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

Oktober 2015

SWITCH

I. XCode Ghost und Stagefright treffen die beiden Branchengiganten Apple und Google und werfen Fragen auf

Sieben Lücken hatten Sicherheitsforscher der Zimperium zLabs Ende Juli in Androids Multimedia-Schnittstelle Stagefright entdeckt. Sie ermöglichten es Angreifern, per SMS oder mit einem Video Geräte unter Android-Systemen vor 5.0 – das sind geschätzt ca. 80% aller Android Mobile-Devices – komplett zu blockieren oder gar als Wanzen zu missbrauchen. Google hatte auf die Warnungen des Zimperiums zunächst nur mit der allgemeinen Ankündigung reagiert, einen regelmässigen monatlichen Patchday einzuführen. Daraufhin haben zLabs Anfang September einen funktionierenden Exploit veröffentlicht, um den Druck auf Google zu erhöhen, die Lücken zu schliessen. Inzwischen sind die ersten Sicherheitsupdates verfügbar, doch haben die Forscher bei Zimperium mit Stagefright 2.0 bereits die nächste Schwachstelle entdeckt. Sie ermöglicht es, Malware mithilfe von MP3 oder MP4-Dateien auf die Geräte zu schleusen.

Noch mehr Löcher hat die Security-Firma Palo Alto Networks in Apps aus Apples App-Store gefunden. Vor allem chinesische Entwickler hatten anstelle der Apple

Original-Entwicklungsumgebung Xcode eine von chinesischen Hackern entwickelte kompromittierte Version eingesetzt. Wieviele Apps letztlich damit infiziert wurden, lässt sich gegenwärtig schwer abschätzen – war zu Beginn der XCodeGhost-Entdeckung von 39 Apps die Rede, ist deren Zahl nach Angaben von Sicherheitsexperten des Anbieters FireEye inzwischen auf über 4.000 angestiegen. Weil sich darunter auch sehr populäre Apps wie WeChat finden, sind wohl mehrere Millionen Nutzer betroffen. Schaden genommen hat auch das grundlegende Vertrauen in die bis dahin als superior geltende Sicherheit des App-Stores aus Cupertino. Apple hat alle Entwickler über die Sicherheitslücken informiert und sie dazu aufgefordert, ihre Apps unter Verwendung des Original-XCodes zu aktualisieren. Alle betroffenen, nicht aktualisierten Apps, von denen Apple wisse, seien aus dem Store entfernt worden und Neuanträge, die XCode-Ghost enthielten, würden blockiert.

Verglichen mit den Dimensionen, die Stagefright und XCodeGhost haben, sind die – erfolgreichen – Versuche, Sperrbildschirme von iOS- und Android-Geräten zu knacken, schon beinahe putzig. Dennoch bleibt auch hier anzumerken, dass beim Thema Sicherheit mobiler Geräte weiterhin Optimierungsbedarf besteht.

Nachzulesen unter:

http://www.nzz.ch/digital/stagefright-exploit-zimperium-zlabs-ld.1896
http://www.spiegel.de/netzwelt/gadgets/android-neue-gefahr-durch-sicherheitsluecke-stagefright-2-0-a-1055865.html
http://www.heise.de/security/meldung/Malware-in-Apples-App-Store-Wie-XcodeGhost-funktioniert-2824035.html
http://www.darknet.org.uk/2015/09/xcodeghost-ios-trojan-infected-over-4000-apps
http://www.theregister.co.uk/2015/09/23/xcodeghost_analysis
http://www.nzz.ch/sperrbildschirm-siri-ios-9-austricksen-ld.2138
http://www.golem.de/news/nach-malware-infektion-apple-raeumt-den-app-store-auf-1509-116473.html

II. BÜPF, NDG und Staatstrojaner: Die Debatte um Sinn, Unsinn, Kosten und Risiken staatlicher Überwachung geht in die nächste Runde

In der August-Ausgabe des Security Reports hatten wir ausführlich über die Affäre um den Ankauf des Staatstrojaners «Galileo» bei der italienischen Firma Hacking-Team durch Schweizer Behörden berichtet. Auch nachdem sich herausgestellt hatte, dass der mehr als eine halbe Millionen Franken teure

Trojaner nach einem Hack beim Anbieter gar nicht eingesetzt werden kann und inzwischen bekannt ist, dass auf der Kundenliste von Hacking Team neben der Schweiz auch Diktatoren, Schurkenstaaten und Kunden mit Verbindungen zur osteuropäischen Mafia stehen, zeigte man sich in Regierungskreisen noch überzeugt davon, bei der Beschaffung von Galileo alles richtig gemacht zu haben. Dagegen führen Kritiker des Einsatzes von Staatstrojanern neben den oben genannten Bedenken ins Feld, dass staatlich eingesetzte Computerangriffe auch Cyberkriminellen sprichwörtlich Türen und Tore öffnen, ohne einen nennenswerten Gewinn zu liefern. Denn zum einen beweise gerade der Hacking-Team-Hack, dass die Bösen Zugriff auf die gleiche Software hätten wie jene, die sie zu deren Bekämpfung einsetzen wollen. Zum anderen seien viele Trojaner – auch Galileo – so angelegt, dass die von ihnen gewonnenen Daten leicht verfälscht werden könnten und damit keine Beweiskraft besässen.

Mit der Annahme des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) am 17. Juni 2015 hat der Nationalrat nun aber grundsätzlich Grünes Licht für den Einsatz von Staatstrojanern in der Schweiz gegeben. Komplementär dazu räumt auch das neue Nachrichtendienstgesetz NDG den Schweizer Überwachungsbehörden deutlich ausgeweitete Möglichkeiten beim Anzapfen, Mitschneiden und Speichern von Kommunikationsdaten und –inhalten ein. Staatsrechtsprofessor Rainer J. Schweizer meint gar, im Gesetzespaket einen grundlegenden Systemwechsel zu erkennen, der darauf hinausläuft, dass die Medienfreiheit deutlich eingeschränkt werde.

Kritiker von BÜPF und NDG haben nun denn auch ein Referendum gegen das NDG lanciert. Dass ein Volksentscheid aufgrund der Erfahrung mit der Fichenaffäre wünschenswert wäre, weil ein «Ja» zum neuen Gesetz Zweifel an der Legitimität des NDB ausräumen würde, meint auch die Berner Zeitung.

Inwieweit «Privatsphäre» aber künftig überhaupt eine schützenswerte Institution bleiben wird, oder ob sie – nach den Worten der GDI-Zukunftsforscherin Karin Frick – in der politischen Diskussion und in den Medien überbewertet wird und durch Convenience und Bequemlichkeit erodiert, bleibt abzuwarten.

Nachzulesen unter:

http://www.computerworld.ch/news/it-branche/artikel/zuercher-regierungsrat-nimmt-stellung-zum-staatstrojaner-von-reue-keine-spur-68658

http://www.computerworld.ch/news/politik-gesellschaft/artikel/falscher-staatstrojaner-kapo-zueri-wird-lukrative-ware-fuer-cyberkriminelle-68790
https://www.digitale-gesellschaft.ch/2015/06/08/offener-brief-zum-ndg
http://www.tagesanzeiger.ch/schweiz/standard/Wir-schaffen-da-eine-geheime-Staatsgewalt/story/21297019
http://www.nzz.ch/schweiz/aktuelle-themen/gegner-des-nachrichtendienstgesetzes-lancieren-referendum-1.18620992
http://folio.nzz.ch/2015/oktober/haendler-ohne-waren
http://www.bernerzeitung.ch/schweiz/volksentscheid-zum-nachrichtendienstgesetz-wuenschenswert/story/16492264

III. Privatsphäre B-2-B: Angriffe auf mittelständische Industrie und kritische Infrastruktur nehmen zu

Während viele Menschen der Schutz ihrer Privatsphäre immer weniger zu interessieren scheint, reklamieren immer mehr Nicht-Privatleute, dass dieser Schutz für sie und ihr Überleben existenziell wird. Unternehmen und Betreiber kritischer Infrastrukturen, wie z. B. Kraftwerken, Stromnetzen, Behörden, Krankenhäusern etc. sehen sich immer öfter immer perfideren Cyberattacken ausgesetzt. Diese zerstören oder kompromittieren Anlagensteuerungen, fischen Kommunikationsdetails heraus, mit denen Wettbewerber Verhandlungen in einem Übernahme-Poker torpedieren oder stehlen Daten von Prototypen, Kunden, Unternehmensstrategien und dergleichen.

Experten verweisen vermehrt darauf, dass sich Cyberangriffe nicht mehr nur gegen grosse Namen und Organisationen wenden, sondern auch im KMU-Bereich gestartet werden, beispielsweise von Wettbewerbern, die die Online-Präsenz eines Unternehmens oder dessen Auffindbarkeit bei Google unterminieren. Mit Verweis auf die stetig steigende Vernetzung in der digitalisierten Produktion und Klumpenrisiken beim Angriff auf ganze Infrastrukturbereiche, wie etwa die Stromversorgung, warnen nicht mehr nur IT- und Security-Experten, sondern auch grosse Unternehmensberater wie KPMG und andere. In Deutschland hat der Gesetzgeber reagiert und Mitte Juni 2015 mit einem neuen IT-Sicherheitsgesetz neue Pflichten zur Einführung von Abwehrmassnahmen gegen - sowie neue Meldepflichten bei - Cyberattacken installiert. Wie gross der Bedarf in diesem Feld ist, zeigt ein Honeypot-Beispiel der Sonntagszeitung, bei dem ein simulierter Server eines Wasserkraftwerks in nur drei Wochen mehrere ernstzunehmende Angriffe verzeichnete: «Ein Hacker aus Vietnam versuchte das System zum Absturz zu bringen; zwei Angreifer aus den USA und einer aus Rumänien [...]

jubelten dem vermeintlichen Kraftwerk einen Fehler unter [...], der dafür hätte sorgen können, dass eine Pumpe plötzlich aussteigt.»

Nachzulesen unter:

http://www.zeit.de/digital/2015-09/industrie-hacker-sicherheit-digitalisierung
http://www.faz.net/aktuell/wirtschaft/unternehmen/der-schaden-durch-hackerangriffe-wird-immer-groesser-13331689-p2.html
https://home.kpmg.com/de/de/home/themen/2014/08/industrie-4-0-wie-hacker-in-industrie-it-eindringen.html
http://www.computerwoche.de/a/security-konzepte-im-praxis-check,3211303
http://www.trendmicro.de/media/wp/industrie-4-und-die-sicherheit-whitepaper-de.pdf
http://www.computerwoche.de/a/bundestag-beschliesst-das-it-sicherheitsgesetz,3210652
http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051
http://blog.kpmg.ch/cyberangriffe-auf-schweizer-wasserkraftwerke-was-man-darueber-wissen-sollte

IV. Die Fingerabdrücke von mindestens 5.6 Millionen US-Angestellten sind weggekommen – who cares?

Über die Cyberattacken auf das US-amerikanische Office for Personnel Management (OPM), bei dem persönliche Daten und Sicherheitsreports von mehr als 21 Millionen Bundesangestellten gestohlen wurden, hatten wir im Security Report vom August bereits berichtet. Nun wurde bekannt, dass auch eine immense Zahl von Fingerabdrücken in die Hände der Cyberkriminellen gefallen sind. War zunächst noch von 1,1 Millionen Betroffenen Bundesangestellten die rede, so wird inzwischen die Zahl offiziell mit 5,6 Millionen angegeben. Bundesangestellte, wohlgemerkt, die mit ihren Fingerabdrücken nicht nur im privaten Bereich das Handy entsperren, sondern auch Zugang zu bundesstaatlichen Einrichtungen erhalten. In einem Ende September veröffentlichten Statement versucht das OPM die Gefährdung durch diesen Diebstahl zu entdramatisieren. Die Folgen des Diebstahls biometrischer Merkmale sind aber nicht nur in den Augen von Alan Woodward, Computerwissenschaftler an der Surrey University und Sicherheitsberater für Europol, gravierend: «If [people] can actually steal something that is unique, like fingerprints, and somebody is relying upon it, then it's just going to cause a nightmare - it really is». Es zeigt sich wieder einmal, dass biometrische «Passwörter» nach einem Klau nur sehr begrenzt erneuerbar sind.

Nachzulesen unter:

https://netzpolitik.org/2015/opm-hack-noch-mehr-fingerabdruecke-von-us-bediensteten-betroffen
http://www.zdnet.com/article/the-opm-breach-deepens-5-6-million-federal-employees-fingerprints-stolen
https://www.opm.gov/news/releases/2015/09/cyber-statement-923
http://www.bankinfosecurity.com/stolen-opm-fingerprints-whats-risk-a-8548
https://www.ccc.de/de/updates/2008/schaubles-finger

V. 007 aus dem Baumarkt: Das Deep Sweep Selbstbauprojekt bespitzelt Satellitenfunk

Es erinnert ein wenig an die witzigen «Spion-und-Spion»-Geschichten aus den Hochzeiten des einstigen Kultcomic-Magazins «MAD»: Die «Critical Engineering Working Group» um den Medienkünstler Julian Oliver hat eine mit High-Tech beladene Sonde entwickelt, um den Funkverkehr in grossen Höhen aufzuzeichnen und auf zeigma.com zu visualisieren. Initiator Oliver hofft darauf, dass die Sonde Funksignale zwischen militärischen Drohnen und Satelliten auffängt, auch wenn er sich bewusst ist, dass diese verschlüsselt unterwegs sind. Wie er dem Magazin WIRED gegenüber verlautbaren liess, ginge es aber in erster Linie darum, Informationen über den Funkverkehr in grossen Höhen zu liefern, der für Funkamateure vom Erdboden aus nicht zu empfangen ist. Beim ersten Versuch wurden allerdings keine Daten aufgezeichnet, beim zweiten erreichte die Sonde nur eine Flughöhe von 10 anstatt der anvisierten 24 bis 30 Kilometer. Es bleibt also im wahrsten Sinne des Wortes noch «Luft nach oben».

Nachzulesen unter:

http://www.heise.de/make/meldung/Hacker-starten-Stratosphaerenballon-um-Drohnen-Funk-mitzuschneiden-2823100.html
http://zeigma.com/deepsweep
http://www.wired.com/2015/09/balloon-spy-probe-deep-sweep
https://criticalengineering.org/projects/deep-sweep
http://www.20min.ch/digital/news/story/Hacker-spionieren-mit-Ballon-Militaer-Drohnen-aus-30099780

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