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

Mai/Juni 2017

SWITCH

I. Zum Heulen! WannaCry verschlüsselt ungepatchte Systeme

Wenn man manchen Medienberichten glaubt, war es der «bislang grösste Cyberangriff der Geschichte». Mit einer Story, die als Thriller das Zeug zum Bestseller hätte: Mit unrühmlicher Beteiligung der üblichen Verdächtigen, wie der NSA und Nordkorea, sowie einem eher zufällig zum Helden gestolperten Malware-Blogger. Und mit lebensbedrohenden Folgen für Leib und Leben realer Menschen.

Die Fakten: Am 12. Mai 2017 verbreitet sich WannaCrypt (auch bekannt als WannaCry, WCry oder WanaCrypt0r) explosionsartig in der Welt nicht gepatchter Windows-Computer, verschlüsselt die dort gespeicherten Daten und verlangt für deren Freigabe 300 US-Dollar in Bitcoins innerhalb von 3 Tagen. Danach soll sich das Lösegeld verdoppeln. Nach 6 Tagen ohne Zahlung drohen die WannaCrypt-Criminals mit der Löschung der Daten. Die Besonderheit zu anderer Ransomware: WannaCrypt verbreitet sich als Wurm. Die Ransomware nutzt dazu eine Schwachstelle in dem Microsoft Server Message Block-Protokoll in der veralteten Version 1 (SMBv1). Diese wurde bekannt, als eine Hackergruppe namens Shadow Brokers mehrere Exploits - darunter auch EternalBlue - der dem US-amerikanischen Geheimdienst NSA nahestehenden Equation Group veröffentlicht hatte. Microsoft stellte daraufhin

entsprechende Patches für aktuelle Betriebssystem-Versionen zur Verfügung, nicht upgedatete Systeme blieben aber natürlich ungeschützt.

Am Montag, 15. Mai, war von bereits mehr als 200.000 infizierten Rechnern in über 100 Ländern die Rede, am Ende sollten es deren 300.000 werden – wobei die Schweiz relativ wenige Schadensfälle registrieren musste. Besonders folgenreich wütete WanaCrypt vor allem bei den britischen National Health Services, wodurch in britischen Spitälern Medienberichten zufolge schlichtweg Chaos ausbrach. Aber auch die Deutsche Bahn hatte gut sichtbar mit komprommitierten Anzeigetafeln zu kämpfen.

Gestoppt wurde die Ausbreitung des Wurms dadurch, dass der Betreiber des Blogs «Malware Tech Blog», der 22-jährige Marcus Hutchins, im Code des Wurms eine vielleicht als Notausschalter (Kill Switch) gedachte Domain entdeckt hatte und diese registrierte.

Versucht man, drei Wochen nach dem Ausbruch von WannaCry eine Bilanz zu ziehen, hat man in verschiedener Hinsicht Grund genug zum Heulen:

Offenbar nehmen nicht nur eine grosse Zahl von Privatleuten und Unternehmen, sondern auch lebens- und infrastrukturkritische Organisationen das Thema Cyber-Security nicht so ernst, dass sie ihre Systeme sicherheitstechnisch à jour halten und Budgets für Wartung, Updates, Erneuerung und Sicherheit in ausreichendem Masse bereit stellen würden.

Und anscheinend sind Geheimdiensten Sicherheitslücken und Zugang zu den Computern der Bürger - für deren Schutz sie ja eigentlich arbeiten sollten – wichtiger, als die Sicherheit der Systeme selbst.

In einem lesenswerten Beitrag über die Learnings aus der WannaCry-Attacke kommt Rob VandenBrink im SANS-Blog zu dem Schluss, dass es um unsere Lernfähigkeit offenbar nicht zum Besten bestellt ist: «Oh wait, we already knew that!» trifft die traurige Tatsache im Kern, dass WannaCry wenn auch nicht verhindert, so doch wohl in seinen Auswirkungen massiv eingeschränkt worden wäre, wenn sich alle an seit Jahren immer und immer wieder propagierte Sicherheitsstandards halten würden.

Nachzulesen unter:

https://www.heise.de/suche/?q=wannacry&search_submit.x=0&search_submit.y=0&rm=search
https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack
https://www.golem.de/news/ransomware-entschluesselungstool-fuer-wanna-cry-veroeffentlicht-1705-127942.html

https://www.golem.de/news/wanna-cry-mehrere-tor-server-in-frankreich-beschlagnahmt-1705-127905.html
https://venturebeat.com/2017/05/19/ransomware-wannacry-causes-fewer-tears-than-feared
https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack
https://isc.sans.edu/diary/What+did+we+Learn+from+WannaCry%3F+-+Oh+Wait%2C+We+Already+Knew+That%21/22444

II. Die WannaCry-Geschwister aus dem NSA-Werkzeugkasten

Während die meisten Darstellungen das Ende von WannaCry darauf zurückführen, dass der 22-jährige Security Blogger Marcus Hutchinson eine merkwürdige Domain im Code des Erpresserwurms fand, diese offiziell registrieren liess und damit dessen weitere Ausbreitung verhinderte, scheint sich die These zu erhärten, dass WannaCry in seiner Verbreitung schon vorher von einer ebenso bösen Schwester gehindert wurde. Sie heisst Adylkuzz und nutzt wie ein weiteres Familienmitglied namens EternalRocks die gleichen Exploits aus dem NSA-EternalBlue-Baukasten. Dabei sind Adylkuzz und EternalRocks keinesfalls Trittbrettfahrer von WannaCry. Vielmehr handelt es sich um völlig eigenständige, aber höchst gefährliche Malware, die Computer via SMB-Schwachstellen angreifen. So berichtet etwa bleepingcomputer.com, dass EternalRocks aus sieben «NSA-Tools» konstruiert wurde, während WannaCry nur deren zwei verwendet. Mit einem Trojaner zum Erpressen oder zum Diebstahl von Login-, e-Banking- oder Identitätsdaten bewaffnet, könnte EternalRocks extrem bedrohlich werden. Wie bedrohlich, das zeigt die Malware Adylkuzz, welche sich seit dem Frühjahr unbemerkt auf vermutlich weit mehr Rechner geschlichen hat, als WannaCry, und ihren cyberkriminellen Urhebern bereits mehr als 1 Million US-Dollar in die Kassen gespült haben soll. Adylkuzz macht dieses Geld nicht mit Datenerpressung, sondern mit «Mining» für die Cryptowährung «Monero» – wie Bitcoin unter den Top Ten der Cryptowährungen. Die technischen Details und das Ausmass der Adylkuzz-Attacke wurden von Sicherheitsforschern des US-Security-Unternehmens Proofpoint veröffentlicht. Da Mining-Software prinzipbedingt sehr hohe Rechnerleistung und Stromressourcen verbraucht, übertragen die Adylkuzz-Hacker die Kosten auf die Besitzer der gekaperten Rechner. Weil sie dabei aber keine weitere Malware-Konkurrenz auf den kompromittierten Systemen brauchen können, schotten sie diese gegen andere Angreifer ab – schliessen also die SMB-Sicherheitslücke auf TCP-Port 455 und haben

so offenbar in vielen Fällen dem WannaCry-Wurm den Zugang auf die Rechner nach dem Motto versperrt: «Der frühe Trojaner stoppt den Wurm.»

Nachzulesen unter:

https://www.bleepingcomputer.com/news/security/new-smb-worm-uses-seven-nsa-hacking-tools-wannacry-used-just-two
http://www.trojaner-info.de/daten-sichern-verschluesseln/aktuelles/adylkuzz-attacke-erbrachte-hackern-1-million-us-dollar.html
https://nzzas.nzz.ch/notizen/adylkuzz-dieser-neue-cyber-parasit-will-mit-unseren-computern-geld-scheffeln-ld.1295250
https://bitcoin-live.de/ethereum-mining-deutsch
https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar
https://arstechnica.com/security/2017/05/massive-cryptocurrency-botnet-used-leaked-nsa-exploits-weeks-before-wcry
http://blogs.flexerasoftware.com/vulnerability-management/2017/05/chasing-wannacry-what-about-adylkuzz.html

III. Keylogger serienmässig: HP-Notebooks lesen mit

Im letzten Security Report hatten wir darüber berichtet, dass zahlreiche fabrikneue Android-Smartphones von verschiedenen Herstellern mit Malware ausgerüstet wurden. Anfang Mai wurde bekannt, dass Spyware ab Werk auch in mehreren Laptops der HP-Serien EliteBook, ProBook, Elite X2 und ZBook wenn auch nicht in böser Absicht, so doch aber serienmässig ausgeliefert wurde: Im Audiotreiber der Notebooks ist ein Keylogger integriert, der alle Tastatureingaben in eine – öffentlich lesbare – Datei schreibt. Inwieweit auch Geräte anderer Hersteller betroffen sind, die das Package des Herstellers Conexant System verbaut haben, ist nicht bekannt. HP hat den Fehler, der offenbar schon seit 2015 existiert, inzwischen eingestanden, aber bis dato noch keine Lösung des Problems anzubieten.

Nachzulesen unter:

https://www.golem.de/news/hp-notebooks-audiotreiber-mit-keylogger-funktion-1705-127769.html
https://www.heise.de/security/meldung/HP-Notebooks-Audio-Treiber-belauscht-Tastatur-3710250.html
http://www.zdnet.com/article/keylogger-found-on-several-hp-laptops
https://www.heise.de/security/meldung/Keylogger-auf-HP-Notebooks-Hersteller-gesteht-Fehler-ein-3712567.html
https://www.netzwelt.de/news/160887-keylogger-hp-notebook-hersteller-veroeffentlicht-statement.html

IV. Hakuna Metadata – Das Gold der Internetsurfer

Im afrikanischen Swahili steht «Hakuna Matata» für «Alles in bester Ordnung!». Wörtlich übersetzt steht «Hakuna» für «Es gibt keine». Wenn also zwei IT-Forscher unter dem Titel «Hakuna Metadata – Let´s have some fun with Sid´s browsing history» der Frage nachgehen, was Metadaten und Browserhistorie über uns verraten, dann steckt schon ein wenig Zynismus in der Geschichte. Und man muss sich fragen, ob wirklich alles in bester Ordnung ist. Denn für Internet Service Provider steckt in diesen Daten ein wahres Vermögen, weil sie eine für Werbenetzwerke äusserst wertvolle Profilierung der Surferinnen und Surfer zulassen, die vor allem in der maschinengesteuerten Werbung (Programmatic Advertising) das A und O für den Werbeerfolg ist. Dies geht so weit, dass der EDRi (European Digital Rights)-Forscher, -Blogger und Coautor des eingangs genannten Artikels den ehemaligen General Counsel der NSA, Stewart Baker, mit den Worten zitiert: «Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.»

In des Wortes wahrstem Sinn todernst werden Metadaten und ihre Verwendung in der Aussage des ehemaligen NSA- und CIA-Direktors Michael Hyaden: «We kill people based on metadata.»

Verglichen damit ist man froh, dass Werbevermarkter, wie der Schweizerische Admeira-Verbund aus SRG, Swisscom und Ringier-Verlag zwar auch den Schatz der Metadaten heben wollen, den Metadaten-Liefernden aber nicht nach dem Leben, sondern «nur» nach deren Vermarktungspotenzial trachten – und anders als die Geheimdienste ein Opt-Out-Angebot für die Erhebung und Nutzung dieser Daten anbieten (siehe letzte Quellenangabe).

Nachzulesen unter:

https://netzpolitik.org/2017/hakuna-metadata-warum-metadaten-und-browserverlaeufe-mehr-ueber-uns-verraten-als-oft-vermutet
https://edri.org/hakuna-metadata-lets-have-some-fun-with-sids-browsing-history
http://www.privacypies.org/blog/metadata/2017/02/28/hakuna-metadata-1.html
https://www.nzz.ch/feuilleton/medien/admeira-swisscom-nutzerdaten-fuer-werbevermarktung-ld.150067
https://www.konsumentenschutz.ch/themen/datenschutz/swisscom-so-kontrollieren-sie-ihre-daten
http://www.admeira.ch/optout

V. Unboxed and Hacked – Der Irisscanner im neuen Samsung Galaxy S8

Schon viel ist auch an dieser Stelle über Sinn und Sicherheit biometrischer Erkennungsmerkmale geschrieben worden. Von Apples TouchID bis zu Samsungs neuem Irisscanner im «Unbox-Your-Phone»-Flaggschiff Galaxy S8 scheint allen eines gemeinsam zu sein: sicher sind sie eben gerade nicht. Ein Doktorand der TU Berlin hat keine vier Wochen nach Auslieferung den Galaxy-Scanner auf den irdischen Boden der Tatsachen zurückgeholt und mit einem Foto seines Auges und einer Kontaktlinse überlistet. Wie schon in den Ausführungen zum TouchID-Hack bei Apples iPhone steht aber auch in diesem Fall zu bedenken, dass viele Smartphones derzeit von Ihren Nutzenden aus Bequemlichkeitsgründen weder mit biometrischer noch einer anderen Zugangssperre geschützt werden. Ironisch bemerkt dazu Matthias Schindler, Mitarbeiter der Europaparlamentarierin Julia Reda, in einem Tweet: «Remember: Always change your iris pattern every 3 months to prevent ID theft and unauthorized access to your phone and accounts!»

Nachzulesen unter:

http://www.zeit.de/digital/datenschutz/2017-05/samsung-galaxy-s8-biometrie-auge-gehackt
https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security

http://www.zeit.de/digital/datenschutz/2014-12/fingerabdruck-merkel-leyen-hack-ccc-31c3

https://twitter.com/presroi/status/866946445550784515

Neu im SWITCH-CERT Security Blog

Why the most successful Retefe spam campaign never paid off
https://securityblog.switch.ch/2017/05/18/why-the-most-successful-retefe-spam-campaign-never-paid-off/

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