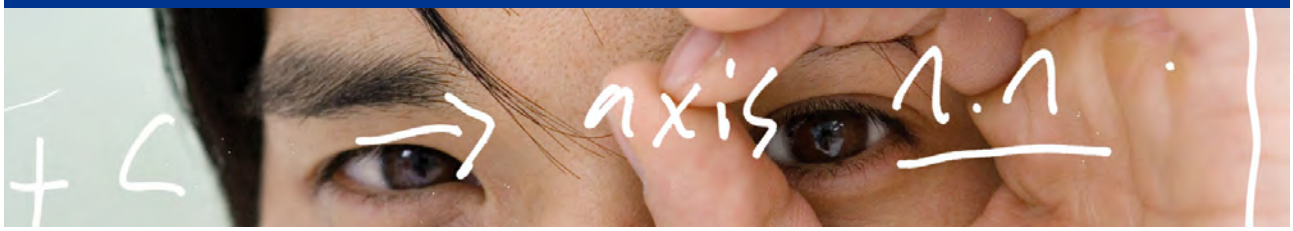
SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Februar 2014



SWITCH

I. Bundesamt nach E-Mail-Sicherheitstest massiv in der Kritik

16 Millionen Benutzernamen und Passwörter verschiedenster Mail-Dienste hatten Forscher und Sicherheitsbehörden bei der Analyse krimineller Botnetze entdeckt. Um schnelle Massnahmen zum Schutz der weltweit betroffenen Nutzer zu ergreifen, hatte man die Daten dem BSI (Bundesamt für Sicherheit in der Informationstechnik) anvertraut. Die deutsche Behörde liess sich jedoch Zeit und landete schliesslich ein derartiges PR-Debakel, dass sie sich nun selbst mangelnde Sicherheitsstandards vorwerfen lassen muss.

Angesichts des grossangelegten Hack-Angriffs, warnte der BSI Mitte Januar, sollten alle Internetnutzer vorsichtshalber ihre Online-Passwörter ändern. Extra dafür habe das BSI eine Webseite eingerichtet, über die man prüfen könne, ob die eigene Mailadresse betroffen sei. In diesem Fall riet das BSI, den eigenen Rechner auf Schadprogramme zu prüfen und sämtliche Passwörter zu Online-Diensten zu ändern. Andernfalls könnten die Hintermänner mit den E-Mail-Passwort-Kombinationen Identitätsdiebstahl betreiben, Facebook-Konten kapern, private und geschäftliche E-Mails lesen oder

unter falschem Namen auf Online-Shoppingtour gehen. Besonders riskant sei die Situation für alle, die ihre E-Mail-Passwort-Kombination mehrfach verwenden.

Unglückliche Krisenkommunikation

Aufgescheucht von der Warnung, wollten viele Internetnutzer schnellstens wissen, ob sie betroffen sind. Das gelang den meisten nicht, da die BSI-Testseite schon nach kurzer Zeit überlastet und nicht mehr erreichbar war. Die Seite sei «immer wieder mal aufrufbar. Am besten probiert man es mehrfach», empfahl der BSI wütenden Nutzern.
Die Kritik an der Behörde wurde noch lauter, als das Nachrichtenmagazin «Der Spiegel» Ende Januar berichtete: Das BSI wusste bereits seit August 2013 von dem Datenklau. Zu diesem Zeitpunkt informierte es aber nur die IT-Verantwortlichen des Bundeskriminalamts über die 600 betroffenen Mailkonten aus Ministerialkreisen. Warum man alle anderen erst Monate später informierte, erklärte BSI-Präsident Michael Hange damit, man habe eben «extrem gut vorbereitet sein» für so eine Aktion. Herausgekommen sei trotzdem wenig Eindrucksvolles, schimpften viele verärgerte Nutzer. Netzjournalist Richard Gutjahr brachte es für viele «Leidgenossen» auf den Punkt, als er in seinem Blog schrieb: «Diese Seite ist technisch derart ‚extrem gut vorbereitet', dass sie sofort in die Knie geht, sobald sie auch nur von zwei besorgten Bundesbürgern gleichzeitig besucht wird».

Als unglücklich erwies sich auch das bereitgestellte Prüfverfahren des BSI: Nur Nutzer, die tatsächlich betroffen waren, erhielten nach dem Selbsttest eine Mail vom BSI. Das sei ungenügend, mahnten Securityexperten. Das blosse Ausbleiben einer E-Mail sei kein geeignetes Verfahren, Entwarnung zu geben. Auch der Inhalt der Antwort-Mail stiess auf Kritik. Er sei, wie das IT-Forum «Heise Security» fand, ein «Musterbeispiel» dafür, «wie eine sicherheitsrelevante Warnung eben nicht beschaffen sein sollte»: ohne Impressum, persönliche Anrede und manipulierbar von Dritten. Ganz zu schweigen von der BSI-Testseite selbst, die zig Sicherheitsschlupflöcher für Angreifer und Trittbrettfahrer böte, so Heise Security. Laut BSI waren bis Ende Januar von rund 12,5 Millionen Nutzeranfragen gut 884 000 Betroffene.

Mehr dazu im Internet unter:

https://www.sicherheitstest.bsi.de/
http://www.br.de/presse/inhalt/pressemitteilungen/radiowelt-michael-hange-100.html

http://www.spiegel.de/netzwelt/web/online-konten-geknackt-mail-adressen-check-beim-bsi-in-der-kritik-a-944739.html
http://gutjahr.biz/2014/01/ich-glaub-es-hackt/

II. Medien verbreiten Panik vor weltweiten Geldautomaten-Ausfällen

Weil Microsoft im April den offiziellen Support für das Betriebssystem Windows XP einstellt, sind Bankkunden in den USA und Europa zurzeit irritiert. Grund dafür ist ein Interview der «Bloomberg Businessweek» mit Robert Johnston, Manager des Technologiekonzerns und Geldautomaten-Herstellers «National Cash Register» (NCR). Darin warnt Johnston davor, dass 95 Prozent aller Geldautomaten weltweit noch auf dem veralteten Betriebssystem laufen. Was seither folgte, war eine mediale Panikmache vor globalen Automaten-Ausfällen.

Bis April 2014 werden nur 15 Prozent aller Geldautomaten in den USA auf das modernere Windows 7 aufgerüstet sein, schätzt Johnston. Dabei sollte das bei den gut drei Millionen Automaten weltweit schon längst passiert sein. Da die meisten «Automatic Teller Machines» noch viel älter sind als das Betriebssystem XP, müssten viele davon ausgetauscht werden, um mit moderneren Betriebssystemen auszukommen. Schon heute sind Rechner mit Windows XP sechsmal anfälliger für Schadprogramme als mit Windows 8. Dies entspricht jedoch nicht der Sicherheitslage bei Bankautomaten, entwarnt Aravinda Korala von «Korala Associates Limited». Der Leiter des Software-Spezialisten für Geldautomaten sagt, es sei völlig «normal», dass der technische Fortschritt bei Geldautomaten langsamer voranschreite als bei PCs.

Schweizer Bankkunden auf der (relativ) sicheren Seite

Auch bei der Deutschen Kreditwirtschaft hält man die Panikmache für verfehlt. Da die Automaten nicht am Internet hängen, sei die Art des Betriebssystems egal, so eine Sprecherin gegenüber dem IT-Newsportal «Golem.de». Experten gehen davon aus, dass nahezu alle Geldautomaten in Deutschland auf Windows XP oder Windows 2000 basieren. Hierzulande schaut die Lage ein wenig besser aus: Wie «inside-it.ch» berichtet, basieren die meisten der Automaten der Schweiz auf einer «Embedded Version» von Windows XP – einer eigenständigen Entwicklungslinie, die Microsoft noch bis 2016 pflegt. Sämtliche neuere Geräte hat NCR bereits mit Windows 7 ausgeliefert. Laut Constanze Ehrt, PR-Managerin bei NCR, ist die Umstellung der

installierten Basis von XP auf Windows 7 Sache der Banken. Automaten des US-Herstellers «Diebold» sind nach Recherchen von Inside-IT bereits aufgerüstet.

Allerdings gibt es auch andere Methoden, um Geldautomaten «offline» zu manipulieren: Das haben zwei Forscher bei einem Treffen des Chaos Computer Clubs erst kürzlich vorgeführt: Die Angreifer hatten dafür ein Loch in den Automaten einer Bank geschnitten, einen präparierten USB-Stick in den Anschluss für Webcam oder Drucker gesteckt und so ihr Schadprogramm in das System des Automaten geschleust. Die verwendete Malware soll dabei auch eine Lücke in Windows XP ausgenutzt haben, um schlussendlich Kontrolle über die Geldausgabe zu erlangen. Den betroffenen Banken fiel dies erst nach Monaten auf, weil immer wieder spurlos Geld aus den Automaten verschwunden war.

Weiterführende Infos:

http://blogs.technet.com/b/mmpc/archive/2014/01/15/microsoft-antimalware-support-for-windows-xp.aspx
http://www.inside-it.ch/articles/35103
http://youtu.be/0c08EYv4N5A
http://www.businessweek.com/articles/2014-01-16/atms-face-deadline-to-upgrade-from-windows-xp
http://www.golem.de/news/ncr-weltweit-95-prozent-aller-geldautomaten-mit-windows-xp-1401-103997.html
http://www.heise.de/ct/heft/2014-3-Signaturen-fuer-Virenscanner-unter-Windows-XP-nach-April-2014-2085393.html
http://www.20min.ch/digital/news/story/Windows-XP--Ein-Risiko-fuer-Geldautomaten--18642174

III. Google Glass schafft Tatsachen in punkto Gesichtserkennung

Freihändig surfen ohne extra aufs Handy schauen zu müssen: Mit diesem Verkaufsargument hatte Google im April 2012 seine Android-basierte Hightech-Brille «Glass» vorgestellt. Seither ist allerdings nicht mehr viel passiert: Der Verkaufsstart wurde mehrfach verschoben, während bislang nur ausgewählte Personen die Testversion der Brille nutzen. Vermutlich, spekulieren Medien und Technikfans, weil es bislang an überzeugenden Einsatzgebieten mangelt. Das scheint Google selbst durchaus bewusst zu sein. Der Konzern hatte genau deswegen im April 2013 die Programmierschnittstelle von Glass veröffentlicht und Entwickler und Firmen weltweit dazu aufgerufen, sich ihrerseits etwas einfallen zu lassen.

Herausgekommen ist bis dato ein buntes Sammelsurium an Programmen, vor allem aus dem Bereich Gesichtserkennung. Dabei hatte Google genau das nach massiven Einsprüchen von Datenschützern explizit ausgeschlossen, wie Kay Oberbeck, Sprecher von Google Nordeuropa, gegenüber der Zeitung «Die Zeit» bestätigt: «Grundsätzlich gilt, dass wir keinerlei Gesichtserkennungs-Apps für Google Glass tolerieren. Sie werden nicht als offizielle 'Glassware' zugelassen.»
Als da etwa die «NameTag»-App der Firma «FacialNetwork» wäre: Mit ihr können sich Glass-Träger direkt Informationen über eine Person einblenden lassen, die vor ihnen steht. Welche Infos das sind, ist laut Hersteller eine Frage der Kooperation: Es wäre zum Beispiel der Live-Abgleich mit Informationen aus Dating-Portalen möglich, aber auch mit sozialen Netzwerken oder gar Strafdatenbanken staatlicher Behörden. Für Entwickler Kevin Alan Tussy ist NameTag jedenfalls der ultimative Weg, um «Menschen besser [zu] verstehen». Die App soll schon bald veröffentlicht werden. Wie sich verhindern lässt, selbst in der NameTag-Datenbank zu landen, verrät Tussy nicht.

«Wearable Computing» erobert den Alltag

Beim US-Startup «Lambda Labs» hat man sich von Googles Cyberbrille zum «Lambda-Hut» inspirieren lassen: einer Android-basierten Baseball-Kappe, die alles aufnimmt, was ihr vor die Nase kommt. Ähnliche Alltagsartikel aus dem Bereich «Wearable Computing» haben mit Google Glass enormen Auftrieb erhalten. Bei Juniper Networks rechnet man 2014 mit einem weltweiten Verkauf von 15 Millionen smarten tragbaren Geräten, bis 2017 sollen es 70 Millionen werden. Und so restriktiv Google die Zulassung von Apps auch handhaben mag: Früher oder später wird auch Google Glass gehackt, warnen Securityexperten. Und spätestens dann kann keiner mehr kontrollieren, was Nutzer mit der Cyberbrille anstellen.

Google Glass als Korrekturbrille

Fraglich ist auch, ob Googles Idee so gut ist, die Datenbrille mit optischen Korrekturgläsern zu kombinieren. Einige der Testpersonen sind mit ihren Glass-Sehhilfen nämlich bereits in die Bredouille geraten: So endete der Kinobesuch eines Google-Glass-Trägers in Ohio damit, dass die Polizei ihn aus dem Saal führte und drei Stunden wegen möglicher illegaler Filmmitschnitte verhörte. In San Diego landete die Autofahrerin Cecilia Abadie wegen Google Glass sogar vor Gericht. Weil nicht geklärt werden konnten, ob die Brille zum fraglichen Zeitpunkt angeschaltet war, sprach das

Gericht Abadie nun frei. In anderen US-Staaten soll das Fahren mit Datenbrillen generell verboten werden – in Grossbritannien ist dies bereits seit August 2013 der Fall ist. Gleichzeitig sucht Google mit dem Projekt «Smart Contact Lenses» bereits einen Weg, Google Glass in Kontaktlinsen zu integrieren.

Zur Erinnerung: Google Glass ist eine gesten- und sprachgesteuerte Brille. Sie verbindet sich per Bluetooth mit dem Smartphone und kann so diverse Informationen im oberen rechten Sichtfeld des Brillenträgers einblenden: Navigationshinweise, E-Mails, Termine und Sonstiges. Zudem kann man damit Videokonferenzen und Telefonate erledigen, fotografieren oder filmen.

Nachzulesen unter:

http://www.heise.de/tr/artikel/OK-Glass-find-a-Killer-App-2076138.html
http://www.androidnext.de/news/nametag-google-glass/
http://www.dispatch.com/content/stories/local/2014/01/21/google-glass-at-easton-theater.html
http://www.latimes.com/local/la-me-google-glass-20140117,0,5347315.story
http://www.zeit.de/digital/mobil/2014-02/google-glass-gesichtserkennung-kommt
http://www.juniperresearch.com/viewpressrelease.php?pr=347
http://www.computerwoche.de/a/google-glass-bereitet-den-weg,1237959

IV. NSA-Update: Kritiker nehmen Anlauf

So langsam verliert man den Überblick darüber, was die «National Security Agency» und die Kollegen vom britischen «Government Communication Headquarters» so alles wissen. Den Enthüllungen der vergangenen Monate zufolge hören und greifen beide vermutlich alles ab, was mit Daten, Kommunikation und Internet zu tun hat:

- Sie überwachen den internationalen Zahlungsverkehr
- Können jeden beliebigen Rechner der Welt kapern
- Standort und Kommunikation von Handys überwachen
- Den gesamten Internetverkehr «live» und direkt am Untersee-Glasfaserkabel abgreifen
- Unternehmensserver anzapfen
- Botnetze übernehmen
- In Standardsoftware und IT-Hardware (Firewalls, Router, Festplatten etc.) Hintertüren einbauen

- Und, und, und.

Strafanzeigen gegen Regierungen in Grossbritannien und Deutschland

Während Otto Normalverbraucher der automatisierten Massenüberwachung mit weitgehender Ignoranz begegnet, formiert sich unter Bürgerrechtlern, Politikern und Netzaktivisten langsam aber deutlich Protest. So steht das Thema am Europäischen Gerichtshof für Menschenrechte in Strassburg gerade ganz oben auf der Tagesordnung: Dort hatten britische Bürgerrechtsorganisationen und der deutsche Chaos Computer Club (CCC) vor Kurzem Beschwerde eingereicht. Laut CCC sollen die Richter «feststellen, ob die jüngst bekanntgewordenen Internetüberwachungsprogramme des britischen Geheimdienstes Rechtsgrundsätze verletzen». Das Gericht soll Grossbritanniens Premier James Cameron bereits dringend dazu aufgefordert haben, zu der millionenfachen anlasslosen Überwachung europäischer Bürger Stellung zu nehmen. Die Beschwerdeführer erhoffen sich gesetzliche Neuregelungen, um die Massenspionage zu stoppen. Denn von Politikern und Geheimdiensten hiess es bisher stets, man halte sich an die Gesetze. Genau das wollen die Beschwerdeführer jetzt von neutraler Stelle prüfen lassen.

Um den öffentlichen Druck zu erhöhen, haben CCC und weitere Bürgerrechtsgruppen parallel dazu bei der Generalbundesanwaltschaft in Deutschland Strafanzeige gegen Bundesnachrichtendienst (BND) und Bundesregierung gestellt. Demnach soll wegen «Verletzung der höchstpersönlichen Lebensbereiche der Bürger» ermittelt werden. Um herauszufinden, «ob sich verantwortliche Personen der Spionage zugunsten der USA schuldig gemacht haben». Bei der Wahrheitsfindung soll laut Anzeige auch Edward Snowden als sachkundiger Zeuge vernommen werden.

Geheimdienste sabotieren das Internet

In den USA haben gerade 50 führende Kryptographie- und Sicherheitsforscher der USA unterdessen in einem offenen Brief die «anlasslose Sammlung, Speicherung und Verarbeitung von beispiellosen Mengen persönlicher Daten» der NSA kritisiert. Wer Hintertüren einbaue, Sicherheitsstandards sabotiere und die Verbindungen zwischen kommerziellen Datenzentren abhöre, öffne Kriminellen Tür und Tor. Die Experten fordern von der Regierung, das Entwickeln von Massenüberwachungsprogrammen und Untergraben von Sicherheitstechnologien zu beenden. Statt dessen sollten neue Technologien zum Schutz der Privatsphäre im Netz gefördert werden – solche, die Menschenrechte, vertraulichen Wirtschaftshandel und technische Innovation stärken.

«No water, no data center»

Auf unkonventionellere Art versuchen Bürgerrechtler und Politiker der staatlichen Datensammelei Einhalt zu gebieten: Indem sie dazu aufrufen, dem gigantischen NSA-Rechenzentrum im Bundestaat Utah das Wasser abzudrehen. Angeblich, heisst es auf der Webseite der selbsternannten Protestkoalition, benötige das Zentrum täglich gut 6,5 Millionen Liter Wasser zum Kühlen der NSA-Server. Für die Gegner die juristische «Achillesferse der NSA».

Verdacht auf Wirtschaftsspionage

Unterdessen bekräftigte Whistleblower Edward Snowden in seinem ersten Fernsehinterview mit dem NDR frühere Aussagen, wonach die NSA gezielt Wirtschaftsspionage betreibe: «Wenn es etwa bei Siemens Informationen gibt, die dem nationalen Interesse der Vereinigten Staaten nutzen, aber nichts mit der nationalen Sicherheit zu tun haben, dann nehmen sie sich diese Informationen trotzdem.»

Mitte Januar versprach Präsident Barrack Obama mehr Transparenz und Zügel für die NSA. So dürfen US-Internetfirmen seit Neuestem laut sagen, wie oft Behörden Zugriff auf die eigenen Daten verlangt haben. Nach der ersten Statistik-Runde ist man allerdings auch nicht viel schlauer: Die ungefähre Zahl staatlicher Zugriffe sollen betroffene US-Internetfirmen jetzt erstmals nennen, viel schlauer ist die Öffentlichkeit dadurch aber nicht geworden.

Mehr zum Thema:

http://www.ccc.de/de/updates/2014/gchq-egmr
http://www.nsa.gov/public_info/press_room/2014/civil_liberties_privacy_officer.shtml
http://online.wsj.com/news/article_email/SB10001424052702303519404579353173552039730-lMyQjAxMTA0MDMwMDEzNDAyWj
http://www.presseportal.de/pm/69086/2648795/-snowden-exklusiv-der-wortlaut-des-interviews-von-ndr-autor-hubert-seipel
http://www.tagesanzeiger.ch/ausland/amerika/Vizeadmiral-Michael-Rogers-soll-die-NSA-umkrempeln/story/23310173
http://offnow.org
http://www.nzz.ch/aktuell/digital/wie-die-nsa-iphones-attackierte-1.18213327

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Der Sicherheitsdienstleister Kaspersky hat einen Cross-Plattform Java-Bot entdeckt, der eine gefährliche Java-Sicherheitslücke ausnutzt. Der Java-Bot funktioniert sowohl auf Windows als auch auf Mac oder Linux:

https://www.securelist.com/en/blog/8174/A_cross_platform_java_bot

Die Netzwerksicherheitsexperten von «Arbornetworks» haben gerade ihren Sicherheitsbericht publiziert. Wichtigste Themen dieses Jahr: Bring Your Own Device (BYOD) und mobile Datennetzwerke, Angriffe auf Firmennetzwerke und IPv6.

http://www.arbornetworks.com/corporate/blog/5112-the-9th-annual-wisr-the-wisr-authors-weigh-in

Der Blog «Krebs-on-Security» berichtet über einen Firmware-Bug in IP-Kameras des chinesischen Kamera-Giganten «Foscam». Der ermöglicht es Unbefugten, via Internet live zuzuschauen oder heimlich Videoaufzeichnungen zu durchforsten:

http://krebsonsecurity.com/2014/01/bug-exposes-ip-cameras-baby-monitors/

Dieser SWITCHcert Security Report wurde von Katja Locker und Frank Herberg verfasst.

Information in eigener Sache: Ab sofort wird der aktuelle Report nach dem Monat seines Erscheinungsdatums benannt. Der Security Report für den Monat Januar heisst damit erstmals «Security Report Februar».