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

November 2014

SWITCH

I. Der «Long Tail»-Effekt von Shellshock, Heartbleed & Co.

«We're just at the beginning of a cycle of vulnerabilities being found in the software we rely on every day.» Diese Schlussfolgerung zieht der Senior Security Advocate bei Akamai, Martin McKeay, daraus, dass mit Heartbleed und Shellshock gleich zwei grosse Sicherheitslücken innerhalb eines Jahres bekannt wurden.

Wie bereits in der Juni-Ausgabe dieses Security Reports dargestellt, ist Heartbleed eine Schwachstelle in der nahezu universell eingesetzten OpenSSL-Softwarebibliothek, die ausgenutzt werden kann, um beispielsweise an Passwörter oder SSL-Schlüssel zu gelangen.

Im September entdeckte ein französischer Entwickler ein Leck in Bash, einer grundlegenden, mehr als 20 Jahre alten Software in Unix- und Linux-Systemen. Der unter dem Namen Shellshock bekannt gewordene Bash-Bug bedroht allerdings nicht nur Unix- und Linux-Server, sondern auch OS X, Netzwerk-Devices wie z.B. Router oder Webcams und verschiedenste andere Geräte im Internet.

Auch Monate nach der Entdeckung von Heartbleed und Shellshock sind diese Sicherheitslecks gemäss einhelliger Meinung von Sicherheitsexperten auf zigtausenden

Geräten immer noch nicht geschlossen. Inzwischen nutzen kriminelle Hacker Shellshock beispielsweise dazu, sich Zugang zu Mailservern zu verschaffen, um Botnetze aufzubauen und zu betreiben. Und auch Open VPN-verschlüsselte Netzwerkverbindungen sind vor Shellshock nicht sicher.

Auch wenn die Mehrzahl der Systemadministratoren schnell reagiert und alle verfügbaren Updates zeitnah einspielt: Bis alle potenziell gefährdeten Devices gepatcht – oder notfalls ausgetauscht – sind, werden noch viele Jahre vergehen.

Und der nächste Shellshock kommt bestimmt, so McKeay: Sicherheitslücken wie Heartbleed und Shellshock befinden sich in Programmcode, der zu Zeiten entwickelt worden ist, als solche Lücken noch keine grosse Relevanz hatten. Dieser Code hat aber überlebt und wurde in aktuelle Software ganz oder teilweise übernommen. Um solche eigentlich uralten Schwachstellen möglichst zu eliminieren, müssten Milliarden von Code-Zeilen geprüft und im Bedarfsfall durch Code auf dem Level aktueller Sicherheitsstandards ersetzt werden.

Ein anderer Aspekt dieser «Altlasten» zeigt sich in dem POODLE genannten Angriff auf SSL/TLS-verschlüsselte Verbindungen, der kürzlich von Google-Forschern veröffentlicht wurde. Hierbei versucht der Angreifer das Sicherheitsniveau einer Verbindung auf das veraltete und unsichere SSLv3-Protokoll herabzustufen, um dieses dann in der Folge zu knacken. Anders als Heartbleed und Shellshock nutzt POODLE also keine Lücke im veralteten Programmcode, sondern im Uralt-Protokoll.

Nachzulesen unter:

http://securityintelligence.com/heartbleed-and-shellshock-the-new-norm-in-vulnerabilities

http://www.switch.ch/export/sites/default/all/cert/downloads/secrep/_files_secrep/SecurityReport_Juni2014.pdf

http://www.spiegel.de/netzwelt/web/sicherheitsluecke-shellshock-bedroht-linux-rechner-und-macs-a-993688.html

http://www.csoonline.com/article/2839054/vulnerabilities/report-criminals-use-shellshock-against-mail-servers-to-build-botnet.html

http://www.heise.de/security/meldung/Angriff-auf-Verschluesselung-Reaktionen-auf-die-Poodle-Luecke-2425244.html

http://blog.erratasec.com/2014/10/some-poodle-notes.html

II. Malvertising: Hacker lernen von den Werbeprofis

«Operation Deathclick» – so nennt das im US-Bundesstaat Virginia beheimatete IT-Sicherheitsunternehmen Invincea eine besonders perfide Variante von Malvertising. Mitte Oktober berichtete das Unternehmen, es habe entdeckt, dass Malvertisers dazu übergehen, ihre Opfer nicht mehr breit gestreut anzugehen, sondern nach spezifischen Zielgruppenmerkmalen zu profilieren, und ihnen per Real Time Bidding manipulierte Werbung auf den Bildschirm zu schicken. Im Real Time Bidding werden während der Ladezeit einer Webseite Werbeplätze in Echtzeit versteigert. Wie bei regulär gebuchter analoger und digitaler Werbung auch, können Zielpersonen dabei nach regionalen, ökonomischen oder soziologischen Kriterien segmentiert, teilweise sogar nach ihrem Profil noch individueller profiliert werden.

Bei der «Operation Deathclick» hatten die Werber der dunklen Seite Mitarbeiter von Luft- und Raumfahrt sowie Rüstungsunternehmen im Visier. Es hat den Anschein, als würde sich wie in der legalen Werbung auch eine deutlichere Trennung zwischen breit streuender B2C (Business-to-Comsumer) vs. schärfer profilierter B2B (Business-to-Business)-Werbung etablieren.

Breit streuende Malvertisements, mit denen sich User aller Art durch Anklicken manipulierter Werbung u.a. auch auf Yahoo oder AOL Ransomware einfangen, sind unvermindert zu beobachten – und für die Opfer nach wie vor teuer. Insbesondere wenn die Verschlüsselung durch Ransomware die komplette Server-Infrastruktur betrifft, wie dies einer grösseren Organisation in den USA kürzlich passierte.

Dass aber auch mit klassischen Werbegeschenken eine Art «Malvertising» betrieben werden kann, bewiesen die Sicherheitsexperten Adam Caudill und Brandon Wilson. Sie haben eine Software veröffentlicht, mit der die als Werbegeschenk sehr beliebten USB-Sticks zu schlimmen Fingern werden, die beim ersten Einstecken Malware auf den Rechner laden, um ihn zu kapern.

Zum Weiterlesen:

https://threatpost.com/apts-target-victims-with-precision-ephemeral-malvertising/108906

http://www.csoonline.com/article/2838025/data-protection/disaster-as-cryptowall-encrypts-us-firms-entire-server-installation.html

http://www.enigmasoftware.com/cryptowall-ransomware-updated-version-2-new-obfuscator

http://www.nzz.ch/mehr/digital/badusb-stick-adam-caudill-und-brandon-wilson-1.18396488

III. Zwischen legitimer Verteidigung von Schutzrechten und dem Öffnen der Büchse der Pandora

Im September berichtete der SWITCH Security Report über laufende Klagen auf Netzsperren gegen österreichische Internetprovider. Zwischenzeitlich sind dort die Webseiten kinox.to und kino4k.to gesperrt worden. Weil im Zuge des Verfahrens auch der Europäische Gerichtshof angerufen worden war, befürchteten Kommentatoren eine europaweite Etablierung einer Zensurinfrastruktur im Netz. Offenbar nicht zu Unrecht: In Grossbritannien wurden dieser Tag sechs Webseiten gesperrt, auf denen Imitate von Cartier-Uhren angeboten worden waren. Dies nicht aufgrund von Urheber- sondern aufgrund von Markenrechtsverletzungen. Geht es nach dem Willen britischer Rechteverwerter, sollen weitere 46.000 Seiten gesperrt werden. Auch in Österreich zielt der Verein für Anti-Piraterie darauf ab, weitere 100 Webseiten sperren zu lassen. Bei geschätzten Kosten von etwa 6.300 Euro pro Seite käme damit auf die Provider eine Kostenlawine zu.

Es zeichnet sich ab, dass die anvisierte Reform des europäischen wie auch die des schweizerischen Urheberrechts (Stichwort «AGUR12») zu einer Generaldiskussion um die Netzfreiheit führen wird.

Derweil kommen auch noch Begehrlichkeiten aus einer ganz anderen Ecke: Ein neuer Gesetzesentwurf in Österreich mit dem unverdächtigen Namen «2. Abgabenänderungsgesetz 2014» sieht vor, dass die österreichischen Finanzbehörden bereits beim Verdacht auf Finanzvergehen Auskunft über Verkehrs- und Zugangsdaten von Internet-Nutzern bei den Telekommunikationsanbietern einholen können dürfen.

Nachzulesen unter:

https://netzpolitik.org/2014/netzsperren-ab-heute-in-oesterreich-bald-in-ganz-europa

http://futurezone.at/netzpolitik/netzsperren-fuer-seiten-mit-gefaelschten-cartier-uhren/93.087.367

http://futurezone.at/netzpolitik/finanz-will-auskunft-zu-ip-adressen/92.820.502

http://www.nzz.ch/aktuell/digital/agur-12-urheberrecht-1.18319514

IV. Das Netz und die Steuer, eine ungarische Posse ohne Witz

Eigentlich könnte man lachen darüber, dass der ungarische Regierungschef Viktor Orbán mit seinem Versuch gescheitert ist, den Datenverkehr im Internet mit 150 Forint (cirka 59 Rappen) pro Gigabyte – bei einer Maximalsteuer für Privatpersonen von 700 Forint (cirka 2,78 Fr) im Monat – zu besteuern. Doch dazu ist das Thema zu ernst. Denn ungarische Bürger und die EU-Kommission sahen in der geplanten Besteuerung des Datenverkehrs nicht nur eine finanzielle Belastung, sondern auch eine Einschränkung demokratischer Freiheiten. Ihre massiven Proteste führten nun zwar dazu, dass Orbán seine Pläne vorläufig zurückgezogen hat. Dennoch will die ungarische Regierung daran festhalten, Umsätze, die im und durch das Netz generiert werden, zu besteuern. Hat neben dem österreichischen (siehe III.) nun auch der ungarische Fiskus das Netz als neue Geldquelle entdeckt?

Nachzulesen unter:

http://www.zeit.de/politik/ausland/2014-10/ungarn-orb-n-zieht-umstrittene-internet-steuer-zurueck

http://www.budapester.hu/2014/10/26/zehntausende-demonstrieren-gegen-internetsteuer

http://www.computerworld.ch/news/it-branche/artikel/widerstand-gegen-internetsteuer-66676

http://ec.europa.eu/avservices/video/player.cfm?ref=I094641

Zum Stöbern: spannende Präsentationen, Artikel und Videos

SSL/TLS-Zertifikate mit DNSSEC absichern: Spannender Vortrag über DANE von Carsten Strotmann (deutsche Sprache):

https://www.youtube.com/watch?v=KZiW-7jXda4

Für jeden etwas dabei: 120+ Präsentationen von der diesjährigen RIPE69 in London:

https://ripe69.ripe.net/presentations/presentation-archive/

Whitfield Diffie, amerikanischer Kryptographie-Experte und Michael Rogers, Leiter der NSA, im «Gespräch»:

https://www.youtube.com/watch?v=yhwy2ZWi_y8

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