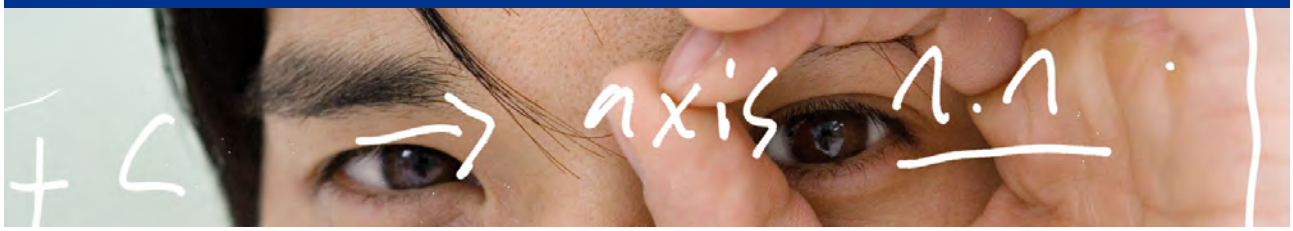
SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

März 2014



SWITCH

I. Zwischen Panik und Ignoranz: Facebook kauft WhatsApp

Da haben sich ja zwei gefunden: Stolze 19 Milliarden US-Dollar legte Facebook-Gründer Mark Zuckerberg Ende Februar auf den Tisch, um den Kurznachrichtendienst WhatsApp samt des dazugehörigen Entwicklerteams aufzukaufen. Ein hoher Preis, sagen Branchenkenner, mit dem sich Zuckerberg seinen grössten Konkurrenten einverleibt.

Spannend dürfte nun die Frage werden, was Facebook mit WhatsApp vorhat und inwiefern sich WhatsApp verändern wird. «Nichts», glaubt etwa der Blogger und IT-Journalist Michael Seeman: «Es geht bei dem Deal gar nicht um irgendwas, das WhatsApp hat, sondern [...] um die Zukunft von Facebook. Seeman würde es nicht mal wundern, wenn sie den Laden einfach dichtmachen.»

Bislang interessierten sich die WhatsApp-Gründer weder für Daten ihrer Nutzer noch für Werbeeinnahmen. Sie finanzierten den Dienst über die Abogebühr von gut einem Dollar pro Jahr. Das soll so bleiben, verspricht Zuckerberg – doch lustigerweise glauben das nicht mal die eigenen Kunden: Ausgerechnet auf Facebook formiert sich ein Grossteil des Widerstand verärgerter WhatsApp-Nutzer. «Von 100 WhatsApp-

© SWITCH 2014

Kontakten in meiner Liste posten 90 fleissig ihr Leben auf FB», spottet ein User im Internetforum von «Futurezone»; «verkehrte Welt, wenn man da eine Alternative zu WhatsApp sucht». Und: «Ich suche einen Messenger, welcher die meisten meiner Kontakte abdeckt, und das ist nun mal WhatsApp. Die Daten sind ja eh schon vorhanden, sprich, FB hat sie schon. Was soll's also.»

Datenschutz versus Bequemlichkeit

Das Datenschützern weltweit der Millionendeal alles andere als gleichgültig ist, wundert hingegen nicht. Seit Jahren schon stehen Facebook und WhatsApp in der Kritik wegen mangelnder Datenschutzstandards. Bei beiden Diensten, warnt etwa das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, stehen den Betreibern «Kommunikations-Metadaten wie auch die -Inhalte lesbar zur Verfügung.» Werden die Daten zusammengeführt, könnten diese leicht «zur Profilbildung ausgewertet und für Werbezwecke kommerziell ausgebeutet werden».

Auf die Frage, warum sich wenig Schweizer für die Übernahme interessieren, erklärt sich der Zürcher Datenschutzbeauftragte Bruno Baeriswyl im Interview mit «20 Minuten» so: «Einerseits wissen die wenigsten, welche Profile von ihnen erstellt werden und was damit geschieht. Andererseits spüren sie im Alltag noch kaum die Nachteile des exzessiven Datensammelns.»
Dabei, räumt Baeriswyl ein, gebe es «tatsächlich Anbieter, die ähnliche Dienste wie WhatsApp und mehr Sicherheit bieten, etwa bei der Verschlüsselung von Daten». Dort müssten Nutzer jedoch mit anderen Einschränkungen leben müssen. «Langfristig», so der Datenschützer, würden Anbieter, die mehr Sicherheit bieten, auf dem Markt einen gewissen Vorteil haben. Letztlich sei es aber «jedem Einzelnen überlassen, ob er sich für mehr Sicherheit oder mehr Bequemlichkeit entscheidet». Oder um es mit den Worten von Twitter-Nutzer und Open-Source-Aktivist Dennis Ploeger zu sagen. «Ob sich eine WhatsApp-Alternative durchsetzt, bestimmt nicht die beste Verschlüsselung, sondern ob Chantal aus der Neunten es hat.»

Schwedens Polizei nutzt WhatsApp – und patzt

Mark Zuckerberg ist jetzt jedenfalls im Besitz eines Tools, das inzwischen selbst Polizeibehörden einsetzen: Berichten des Nachrichtenmagazins «Der Spiegel» zufolge nutzen schwedische Ermittler «WhatsApp», um Informationen zu laufenden Ermittlungen auszutauschen. Weil sich ein Beamter bei der Eingabe der

© SWITCH 2014

Telefonnummern vertippt hatte, wurde versehentlich IT-Berater Jan Svärdhagen in zur Ermittlungs-Chat-Gruppe eingeladen. Wie Svärdhagen dem IT-Magazin «ComputerSchweden» schilderte, erhielt er Zugriff auf Informationen zu laufenden Ermittlungen, Daten von Verdächtigen, Fotos und Ausschnitte von Polizeiakten. Der verantwortliche Polizist entschuldigte sich für das Datenmalheur mit dem Hinweis, zum schnellen Austausch mit den Kollegen auf WhatsApp angewiesen zu sein. Die dafür vorgesehenen BlackBerrys habe man den Beamten nicht zur Verfügung gestellt.

Mehr dazu im Internet unter:

http://www.br.de/presse/inhalt/pressemitteilungen/radiowelt-michael-hange-100.html
http://www.srf.ch/wissen/digital/facebook-und-whatsapp-damit-die-sonne-im-reich-niemals-untergeht
http://futurezone.at/produkte/whatsapp-alternative-threema-verdreifacht-user-anzahl/52.561.981
http://www.shz.de/nachrichten/newsticker-nord/datenschuetzer-weichert-warnt-vor-kombination-facebook-whatsapp-id5791121.html
http://mspr0.de/?p=3974
http://www.handelsblatt.com/unternehmen/it-medien/instant-messenger-whatsapp-alternative-threema-waechst-rasant/9519942.html
http://de.statista.com/infografik/1931/anzahl-der-aktiven-nutzer-von-whatsapp/
https://threema.ch
http://www.20min.ch/schweiz/news/story/13345327
http://computersweden.idg.se/2.2683/1.547026/polisens-chatt-miss-hemlig-spaninfo-pa-drift-i-%20WhatsApp

II. Google, Apple und Co. wollen Auto der Zukunft mitgestalten

Der Wettkampf um einen Platz im internetfähigen Auto der Zukunft ist eröffnet: Weil moderne Fahrzeuge mit immer mächtigeren Bordcomputern und schnelleren Internetverbindungen ausgestattet sind, wandelt sich auch die Bedienung der Fahrzeuge rasant. Entsprechend Gas geben jetzt die grossen IT-Konzerne, um sich einen Platz in den Automobilen neuerer Generationen zu sichern. Beim jüngsten Genfer Autosalon kann man klar sehen, wohin die Richtung geht: Neue Modelle setzen auf grosse Touchpad-Displays, Internet im Auto und Smartphone-Anbindung. Die jüngsten Fahrzeuggenerationen sind zudem durch die Bank mit Kameras ausstaffiert, die 360-Grad-Aufnahmen à la Google Street View auf einen Monitor zaubern.

«Intelligenter, sicherer, spassiger»

So arbeitet Apple seit einiger Zeit mit Ferrari, Mercedes und Volvo am Kommunikations-System «CarPlay»: Eigenen Aussagen zufolge der «intelligentere,

© SWITCH 2014

sicherere und mehr Spass bringende Weg, das iPhone im Auto zu nutzen» beschrieben. Dabei soll Apples mobiles «iOS»-Betriebssystem sozusagen in die Armaturen von Fahrzeugherstellern bzw. tief in das Autosystem integriert werden. Eine besondere Rolle spielen dabei der Sprachassistent «Siri» und Apples Touchscreen. Google hingegen macht mit der «Open Automotive Alliance» seit Anfang des Jahres gemeinsame Sache mit den Autoherstellern Audi, General Motors, Honda und Hyundai. Auch hier suchen alle Beteiligten nach Wegen, das Smartphone-Betriebssystem «Android» sinnvoll ins Auto zu überführen. Audi-Entwicklungschef Prof. Ulrich Hackenberg stellt sich das so vor: «Das Fahrzeug wird intensiv vernetzt sein, wird mit allen Informationen, die über das Verkehrsgeschehen erhältlich sind, gefüttert werden, wird mit anderen Fahrzeugen und mit der Infrastruktur kommunizieren. Und die Fahrzeuge werden auch in der Lage sein, Entscheidungen zu fällen – sie dem Lenker anbieten oder sie selbst ausführen.» Vernetzte Fahrzeuge sollen auch miteinander agieren, um im Gefahrenfall Alarm zu schlagen. Zum Beispiel «Achtung, nicht-vernetztes Fahrzeug unterwegs», prognostiziert Hackenberg.

Unterdessen basteln BMW und der Softwarekonzern SAP an einer Infrastruktur für zahlreiche mobile Dienste in Fahrzeugen, und zwar auf Basis der «SAP HANA Cloud Platform». Informationen aus Diensten, die von externen Partnern angeboten werden, sollen dabei orts- und routenbezogen aggregiert und Autofahrern direkt im Fahrzeug angezeigt werden (Stichwort: «Location Based Services»). Zwei Prototypen wurden dafür schon realisiert: Zum einen die selbstständige Suche nach geeigneten Parkplätzen durch das Fahrzeug; zum anderen das «Couponing», bei dem der Fahrer je nach Vorlieben, aktueller Position und gewählter Reiseroute Werbeangebote auf seinem Smartphone abrufen kann.

Noch auf der Suche nach interessierten Herstellern sind die Macher der Smartphone-App «Smart Trailer Parking». Ihre Einparkhilfe für Fahrzeug mit Anhängern verknüpft das Handy online mit Lenkung und Antrieb des Autos. Bei schwierigen Parkmanövern steigt der Fahrer dann theoretisch nur noch aus «und fährt mit dem Finger».

Welches Potenzial in der Vernetzung der Fahrzeuge miteinander steckt, zeigte Volvo gerade anhand eines Pilotprojekts beim Mobile World Congress: Autobesitzer können ihr Fahrzeug als Zustellort für Online-Bestellungen nutzen. Schätzungen zufolge

© SWITCH 2014

kosten unzustellbare Sendungen die Industrie jedes Jahr gut eine Milliarde Euro. «Es geht darum, Lösungen zu finden, die intuitiv und einfach genutzt werden können und unseren Kunden im Alltag Vorteile bringen», so Klas Bendrik, Group Chief Information Officer der Volvo Car Group.

Die Kehrseite der Bequemlichkeit hinterm Lenkrad

Bei allem Nutzwert solcher Dienste dürfe man nicht die Augen «vor den stillen Kalkülen» der Unternehmen verschliessen», warnt Journalist Daniel Hüfner im Technologie-Newsportal «t3». Noch sei der PKW einer der wenigen Zufluchtsorte jenseits des omnipräsenten Internets. «Denn hier googeln wir nichts, wir bestellen auf der Autobahn auch nichts bei Amazon und checken nicht bei Foursquare ein.» Dabei sind täglich Milliarden von Menschen im Auto unterwegs. «Ein riesiges Potenzial, das auch den Akteuren aus der Tech-, Werbe- und Überwachungsindustrie bekannt ist – und die werden auf den heißen Datenbraten kaum verzichten wollen.»

Mit der Vernetzung von Verkehrs- und Motordaten, warnen Datenschützer, macht man Autos genauso anfällig für Hackerangriffe wie Handys. Ganz abgesehen von den offenen rechtlichen Fragen, die entstehen, wenn Fahrzeuge intime Daten sammeln. «Selbst der neue VW Passat ermittelt, wann der Fahrer eine Kaffeepause braucht, und blendet im Cockpit eine Kaffeetasse mit einem Fragezeichen ein. Wenn einer dann nicht anhält, weiterfährt und unschuldig in einen Unfall verwickelt wird, stehen seine Chancen schlechter, wenn die Fahrzeugdaten ausgelesen werden, seine Unschuld zu beweisen. Bewegungsprofile, aggressives Fahrverhalten – vieles wird lautlos vom Auto aufgezeichnet und kann gegen den Fahrer verwendet werden», schreibt Niklas Maak in der Frankfurter Allgemeinen Zeitung.

Dann doch lieber einen alten Gebrauchtwagen...

Gegenüber dem Schweizer Radio und Fernsehen gibt auch Roger Löhrer, Leiter Mobilitätsberatung vom TCS, zu bedenken: «Grundsätzlich können alle Daten gespeichert werden. Zudem sind aus den Daten, die heutzutage gespeichert werden müssen, Rückschlüsse auf Fahrbedingungen und Fahrverhalten möglich.» So erlaubten die Airbag-Steuerungsgeräten bereits Rückschlüsse auf die Umstände des Unfalls. Ausserdem werden die Öffnungs- und Schliessvorgänge von Türen und Fenstern nach Uhrzeit und Datum gespeichert. Die Daten werden zurzeit nur lokal im Autosystem gespeichert, so dass sie bei Bedarf vom Vertragshändler abgerufen werden. Sollte sich

© SWITCH 2014

das ändern – würden die Daten etwa per Internet live an Versicherungen oder Hersteller weitergegeben – bleibt dem Autofahrer nur, auf ältere Gebrauchtwagen auszuweichen. Für den Schweizer Datenschützer Hanspeter Thür ist klar: «Es muss transparent sein, was für Daten gesammelt werden und der Eigentümer des Autos muss wissen, was mit den Daten passiert.» Angesichts aktueller EU-Pläne dürfte das nicht allzu leicht werden: Ab 2015 muss jeder Neuwagen mit dem automatischen Notrufsystem «eCall» ausgestattet sein. Das System enthält eine SIM-Karte, die etwa im Notfall selbstständig die Ambulanz kontaktiert. Dann, sagt TCS-Experte Löhrer, habe der Fahrer «grundsätzlich keine Kontrolle, wo die Daten wann rausgehen.»

Weiterführende Infos:

http://futurezone.at/digital-life/audi-das-auto-der-zukunft-entscheidet-selbst/51.788.826
http://www.newsxs.com/de/go/4748896/2845/
http://t3n.de/news/smartes-autofahren-startups-526202/
http://www.multivu.com/mnr/65010-volvo-pilots-roam-delivery-service
http://www.faz.net/aktuell/feuilleton/vernetztes-fahren-das-geschaeft-mit-den-intimen-daten-aus-dem-auto-12773929.html#null
http://www.srf.ch/konsum/themen/umwelt-und-verkehr/der-glaeserne-fahrer-datensammelwahn-im-auto

III. Harter Kampf um Kundendaten: Weg mit den Blockern, her mit der Reklame

Ein gelber Balken im Stile einer Browser-Warnung auf Gmx und Web.de sorgte diesen Monat für schwere Irritationen bei Nutzern und Verbraucherschützern. «Wenn man da draufklickt, kommt man bei browsersicherheit.info raus, das – ähnlich wie der gelbe Balken eben auch – nach dem Rezeptbuch der Malware-Mafia so designed wurde, dass es optisch wie die Chrome-Einstellungen aussieht. Dort wird dem Leser dann suggeriert, er habe sich ein Malware-Add-on eingefangen und müsse das dringend wegmachen. So was kennt man sonst nur von Botnet-Betreibern und Schlangenöl-Resellern. Ihr wisst schon, diese Scareware-Popup-Leute.» Mit diesen blumigen Worten warnte der Blog «fefe.de» Gmx- und Web.de-Nutzer als Erstes vor dem, was sich als aggressive Kampagne zur Erhöhung der eigenen Werbeeinnahmen entpuppte.

Um Kunden zur Entfernung ihrer Werbeblocker im Browser zu bewegen, wurde ihnen beim Besuch vom Gmx und Web.de suggeriert, besagte Blocker gefährdeten ihre

© SWITCH 2014

Computersicherheit. Genaue Anweisungen zum Entfernen der Add-Ons gab es dann auf der Seite «browsersicherheit.info», die dem Mutterkonzern «United Internet» gehört. Unter den dort aufgeführten vermeintlich gefährlichen Browser-Erweiterungen waren jedoch gut die Hälfte harmlose «Adblocker»: Programme für Firefox, Chrome, Safari und Co., die den Nutzer beim Surfen vor Werbeeinblendungen, Tracking-Programmen oder per Werbediensten verbreiteter Malware bewahren.

Internetfirmen sind oft finanziell auf die Einnahmen von Online-Werbung angewiesen. Das Werbeblocker wie «Ghostery» und Marktführer «Adblock Plus» (50 Millionen Nutzer weltweit) für Netzbetreiber ein ernstes Problem darstellen, ist kein Geheimnis. Anfang Februar hiess es erstmals, United Internet wolle technisch und juristisch gegen die Adblocker vorgehen. Dass sie dabei so aggressiv handeln, überraschte jedoch selbst Branchenkenner. Der Konzern rechtfertigte die Guerilla-Aktion damit, aus «Sorge» agiert zu haben: «Wir verstehen die Warnmeldungen als Beitrag für mehr Sicherheit im Netz, denn insbesondere die Software auf den Endgeräten der Nutzer ist häufig ein Einfallstor für Angriffe. Nicht alle Nutzer sind sich bewusst, was sie für Add-Ons installiert haben und welche Risiken sich durch den Eingriff in die Webseite ergeben können», so Jörg Fries-Lammers, Pressesprecher von «1&1 Internet AG», die ebenfalls zu United Internet gehört.

Ganz selbstlos handeln aber auch die Anbieter der Werbe-Blockierer nicht. Marktführer Adblock Plus zum Beispiel soll Gerüchten zufolge gut 30 Millionen US-Dollar von Amazon, Google, Ebay und Yahoo kassiert haben, damit deren Werbebanner nicht gefiltert werden. Das behauptet Netzblogger Sascha Pallenberger, der sich auf das Thema Adblocker spezialisiert hat. Pallenberger spricht bei Adblock Plus von einem «mafiösen Werbenetzwerk», hinter dem angeblich finanzstarke Werbekonzerne stecken. Pallenberger hat in der Vergangenheit schon mehrfach undurchsichtige Verbindungen zwischen Adblock-Programmen und Werbefirmen aufgedeckt (siehe Security Report Juni 2013).

Nachzulesen unter:

http://blog.fefe.de/
http://www.nzz.ch/aktuell/digital/gmx-webde-united-internet-11-adblocker-werbung-warnung-browser-1.18252530
http://labs.bromium.com/2014/02/21/the-wild-wild-web-youtube-ads-serving-malware/

© SWITCH 2014

http://www.mobilegeeks.de/adblock-plus-zahltag-30-mio-von-amazon-ebay-google-und-yahoo/
http://blogs.wsj.de/wsj-tech/2014/02/27/gmx-und-web-de-werbeblocker/

IV. Der tiefe Fall der grössten Bitcoin-Börse Mount Gox

Angeblich wegen eines Zahlendrehers ist die einst grösste virtuelle Handelsbörse «Mount Gox» jetzt pleite. 850 000 Bitcoins sollen spurlos im digitalen Orkus verschwunden sein, entschuldigte sich Geschäftsführer und Hauptverantwortliche Mark Karpelès. Den Kunden bleibt seine Börse damit umgerechnet rund 56,7 Millionen CHF schuldig.

Schuld an der Pleite, sagt zumindest ein im Web kursierendes Dokument, soll ein Fehler im eigens entwickelten Überweisungssystem sein. Offenbar blieben seit Ende Januar immer mehr Bitcoin-Transaktionen im System «hängen», so dass die Börse schliesslich drei Wochen später eingefroren werden musste. Das, melden sich Finanzexperten weltweit zu Wort, sei das gerechte Ende einer ganzen Serie technischer Pannen bei Mt. Gox. Mit fragwürdigen Sicherheitsstandards habe das japanische Unternehmen den Kurs der virtuellen Bitcoins schon seit 2011 bedroht, immer wieder Panik-Verkäufe ausgelöst und den weltweiten Bitcoin-Handel zum Kollabieren gebracht. Noch im August 2013 wurden fut 60 Prozent des weltweiten Bitcoin-Handelsvolumens über Mt. Gox abgewickelt. Zuletzt waren es noch gut 20 Prozent.

Unabhängig davon boomt jedoch der Handel mit der Kryptographie-Währung. Bitcoins wurden 2009 als schnelle, verschlüsselte virtuelle Währung entwickelt. Die Coins werden in komplexen Prozessen auf den Rechnern der Nutzer erzeugt und kommen vor allem beim Internethandel zum Einsatz. Der Bitcoin-Handel erfolgt ohne behördliche, institutionelle oder staatliche Aufsicht – selbstreguliert innerhalb des Community-Netzwerks. An Online-Börsen können Bitcoins schliesslich gegen «echte» Währung getauscht werden.
Den verschiedenen Börsen-Betreibern ist so etwas wie eine Einlagensicherung nicht vorgeschrieben. Daher dürfte das Gros der Mt.Gox-Gläubiger auf ihren Schulden sitzen bleiben. Karpelès, berichten US-Medien, dürfte sich jetzt auf eine Klagewelle geprellter Kunden gefasst machen.

© SWITCH 2014

Bei der Frage, was der Börsencrash für die Zukunft der Bitcoins bedeutet, gehen die Meinungen auseinander: Banken, Finanzbehörden und Politiker, denen der Bitcoin-Handel aufgrund des undurchsichtigen Schwarzgeld-Verkehrs längst ein Dorn im Auge ist, sehen die Pleite als deutliche Warnung: «Völlig überschätztes Spielgeld», spotten die einen, anderswo ist von «Inkompetenz und Wahnsinn» die Rede, von verfehlter Selbstüberschätzung der Kunden» und dem Bitcoin-Handel insgesamt als unsinniger Modeerscheinung. Banken – die Europäische Bankenaufsicht genauso wie die Schweizer Bundesbank – boykottieren die Anerkennung der Bitcoins als echte Währung schon lange. «Digitale Geldbörsen seien ohnehin nicht sicher, da es zu Hardware-Fehlern kommen könne oder weil Passwörter ausgespäht werden, verloren gehen oder gar vergessen werden könnten.», schreibt die NZZ. Dem widerspricht Luzius Meisser, Präsident der Bitcoin Association Schweiz: «Das Debakel wäre nicht passiert, wenn es einen freien Markt gäbe.»

Laut Bitcoin-Stiftung sind die Betreiber von Mt. Gox selbst schuld an der Misere. « Die Aufsichtsregeln wurden nicht befolgt. Die Nutzer hätten ihre Bitcoins vermutlich besser auf ihrem Laptop oder dem Smartphone behalten», so Stiftungsdirektor Jon Matonis. Zudem habe Japans Regierung versagt, die Börse entsprechend zu regulieren. Geprellten Bitcoin-Händlern bleibt nun, auf seröser eingestufte Alternativen wie bitcoin.de, bitstamp.net, kraken.com oder localbitcoins.com zu wechseln.

Mehr zum Thema:

http://www.wired.com/wiredenterprise/2014/02/bitcoins-mt-gox-implodes/
http://online.wsj.com/news/article_email/SB10001424052702303801304579410010379087576-lMyQjAxMTA0MDIwNzEyNDcyWj
http://de.scribd.com/doc/209050732/MtGox-Situation-Crisis-Strategy-Draft
http://futurezone.at/digital-life/chef-von-bitcoin-boerse-mt-gox-dementiert-flucht/53.476.152
http://www.heise.de/tr/blog/artikel/Warum-Bitcoin-ruhig-sterben-darf-2125380.html
http://www.nzz.ch/finanzen/devisen-und-rohstoffe/devisen/bitcoins-disqualifizieren-sich-als-waehrung-1.18207689

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Poul-Henning Kamp, bekannter FreeBSD Kernel-Entwickler und Tool-Autor, stellte auf der FOSDEM 2014 in Brüssel die fiktive «NSA-Operation ORCHESTRA» vor: eine

© SWITCH 2014

Sammlung sehr wirkungsvoller Geheimdienstaktivitäten. Kamp gibt ein Status-Update zu dem Programm vor einem ebenfalls fiktiven Publikum im NATO-Headquarter:

https://fosdem.org/2014/schedule/event/nsa_operation_orchestra/
http://ftp.osuosl.org/pub/fosdem//2014/Janson/Sunday/NSA_operation_ORCHESTRA_Annual_Status_Report.webm

Können schöne Sonnenuntergangsbilder dazu beitragen, Ihr Bankkonto zu plündern? Jérôme Segura, Senior Security Researcher bei Malwarebytes, erklärt, wie sich der Zeus-/Zbot-Trojaner Steganografie in Bildern zunutze macht:

http://blog.malwarebytes.org/security-threat/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/

«La Quadrature du Net» ist eine Non-Profit-Organisation, die für die Rechte und die Freiheit der Internet-Bewohner kämpft. Seit Sommer 2013 hat sie alle öffentlichen verfügbaren Informationen zu den NSA-Überwachungsprogrammen gesammelt und aufbereitet. Ihre«NSA-Observer»-Datenbank ist frei verfügbar und umfasst zurzeit 359 verschiedene NSA-Programme, -Angriffsvektoren und -Abteilungen:

https://nsa-observer.laquadrature.net/

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

Der Security Report widerspiegelt nicht die Meinung von SWITCH sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.

© SWITCH 2014