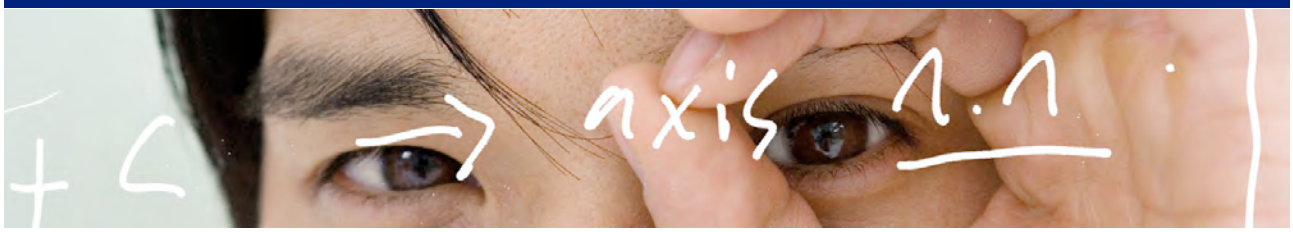
SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Dezember 2013



SWITCH

I. Start-ups versprechen Hilfe zur digitalen Selbstverteidigung – und halten nicht immer Wort

Zugegeben, von einem «Exodus» bei kommerziellen Anbietern wie Google, Facebook oder WhatsApp kann man nicht gerade sprechen. Dennoch beobachten Branchenkenner seit Bekanntwerden der NSA-Spionage deutlich steigendes Interesse an alternativen Wegen zum Chatten, Mailen und Surfen. Mehr denn je interessieren sich Firmen und Verbraucher für Verschlüsselung und private Kommunikation. Experten sehen darin einen der grössten Wachstumsmärkte der kommenden Jahre, bestätigt Wirtschaftsjournalist Steffan Heuer. «Man kann das mit dem Aufziehen von Antivirussoftware vergleichen, die heute als Standard gar nicht mehr hinterfragt wird.»

Kein Wunder also, dass Start-ups, die Internetnutzern mit ihren Produkten zur «digitalen Selbstverteidigung» verhelfen wollen, gerade wie Pilze aus dem Boden schiessen. Bestes Beispiel: der schwedische Instant-Messaging-Anbieter «Hemlis» («Geheimnis»), der Branchengrössen wie WhatsApp die Stirn bieten will. «Sämtliche

Kommunikation, die über Netzwerke geführt wird, wird von Behörden und privaten Unternehmen überwacht. Die Politik wird das nicht ändern. Deshalb haben wir uns entschlossen, einen Dienst zu entwickeln, der nicht ausspioniert werden kann», verspricht Mitbegründer Peter Sunde. Mit Erfolg, wie steigende Userzahlen beweisen. Bei «Hemlis» wird verschlüsselt kommuniziert, dabei nichts zentral gespeichert.

Über Zulauf freuen sich auch europäische Suchmaschinenanbieter wie «Startpage» und «Ixquick», deren Server ausserhalb der Reichweite von US-Behörden stehen. Allerdings gibt es auch schwarze Branchenschafe, die vom gesteigerten Sicherheitsbedürfnis zu Unrecht profitieren: Etwa die Suchmaschine «DuckDuckGo». Deren Firmenchef Gabriel Weinberg wirbt damit, man speichere keinerlei Nutzerdaten, verschlüssle die Nutzerdaten sauber und verzichte auf Cookies und Trackingprogramme. Dumm nur, dass DuckDuckGo ein US-Unternehmen ist, seinen Dienst zudem auf Amazon-Servern betreibt und somit allemal der NSA unterliegt. Dass sich die Userzahlen von DuckDuckGo in den letzten Monaten dennoch auf vier Millionen pro Tag verdoppelt haben, bezeichnet «Die Zeit»-Journalist Patrick Beuth als Ausdruck einer «Verzweiflungstat» der Internetnutzer, die auf der Suche sind nach einem überwachungsfreien Aufbewahrungsort für ihre Daten.

Ob es den überhaupt gibt, bezweifelt mittlerweile allerdings fast jeder: Einer Umfrage des deutschen Branchenverbandes Bitkom zufolge halten 80 Prozent der Internetnutzer ihre Daten im Netz generell für unsicher.

Mehr dazu im Internet unter:

http://futurezone.at/digital-life/privatsphaere-ist-wieder-gefragt/41.877.492
http://www.zeit.de/digital/datenschutz/2014-01/duckduckgo-startpage-ixquick-nsa
http://techcrunch.com/2014/01/12/duckduckgos-popularity-exploded-in-2013-following-the-nsaprism-leaks/
http://www.bitkom.org/de/presse/78284_78077.aspx
http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores
http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/
http://www.heise.de/newsticker/meldung/Target-Kartenraubzug-Weihnachten-fuer-Kriminelle-2071721.html

II. Cloud-Branche sortiert sich neu – die Kunden auch

Bereits im August – als bekannt wurde, dass die NSA vollkommen legal Daten von den Servern führender Cloudanbieter wie Google, Amazon und Microsoft saugt – prognostizierten Fachleute der Branche düstere Aussichten: etwa 35 Milliarden Dollar Schaden käme auf die Branche in den kommenden drei Jahren zu, schätzte etwa die «Information Technology & Innovation Foundation». Andere Schätzungen kommen gar auf bis zu 180 Milliarden Miese.

Die Konkurrenz in Europa reibt sich seither die Hände und hat ihrerseits eine Security-Werbeoffensive gestartet. In Deutschland hat der deutsche Softwarehersteller SAP soeben angekündigt, den Ausbau seiner weltweiten Rechenzentren voranzutreiben. Die Kundendaten unterliegen dort jeweils deutschem Recht.
Hierzulande will etwa die Swisscom einen höheren Gang einlegen: 2014 soll ein neues zentrales Rechenzentrum für sämtliche Cloud-Angebote in Betrieb genommen werden, flankiert mit neuen Diensten. Laut Sprecher Olaf Schulz sei die Schweiz gerade in diesen Tagen ein attraktiver Speicher- und Datenverarbeitungsstandort für Europas Kunden. Deren Daten seien hierzulande nämlich doppelt geschützt: durch das Schweizer Datenschutz- sowie das Fernmeldegesetz.

Doppelt verschlüsselt hält besser

Cloud-Anbieter, die dauerhaft das Kundenvertrauen gewinnen wollen, können nicht einfach mit der NSA-freien Zone werben, warnte Experte Bruno Crispo von der Universität Trento schon im Oktober. Einerseits, weil auch der britische Geheimdienst massiv Daten abgreift. Andererseits, weil es wohl schwierig sein wird, eine Cloud anzubieten, die auch nur auf europäischer Soft- und Hardware basiert. Er rät zu dem, was auch US-Anbieter Google, Amazon und Co. jetzt gelobt haben: die eigenen Sicherheitsstandards zu verbessern und Nutzern Ende-zu-Ende-Verschlüsselung anzubieten. Dabei kann der Nutzer seine Daten schon lokal verschlüsseln, bevor er sie zum jeweiligen Cloud-Dienst sendet. Der Dienstanbieter kennt dabei den Schlüssel nicht.

Cloud-Beratung vom Juristen

Firmen, die Flexibilität und Effizienz globaler Clouds nutzen wollen, empfehlen Rechtsexperten jetzt explizit, sich auf Europas Anbieter zu konzentrieren. Allerdings

sollte man auch hier aufs Kleingedruckte schauen. Wie Anwalt Dr. Thomas Jansen erläutert, sei nicht nur der Sitz des Cloud-Anbieters wichtig, sondern auch dessen Serverstandorte: «Rechtlich gibt es enorme Unterschiede, je nachdem, ob die Daten oder Sicherheitskopien der Daten vom Anbieter auf IT-Systemen in Deutschland, der Schweiz, Malta, Kanada, den USA, in Indien oder China gespeichert werden. Oft werden Daten auch an mehreren Standorten gleichzeitig gespeichert. Hier sind eindeutige und verbindliche vertragliche Zusicherungen wichtig und eine rechtliche Überprüfung unentbehrlich.» Bei Clouds mit Datenspeicherung in Niedriglohnländern käme das Risiko hinzu, «dass Dritte durch Bestechung von Mitarbeitern teils sehr schnell und einfach an Daten kommen können.» Seine Empfehlung: Je weniger klare Gesetzesvorgaben für Cloud Computing vorlägen, desto wichtiger sei ein gründlicher Vertrag.

Mehr dazu im Internet unter:

http://www2.itif.org/2013-cloud-computing-costs.pdf
http://www.tagesanzeiger.ch/wissen/technik/Jetzt-bauen-die-Europaeer-eigene-Clouds/story/20482995
http://www.itmittelstand.de/home/a/rechtliche-grundlagen-fuer-die-cloud.html

III. Das Weihnachtsgeschäft floriert – Karten- & Identitätsdiebstahl auch

Mitten im Weihnachtstrubel wurde die US-Einkaufskette «Target» – mit gut 1900 Filialen eine der grössten des Landes – Opfer eines massiven Cybereinbruchs: Zwei Wochen lang konnten Angreifer dabei ab Ende November die Kredit- und EC-Karten-Daten von gut 70 Millionen Kunden aus der Target-Datenbank abzapfen.

Zutage gebracht hatte der IT-Spezialist und Blogger Brian Krebs den Vorfall: Im Auftrag einer Bank hatte er sich auf dem Karten-Schwarzmarkt umgesehen und war dabei auf die entwendeten Target-Datensätze gestossen. Die Karten-Kopien werden dort paketweise für bis zu 100 US-Dollar das Stück feilgeboten. Mit enthalten ist jeweils auch die Postleitzahl des Karteninhabers – für Betrüger sehr praktisch, «weil die Sicherheitsmechanismen der Banken bei in der Umgebung des Karteninhabers getätigten Käufe nicht so schnell anschlagen», wie das IT-Newsportal heise.de

schreibt. Laut Nachrichtenagentur Reuters sollen auch die verschlüsselten PINs der Karten entwendet worden sein. Damit, warnen Sicherheitsexperten, verfügen die Angreifer über alles Nötige, um die Karten zu duplizieren und Bargeld abzuheben. Mindestens vier weitere Einzelhändler sollen ebenfalls betroffen sein, so Reuters.
Gerade die verkaufsstarken Zeiten sind ideal für Angriffe, sagt Kryptographieexperte Paul Kocher. Betrugswarnsysteme können dann angesichts des Kundenansturms nicht mehr unterscheiden, welche Transaktion legal und welche falsch seien.

Rekord-Onlineverkäufe dank Tablets und Smartphones

Angesichts wachsender Umsätze muss sich der Einzelhandel aber trotzdem keine grossen Sorgen machen. Adobes «Digital Index» zufolge erledigten 2013 in Amerika doppelt so viele Kunden ihre Weihnachtseinkäufe per Mobilgerät als im Jahr zuvor: An den beiden verkaufskräftigsten Tagen Thanksgiving und Black Friday ging ein Viertel der Gesamtumsätze auf das Konto mobiler Einkäufer mit Tablet (15,6 Prozent) oder Smartphone (8,6 Prozent). Die Zahlen basieren auf der Analyse von rund 400 Millionen Besuchen auf den Webseiten der gut 2000 US-Einzelhändler, die Adobes Analysetool «Marketing Cloud» einsetzen. Einzelhändler waren auf die mobile Shopping-Offensive bestens vorbereitet, hatten mit Gratis-Wlan in den Filialen, überarbeiteten Online-Shops, erweiterten App-Angeboten und Bildschirm-optimierten Webseiten (Stichwort: Responsive Design) den mobilen Zugriff gefördert.

Mehr dazu im Internet unter:

http://www.reuters.com/article/2013/12/25/us-target-databreach-idUSBRE9BNOL220131225
http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores
http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/
http://www.heise.de/newsticker/meldung/Target-Kartenraubzug-Weihnachten-fuer-Kriminelle-2071721.html
http://www.enhancedonlinenews.com/news/eon/20131129005409/en/Adobe/Thanksgiving/Black-Friday
http://t3n.de/news/drops-noch-gelutscht-uns-2014-520509/

IV. Neues vom Mobile-Payment-Markt: Paypal setzt auf Bezahlen per Zuruf

Auf der Suche nach dem Durchbruch in Sachen «mobiles Bezahlen» herrscht zurzeit ein harter Konkurrenzkampf unter Zahlungsanbietern, Einzelhandel, Kreditkarten- und Mobilfunkfirmen. Als echter Problemlöser versucht sich «Paypal» in diesen Tagen zu positionieren: «Nie wieder Schlange stehen» hat Firmenchef David Marcus jüngst auf der Internetkonferenz «Le Web» versprochen. Und zwar allen, die sich die «Beacon»-App aufs Handy laden. Der Einzelhandel wiederum profitiere mit gesteigerter Kundenbindung. Die «Beacon»- oder «Sender-Empfänger»-Technik funktioniert so: Betritt ein Kunde mit seinem Handy ein Geschäft, empfängt das Gerät Signale von Funkmodulen, die der Händler dort eingerichtet hat. Daraufhin übermittelt das Handy per Bluetooth Foto, Einkaufshistorie oder aktuelle Position des potenziellen Kunden an den Händler, der von ihm nun individuell beraten werden kann. Für die Bezahlung genügt schliesslich eine mündliche Bestätigung des Kunden – im Promotion-Video beispielsweise beim Verlassen des Geschäfts.

Kunden-Anonymität war gestern

Paypal-Firmenchef David Marcus sieht in der Beacon-Technik einen wichtigen Baustein für den Wandel des Einzelhandels. Der Nutzer könne dabei jene Geschäfte definieren, in denen er automatisch bezahlen lassen will und solche, die eine spezielle Autorisierung erfordern. Damit sei auch dem Datenschutz Genüge getan. Ganz so rosig sehen Securityexperten das nicht: Komfort ginge hier mal wieder zu Lasten des Datenschutzes, so der Tenor. Ganz zu schweigen von einer ganzen Reihe an Missbrauchs- und Sicherheitsfragen, die es zu klären gebe. Angefangen bei der, wie die Kundendaten gespeichert werden oder was bei einem Handydiebstahl passieren soll.

Laut Marcus wird Beacon bereits europaweit getestet. Das Bezahlen per Gesichtserkennung probiert Paypal ebenfalls bereits aus.

iBeacon heisst übrigens ein ähnliches Indoor-Navigationssystem, das Apple in sein jüngstes Mobil-Betriebssystem iOS7 integriert hat und schon seit Dezember in 250 US-Läden testet: Innerhalb eines Geschäfts werden Kunden per Bluetooth auf Sonderangebote hingewiesen oder zu Produkten navigiert, die sie interessieren.

Eine App für jeden Supermarkt

An einen Durchbruch der vielen Angebote, die den Verbraucher zurzeit umschwirren, glauben Branchenkenner zumindest in diesem Jahr noch nicht: Mangelnde Standards, wenig Akzeptanz und zu viele Insellösungen machen es Kunden schwer, einen Mehrwert zu erkennen. Allein in Deutschland gibt es gut 30 verschiedene Zahlungsanbieter, die alle ihr eigenes (App-)Süppchen kochen. Und damit, dass sich die Käufer zig verschiedene Apps auf ihr Handy laden, darf man wohl nicht rechnen. Hierzulande bastelt etwa die Swisscom an der «Tapit»-App zum bargeldlosen Bezahlen in Coop-Filialen, die 2014 lanciert werden soll. Während man beim Konkurrenten Migros lieber auf bargeldloses Bezahlen per Nearfield Communication setzt.

Nachzulesen unter:

http://youtu.be/g8h_i8qv1FY
http://techcrunch.com/2014/01/13/paypal-debuts-a-simpler-native-checkout-experience-for-merchants-and-expand-beacon-internationally/
http://www.spiegel.de/netzwelt/apps/beacon-paypal-kuendigt-gegenstueck-zu-apples-indoor-navigation-an-a-938220.html

V. 30. Treffen des Chaos Computer Clubs ganz im Snowden-Fieber

Aufbruchstimmung und Kampfesgeist herrscht zurzeit unter den Internetaktivisten und Hackern weltweit. Das war beim 30. Kongress des Chaos Computer Clubs (CCC) in Hamburg nicht zu übersehen. Über 8000 Besucher, mehr als je zuvor, waren angereist, um vier Tage lang zu diskutieren, wie es nach den massiven Spionageenthüllungen überhaupt weitergehen soll mit der Freiheit im Internet. Anschliessend war klar: Ganz so einfach wird es nicht.

Gleich zu Beginn gab es Standing Ovations für Hauptredner Glenn Greenwald, als er die Masse per Videoschaltung zur digitalen Befreiung aufruft. Greenwald war bis vor Kurzem Reporter des britischen «Guardian» und gehört als Vertrauter von Edward Snowden zu denjenigen, die das Ausmass der Enthüllungen öffentlich fassbar gemacht haben. «Die NSA will die Privatsphäre auf globaler Ebene eliminieren.» Deshalb

müsse sich jeder für den Schutz der Privatsphäre stark machen. Bezeichnenderweise, gestand Greenwald, habe er die «Snowden-Story» um ein Haar verpasst: Weil ihm die PGP-Technik, mit der Edward Snowden seine E-Mails verschlüsselte, zu kompliziert war.

Während Greenwald die Hacker noch beschwor, sich nicht in den Dienst von Geheimdiensten zu stellen, tat Wikileaks-Gründer Julian Assange interessanterweise genau das Gegenteil: Ebenfalls per Video zugeschaltet, aus der ecuadorianischen Botschaft in London, appellierte Assange speziell an Systemadministratoren, ihre Macht und Netzwerkkenntnisse zu nutzen. «Tretet in die CIA ein!» Die so genannten «Sysadmins» sollten Geheimdienste und Firmen unterwandern, Informationen sammeln und diese publik machen. «Wir sind die letzte freie Generation.»

Blieb zum Schluss der Konferenz die Frage, die nicht nur Greenwald, sondern Internetaktivisten weltweit umtreibt: «ob das Internet wirklich ein Instrument der Befreiung und der Demokratie ist, oder ob es das schlimmste Unterdrückungsinstrument aller Zeiten ist».

Mehr zum Thema:

http://youtu.be/qqk4ltPjU5g
http://www.golem.de/news/glenn-greenwald-sie-muessen-angst-vor-uns-bekommen-1312-103605.html
http://www.faz.net/aktuell/feuilleton/debatten/abschied-von-der-utopie-die-digitale-kraenkung-des-menschen-12747258.html
http://www.faz.net/aktuell/feuilleton/chaos-communication-congress-ein-tor-zur-anonymitaet-12729573.html

VI. Facebook entgeht nichts - auch nicht das, was keiner wissen soll

Um herauszufinden, ob und wie oft Facebook-Nutzer einen Kommentar oder ein Status-Update tippen, im letzten Moment aber doch wieder löschen, hat das grösste soziale Netzwerk der Welt eine Studie zur «Selbstzensur auf Facebook» lanciert. Dazu haben sich der Datenanalyst Adam Kramer und Doktorand Sauvik Das die Metadaten der unveröffentlichten Einträge von rund vier Millionen englischsprachigen Nutzern genauer angesehen. Resultat: 71 Prozent der Facebook-Nutzer verfassten innerhalb von 17 Tagen mindestens einen Eintrag, den sie dann jedoch in letzter Sekunde wieder

löschen. Bei 51 Prozent war das eine bereits getippte Statusmeldung auf der eigenen Profilseite, bei 44 Prozent ein Kommentar auf der Seite eines Freundes. Aber warum interessiert das Facebook überhaupt? Weil das Netzwerk durch nicht geteilte Inhalte an Wert verliere, sagen die Analysten. Da das soziale Netzwerk von der Offenbarung seiner Mitglieder lebt, will es deren Selbstzensur reduzieren.

Mal wieder steht von der Speicheroffensive kein Wort in Facebooks Datenschutzbestimmungen. Dort heisst es lediglich, man sammle Daten, «wenn wir uns Dinge ansehen oder in anderer Weise interagieren.» Wer sich darüber aufregt, sollte sein Mitgliedskonto direkt auf Eis legen: Wie Das und Kramer zum Schluss ihrer Studie durchblicken lassen, werden sie demnächst noch einen Schritt weiter gehen: Dann sollen die Inhalte der wieder gelöschten Posts untersucht werden. Damit will Mark Zuckerberg herausfinden, was genau und warum wieder gelöscht wird.

Weltweit hat Facebook geschätzte 1,19 Milliarden Mitglieder, hierzulande sind es 3,3 Millionen – acht Prozent mehr als 2012. Bei den unter 20-Jährigen schwindet das Interesse allerdings nach wie vor.

Näheres im Internet:

http://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350
http://www.spiegel.de/netzwelt/web/was-ein-forscher-mit-facebooks-datenschatz-anstellt-a-934893.html
http://www.pctipp.ch/news/web-dienste/artikel/schweizer-facebook-nutzer-werden-aelter-70315/

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Vom 27. bis 30. Dezember 2013 fand zum dreissigsten Mal der Chaos Communication Congress (30C3) in Hamburg statt. 140 Videos wurden zu den Talks veröffentlicht. Ein Anspieltipp ist der Talk von Linus Neumann zum Thema Internet «made in Germany»:

http://media.ccc.de/browse/congress/2013/index.html
http://media.ccc.de/browse/congress/2013/30C3_-_5210_-_de_-_saal_g_-_201312282030_-_bullshit_made_in_germany_-_linus_neumann.html

Zur Security-Konferenz Hack-in-the-Box gibt es neben den Slides auch ein Magazin, in denen Sie die vielen interessanten Vorträge nochmal nachlesen können:

http://magazine.hackinthebox.org/hitb-magazine.html

Glenn Wilkinson hielt anlässlich der SECURE 2013 in Polen einen interessanten Vortrag zum Thema Mobile Device Tracking – «The Machines that Betrayed their Masters»:

http://www.youtube.com/watch?v=O3iEaKPRb9A

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