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

Dezember 2016

SWITCH

I. Macht & Cybercrime: Massiver Diebstahl von Userdaten bei zwei aktuellen Hacks

Mehr als 400 Millionen Kunden von «Friend Finder Network Inc.» stehen datentechnisch entblösst da, nachdem die Server des Betreibers von Plattformen wie «adultfriendfinder.com», «cams.com» oder «penthouse.com» im Oktober 2016 gehackt wurden. Beim grössten Datendiebstahl des zu Ende gehenden Jahres gelangten die Daten von 412.214.295 Accounts in die falschen Hände, bzw. Datenspeicher. Peinlich ist dieser Hack nicht nur für die User, sondern auch für den Plattformbetreiber – und das gleich mehrfach: Denn zum einen wurde Friend Finder Network bereits im Mai 2015 gehackt. Zum andern sind gemäss Recherchen von leakedsource auch Daten von knapp 16 Mio. Accounts entwendet worden, deren Löschung zwar schon länger beantragt war, die aber von Friend Finder Network weiter gespeichert wurden. Und zum dritten bezichtigt leakedsource den Sexplattformbetreiber der groben Fahrlässigkeit, weil Passwörter angeblich in Klartext bzw. als alles andere als sicherer SHA1-Hash gespeichert wurden. Schwacher Trost für die User: nach Informationen von ZD-Net seien im aktuellen Hack wenigstens keine

Daten zu «sexuellen Vorlieben» gestohlen worden. Ob das auch für das Live-Cam-Material der entsprechenden Friend Finder Plattformen gilt, bleibt jedoch unklar, weil Friend Finder Network auf weitergehende Fragen zum Datenklau keine Auskünfte erteilen wollte.

Auf grobe Missstände – diesmal auf Regierungswebseiten in Italien – deutet auch der zweite grosse Datendiebstahl des vergangenen Monats hin. Dem Hacker Kapustkiy gelang es mit einer einfachen SQL-Injektion 45.000 User-Daten zu stehlen. Darunter sind auch Zugangsdaten zu Diensten verschiedener italienischer Städte. Besonders misslich ist aber die Tatsache, dass der Hack von den italienischen Behörden bis heute schlicht und ergreifend ignoriert wird. Kapustkiy hat nach eigenen Angaben sogar die Webseitenadministratoren auf das Leck hingewiesen, bis heute aber ebenso keine Antwort bekommen wie verschiedene Security-Sites auf ihre Anfragen an offizielle Regierungsstellen zum gleichen Thema. Immerhin wurde die kompromittierte Seite inzwischen vom Netz genommen, gefixt und wieder online gestellt.

Nachzulesen unter:

https://www.leakedsource.com/blog/friendfinder
https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record
http://de.engadget.com/2016/11/14/friendfinder-networks-gehackt-uber-412-millionen-nutzerkonten-b
http://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users
http://news.softpedia.com/news/hacker-breaks-into-italian-government-website-45-000-users-exposed-510332.shtml
http://securityaffairs.co/wordpress/53575/data-breach/kapustkiy-italian-website.html

II. Wenn angebliche Sicherheits-Addons Surfer ausspionieren

«Web of Trust» ist eine Browsererweiterung, die bereits im Namen um das Vertrauen von Internetsurfern wirbt und jahrelang als sinnvolles Sicherheits-Addon eingestuft und empfohlen wurde. Im November wurde bekannt, dass die Erweiterung mit dem verheissungsvollen Namen ihre Nutzer ausspioniert und die Daten an Dritte weiterleitet. Zuvor war es Reportern des NDR gelungen, ein auf dem freien Markt erhältliches Datenpaket eines ausländischen Anbieters von Nutzerdaten auszuwerten. Darin verpackt: alle im August aufgerufenen Webseiten von rund drei Millionen

Nutzern mit mehr als drei Milliarden Einträgen jeweils mit Datum, Nutzerkennung und der Surf-Historie mit mehreren Web-Adressen. Die sind im auf rund 122 Milliarden-US-Dollar geschätzten Markt für Big-Data-Analysen und begleitenden Dienstleistungen (IDC-Schätzung für 2015) besonders wertvoll, weil sie User und ihr Surf- und Informationsverhalten besonders transparent machen.

Umso perfider ist der «Verrat» von Web of Trust (WOT), den die NDR-Reporter aufdeckten, als sie sich auf die Suche nach den Quellen dieser Daten machten. Denn eigentlich suggeriert WOT den Usern, dass sie damit sicherer und vertrauensvoller surfen könnten. Zu diesem Zweck prüft WOT die Integrität einer im Browser eingegebenen Zieladresse und zeigt mit Hilfe einer Ampel schnell und einfach die Vertrauenswürdigkeit der Seite. WOT weist aber auch im Kleingedruckten darauf hin, dass diese Daten gespeichert und an Dritte weitergegeben werden, betont dabei allerdings, dass die Daten anonym seien. Dass sie dennoch mit anderen Daten verknüpft deanonymisierte, personalisierte und damit in Deutschland und der Schweiz rechtlich nicht zugelassene Nutzerprofile ermöglichen, konnten die Reporter nachweisen. Zudem erhärtete sich ihr Verdacht, dass auch andere Addons, wie z.B. Proxtube, ihre Kunden verraten.

Kräftig spioniert haben auch 120.000 Smartphones, die der chinesische Hersteller Blu im amerikanischen Markt verkauft hat. Mitte November veröffentlichten Forscher der amerikanischen Sicherheitsfirma Kryptowire, dass die in den Android-Geräten BLU R1 HD eingesetzte Firmware AdUps der Firma Shanghai Adups Technology Co. Ltd. alle drei Tage das Adressbuch, Nachrichten und den Standort an Server in China gesendet hatten. Adups bemühte sich umgehend, zu betonen, das Unternehmen hätte keinerlei Verbindung zur chinesischen Regierung. Dafür stehen aber auch die Smartphone- und Tablethersteller ZTE und Huawei auf der AdUp-Kundenliste. Im Gegensatz zu AdUps üben sich beide Unternehmen in völligem Schweigen zu diesem Thema, doch konnte die NZZ in Erfahrung bringen, dass AdUps auf ca. 700 Millionen Mobilgeräten und Automotive Systems eingesetzt wird. Huawei gehört als weltweite Nummer zwei unter den Netzwerkausrüstern auch in der Schweiz zu den grossen Playern, arbeitet mit nahezu allen Telekommunitaionsanbietern hierzulande und hat u.a. zum September 2016 den IT-Bereich des Telekommunikationsanbieters Sunrise übernommen.

Nachzulesen unter:

http://www.tagesschau.de/inland/tracker-online-101.html
http://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html
https://www.heise.de/newsticker/meldung/Millionen-Surf-Profile-Daten-stammen-angeblich-auch-von-Browser-Addon-WOT-3453820.html
https://www.heise.de/newsticker/meldung/Bericht-Auch-Add-on-Proxtube-leitet-Surf-Historie-aus-3491498.html
https://netzpolitik.org/2016/nackt-im-netz-auch-das-browser-plugin-proxtube-sendet-deine-besuchten-webseiten-an-dritte-sofort-loeschen
http://www.nzz.ch/digital/it-sicherheit-smartphones-schickten-daten-aus-den-usa-nach-china-ld.128678

III. Mirai zum zweiten: Botnetz legt 900.000 Telekom-Router lahm

Nachdem das weltweit aktive Botnetz Mirai bereits im Oktober mit massiven DDoS-Attacken via IoT-Devices weite Teile des US-amerikanischen ebenso wie des globalen Internets lahmgelegt hatte, schlug das Monster-Malware-Netz am letzten November-Wochenende erneut in grossem Massstab zu und führte zum zeitweilig länger dauernden Ausfall von ca. 900.000 Routern der Deutschen Telekom. User, die sich über einen Speedport-Router des Unternehmens mit dem Internet verbinden wollten, konnten weder aufs Netz zugreifen, noch mailen, telefonieren oder fernsehen. Experten des Betreibers bemühten sich, umgehend ein Softwareupdate zur Verfügung zu stellen und sie forderten die User via frei empfangbare Radio- und Fernsehkanäle auf, die Router von Stromnetz und Internet zu trennen und nach 5-minütiger Pause erneut anzuschlissen, damit über den manuellen Reset die Software eingespielt werden könne. Offenbar gelang es der Telekom, damit bis zum Abend des folgenden Montags alle Verbindungen wieder herzustellen.

Dennoch zeichnen verschiedene Kommentatoren, u.a. die F.A.Z. beinahe apokalyptische Szenarien und fordern deutlich mehr Regelungen zur Erhöhung der bekannt schlechten Sicherheitsausrüstung von Geräten im Internet der Dinge (auch im SWITCHcert Report haben wir immer wieder auf die mangelhafte, oft nicht existierende Sicherheitsausstattung von IoT-Devices hingewiesen). Angesichts einer Schadenssumme durch Cyberkriminalität, die allein für Deutschland auf 22 bis 25 Mrd. Euro geschätzt wird, sollten einige Cent pro Device eigentlich kalkulierbar sein. Denn Mirai wird von vielen Experten erst als ein Anfang grossflächiger Angriffe auf digitale Netze gesehen.

Nachzulesen unter:

http://www.n-tv.de/technik/Stoerung-bei-Telekom-Hacker-sollen-verantwortlich-sein-article19198236.html
http://www.faz.net/aktuell/feuilleton/medien/nach-dem-telekom-hacking-der-preis-der-sicherheit-14556876.html
http://www.n-tv.de/technik/Monster-Botnetz-griff-Telekom-Router-an-article19207981.html
http://www.bocquel-news.de/Hacker-Attacken-Schäden-finanziell-aushebeln.36384.php

IV. Es gibt auch gute Nachrichten: Botnetz Avalanche ist zerschlagen

Im Zusammenhang mit der Mirai-Attacke auf die deutsche Telekom sprach der Chef des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) von einem «Wettlauf zwischen Hase und Igel». Offenbar haben nun einmal die Guten das Rennen gemacht und das Phishing-Netzwerk Avalanche zerschlagen. Avalanche gehört zu den wichtigsten Netzwerken Cyberkrimineller. Als Phishing-Netzwerk ermöglichte es Avalanche den Hackern, LogIn-Daten fürs e-Banking zu stehlen und Geld von den Konten mit kompromittierten Accounts abzuziehen. Seit 2009 wurden über die Botnetz-Struktur auch bösartige E-Mails mit Malware verschickt.

Wie das Mirai-Botnetz gilt auch Avalanche als eine der grössten Infrastrukturen zum Betrieb von Botnetzen. Cybercrime-Experten aus 41 Staaten, darunter das FBI, das BSI und andere haben nun in einer konzertierten Aktion weltweit 39 Server und mehrere Hunderttausend Domains gleichzeitig beschlagnahmt und alleine in Deutschland mehr als 50.000 infizierte Computer der Kontrolle durch die Cyberkriminellen entzogen.

Nachzulesen unter:

http://www.golem.de/news/avalanche-botnetz-weltweites-cybercrime-netzwerk-zerschlagen-1612-124829.html
http://www.zeit.de/digital/datenschutz/2016-12/phishing-netzwerk-avalanche-botnetz-infrastruktur-zerschlagen
https://krebsonsecurity.com/2016/12/avalanche-global-fraud-ring-dismantled

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