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

Juni 2014

SWITCH

I. Heartbleed ist noch nicht vorbei

Anfang April musste alles ganz schnell gehen: Eine gravierende Schwachstelle in der allgegenwärtigen OpenSSL-Softwarebibliothek wurde bekannt, die das Potenzial hatte, Passwörter und SSL-Schlüssel zu exponieren. Man sprach von einem Internet-GAU. Systembetreiber auf der ganzen Welt waren aufgerufen, schnellstmöglich zu reagieren, vorhandene Patches einzuspielen und Schlüssel zu tauschen.

Nun, nachdem sich der Staub gelegt hat, lohnt es sich, nochmal einen Blick auf das Szenario zu werfen, denn nicht alles ist gut gelaufen. Untersuchungen verschiedener Security Researcher ergeben folgendes Bild:

- Etwa 7% der gepatchten Systeme wurden zwar mit neuem SSL-Zertifikat versehen, benutzen aber nach wie vor den alten Schlüssel.
- Tausende Administratoren haben offenbar OpenSSL zwar upgedatet, allerdings von einer älteren von Heartbleed nicht betroffenen Version zu einer unsicheren - und damit Heartbleed auf ihren Servern erst eingeführt.
- Mindestens ein Viertel der betroffenen Server wurden einen Monat nach dem Bekanntwerden der Sicherheitslücke noch nicht gefixt.

Auch wenn wohl die Mehrheit der Systemadministratoren schnell und bedacht reagiert hat, kann also noch keine generelle Entwarnung ausgesprochen werden.

Und dies noch aus einem weiteren Grund: Im Fokus der Aufmerksamkeit standen bisher vor allem Webserver. OpenSSL wird aber auch an vielen anderen Stellen eingesetzt, die nicht weniger kritisch sind. Die Palette reicht von Servern für E-Mail, Video-, Telefon- und anderen Diensten, über Firewalls und VPN-Endpunkten bis hin zu Steuerungssystemen von Industrieanlagen.

Neue Angriffsvektoren werden derweil noch erforscht. So untersucht beispielsweise Security Researcher Luis Grangeia die Möglichkeit, Heartbleed über Wireless-Authentifizierung (EAP) auszunutzen und damit WLAN-Clients anzugreifen. Gegenüber «Threatpost.com» sagte er kürzlich: «Diese Schwachstelle hat das Potenzial, Angreifern die Tür in Unternehmensnetzwerke zu öffnen.»

Nachzulesen unter:

http://news.netcraft.com/archives/2014/05/09/keys-left-unchanged-in-many-heartbleed-replacement-certificates.html

http://blog.erratasec.com/2014/05/300k-servers-vulnerable-to-heartbleed.html

http://www.csoonline.com/article/2154240/data-protection/research-gives-reason-to-double-check-heartbleed-fix.html

http://www.theregister.co.uk/2014/05/09/unpatched_failboxes_see_thousands_join_heartbleed_club/

http://threatpost.com/heartbleed-exploitable-over-enterprise-wireless-networks/106422

II. Ein Jahr NSA-Skandal und kein Ende

Das Fazit nach 12 Monaten «Snowden-Leaks» fällt ernüchternd aus: NSA, GCHQ und nahezu alle Geheimdienste dieser Welt setzen ungeachtet aller Kritik ihren bisherigen Kurs der unkontrollierten und massenhaften Überwachung und Datensammlung fort. Im Mai erhärtete die Veröffentlichung weiterer NSA-Dokumente den Verdacht, dass die NSA-Gruppe TAO (Tailored Access Operations) auf dem Postweg verschickte Hardware abfängt, um darauf Spyware, sogenannte «beacon implants», zu installieren. Dass die NSA auf diese Weise manipulierte Server, Router und andere Netzwerkgeräte zugreifen kann, hatte schon der 2001 zurückgetretene NSA-Technikchef William Binney publik gemacht.

Anfang Juni berichtete die New York Times, dass die NSA seit 2011 auf allen Kommunikationswegen gezielt Fotos scannt. Millionen Bilder werden täglich durch die Gesichtserkennungs-Software «Tundra Freeze» gefiltert, bis zu 55.000 Bilder täglich seien verwertbar. Laut einem internen NSA-Papier sollen damit nicht nur Terroristen, sondern auch andere «Bösewichte» erkannt und verfolgt werden.
Dass damit auch Schweizer Banker gemeint sein könnten, steht zu befürchten – betont doch der Snowden-Vertraute Glenn Greenwald im Interview mit dem Tagesanzeiger, dass es Hinweise gäbe, dass die NSA auch das Schweizer Bankensystem ausspioniere.

Da erscheint es geradezu logisch, dass in Schweizer bzw. in der Schweiz ansässigen Forschungseinrichtungen an neuen Internet- und Sicherheitsstandards gearbeitet wird. So entwickelt die Network Security Group der ETH gerade eine neue Internetarchitektur mit deutlich höheren Sicherheitsstandards. Scion, so der Projektname, soll es u.a. ermöglichen, dass Sender und Empfänger das Routing ihrer Daten selbst lenken und abhörgefährdete Wege vermeiden können. Unterdessen haben ehemalige Wissenschaftler vom CERN ein Start-up gegründet und einen neuen, abhörsicheren E-Mail-Dienst lanciert: Protonmail. Die strikte Trennung von Authentifizierung und Entschlüsselung, der obligatorische Einsatz von zwei Passwörtern für das Login und der Standort der Mailserver ausschliesslich in der Schweiz machen Protonmail nach Aussagen seiner Entwickler auch «NSA-sicher».

Zum weiterlesen:

http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html

http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy

http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=0

http://www.netsec.ethz.ch/research/SCION

http://home.web.cern.ch/about/updates/2014/05/cern-inspires-entrepreneurs-email-encryption

III. Das Internet lernt Vergessen

Google stellt seit einigen Tagen für europäische Kunden ein Webformular zur Verfügung, mit dem sie das Entfernen bestimmter Suchergebnisse zu ihrem Namen beantragen können. Damit reagiert der Suchmaschinenriese auf ein Urteil des Europäischen Gerichtshofs vom 13. Mai. In diesem wird Personen unter bestimmten Umständen ein «Recht auf Vergessen» im Internet zugesprochen.

Entsprechende Anträge sind laut Urteil direkt an den Suchmaschinenbetreiber zu richten, der dann «sorgfältig ihre Begründetheit zu prüfen» hat. Lehnt dieser den Antrag ab, können sich Betroffene noch an den zuständigen Datenschutzbeauftragten wenden oder aber klagen.

Der Eidgenössische Datenschutzbeauftragte Hanspeter Thür sieht in dem Urteil einen «starken Entscheid». Gegenüber dem «Tagesanzeiger» sagt er: «Das ist ein guter Tag für den Datenschutz. Erstmals wurde festgestellt, dass auch Suchmaschinen Daten bearbeiten und damit dem Datenschutzgesetz unterstellt sind. Die Rechtslage der Betroffenen hat sich massiv verbessert.»

Der vom Gericht mit diesem Urteil anerkannte «notwendige Ausgleich der Interessen zwischen Betroffenen und Nutzern» wird aber nicht von allen Seiten gleich gewertet. «Es muss verhindert werden, dass Suchmaschinen beim Löschen von Meinungen und Informationen willkürlich vorgehen», zitiert «Handelsblatt.de» Ole Schröder, den zuständigen Staatssekretär im deutschen Innenministerium. Auch der Deutsche Journalisten-Verband zeigt sich alarmiert: «Der freie Informationszugang muss den gleichen Stellenwert haben wie der Datenschutz.", sagt DJV-Bundesvorsitzender Michael Konken. Auch BITKOM sieht das Urteil des EuGH kritisch: Eine Einzelfallprüfung in der verschiedene Interessen wie Persönlichkeitsrecht und Informationsfreiheit abgewogen werden, ist laut dem IT-Branchenverband für Suchmaschinenbetreiber nicht umsetzbar.

Inwieweit das Verfahren von Google funktioniert, darüber äussert sich bisher noch niemand. Gerüchteweise gibt es bereits Tausende von Löschanfragen an Google. Zu einer solchen muss man übrigens zur Authentifizierung eine Kopie eines gültigen Lichtbildausweises hochladen. Ein Verfahren, dass laut Rechtsanwalt Thomas Stadler zumindest in Deutschland problematisch ist: «Der Ausweis darf zwar zum (elektronischen) Identitätsnachweis verwendet werden, er darf aber bei Google nicht gespeichert werden. Letzteres passiert freilich nach Übersendung einer Datei zwangsläufig.» schreibt er in seinem Blog.
Abzuwarten bleibt ausserdem, wie andere Suchmaschinenbetreiber, wie Microsoft oder Yahoo, auf das Urteil reagieren.

Mehr dazu:

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf

https://support.google.com/legal/contact/lr_eudpa?product=websearch

http://www.tagesanzeiger.ch/schweiz/standard/Ein-guter-Tag-fuer-den-Datenschutz/story/11314698

http://www.golem.de/news/nach-eugh-urteil-google-schlichtungsstelle-soll-recht-auf-vergessen-regeln-1405-106768.html

http://www.nzz.ch/aktuell/digital/google-setzt-recht-auf-vergessenwerden-um-1.18312335

http://www.bitkom.org/de/presse/8477_79340.aspx

http://www.internet-law.de/2014/05/google-stellt-formular-fuer-antrag-auf-entfernung-aus-den-suchergebnissen-gemaess-europaeischem-datenschutzrecht-online.html

Zum Stöbern: spannende Präsentationen, Artikel und Videos

SSL-Zertifikat-Fuzzing: US-Amerikanische Forscher haben eine Methode entwickelt, um mit Hilfe von zufällig mutierten und zusammengewürfelten Zertifikaten Bugs in SSL-Bibliotheken zu finden:

http://www.heise.de/security/artikel/SSL-Fuzzing-mit-Frankencerts-2166135.html

Das Netzwerksicherheits-Unternehmen FireEye hat seinen Advanced Threat Report 2013 für Europa heruntergebrochen. Die Schweiz belegt dort prozentual gesehen Platz 2 bei den Infektionen (Unique Infections by Country). «Higher Education» ist im Bereich «Unique Infections by Industry Vertical» mit Rang 4 recht prominent vertreten:

http://www.fireeye.com/blog/corporate/2014/04/the-fireeye-advanced-threat-report-2013-european-edition.html

Auf der diesjährigen Troopers14 Securitykonferenz hat sich Enno Rey grundsätzliche Gedanken dazu gemacht, warum IPv6-Security so schwierig ist. Dieser und 26 weitere Talks von der Konferenz sind online:

http://www.youtube.com/channel/UCPY5aUREHmbD04PtR6AYLfQ

Dieser SWITCHcert Security Report wurde von Frank Herberg und Dieter Brecheis verfasst.