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

November 2016

SWITCH

I. IT-Securityforscher zeigen Schwachstellen im Photo-TAN-Verfahren für mobiles Banking auf

Einfach, schnell, sicher – mit diesem Versprechen bewerben mehrere deutsche, aber auch Schweizer Banken ihr Smartphone-Banking. Die Idee, die reinen Bankingdaten (Absender- und Empfängerkonto, Betrag) über eine Banking-App einzugeben und dann mithilfe einer zweiten App eine Photo-TAN zu erzeugen, die die Zahlungsanweisung autorisiert, gilt als sicheres Banking via Smartphone. Nun haben die beiden IT-Sicherheitsforscher Vincent Haupert und Tilo Müller an der Friedrich-Alexander-Universität Erlangen-Nürnberg diesen Hoffnungen einen Dämpfer verpasst. Ihnen ist es gelungen, die Photo-TAN-App zu hacken und Überweisungen auf fremde Konten umzuleiten, ohne dass die Kontoinhaber (bis zum Eintreffen der Kontoauszüge) davon etwas mitbekommen hätten. Als besonders problematisch sehen Haupert und Müller, dass beide Apps auf ein und demselben Device installiert sind. Denn dabei geht unter anderem das Sicherheitsplus eines Medienwechsels verloren, wie er in anderen Autorisierungsverfahren verwendet wird. Eine detaillierte Beschreibung der Attacke geben die Forscher in Kapitel 4.3. des unten zitierten PDFs.

Nachzulesen unter:

http://www.finews.ch/news/banken/16375-mobile-banking-pctipp-online-banking-raiffeisen-postfinance
http://www.sueddeutsche.de/digital/it-sicherheit-mobiles-banking-hacker-knacken-photo-tan-app-1.3208810
http://www.zeit.de/digital/2016-10/mobile-banking-photo-tan-verfahren-manipulation-android-smartphones
https://www1.cs.fau.de/content/app-based-matrix-code-authentication-online-banking
https://www1.cs.fau.de/filepool/projects/matrix-code/appauth.pdf

II. DDoS-Attacke via IoT-Botnet legt Teile des Internets lahm

In der letzten Ausgabe unseres Security-Reports hatten wir darüber berichtet, dass Sicherheitsforscher im August 2016 im Internet of Things einen Trojaner gefunden haben, der es erlaubt, IoT-Geräte, die eine veraltete, auf Linux basierende Firmware nutzen, zu Botnetzen zusammenzuschliessen und darüber Spam oder Malware zu verbreiten. Am 21. Oktober 2016, also keine drei Wochen später, erfolgte dann unter Einsatz eines gigantischen Botnets aus vernetzten Heimgeräten die erste globale DDoS-Attacke auf Hunderte von Websites. Nach heutigem Wissensstand griff die namensgebende Malware Mirai dabei zunächst drei Dyn Datencenter im Nordwesten der USA, dann weitere vierzehn weltweit an und störte auch die Seiten von Airbnb, Amazon, Financial Times, Netflix, New York Times, Paypal, Reddit, Spotify und Twitter erheblich. Einen wesentlichen Anteil an der Verbreitung von Mirai hatten Botnets aus vernetzten Überwachungskameras und digitalen Videorekordern.

Bereits im Oktober berichtete der Blog KrebsOnSecurity über eine DDoS-Attacke gegen die eigenen Server und machte publik, dass der Sourcecode für Mirai veröffentlicht sei. Gleichzeitig warnte KrebsOnSecurity davor, dass neben Mirai mindestens eine zweite Malware-Familie namens Bashlite mit ähnlichem Funktionsprinzip ihr Unwesen im Netz treibt. In beiden Fällen sucht die Malware nach leicht angreifbarer Hardware, die entweder mit den werksseitigen (und oft nicht existierenden) Sicherheitseinstellungen oder einfach zu knackenden Codes (1234, 9999, 0, admin) «gesichert» sind, und schliesst diese in kürzester Zeit zu Botnets zusammen. Auf das von vernetzten und schlecht bis nicht gesicherten Druckern ausgehende Sicherheitsrisiko verweist auch die Swisscom in einem KMU-Newsletter. Der amerikanische Sicherheitsexperte Bruce Schneier fordert gar ein Eingreifen des Staates. Denn einerseits stellt jeder IoT-Knoten potentiell ein Sicherheitsrisiko dar. Andererseits zeigten die Hersteller entsprechender Geräte, dass sie nicht willens oder nicht in der Lage sind, die grundlegenden Sicherheitsprobleme von IoT-Devices zu lösen. Schneier schlägt die Einrichtung eines staatlichen Prüflabors vor, gibt aber

gleichzeitig zu bedenken, dass private Institutionen wohl agiler und schneller wären. Angesichts der «Time-to-Market»-Geschwindigkeit, mit der sich IoT-Botnets offenbar etabliert haben, sicher eine überlegenswerte Alternative.

Nachzulesen unter:

http://www.nzz.ch/digital/cyberattacken-auf-amerikanische-websites-kriminelle-legen-amazon-twitter-und-andere-online-sites-lahm-ld.123523
https://www.flashpoint-intel.com/action-analysis-mirai-botnet-attacks-dyn
http://www.thehostingnews.com/17+Dyn+Data+Centers+Were+DDoSed+Globally
http://www.thewhir.com/web-hosting-news/report-mirai-botnet-ddosed-17-dyn-data-centers-globally
https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released
http://www.securityweek.com/mirai-iot-botnet-not-only-contributor-massive-ddos-attack-akamai
http://www.nzz.ch/meinung/kommentare/computersicherheit-das-internet-der-dinge-als-gefahrenquelle-ld.123915

III. Dreifacher Rekord: Yahoo verliert eine halbe Milliarde Kundendaten, so viel Vertrauen wie noch nie und 1 Milliarde an Übernahmepreis

Am 22. September 2016 gestand Yahoo, dass bei einem Hack im April 2014 – also fast 30 (in Worten: dreissig!) Monate zuvor – eine halbe Milliarde (in Zahlen: 500.000.000) Kundendaten gestohlen worden waren. Neben Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten und Passwort-Hashes sind offenbar auch verschlüsselte oder unverschlüsselte Sicherheitsfragen und -antworten in falsche Hände gelangt. Yahoo spricht zwar von «einigen Fällen», sieht sich aber der Tatsache gegenüber, dass sich angesichts der desaströsen Veröffentlichungspolitik niemand so recht davon beruhigen lassen will. Denn «schon» im Juli 2016 hatte das Onlinemagazin «Motherboard» berichtet, dass 200 Millionen Yahoo-Accounts mit allen dazugehörigen Daten im Darknet verkauft würden. Zu diesem Zeitpunkt hatte Yahoo den Diebstahl nicht bestätigen wollen. Nun musste Yahoo nicht nur den Hack selbst, sondern auch noch zugeben, dass die Beute mehr als doppelt so gross war. Denn die 500 Millionen Kundendaten werden nicht nur für den Zugang zu Yahoo selbst verwendet, sondern auch für Dienste wie Flickr oder Tumblr.

Der Mobilriese Verizon steht kurz vor der Übernahme des gesamten Pakets, ist nach der Bestätigung des Rekord-Hacks aber verärgert, weil Yahoo in einer Pflichterklärung vor den Verhandlungen mit Verizon angegeben hatte, dass ihm nichts von einem Datendiebstahl bekannt sei. Am 6. Oktober berichtete dann die New York Post, dass Verizon einen 1-Milliarde-Dollar-Discount von seinem 4,8-Milliarden-

Dollar-Angebot gefordert habe. Das wohl auch deshalb, weil nicht nur Gender-Klagen gegen Ex-Yahoo-Chefin Marissa Meyer hängig sind, der vorgeworfen wird, Männer systematisch aus ihren Jobs gemobbt zu haben. Viel schwerer wiegt der Vorwurf, dass Yahoo gegen die eigene Security-Abteilung gearbeitet und für nicht näher genannte US-Geheimdienste Software geschrieben haben soll, die es den Diensten ermöglicht haben soll, den gesamten Mailverkehr aller Yahoo-Mail-Nutzer zu scannen. Es ist nicht bekannt, ob diese Überwachung andauert.

Eine bekannte deutsche Bank hatte einmal mit dem Slogan geworben: «Vertrauen ist der Anfang von allem.» Es sieht so aus, als wäre nicht nur dort, sondern auch bei Yahoo der Verlust des Vertrauens der Anfang vom Ende.

Nachzulesen unter:

https://www.heise.de/security/meldung/Rekordhack-bei-Yahoo-Daten-von-halber-Milliarde-Konten-kopiert-3330083.html
https://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web
http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports
https://www.heise.de/security/meldung/Alle-Mails-gescannt-Yahoo-arbeitete-fuer-Geheimdienste-3340778.html
http://www.spiegel.de/international/business/the-story-of-the-self-destruction-of-deutsche-bank-a-1118157.html

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.