu wünschen ist

Nachzulesen unter:

http://www.zeit.de/digital/internet/2017-08/dna-malware-hacker
http://www.washington.edu/news/2017/08/10/dna-sequencing-tools-lack-robust-protections-against-cybersecurity-risks
https://techcrunch.com/2017/08/09/malicious-code-written-into-dna-infects-the-computer-that-reads-it
https://www.theguardian.com/technology/2017/aug/11/hacking-computer-dna-university-of-washington-lab
https://www.technologyreview.com/s/608596/scientists-hack-a-computer-using-dna

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