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

September 2016

SWITCH

I. Bug Bounties und Cyber Grand Challenge

Es gab eine Zeit, da haben Hacker noch viel auf ihre Non-Konformität gegeben. Wenn es aber um die Ökonomisierung geht, stehen sie anderen Bereichen der Gesellschaft in nichts nach. Bugs und Sicherheitslücken zu entdecken und Zero-Day-Exploits zu schreiben soll sich schliesslich nicht nur ideell, sondern auch finanziell lohnen. So zitiert The Guardian den 21-jährigen Nathaniel Wakelam, der behauptet, pro Jahr mit seinem Macbook von Coffeeshops aus 250.000 Dollar als Bug Bounty-Hunter zu verdienen. Doch auch, wo nicht mit Dollars, sondern beispielsweise mit Flugmeilen belohnt wird, steigt das Hackerinteresse. Golem.de berichtete jüngst von einem 19-jährigen Niederländer, der für die Entdeckung von Sicherheitslücken bei United Airlines bisher insgesamt eine Million Meilen gesammelt haben soll.

Und trotz Dementis der zuständigen Stellen halten sich die Gerüchte, dass das FBI für die Entsperrung des iPhones eines der San Bernardino-Attentäter (wir berichteten im Security Report März und Mai 2016) eine Prämie von mehr als einer Million Dollar bezahlt haben soll. Der Fall scheint Apple dazu bewogen zu haben, auf der jüngsten Black-Hat-Konferenz Ende Juli in Las Vegas ein Bug Bounty-Programm

anzukündigen und Gelder von bis zu 200.000 US-Dollar in Aussicht zu stellen. Auch Kaspersky kündigte ein solches Programm an, wenn auch mit deutlich niedrigeren Prämien.

Anders als Google, Facebook, Amazon und Microsoft hatte Apple bis dato keinerlei Prämien ausgelobt, sondern die Lücken-Entdecker lobend auf der Website erwähnt. Grund dafür war Apples Befürchtung, dass mit einem Bug Bounty-Programm ein Bieterwettbewerb um Sicherheitslücken entstehen könnte, bei dem die Sicherheit von Millionen Usern gegenüber der Bereicherung einzelner den Kürzeren ziehen könnte.

Der Beweis dafür, dass dahinter keine kulturpessimistische Rechtfertigungsrhetorik, sondern solide Menschenkenntnis steckt, folgte denn auch auf dem Fusse: Der Exploit-Händler Exodus Intelligence bot umittelbar nach Bekanntwerden des Apple Bug Bounty-Programms 500.000 Dollar für eine Zero-Day-Lücke in iOS. Exploit-Dealer wie Exodus Intelligence verkaufen ihre heisse Ware meistbietend – auch an Regierungen und Geheimdienste.

Dass auch renommierte Wissenschaftler am Software Engineering Institute SEI der Carnegie Mellon University dem Lockruf des Geldes nicht widerstehen konnten und gegen Zahlung von mindestens einer Million Dollar dem FBI halfen, Tor-User zu deanonymisieren, berichteten wir im Security Report vom März 2016.

Dagegen zeigten die Kollegen des AllForSecurity-Teams der gleichen Uni an der ebenfalls in Las Vegas ausgetragenen Cyber Grand Challenge (CGC), dass man auch ohne Gefährdung des eigenen guten Rufs zur doppelten Summe kommen kann. In dem erstmals ausgetragenen reinen Machine-2-Machine-Contest versuchten autonome Server, sich gegenseitig zu hacken. Die Siegprämie von 2 Millionen Dollar ging an das AllForSecurity-Team. Zwar reichen die Fähigkeiten der Server, nach Aussagen des CGC-Leiters Mike Walker, noch nicht an die menschlicher Hacker heran. Die Ökonomisierungstendenzen werden sich aber vielleicht künftig aber auch auf ihre humanen Betreiber auswirken.

Nachzulesen unter:

http://www.golem.de/news/united-airlines-bug-bounty-programm-19-jaehriger-hacker-ist-meilenmillionaer-1608-122595.html
https://www.theguardian.com/technology/2016/aug/22/bounty-hunters-hacking-legally-money-security-apple-pentagon
http://www.zeit.de/digital/datenschutz/2016-08/bug-bounty-apple-black-hat
https://techcrunch.com/2016/08/04/apple-announces-long-awaited-bug-bounty-program

http://www.trojaner-info.de/daten-sichern-verschluesseln/aktuelles/kaspersky-startet-bug-bounty-programm-mit-hohen-erfolgspraemien.html
http://m.heise.de/mac-and-i/meldung/iOS-Bug-Bounty-Programm-Exploit-Haendler-will-mehr-zahlen-als-Apple-3293301.html
http://www.golem.de/news/united-airlines-bug-bounty-programm-19-jaehriger-hacker-ist-meilenmillionaer-1608-122595.html
https://www.theguardian.com/technology/2016/aug/22/bounty-hunters-hacking-legally-money-security-apple-pentagon
https://www.technologyreview.com/s/602224/a-bug-hunting-hacker-says-he-makes-250000-a-year-in-bounty
http://www.spiegel.de/netzwelt/games/cyber-grand-challenge-in-las-vegas-server-gegen-server-a-1106293.html
http://www.csoonline.com/article/3104823/security/supercomputers-give-a-glimpse-of-cybersecuritys-automated-future.html

II. Pegasus spioniert Apple-Geräte aus, QuadRooter bedroht Android

Dass und in welchem Ausmass Apple-Geräte Angriffsziel für bösartige Software geworden sind, zeigte sich beim Bekanntwerden der Spionagesoftware «Pegasus». Anfang August entdeckte ein Menschenrechtsaktivist einen verdächtigen Link auf seinem iPhone und schaltete die IT-Sicherheitsfirma Lookout ein, die «die ausgeklügeltste Attacke, die wir je auf einem Endgerät gesehen haben» entdeckte. Die Spyware nutzte gleich drei Schwachstellen im iOS-Betriebssystem für iPhones, iPads und dem Mediaplayer iPod touch, um de facto alles, was auf den Geräten geschieht, abzugreifen. Ihren Ursprung hat sie in der israelischen Cyberwaffenschmiede NSO, die einem US-Investor gehört, und die Spyware nach eigenen Angaben konform mit allen Ausfuhrbestimmungen ausschliesslich an Regierungsbehörden verkauft – die letztere freilich auch dazu nutzen, um Menschenrechtler und Journalisten auszuspähen. Zwei Wochen nach der Entdeckung von Pegasus hat Apple ein gepatchtes Update für iOS bereitgestellt und am 1. September auch ein Sicherheitsupdate für Laptops und Desktops unter OS X nachgeschoben, weil Pegasus auch auf diesen Geräten vor sich hin galoppiert war. Auch Lookout ist nicht untätig gewesen und hat die Beschreibung von Pegasus im hauseigenen Blog gepostet. Zudem informiert ein PDF, wie Benutzer kompromittierte Geräte erkennen können.

Szenariowechsel Android-Sicherheitslücken: Diesmal sind es gleich vier, daher der Name QuadRooter. Wieder ist eine israelische Sicherheitsfirma involviert, diesmal aber auf Seiten der «Guten». Denn das Unternehmen «CheckPoint» hat QuadRooter entdeckt und auf der Hackerkonferenz Defcon Anfang August in Las Vegas veröffentlicht. Anders als der gute alte Vorsatz «What happens in Vegas stays in

Vegas» suggeriert, soll QuadRooter weltweit unterwegs sein und mehr als 900 Millionen Android-Geräte bedrohen. Drei der vier Sicherheitslücken hat Google inzwischen geschlossen. Nur dauert es aufgrund der unterschiedlichen Marktstrukturen weitaus länger als bei iOS-Geräten, bis Updates auf Android-Devices aller Hersteller und zur Verfügung stehen.

Wesentlich schneller waren da offenbar die Hacker auf der dunklen Seite. Denn Sicherheitsexperten von RiskIQ hatten zwischenzeitlich im offiziellen Google sowie in zahlreichen inoffiziellen App-Stores 27 bösartige Apps entdeckt, die unter dem Vorwand, QuadRooter zu entdecken und/oder unschädlich zu machen, selbst Malware auf die Geräte bringen. So warnt RiskIQ auch ausdrücklich davor, Apps aus inoffiziellen Stores zu beziehen. Inzwischen verwies Google darauf, dass gar keine fremden Apps gebraucht würden, weil die seit Android 4.2 standardmässig installierte Funktion «App überprüfen» gefährliche Apps überprüfen, identifizieren und entfernen könne. 90% aller 900 Millionen Geräte seien damit gegen QuadRooter-Angriffe geschützt, auch wenn die Lücke auf den Qualcomm-Chips weiter bestehe, bis entsprechende Patches installiert seien.

Nachzulesen unter:

http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/forscher-entdecken-gefaehrliche-spionage-software-fuer-iphones-14406241.html
http://derstandard.at/2000043729494/OS-X-Update-Apple-stopft-Pegasus-Luecke-auch-auf-Macs
http://www.heise.de/newsticker/meldung/Gegen-Spionagesoftware-Pegasus-fuer-iPhones-iOS-9-3-5-behebt-Sicherheitsluecken-3305339.html
https://blog.lookout.com/blog/2016/08/25/trident-pegasus
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-how-to-tell-impacted.pdf
http://www.zeit.de/digital/mobil/2016-08/android-quadrooter-sicherheitsluecke-900-millionen
http://www.nzz.ch/digital/quadrooter-fast-eine-milliarde-android-geraete-mit-sicherheitsluecken-ld.109608
http://blog.checkpoint.com/2016/08/07/quadrooter
http://www.welivesecurity.com/2016/08/11/quadrooter-vulnerabilities-leaves-900-million-android-devices-risk-attack
http://www.infosecurity-magazine.com/news/malicious-quadrooter-apps
http://www.heise.de/security/meldung/Grossteil-der-Android-Geraete-ist-standardmaessig-gegen-QuadRooter-Luecke-gewappnet-3293022.html

III. Zahltag für eine 22 Milliarden-Investition: WhatsApp teilt Telefonnummern mit Facebook

Vor knapp 2 Jahren verwunderte die Nachricht, dass Facebook kolportierte 22 Milliarden Dollar investierte, um den Messengerdienst WhatsApp zu übernehmen. Einer, der wusste warum, war Mikko Hippönen von der finnischen Sicherheitsfirma F-Secure. In seiner auf YouTube verfügbaren USI-Keynote vom Juli 2015 stellt er dar, dass erst die Mobiltelefonnummer die eindeutige Verknüpfung eines Daten-Profils mit einer realen Person – und damit mit anderen Daten-Profilen – ermöglicht und vermutete darin den Grund für Facebooks Investition.

Nun schlägt der Facebook-Deal erneut mediale Wellen, denn Ende August vermeldete The Guardian, das WhatsApp die Telefonnummern seiner User an Facebook übermittle, damit der Mutterkonzern damit nach eigenen Angaben «gezieltere Werbung» und eine «verbesserte Suche nach Freunden» realisieren könne. Zwar räumte Facebook WhatsApp-Nutzern eine 30-Tage-Frist ein, der Verwendung ihrer Daten zu Werbezwecken durch Facebook zu widersprechen, die Übermittlung der Daten von WhatsApp zu Facebook bleibt davon aber unberührt. Nun prüft EU-Wettbewerbskommissarin Margrethe Vestager, ob sie das Fusionskontrollverfahren neu aufrollen muss. Freude herrscht dagegen wohl beim Schweizer Messengerdienst Threema, dessen App-Downloads sich seit Bekanntwerden der Tauschabsichten verdreifacht haben sollen.

Nachzulesen unter:

https://www.youtube.com/watch?v=Umm-97wb_aE
https://www.theguardian.com/technology/2016/aug/25/whatsapp-to-give-users-phone-number-facebook-for-targeted-ads
http://www.golem.de/news/fuer-werbezwecke-whatsapp-teilt-alle-telefonnummern-mit-facebook-1608-122902.html
http://www.spiegel.de/netzwelt/apps/facebook-eu-kommission-ueberprueft-whatsapp-uebernahme-a-1110682.html
https://www.wired.de/collection/business/dank-wahtsapp-explodieren-die-downloadzahlen-des-messaging-diensts-threema

IV. Wir sind dann mal weg: Der nächste Multi-Millionen-Bitcoin-Diebstahl

Um grosse Zahlen geht es auch beim neuerlichen Verschwinden von Bitcoins. Am 3. August teilte die Hongkonger Bitcoin-Handelsplattform Bitfinex mit, dass sie den Betrieb eingestellt habe, nachdem man feststellen musste, dass Hacker bei einem Angriff 120.000 Bitcoins im Gegenwert von ca. 58 Millionen US-Dollar erbeutet hatten. Verglichen mit den 500 Millionen Dollar, deren Diebstahl im Jahr 2014 das Aus für die Tokioter Bitcoinbörse Mt. Gox bedeutet hatten, nimmt sich die Bitfinex-Beute zwar bescheiden aus. Doch ist der Bitcoin-Kurs nach Bekanntwerden des Überfalls um mehr als 20% gesunken und das Vertrauen in virtuelle Währungen generell weiter beschädigt worden. Zumal ja bereits im Juli diesen Jahres ein Hacker aus dem Dao-Projekt ETHER im Wert von mehr als 50 Millionen Dollar abzweigen konnte (wir berichteten im Security Report vom Juli 2016). Die Konsequenzen aus jenem Fall sind eigentlich viel gravierender. Denn anders als im Bitfinex- und im Mt.Gox-Diebstahl wurde beim Dao-Projekt eine Blockchain erfolgreich gehackt und der Mythos zerstört, dass die bis dahin als bombensicher geltende Technologie bedenkenlos als Basistechnologie für Fintech-Anwendungen eingesetzt werden könnte.

Nachzulesen unter:

http://www.spiegel.de/netzwelt/web/bitcoin-hacker-erbeuten-digitalwaehrung-in-millionenwert-a-1105932.html
http://www.nzz.ch/finanzen/uebersicht-finanzen/bitcoin-unfaelle-der-mythos-virtuelle-waehrung-broeckelt-weiter-ld.109742
http://www.heise.de/security/meldung/Bitfinex-Hack-58-Millionen-Euro-gestohlen-Bitcoin-Kurs-eingebrochen-3286784.html

V. DiskFiltration und Fansmitter proben die Überwindung des Air-gaps

Weil letztlich alle Systeme, die über das Internet oder andere Netzwerke erreichbar sind, gehackt werden können, gibt es solche, die weder über das Internet noch andere Netzwerke erreichbar sind: Air-Gap-Systeme. Die Frage, wie man an die zumeist hochsensiblen Daten herankommt, die von solchen Systemen gespeichert und verwaltet werden, beschäftigt Hacker und Sicherheitsforscher rund um den Globus. Nun haben Researcher der Ben-Gurion-Universität eine weitere Antwort darauf

präsentiert: Die von ihnen entwickelte Malware DiskFiltration kann dem Lese-/Schreibkopf von Harddisks Geräuschmuster entlocken, mit denen sich z.B. Passwörter auslesen lassen sollen.

Der Erfolg der Malware ist allerdings fragil an verschiedene Faktoren geknüpft. Das Audio-Aufnahme-Gerät muss sich im Umkreis von zwei Metern um das Air-Gap-System befinden. Die Malware muss von aussen, etwa auf einem USB-Stick, ins Air-Gap-System gebracht werden. Und DiskFiltration funktioniert aufgrund des fehlenden Lese-/Schreibkopfes nicht bei SSD-Festplatten.

Eine andere aktuelle Forschungsarbeit von der Ben-Gurion-Universität des Negev in Israel nutzt für die Überwindung des Air-gaps den Computerlüfter.

Dass man akustische Signale dazu benutzen kann, Computer miteinander zu verbinden, macht sich auch Google Tone zunutze. Die App ist als Addon für Google Chrome erhältlich und ermöglicht den Austausch von URLs über das Air-gap.

Nachzulesen unter:

http://www.heise.de/newsticker/meldung/Das-Schnurren-einer-Festplatte-verraet-Geheimnisse-3295965.html
http://www.techworm.net/2016/06/now-fan-noise-can-used-steal-data-air-gapped-computers.html
https://chrome.google.com/webstore/detail/google-tone/nnckehldicaciogcbchegobnafnjkcne?hl=en

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