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

Juni 2015

SWITCH

I. Was haben Steuerbehörden und Kontaktbörsen gemein? Sie können ihre Kundendaten nicht schützen

Drei prominente Datendiebstähle im grossen Stil sind in den letzten Tagen publik geworden. Die Hacker machten bei ihren Angriffen auf die Kontaktbörse «Adult Friend Finder», die US-amerikanische Steuerbehörde IRS und die Japanische Pensionskasse reiche Datenbeute.

Nach Recherchen der Security-Bloggerin Bev Robb hat ein thailändischer Hacker aus Rache Geburtsdaten, E-Mail- und Postadressen sowie sexuelle Vorlieben von 3,9 Millionen Usern der Erotikkontaktbörse «Adult Friend Finder» gestohlen und im Tor-Netzwerk veröffentlicht. Unklar bleibt, ob dem Hacker auch Kreditkartendaten in die Hände fielen. Denn die könnte er vor Veröffentlichung zur «weiteren Verwendung» entfernt und gespeichert haben.

Zwischen Februar und Mitte Mai haben Hacker versucht, Zugang zu rund 200.000 Nutzerkonten amerikanischer Steuerzahler zu bekommen. In ca. 100.000 Fällen gelang es ihnen, persönliche Daten wie Geburtsdaten, Adressen und

Sozialversicherungsnummern zu erbeuten. Dazu verschafften sie sich Zugang zu einem System namens «Get Transcript», das Nutzern Einblick in alle ihre Vorgänge bei der Steuerbehörde gewährt. Den mehrstufigen Authentifizierungsprozess unterliefen sie mit Hilfe vorab in ihren Besitz gebrachter Daten. Get Transcript wurde daraufhin von der IRS vorläufig abgeschaltet.

Um gut den Faktor 10 grösser ist die Anzahl der um ihre Identität bestohlenen ca. 1,25 Millionen Kunden der Japanischen Pensionskasse. Namen, Pensionskontonummern, Geburtsdaten und Adressen fielen Cyberkriminellen in die Hände, nachdem ein Angestellter eine Virus-befallene E-Mail geöffnet hatte.

Gemeinsam ist allen drei Attacken die Erkenntnis, dass offenbar weder private noch staatliche Organisationen sensible Kundendaten zuverlässig schützen können. Angesichts dieser ernüchternden Schlussfolgerung erscheinen beispielsweise die Pläne zum zentralen Sammeln von persönlichen Gesundheitsdaten (siehe Security Reports 5/2015 und 12/2014) in einem düsteren Licht.

Nachzulesen unter:

https://teksecurityblog.com/blog/2015/04/13/hacked-how-safe-is-your-data-on-adult-social-sites
http://www.heise.de/security/meldung/Sexboerse-Adult-Friend-Finder-gehackt-Nutzerdaten-im-Netz-verteilt-2663029.html
http://www.golem.de/news/hack-auf-datingplattform-sexuelle-vorlieben-von-millionen-menschen-veroeffentlicht-1505-114219.html
https://krebsonsecurity.com/2015/05/irs-crooks-stole-data-on-100k-taxpayers-via-get-transcript-feature
http://www.bankinfosecurity.com/irs-100000-taxpayer-accounts-breached-a-8261
http://www.spiegel.de/netzwelt/web/irs-online-angriff-auf-die-us-steuerbehoerde-a-1035706.html
http://www.zeit.de/news/2015-06/01/japan-japans-pensionskasse-gehackt-01124207

II. Gute Freunde hören zu – der BND hört mit. Und der Skandal hört nicht auf

Darauf, dass Feinde mithören, verwiesen im 2. Weltkrieg alle kriegführenden Mächte in gross angelegten Informationskampagnen: «The ENEMY is listening. He wants to know what you know KEEP IT TO YOURSELF», warnte z.B. das United States Office of War Information (OWI). Nun wird immer offensichtlicher,

dass einer der Geheimdienste eben jener Vereinigten Staaten, die NSA, in unseren Tagen auch von befreundeten Nachrichtendiensten wie dem deutschen BND Dinge wissen wollte (und will), die der BND selbst nicht wusste (und weiss). Im Klartext: Gemäss Aussagen des BND-Präsidenten Schindler hat die NSA die freundschaftlichen Dienste des BND zur Wirtschafts- und anderer Spionage genutzt und diesen dazu «ermuntert», weitere Freunde, wie die Schweiz, Belgien oder die Europäische Union zu bespitzeln. Inwieweit sie das immer noch tut, kann gegenwärtig nicht beurteilt werden. Fakt ist wohl, dass dem BND bereits 2005 aufgefallen war, dass auf den sogenannten Selektoren-Listen mit Suchbegriffen der NSA auch Namen von Unternehmen, europäischen Institutionen, hochrangigen Politikern und Firmen im Ausland standen. Zudem berichtet «Zeit Online», dass der BND neben den Selektoren-Daten monatlich auch ca. 1,3 Milliarden (!) Metadaten auf NSA-Rechner schickt.

Gemäss eigenen Aussagen informierte der BND das Bundeskanzleramt bereits 2008 in einem vertraulichen Bericht über den Datenaustausch, dem 2010 ein weiterer folgte. Geschehen ist bis zu den Snowden-Leaks aber nichts, wohl auch, weil sich (nicht nur) die Bundesregierung in Zeiten neuer Sicherheitsbedrohungen zu abhängig von den Informationen der amerikanischen Geheimdienste fühlt.

Aktiv geworden ist nun aber Airbus mit einer Strafanzeige wegen Spionage. Auch in der Schweiz und Belgien stösst das, was man in Anspielung auf den zynischen Begriff des «Friendly Fire» als «Friendly Spying» bezeichnen könnte, auf Verwunderung und Empörung. Auch die amerikanischen Geheimdienste zeigen sich zunehmend enerviert. Und zwar darüber, dass deutsche und europäische Politiker nun eine restlose Aufklärung des Skandals fordern.

Nachzulesen unter:

https://netzpolitik.org/2015/internes-dokument-belegt-bnd-und-bundeskanzleramt-wussten-von-wirtschaftsspionage-der-usa-gegen-deutschland
http://www.spiegel.de/politik/deutschland/bnd-affaere-weitere-listen-mit-brisanten-suchbegriffen-a-1035018.html
http://www.zeit.de/digital/datenschutz/2015-05/bnd-affaere-selektoren-nsa-liste/komplettansicht
http://www.zeit.de/politik/deutschland/2015-05/bnd-nsa-milliarden-metadaten
http://www.golem.de/news/bnd-chef-schindler-wir-sind-abhaengig-von-der-nsa-1505-114201.html
http://www.handelsblatt.com/politik/deutschland/bnd-affaere-airbus-stellt-strafanzeige-wegen-nsa-spionage/11715836.html
http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890
http://www.heise.de/newsticker/meldung/Belgien-erwartet-Antworten-von-Deutschland-zu-BND-Spaehvorwuerfen-2671162.html

http://www.heise.de/newsticker/meldung/Der-grosse-Bruder-reagiert-genervt-2663846.html
http://www.sueddeutsche.de/politik/no-spy-abkommen-geschichte-eines-taeuschungsmanoevers-1.2494417
http://www.faz.net/aktuell/politik/ausland/amerika/entscheidung-im-senat-nsa-spaehprogramm-vor-dem-aus-13622851.html

III. Bundestrojaner mal anders: Cyber-Angriff auf gesichertes Netz des Deutschen Bundestags

Wäre der Cyberangriff auf das gesicherte Netz des Deutschen Bundestags in seiner Ausführung und Tragweite nicht so ernst in seinem Charakter und so katastrophal in seinen Auswirkungen, er wäre beinahe schon ein Treppenwitz der Geschichte der Cyberkriminalität. Denn das Deutsche Parlament, das mehrheitlich dem Einsatz sogenannter Bundestrojaner zugestimmt hat, ist Anfang Mai selbst Ziel eines Trojaner-Angriffs geworden. Und der ist immer noch in vollem Gange, weil er so mysteriös und ausgeklügelt geführt wurde, dass ihn auch die IT-Sicherheitsexperten des Bundestags bis heute nicht stoppen oder gar beseitigen konnten. Niemand weiss, seit wann, wie lange noch und vor allem wohin von der Malware auf den Rechnern der Abgeordneten Daten abfliessen und verschickt werden. Deshalb vermuten nicht nur Parlamentarier, dass der Trojaner von einem ausländischen Geheimdienst eingeschleust wurde. Falls es nicht gelingen sollte, die Malware zu stoppen, müsste die gesamte IT-Infrastruktur des Bundestags neu aufgesetzt werden.

Nachzulesen unter:

http://www.zeit.de/digital/datenschutz/2015-05/hackerangriff-bundestag-sommerpause
http://transdata.info/schwerer-angriff-auf-das-bundestagsnetz-seit-mai-2015
http://www.heise.de/security/meldung/Cyber-Angriff-auf-Bundestag-bleibt-ausser-Kontrolle-2662336.html
http://www.nzz.ch/international/bei-hackerangriff-auf-bundestag-wurden-daten-gestohlen-1.18551627
http://www.spiegel.de/netzwelt/netzpolitik/bundestag-ermittler-vermuten-geheimdienst-hinter-cyberangriff-a-1034790.html

IV. Reload nach dem Reset – Android-Smartphones behalten Daten auch nach Factory-Reset

Bis heute ist die Frage auf dem Titel der deutschen Fassung von Philip K. Dicks legendärem Sci-Fi-Klassiker «Bladerunner» nicht geklärt: «Träumen Androiden

von elektrischen Schafen?» Dagegen dürften viele (Ex-)Besitzer von Smartphones mit Android-Betriebssystemen der Versionen 2.3.x bis 4.3 von Alpträumen heimgesucht werden, wenn sie die beiden Studien von Laurent Simon und Ross Anderson von der Cambridge University gelesen haben. Denn in der unten erst-zitierten Studie wurde der Nachweis erbracht, dass auch nach dem Zurücksetzen eines Android-Smartphones auf den Fabrikzustand (Factory-reset) sensible Daten, wie z.B. Log-in-Daten, Textnachrichten, E-Mails oder Fotos, wiederhergestellt werden können. Simon und Anderson behaupten, dass sie dies auch auf Geräten erreicht hätten, deren Daten mit Android-Vollverschlüsselung gesichert waren, auch wenn sie dafür deutlich mehr Zeit und Mühe hätten investieren müssen.

Die Hoffnung darauf, dass die wohl auf mangelnde Sorgfalt der Hersteller zurückzuführende Sicherheitslücke mit dem Einsatz sogenannter Wiping-Tools geschlossen werden könnte, zerschlagen Simon und Anderson in ihrer zweiten Studie. Fazit dort: Von den meistgenutzten Apps zum Löschen des Gerätespeichers, entfernen zehn die Daten nicht so, dass sie nicht wiederherstellbar wären. Eine forensische Untersuchung von Steve Mellings, Gründer der Asset Disposal & Information Security Alliance (ADISA) und Andrew Blyth, Professor an der University of South Wales kommt zu einem ähnlichen Schluss, zieht aber noch einen Vergleich mit Blackberry- und Apple iOS-Geräten: «In summary, the factory reset function, when performed on the sample of BlackBerry and Apple devices, erases the user data from the device such that using standard forensic tools and techniques it is impossible to recover the data … However, the story with the Android devices is very different. The research findings show that the factory reset function, when performed on certain Android devices is not sufficient and that data can be recovered.»

Nachzulesen unter:

http://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf
http://www.cl.cam.ac.uk/~rja14/Papers/mav_most15.pdf
http://www.heise.de/security/meldung/Daten-von-Millionen-zurueckgesetzten-Android-Smartphones-wiederherstellbar-2663267.html
http://www.informationsecuritybuzz.com/forensic-analysis-of-smartphone-factory-reset-function

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Sune Lehmann hat sich in einem Forschungsprojekt angeschaut, wie gut man mobile Nutzer mit Hilfe von Wifi-Informationen tracken kann, vielleicht auch wenn sie Wifi auf ihrem Gerät abgeschaltet haben:

http://sunelehmann.com/2015/05/26/tracking-human-mobility-using-wifi-signals/

Ein aktueller Exploit-Kit greift vom heimischen PC aus den lokalen Router an, um ihn für seine Zwecke umzukonfigurieren. Im «Malware don't need Coffee» Blog gibt's eine Analyse dazu:

http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html

http://www.heise.de/security/meldung/Exploit-Kit-greift-ueber-50-Router-Modelle-an-2665387.html

PGP-Erfinder Phil Zimmermann ist aus den USA in die Schweiz gezogen. Im Interview mit dem Guardian erklärt er, warum er sich hier sicherer fühlt.

http://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy

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