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

Juli 2015

SWITCH

I. Cybercrime – Next Level: Duqu 2.0-Angriff auf Kaspersky zieht Kreise bis in die Schweiz

«Willkommen im Jahr 2015: Wir sind nun zum Ziel geworden!» Mit diesen Worten begrüsste der Sicherheitsexperte Mikko Hypponen in seiner Keynote knapp 800 Sicherheitsexperten, die Mitte Juni aus aller Welt nach Berlin gekommen waren. Kurz zuvor hatte Eugen Kaspersky persönlich bekanntgegeben, dass sein Unternehmen Ziel eines ausgeklügelten Cyberangriffs geworden sei. Der inzwischen als Duqu 2.0 bezeichnete Trojaner sei eine überaus aufwändige und ausgeklügelte Weiterentwicklung des mit dem Cyberworm Stuxnet (dessen Entwicklung und Einsatz gegen das iranische Atomprogramm amerikanischen oder israelischen Geheimdienstkreisen zugeschrieben wird) verwandten Schädlings Duqu. Das Infosec-Institute betitelt Duqu 2.0 in seiner Analyse gar als «The Most Sophisticated Malware Ever Seen». Die exorbitanten Entwicklungskosten von geschätzten 10 Mio. USD lassen Experten wie Kaspersky vermuten, dass die Attacke von einem staatlichen Geheimdienst geführt wurde, weshalb Hypponen den Kaspersky-Angriff auch mit einem Verstoss gegen die Genfer Konventionen verglich.

Dass IT-Sicherheitsfirmen zum Ziel von Hackerattacken der amerikanischen NSA und der britischen GCHQ erklärt wurden, belegen Snowden-Dokumente, die The Intercept wenig später publizierte. Auf der Liste der globalen Alles-und-Jeden-Bespitzler aus Fort Meade und Cheltenham stehen so prominente Namen wie Kaspersky Lab, F-Secure, ESET, Avast, BitDefender, AVG, Avira und Checkpoint. In diesem Zusammenhang ist es auch nicht verwunderlich, dass Duqu 2.0 nach Angaben von Kaspersky auch nachweislich dazu eingesetzt worden sei, die Gespräche über das iranische Atomprogramm in Genf und Wien abzuhören. Die Manipulation von Aufzügen, Alarmanlagen, Telefonen und Computern in den Hotels der Delegationen und an weiteren insgesamt 100 Zielen trägt nach Meinung des Wall Street Journals ebenso wie der Jerusalem Post die Handschrift israelischer Geheimdienste, was der israelische Aussenminister aber umgehend und vehement bestritt. Vielleicht gelingt ja Schweizer Ermittlern die Sensation, Licht ins maliziöse Dunkel zu bringen und die Hintermänner zu enttarnen. Jedenfalls hat die Schweizer Bundesanwaltschaft ein Ermittlungsverfahren gegen Unbekannt eingeleitet.

Nachzulesen unter:

http://futurezone.at/digital-life/f-secure-angriff-auf-kaspersky-neue-stufe-von-cybercrime/136.396.004
http://www.heise.de/newsticker/meldung/Spionage-Trojaner-wuetete-im-Netzwerk-von-Kaspersky-2687375.html
https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky
http://securityaffairs.co/wordpress/38020/cyber-crime/nsa-gchq-spy-kaspersky.html
http://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen
http://www.heise.de/newsticker/meldung/Kaspersky-Trojaner-hatte-auch-Atomverhandlungen-im-Visier-2689929.html
http://www.srf.ch/news/international/cyber-spionage-bei-atomkonferenz-in-genf
http://derstandard.at/2000017405238/Iran-an-Wien-Besorgnis-ueber-Cyberangriff-auf-Atomgespraeche
http://www.tagesanzeiger.ch/schweiz/standard/Wurden-die-iranischen-Atomgespraeche-in-Genf-abgehoert/story/23916270

II. Freundschaft – Next Level: Die NSA-Bespitzelung der deutschen und der französischen Regierung zieht immer weitere Kreise

Eigentlich stand schon fast zu befürchten, dass die Bespitzelung befreundeter Regierungen durch NSA und GCHQ und die Weitergabe der daraus gewonnenen Erkenntnisse an die anderen drei Partner des als Five Eyes bezeichneten Geheimdienst-Verbunds Kanada, Australien und Neuseeland weder beim Handy der

deutschen Kanzlerin aufhörte, noch beim Ausforschen deutscher und französischer Unternehmen zum Zweck der reinen Wirtschaftsspionage (siehe dazu auch den SWITCH Security-Report vom Juni 2015). Inzwischen ist bekannt, dass auch Minister, hohe Beamte und die EZB im Visier der Dienste standen (und vermutlich noch stehen). Wirklich überraschend sind daher eher nicht die enthüllten Tatsachen, sondern der Fakt, dass die als Top Secret klassifizierten Dokumente, die all dies belegen, nicht aus dem Fundus Edward Snowdens stammen, sondern von einer neuen unbekannten Quelle in der NSA auf der Enthüllungsplattform Wikileaks publiziert worden sind.

Nachzulesen unter:

http://www.zeit.de/digital/datenschutz/2015-01/regin-trojaner-nsa-spionage-cyberkrieg
http://www.faz.net/aktuell/politik/inland/wikileaks-nsa-spaehte-weite-teile-der-bundesregierung-aus-13680122.html
https://wikileaks.org/nsa-germany
https://wikileaks.org/nsa-france
http://www.sueddeutsche.de/politik/nsa-ueberwachung-obama-verspricht-hollande-ende-der-bespitzelung-1.2535172
http://www.nzz.ch/international/europa/nsa-soll-frankreichs-praesidenten-abgehoert-haben-1.18567907
http://www.tagesanzeiger.ch/ausland/europa/Auch-Briten-sollen-deutsche-Regierung-abgehoert-haben/story/23153235

III. Nichts mehr im Lot: IT-Angriff groundet Flugzeuge der polnischen Airline LOT

Im SWITCH Security-Report vom Mai 2015 hatten wir erstmals das Thema «In-Flight-Hacking» aufgegriffen. Nun zeigt der Angriff auf die Bodensysteme der polnischen Fluglinie LOT, dass Airlines und ihre IT offenbar zunehmend ins Visier von Cyberkriminellen geraten. Am 21. Juni waren auf dem Warschauer Chopin Flughafen die IT-Systeme, mit denen LOT ihre Flugpläne erstellt und ausgibt, für mehr als 5 Stunden ausser Gefecht gesetzt. In der Folge blieben 10 Flugzeuge am Boden und bei einem guten Dutzend weiterer Flüge ab Warschau Chopin kam es zu teils erheblichen Verzögerungen. LOT informierte umgehend, dass dies der erste Angriff dieser Art sei, den die Airline erfahren musste, betonte, dass die Sicherheit von Passagieren und Flugzeugen gewährleistet sei und gab nach Behebung der Störung entsprechend Entwarnung. The Register berichtete unterdessen, dass die LOT-Flugplanrechner offenbar einer einfachen DDoS-Attacke zum Opfer gefallen waren.

Dennoch warnen Experten wie der SATCOM-Spezialist Ruben Santamarta davor, dass Cyberangriffe auf Airlines und Flugzeuge zunehmen könnten. Er begründet dies unter anderem damit, dass veraltete Firmware und mangelhaftes Software-Design geradezu zum Hacking einladen würden. Tatsächlich sind Airlines immer wieder von Computerproblemen betroffen, die vermutlich auf Hackerattacken zurückzuführen sind, wie unter anderem das Beispiel von United Airlines zeigt. Ein Sprecher der deutschen Pilotenvereinigung Cockpit hat deshalb die Fluggesellschaften aufgerufen, mehr für den Schutz ihrer IT-Systeme am Boden und in den Maschinen zu tun.

Nachzulesen unter:

http://www.databreachtoday.com/hack-attack-grounds-airplanes-a-8331
http://www.bankinfosecurity.com/airline-hack-was-denial-service-a-8342
http://corporate.lot.com/pl/en/press-news?article=772922
http://corporate.lot.com/pl/en/press-news?article=772947
http://www.theregister.co.uk/2015/06/23/planegrounding_airport_attack_revealed_to_be_ddos
http://www.zdnet.com/article/lot-airline-hack-signals-the-first-in-emerging-cyberthreat-trend
http://www.heise.de/newsticker/meldung/Nach-Hackerangriff-auf-LOT-Piloten-fordern-mehr-Sicherheit-2724404.html
http://www.spiegel.de/netzwelt/web/united-airlines-vermutliche-hacker-attacke-auf-flugzeuge-a-1036893.html

IV. Detoxing – Der letzte Ausweg, wenn Geschäfte aus dem Darknet ans Licht kommen?

«Yesterday, 2nd June 2015, I decided to quit. Plan A was to stay quiet and hidden. Well, I think I screwed up. It's been funny, … but I don't want to be a criminal …» Dieser Text ist eine Verkaufsanzeige. Und zwar für ein Unternehmen, das so erfolgreich geworden ist, dass es seinem Erfinder und Betreiber – nach eigenen Angaben ein/e Student/in im Teenager-Alter – nun zu heiss geworden ist: Tox.

Tox ist ein typischer – und offenbar besonders erfolgreicher – Vertreter des Geschäftsmodells «Malware-as-a-Service» im Darknet, also auf der dunklen, und in diesem Fall der kriminellen Seite des Internets. Insoweit zeugt der Satz «I don´t want to be a criminal» von reichlich infantiler Einfalt der sich ebenfalls Tox nennenden Person, denn schliesslich ist er/sie genau das. Und zwar seit dem Moment, in dem der Dienst online gestellt wurde. Denn Tox eröffnet auch Anfängern im Cybercrime-Geschäft die Möglichkeit, mit wenigen Klicks aus bereitgestellten Softwaretools einen hochfunktionellen Krypto-Trojaner zur Internet-Erpressung zu konfigurieren.

Kostenlos, wahlweise mit persönlicher Nachricht und inklusive einer Anleitung fürs cyberkriminelle Vorgehen. Integraler Bestandteil des Tox-Servicepakets ist zudem die anonyme Abrechnung in Bitcoins und im Netzwerk von Tors Hidden Services. Als Gegenleistung behält Tox nach anfänglich 20% – später 30% – der erpressten Bitcoin-Beträge ein. Nachdem das Security-Unternehmen McAfee eine Warnung vor Tox veröffentlicht hatte, stiegen die Userzahlen, kurze Zeit später auch die Schadensfälle nach Angaben von Tox selbst sprunghaft an.

Darauf, dass sich «Malware-as-a-Service» als einträgliches Geschäftsmodell im Darknet etabliert, weist auch Pierluigi Paganini in seinem Securityaffairs-Blog hin. Nach seinen Aussagen überzeugen vor allem solche Angebote, bei denen Cyberkriminelle auch ohne technische IT-Kenntnisse schnell und einfach zu bösartiger Software und/oder Infrastruktur zu kommen. Sei es, dass ganze Botnets zur Benutzung vermietet werden oder eben wie im Fall Tox einfach zu bedienende webbasierte Anwendungen quasi-individuelle Malware produzieren, die obendrein von klassischen Virenscannern nicht entdeckt werden, weil sie jedesmal neu erstellt werden.

Nachzulesen unter:

http://securityaffairs.co/wordpress/37639/cyber-crime/tox-ransomware-for-sale.html
http://www.golem.de/news/tox-kostenloser-digitaler-erpressungsdienst-1505-114301.html
http://www.heise.de/newsticker/meldung/Malware-as-a-Service-Entwickler-des-Tox-Trojaners-steigt-aus-2679743.html
http://securityaffairs.co/wordpress/31455/cyber-crime/cybercrime-as-a-service-model.html

V. Pass the Password: Angriffe auf LastPass und Apple Keychain

Passwortmanager sind für ihre Nutzer willkommene Arbeitshilfen, um Benutzernamen, Passwörter, Bookmarks, Netzwerk-, aber auch Kreditkartendaten zu speichern und auf allen Geräten à jour zu halten. Der Preis für den damit gewonnenen Komfort ist das Risiko, dass Passwortmanager auf Cyberkriminelle eine ebenso grosse Anziehungskraft haben wie Dagobert Ducks Geldspeicher auf die Panzerknacker. Entsprechend hoch sind die Sicherheitsvorkehrungen. Dennoch gibt es auch für Passwortmanager keinen 100%-igen Schutz. So meldete der Online-Passwortmanager LastPass im Juni einen Einbruch, bei dem sich Unbekannte Zugriff auf «E-Mail-Adressen, Passworterinnerungen und Authentifizierungshashes einiger Nutzer»

verschafft hätten. Die Passwörter selbst sind dabei geschützt geblieben. Dennoch lässt sich mit den gestohlenen Daten einiges anfangen, wie Martin Vigo in seinem Sicherheitsblog berichtet.

Dass sich auch Apples Schlüsselbund knacken lässt, wurde ebenfalls im Juni publik. Ein Team aus sechs Sicherheitsforschern unter Luyi Xing von der Indiana University Bloomington nutzte verschiedene Zero-Day-Lücken in iOS und OSX, um Apples Schlüsselbund und zahlreiche Sandbox-Container zu knacken sowie neue Schwachstellen in der Kommunikation zwischen Apps und Programmen unter iOS und OSX aufzudecken. Xing hatte bereits im Oktober 2014 an Apple gemeldet, dass dass von 1.612 untersuchten OSX- und 200 iOS-Apps 88% gegen so genannte XARA (Unauthorized Cross-App Resource Access)-Angriffe keinen Schutz bieten. Dort hatte man Xing zu verstehen gegeben, dass die Ernsthaftigkeit der Bedrohung erkannt sei, man aber mindestens sechs Monate zur Korrektur bräuchte. Im Februar diesen Jahres forderte Apple dann von Xing das ausführliche Paper an. Inwieweit die Schwachstellen inzwischen behoben sind, ist derzeit nicht zu klären. Am 19. Juni nun hat Apple entgegen aller bisher gezeigten Kommunikationspolitik angekündigt, gemeinsam mit Xing und seinem Team an einer schnellen Lösung zu arbeiten. Es bleibt zu hoffen, dass diese kurzfristig gefunden wird.

Nachzulesen unter:

https://blog.lastpass.com/de/2015/06/lastpass-security-notice.html/
http://www.zeit.de/digital/datenschutz/2015-06/lastpass-passwortmanager-hack-sicherheit
http://www.martinvigo.com/about-todays-lastpass-breach
http://www.darknet.org.uk/2015/06/apples-password-storing-keychain-cracked-on-ios-os-x
http://9to5mac.com/2015/06/17/major-zero-day-security-flaws-in-ios-os-x-allow-theft-of-both-keychain-and-app-passwords/
http://www.golem.de/news/security-zero-days-in-mac-os-x-und-ios-veroeffentlicht-1506-114729.html
http://www.theregister.co.uk/2015/06/17/apple_hosed_boffins_drop_0day_mac_ios_research_blitzkrieg
http://www.netzwelt.de/news/153189-kritische-xara-luecken-ios-os-x-apple-verspricht-fixes.html

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Wie unsicher sich viele VPN-Dienste in einer Dual-Stack-Umgebung verhalten, haben Forscher an den Universitäten in Rom und London untersucht:

http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf

Die Vortragsslides der Schweizer IPv6V Konferenz – beispielsweise zum Thema IPv6 Advanced Security – sind online verfügbar:

http://www.ipv6conference.ch/sessions/

Das Thema «Security and the Internet of Things» ist in aller Munde. computersciencezone.org hat dazu eine schöne Visualisierung gemacht:

http://www.computersciencezone.org/security-internet-of-things/

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