Das grosse Schlüsselrasseln

Die Nachfrage nach E-Mail-Verschlüsselung «made in Switzerland» wächst stark

Als Folge der NSA-Affäre gewinnt E-Mail-Verschlüsselung an Bedeutung. Die Aktivitäten amerikanischer Geheimdienste haben die Position amerikanischer Software-Firmen geschwächt.

Stefan Betschon

Zwei kleine amerikanische Internetfirmen haben ihre Geschäftstätigkeit eingestellt. Es waren kleine Firmen – Silent Circle und Lavabit –, und doch hat das Ereignis weltweit für Aufregung gesorgt. Beide offerierten verschlüsselte E-Mail-Dienste. Die 2004 gegründete texanische Lavabit zählte zu ihren Kunden auch einen gewissen Edward Snowden, der durch seine Berichte aus dem Innern der amerikanischen National Security Agency (NSA) berühmt geworden ist. Jetzt hat der Inhaber von Lavabit das Geschäft aufgegeben. Er sei durch Regierungsbehörden dazu gezwungen worden. Er habe keine andere Wahl gehabt: entweder die Kunden ans Messer zu liefern oder das Geschäft zu schliessen. Es sei ihm gesetzlich nicht erlaubt, öffentlich über die genauen Umstände der Firmenschliessung zu reden. Nur so viel: «Ich würde jedem abraten, seine Daten einer amerikanischen Firma anzuvertrauen.»

Crypto-Abstinenz

In den USA galten noch in den 1990er Jahren Computerprogramme zur Absicherung von elektronischer Kommunikation als Waffen und durften nicht exportiert werden. Phil Zimmermann, ein Programmierer aus Florida, der eine Verschlüsselungssoftware namens Pretty Good Privacy (PGP) entwickelt und im Internet publiziert hatte, geriet deshalb ins Fadenkreuz der Strafverfolgungsbehörden. Er sah sich mit dem Vorwurf konfrontiert, er habe die nationale Sicherheit der USA gefährdet, und musste befürchten, zu einer Gefängnisstrafe verurteilt zu werden. 1995 liess er den Quelltext seiner Software als Buch drucken. In dieser Form durfte sein Werk – geschützt durch die Meinungsfreiheit – exportiert werden. Dutzende von Freiwilligen, so wird kolportiert, hätten dann das Buch abgetippt und wieder in Computercode zurückverwandelt. Vielleicht haben sie es auch nicht abgetippt, sondern auf Kopien des Codes zurückgegriffen. Wie auch immer: Jetzt war die Verbreitung dieser Sicherheitssoftware mit juristischen Mitteln nicht mehr zu stoppen. Die Kryptologie war den amerikanischen Geheimdiensten entrissen worden, alle Menschen weltweit könnten jetzt diese Hilfsmittel nutzen – die wenigsten tun es.

Viele Computer-Unternehmer glaubten damals, mit Verschlüsselung sei Geld zu machen. Die meisten sind gescheitert, allen voran Phil Zimmermann als Teilhaber der PGP Corp. Zimmermanns jüngste Firma, Silent Circle, hat jetzt ihre Secure-Mail-Dienste eingestellt, aus Furcht, den eigenen Ansprüchen nicht gewachsen zu sein und die Privatsphäre der Kunden vor den zudringlichen Blicken amerikanischer Behörden nicht schützen zu können.

In der Schweiz ging im Jahr 2000 die Firma Onaras an den Start, doch das Geschäft mit Kryptologie entwickelte sich nur sehr zögerlich. Die Firma verschwand 2005, doch das Kernprodukt hat überlebt: Es heisst Seppmail und wird von der gleichnamigen aargauischen Firma vertrieben. In dem Produkt – eine sogenannte Appliance, eine Kombination von Hardware und Software – steckten 20 Personenjahre Arbeit, berichtet Stefan Klein, CEO von Seppmail. Einige Innovationen konnten patentiert werden. Verschlüsselte Mails können hier auch Menschen zugänglich gemacht werden, die keine Verschüsselungssoftware benutzen.

Mit Secure Mail würden heute in der Schweiz rund drei bis vier Millionen Franken umgesetzt, schätzt Klein. Erst vor rund zwei Jahren habe sich das Geschäft belebt, und jetzt, nach den Enthüllungen Snowdens, sei eine «deutliche Steigerung» der Nachfrage zu verzeichnen. Die Kundschaft von Seppmail ist laut Klein sehr vielfältig, Unternehmen aus der Finanzbranche sind dabei, aber etwa auch der Bauernverband. Es habe kleine Firmen darunter, aber auch einen landesweiten Verbund von Spitälern und Arztpraxen, wo mehr als 100 000 Anwender im Rahmen eines Health Info Network verschlüsselt miteinander elektronisch kommunizierten.

«Operative Hektik»

Zu den Schweizer Pionieren bei der Absicherung von elektronischem Datenverkehr gehört auch die Küsnachter Totemo. Die 2001 gegründete Firma ist international tätig, zu den Kunden gehören etwa der deutsche Volkswagen-Konzern, Banken, Novartis oder die Schweizerische Post. Die jüngsten Ereignisse im Zusammenhang mit der NSA hätten die Nachfrage gestärkt, berichtet Marcel Mock, Chief Technical Officer und Mitbegründer des Unternehmens. «Wir bemerken derzeit eine operative Hektik»: «Man will etwas tun, man möchte schnell etwas tun, aber leider fehlt es vielen Verantwortlichen an Fachwissen.»

Wenn er dieser Tage die aufgeregten Medienberichte lese, müsse er schmunzeln, sagt Mock. Er denkt dabei etwa an die Deutsche Telekom und United Internet, die mit ihrer medienwirksam lancierten Brancheninitiative «E-Mail made in Germany» einen neuen Sicherheitsstandard etablieren möchten. Mock: «Das ist nur Augenwischerei, ein echter Schutz ist hier nicht gewährleistet.» Wie Klein glaubt auch Mock, dass bei den technischen Grundlagen der Trend weg von Open PGP hin zu Secure Multipurpose Internet Mail Extensions (S/Mime) gehe.

Eine Schwierigkeit für den Einsatz von Verschlüsselung sieht Ralf Hauser in der Fragmentierung des Marktes, die sich durch inkompatible Lösungen ergebe. Hauser ist Geschäftsführer und Gründer der Zürcher Firma Privasphere. Hinter den Inkompatibilitäten vermutet er auch die Absicht einzelner Anbieter, ihre Kunden eng an sich zu binden. Die 2002 gegründete Privasphere offeriert ihren Kunden eine übers Web zugängliche Dienstleistung. Als Vorteil der eigenen Lösung hebt Hauser die «Beziehungsvertraulichkeit» hervor: Während andere Lösungen zwar den Inhalt der Mails, aber nicht die Metadaten – Absender, Empfänger, Betreff, Dateinamen von Anhängen – schützen, bleibt bei Privasphere die Beziehung zwischen Sender und Empfänger geheim.

Heimisches Schaffen

Laut Andreas Jacob von Avantec sind hiesige Firmen gut beraten, sich bei der Absicherung des E-Mail-Verkehrs auf Schweizer Software-Firmen und Zertifikatsanbieter zu verlassen. Die Zürcher Avantec beschäftigt sich seit 18 Jahren mit Computersicherheit. Er habe sich in den 1990er Jahren über die bescheidene Nachfrage nach Verschlüsselungssoftware oft gewundert, sagt Jacob. Jetzt sei das Interesse riesig. «Dass E-Mail-Sicherheit kompliziert und teuer sei, ist ein Vorurteil.»

DIGITAL IN KÜRZE

Hacker im Internet der Dinge

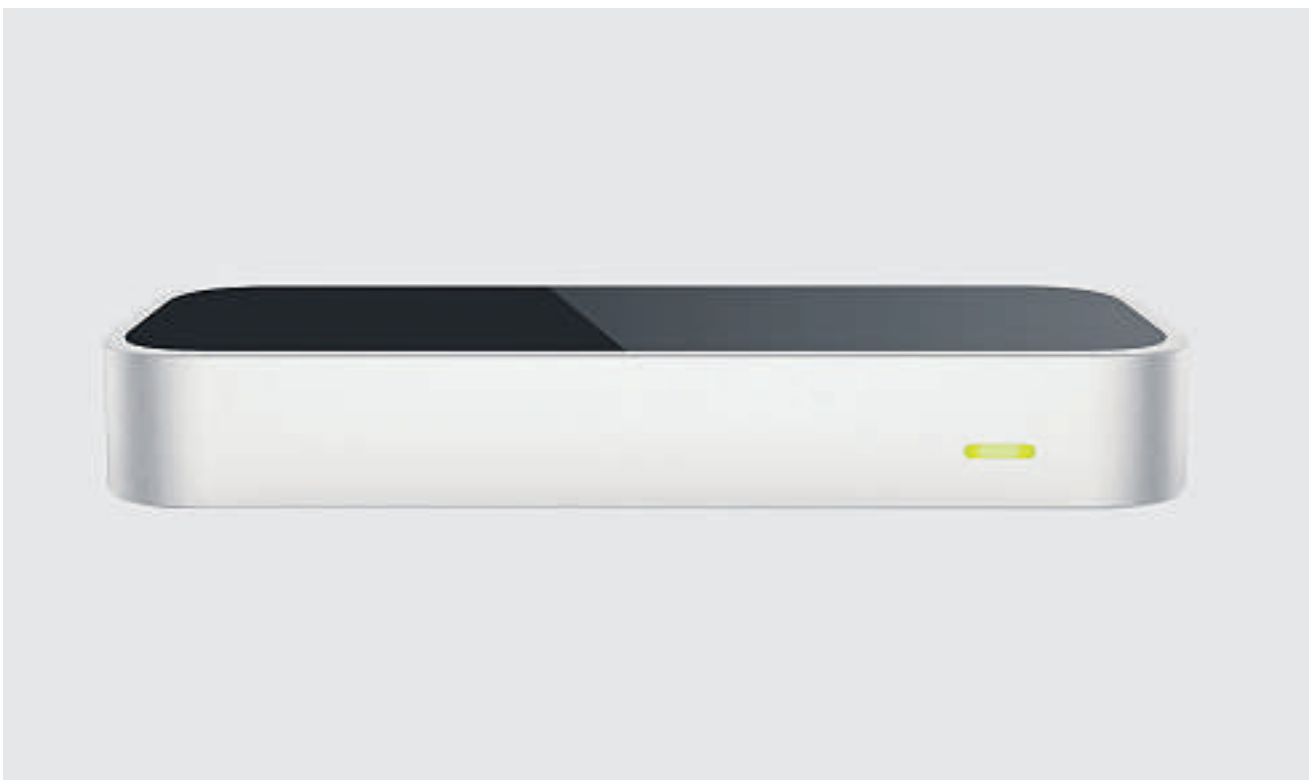
hes. · Nitesh Dhanjani hat auf Sicherheitsprobleme von Philips Hue hingewiesen. Philips offeriert für E27-Fassungen LED-Glühbirnen, die sich per iPhone, iPad oder Android-Handy steuern lassen. Die Befehle des Handys werden im Haus auf eine mit dem Internet verbundene Smartbridge übertragen, von dort per Zigbee-Funk an die Glühbirnen weitergeleitet. Angreifer könnten ihre Opfer nun auf präparierte Websites locken, um Schadsoftware auf ihre Rechner zu bringen, welche Unbefugten die Fernsteuerung der Lichtquelle erlaubt, wenn sie sich im selben Netzwerk befinden. Dhanjani will seinen Report als Warnung vor allzu sorglosem Umgang mit dem Internet der Dinge verstanden wissen. Der Sicherheitsexperte hat laut eigenen Angaben versucht, mit Philips Kontakt aufzunehmen, dabei aber keine Rückmeldung erhalten.

Schutz vor Piraten

hes. · Seit Februar 2012 müssen Blu-Ray-Player mit der Technologie Cinavia des Unternehmens Verance ausgestattet sein. Diese soll die Verbreitung von Raubkopien verhindern. Wie das «Wall Street Journal» meldet, wurden 2012 in den USA etwa die Hälfte der 50 wichtigsten Kinofilme mit einem Audiosignal versehen, das Blu-Ray-Player die Wiedergabe nach 20 Minuten beenden lässt, wenn es sich um eine abgefilmte Kopie handelt.

Geld von Google

hes. · Google hat in den vergangenen drei Jahren zwei Millionen Dollar an Entwickler ausgeschüttet, die das Unternehmen über Fehler in seinen Produkten informierten. 2000 entsprechende Meldungen sind in diesem Zeitraum beim Suchmaschinisten eingegangen, wie er nun mitteilte. Facebook teilte kürzlich mit, dass man 329 Fehlermeldern in den vergangenen zwei Jahren insgesamt über eine Million Dollar gezahlt habe.



Leap Motion: Das Eingabegerät kann die Position der Hände, aber auch einzelner Finger erkennen. PD

Hände hoch

Der Bewegungssteuerung Leap Motion fehlen nicht nur Apps

hes. · Mit etwa einem Jahr Verzögerung ist nun Leap Motion verfügbar. 80 Dollar kostet der feuerzeuggrosse Sensor, der per USB an den Windows-PC oder Mac angeschlossen wird. Praktisch: Ist er zu stark verschmutzt, informiert er den Nutzer per Warnmeldung. Läuft er tadellos, erzeugt er ein etwa 60 Zentimeter hohes Feld für die Gestenerkennung, die deutlich präziser als bei Microsofts Kinect ist: Einzelne oder mehrere Finger werden erkannt.

Knapp 60 Applikationen, derzeit vor allem Games, sind jeweils für die beiden Betriebssysteme im App Store namens AirSprace verfügbar. Das Gros ist kostenpflichtig. Ins Auge sticht die Anwendung der «New York Times». Ihre App ist die einzige eines Medienhauses. Die Navigation ist gelungen. Man sieht Artikel auf Karten. Lässt man den Finger im Uhrzeigersinn kreisen, scrollt man nach unten – und umgekehrt. Doch bei alldem stellt sich die Frage, wer das braucht, denn zwar betonen die Macher immer wieder, Leap Motion solle allenfalls eine Ergänzungen zu Maus, Tastatur und Touchscreen sein. Doch die meisten Anwendungen sind für eine dieser Eingabearten optimiert, und so erschliesst sich der Zusatznutzen nicht auf den ersten Blick. Das gilt auch für eine App wie Swish, mit der man auf dem Mac unter anderem per individueller Geste die Lautstärke ändern kann. Leap Motion könnte interessant werden, wenn die Technologie beispielsweise in andere Eingabegeräte integriert wird.

Exemplarisch zeigt sich der fehlende Zusatznutzen an der App Touchless. Denn zwar kann man so Standardprogramme mit Gesten bedienen, doch diese wurden dafür nicht optimiert, was sich in zu kleinen Buttons äussert. Besser ist die Anatomie-App Cyber Science 3D Motion. Der Totenschädel rotierte rasant unter unseren Händen. Auch das Fliegen durch Google Earth macht grossen Spass. Die Technologie von Leap Motion ist interessant, aber noch nicht ausgereift. Dies äussert sich im Kleinen auch daran, dass die Hardware des Rechners stark beansprucht wird. Es fehlt ein attraktives App-Angebot.

META-TAG

Bald ist September

Stefan Betschon · Die Sonne brennt, der Asphalt kocht, träge blubbert das Blut in seinen Bahnen. Ein Lufthauch, die Ahnung eines Schattens kommt auf, die Vorfreude auf einen Gedanken, der wie ein Vogel aufsteigen würde in kühlere Gefilde, eine Idee – nichts. Geblendet schliessen sich die Augen, ermattet sinkt der Kopf zurück ins feuchte Frottee.

Nichts. Die Branche in den Ferien, der Betrieb geschlossen. Nichts. Keine Idee. Nur gerade das: Apple wird am 10. September neue iPhone-Modelle vorstellen. Die Meldung tröpfelt von News-Outlet zu News-Outlet. Der Fluss der Nachrichten hat sich zu einem dünnen Rinnsal verengt.

In den Rechenzentren der NSA summen die Ventilatoren. Die Hitze wogt hin und her. Niemand da. Weil Mitarbeiter auf die Idee kommen können, sich über ihre Arbeit Gedanken zu machen und die Gesetzmässigkeit und die Sittlichkeit ihres Handelns zu hinterfragen, hat Keith Alexander, Chef der NSA, angekündigt, 90 Prozent der Systemadministratoren zu entlassen. Die Informatiker können baden gehen, sie sollen durch Computer ersetzt werden. Und wer überwacht diese Computer? Eine iPhone-App vielleicht? Apple wird am 10. September neue iPhone-Modelle vorstellen.

Rot wie Erdbeerglace, gelb wie Zitrone, blau und grün: Die neuen iPhones sollen in vielen Farben erhältlich sein. Sind das nicht die Farben von Google? In einem Hintergrundartikel hat das britische Online-Magazin «The Register» die immaterialgüterrechtlichen Probleme des neuen Apple-Produkts analysiert. «Wir sehen jahrelange schmutzige Rechtshändel auf uns zukommen vor Bezirksgerichten, vor der internationalen Handelskommission, der Europäischen Kommission und vielleicht auch vor den Vereinten Nationen», schreibt der britische Journalist «tongue-in-cheek», wie er sagt, beim Glace-Essen vermutlich.

25 Grad am Freitag, 26 Grad am Samstag. Beim Regen bleibt sich alles gleich: 0 Millimeter. Für September sind News angesagt. In einer Twitter-Botschaft an die Welt beklagte sich Donald Trump: «Ich kann nicht glauben, dass Apple sich nicht beeilt, einen grösseren iPhone-Bildschirm zu kreieren.» Ob wohl Trump auf dem kleinen Display übersehen hat, dass Apple am 10. September neue iPhone-Modelle vorstellen wird? «Den Gerüchten gemäss», so schreibt ein Online-Journalist, werde das neue iPhone «gewisse Ähnlichkeiten» mit dem alten aufweisen.

Damit dürfte sich Trump nicht zufriedengeben. Seine Tochter wurde kürzlich in Palm Beach gesichtet, seine Ex-Frau Ivana beschäftigt derzeit im hellblauen Bikini die Paparazzi in Sardinien. Trumps Tweets tröpfeln von News-Outlet zu News-Outlet. «Bringt Steve Jobs zurück», fordert Trump. Ein anderer Multimilliardär pflichtet ihm bei: «Larry Ellison sieht ohne Steve Jobs dunkle Zeiten auf Apple zukommen», schreibt ein Online-Journalist. Bald ist September.

Trojaner gegen Exiltibeter

hes. · Die Website der tibetischen Exilregierung leitete Besucher zu einem Java-Exploit weiter, um den Trojaner Swysin auf den Opferrechnern unterzubringen. Wie Kurt Baumgartner von Kaspersky Lab im Unternehmensblog schreibt, sollen die Angriffe nur über die chinesische Version der Central Tibetan Administration (CTA) ausgeführt worden sein. Am Montag soll der Fehler behoben worden sein.