c't wissen

Sichere E-Mail

NSA aussperren – Privates schützen

Phishing & Tracking abwehren
De-Mail und ePost statt E-Mail?
Raspberry Pi als Mail-Server
Das NSA-sichere Post-Archiv

Verschlüsseln für alle

PGP professionell einrichten, nutzen und verbreiten

16 Mail-Dienste im Sicherheits-Check
So klappt der Provider-Wechsel
Thunderbird einrichten und absichern
22 Mail-Clients für Android & iOS im Test

www.ctspecial.de

Surfen Sie die richtige Welle

Im neuen c't-Sonderheft Android geht es zur Sache: Ausführliche Tests aus dem c't-Labor helfen Ihnen bei der Wahl des richtigen Gerätes. Mit praktischem Zubehör wie SmartWatches oder Aufsteckkameras bekommen Sie noch mehr Spaß mit Ihrem Tablet oder Smartphone.

» **Inklusive ESET Mobile Security – 1 Jahr GRATIS Schutz für Sie**

Gleich mitbestellen und mehr als 10 % sparen! ›

T-Shirt Android fixed it
statt 15,90 €
nur **13,90 €**

Bestellen Sie Ihr Exemplar für 9,90 € portofrei bis 23. März 2014*:

shop.heise.de/android-2014 service@shop.heise.de 0 21 52 915 229

*danach portofreie Lieferung für Zeitschriften-Abonnenten des Heise Zeitschriften Verlags oder ab einem Gesamtwarenkorb von 15 €

heise shop
shop.heise.de/android-2014

Editorial

Liebe Leserin, lieber Leser!

„Eine Mail ist ohne weitere Vorkehrungen eine Art ‚elektronische Postkarte' – meist schneller befördert, dafür jedoch von weniger vertrauenswürdigen Postboten, und sogar automatisch auswertbar." Als dies in c't stand, war Edward Snowden gerade mal 12 Jahre alt. Was haben die Dokumente, die er weitergab, also Neues enthüllt?

Etwas sehr Wichtiges: Niemand erwartete ernsthaft, dass Schnüffler in den Briefzentren der Post sitzen und Millionen von Postkarten lesen und kopieren. Geheimdienste, nicht nur die der USA, tun aber genau das mit E-Mail. Ob Sie Dokumente von der Arbeit nach Hause schicken, Ihren Eltern vom letzten Arztbesuch berichten oder eine Anfrage an Ihre Bank stellen – die Nachricht kann gespeichert, ausgewertet und gelesen werden.

Der damalige Artikel handelte von „weiteren Vorkehrungen", die E-Mail vor Schnüfflern schützen: Verschlüsselung mit PGP. Leider ist diese Technik in den letzten 20 Jahren nicht zum Standard geworden. Snowdens Enthüllungen belegen aber, dass sie wichtiger ist als je zuvor.

In diesem Heft zeigen wir Ihnen daher, wie Sie sich schützen: Welchem Provider Sie Ihre Mails anvertrauen sollten, wie Sie die besten Werkzeuge richtig benutzen und wie Sie vertrauliche Nachrichten sicher verschlüsseln. Auch gegen die schmutzigen Phishing- und Tracking-Tricks können Sie sich wehren – wir sagen Ihnen wie.

Axel Kossel

Inhalt

PRIVATSPHÄRE SCHÜTZEN

Geheimdienste schnüffeln, Absender spionieren durch Tracking und Kriminelle wollen an Zugangsdaten: Nur wer alle Gefahren kennt, kann ihnen aus dem Weg gehen.

8 Mail ohne Mitleser
12 Betrügerische Mails erkennen
16 Tracking aufspüren und abstellen

SICHEREN MAIL-DIENST FINDEN

Wer den Komfort eines Webmailers vorzieht, ist darauf angewiesen, dass der Betreiber für Sicherheit sorgt. Leider versagen dabei etliche. Dann steht der Wechsel des Providers an.

20 E-Mail-Provider im Test
32 E-Mails und Kontakte umsiedeln
36 Alternativen zur E-Mail: De-Mail & Co

MAIL-CLIENTS EINRICHTEN

Egal ob auf PC oder Handy: Ein optimal eingestellter Client ist die Grundlage für sichere E-Mail und verhindert, dass Vertrauliches den Schnüfflern in den Schoß fällt.

42 Thunderbird statt Webmail
50 E-Mail-Apps für Android und iOS
64 E-Mails unter eigener Kontrolle archivieren

EIGENEN SERVER BETREIBEN

Ein eigener Server entzieht die Mails dem Zugriff der Schnüffler. Er ist schnell und preiswert installiert, bringt aber auch einiges an Verantwortung mit sich.

68 Raspberry Pi als privater Server
74 Rechtlicher Rahmen für Mailserver

SICHER VERSCHLÜSSELN

Nur richtig angewendete Verschlüsselung schützt den Nachrichteninhalt vor neugierigen Schnüfflern. Das ist gar nicht so schwierig, wenn man ein paar Tricks kennt.

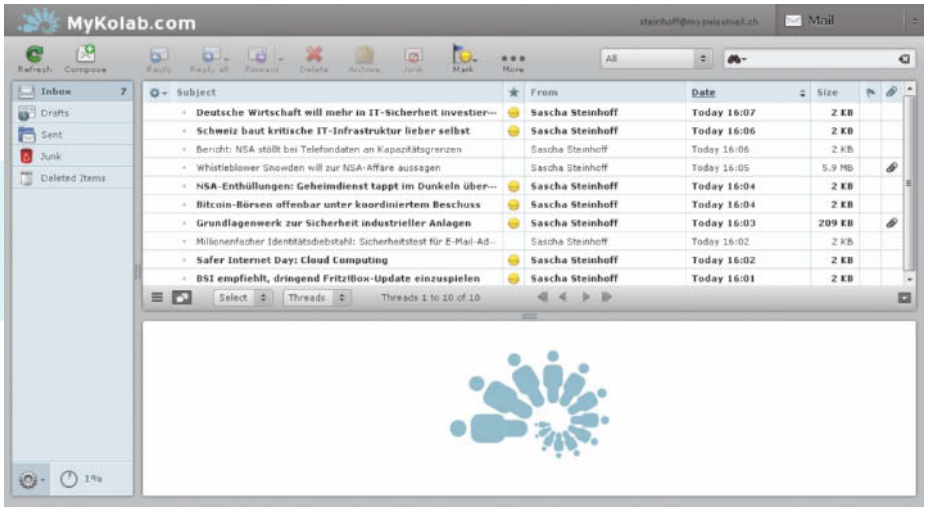
78 Vertraulich kommunizieren
82 Verschlüsseln und signieren mit PGP
92 Verschlüsseln mit S/MIME
98 Recht auf Verschlüsselung
100 Verschlüsseln mit selbst signierten Zertifikaten
110 SSL-Verbindungen besser sichern

ZUM HEFT

3 Editorial
6 Aktion
7 Impressum
7 Inserentenverzeichnis

AKTION: 30 % Rabatt bei sicherem Mail-Dienst

AKTION



Sichere Mail und mehr mit MyKolab.com

KolabSystems unternimmt ein Maximum, um die verwalteten E-Mails und Nutzerdaten zu schützen. c't-Lesern gewährt das Unternehmen ein Jahr lang einen Rabatt von 30 Prozent.

Der Mail-Account von KolabSystems gehört zu den besten bei unserem Mail-Provider-Test, bei dem wir besonderes Augenmerk auf die Sicherheitseinstellungen gelegt haben (siehe Seite 20). Man merkt der Verschlüsselung der Server von MyKolab deutlich an, dass „sichere E-Mail" hier kein bloßes Lippenbekenntnis ist. Bei jeder einzelnen getesteten Option setzte der Schweizer Anbieter das aktuell sinnvolle Optimum an Sicherheit ein.

Dabei muss der Nutzer des Web-Frontend nicht auf Bequemlichkeiten verzichten. Nachrichten lassen sich auf dem Server vorsortieren und so bequem verarbeiten wie mit einem Desktop-Client.

Außer reinen E-Mail-Accounts betreibt KolabSystems auch die Groupware Kolab. Sie enthält zusätzlich zur Mailbox einen Kalender, eine Aufgabenverwaltung und Speicherplatz in der Cloud. Kalenderdaten auf Mobilgeräten lassen sich via ActiveSync, CalDAV und CardDAV synchronisieren, Dateiverzeichnisse per WebDAV auf dem PC einbinden. MyKolab bietet unterschiedliche Pakete vom einfachen Mail-Account bis zur Workgroup-Suite.

DAS RABATTANGEBOT

c't-Leser bekommen von MyKolab.com einen Rabatt von 30 Prozent auf alle Produkte, der Rabatt gilt für ein Jahr. Nach dem Ende der Laufzeit verlängert der Anbieter das Abo zwar automatisch, aber es liegt im Ermessen des Kunden, ob er dem zustimmt.

Eine Zahlungsverpflichtung für die Aboverlängerung besteht ausdrücklich nicht.

Wer den Dienst weiter nutzen möchte, zahlt die zugeschickte Rechnung. Wer für die Verlängerung einfach nicht zahlt, beendet damit formlos und ohne weitere Verpflichtung die Nutzung. In dem Fall schaltet MyKolab das Konto erst passiv – es können nur noch Mails empfangen werden. Zu einem späteren Zeitpunkt wird der Account dann komplett deaktiviert.

Paypal, Bitcoin und Banküberweisungen sind die derzeit akzeptierten Zahlungsmethoden, zukünftig soll auch Kreditkartenzahlung möglich sein.

Das rabattierte Angebot erreichen c't-Leser über den nebenstehenden c't-Link.

Am 31. 8. 2014 endet die Laufzeit der Aktion. (sts) c't

Alle Links zum Artikel
www.ct.de/hb1401006

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.ct-special.de

Leserbriefe und Fragen zum Heft: ctwissen@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx" oder „xxx" bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Dr. Jürgen Rink (jr)
(verantwortlich für den Textteil)

Konzeption: Axel Kossel (ad)

Koordination: Angela Meyer (anm)

Redaktion: Jo Bager (jo), Kristina Beer (kbe), Daniel Berger (dbe), Holger Bleich (hob), Mirko Dölle (mid), Reiko Kaps (rek), Axel Kossel (ad), Jürgen Schmidt (ju), Peter Schmitz (psz), Peter Siering (ps), Sascha Steinhoff (sts), Dušan Živadinović (dz)

Mitarbeiter dieser Ausgabe: Joerg Heidrich, Sven Neuhaus, Prof. Dr. Noogie C. Kaufmann

Assistenz: Saskia Bugdoll (skb), Susanne Cölle (suc), Tim Rittmeier (tir), Sebastian Seck (sbs), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Wolfgang Otto (Ltg.), Ben Dietrich Berlin, Martina Bruns, Martina Fredrich, Ines Gehre, Jörg Gottschalk, Birgit Graff, Angela Hilberg, Anja Kreft, Martin Kreft, Astrid Seifert, Edith Tötsches, Dieter Wahner, Dirk Wollschläger, Brigitta Zurheiden

Layout-Konzept: Hea-Kyoung Kim (Art Director Junior)

Art Direction, Titel, Aufmacher: Hea-Kyoung Kim

Fotografie: Andreas Wodrich, Melissa Ramson

Verlag

Heise Zeitschriften Verlag GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Udo Elsner (-222)
(verantwortlich für den Anzeigenteil)

Stellv. Anzeigenleitung: Simon Tiebel (-890)

Anzeigendisposition: Maik Fricke (-165)

Anzeigenkoordination: Simon Tiebel (-890)

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG, Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL echter druck GmbH, Delpstraße 15, 97084 Würzburg

Vertrieb Einzelverkauf:
VU Verlagsunion KG
Am Klingenweg 10, 65396 Walluf
Tel.: 0 61 23/62 01 32, Fax: 0 61 23/62 01 332
E-Mail: info@verlagsunion.de

Einzelpreis: € 8,40; Österreich € 9,40; Schweiz CHF 12,50; Benelux, Italien, Spanien € 9,40

Erstverkaufstag: 27. 2. 2014

INSERENTENVERZEICHNIS

Heinlein Support GmbH, Berlin 39
mail.de GmbH, Nordhastedt 77
Net at Work Netzwerksysteme GmbH, Paderborn 41
PSW Group GmbH & Co. KG, Fulda 35
Strato AG, Berlin 27
www.webtropia.com, Düsseldorf 11

Mail ohne Mitleser

Die Snowden-Enthüllungen haben klargemacht, dass E-Mail systematisch abgehört wird. Identitätsdiebe kapern Mail-Konten und Werbenetzwerke spionieren uns mit Spam aus. Gegenwehr ist nicht einfach, da grundlegende Sicherheitsmechanismen fehlen oder Provider sie nicht nutzen. Wir zeigen Wege, den Angreifern das Leben schwer zu machen.

Von **Holger Bleich, Axel Kossel**

Fast 200 Milliarden E-Mails rasen täglich durch die Internet-Leitungen. Okay: Der größte Teil davon ist Spam und wird vor der Zustellung geblockt – Studien zufolge 90 bis 95 Prozent. Als relevanter Anteil bleiben aber täglich 10 bis 20 Milliarden berufliche und persönliche Botschaften, Verabredungen, Bestell- und Lieferbestätigungen, Rechnungen, Mahnungen, Shopping-Angebote, Newsletter, Benachrichtigungen aus sozialen Netzwerken und anderes mehr.

Wer Zugriff auf unsere gespeicherten Mails erlangt, erfährt folglich eine Menge über unsere Bekannten, Freundeskreise, Verwandten, berufliche Kontakte, Konsuminteressen, Termine, Orte, soziale Netzwerke sowie unsere finanzielle und gesundheitliche Situation. Nutzen Sie Mail intensiv, dann legen Sie nicht nur ein Verhaltensarchiv an, sondern geben auch Hinweise auf Ihre Entwicklung. Ein solches Archiv ermöglicht sogar Prognosen zu Ihren zukünftigen Beziehungen und Handlungen.

Das Medium E-Mail, wie es heute in der Praxis umgesetzt ist, bietet erst einmal wenig Schutz der Privatsphäre. Es heißt nicht von ungefähr: „Mails sind höchstens so vertraulich wie Postkarten“. Das ist auch kein Wunder, denn elektronischer Mail-Versand wurde vor knapp 40 Jahren als Kommunikationsform für Wissenschaftler erfunden, die sich untereinander vertrauen. Authentifizierung, Signierung, Transportverschlüsselung – all das war zu Beginn weder nötig noch vorgesehen. Nach und nach wurden derlei Techniken angeflanscht, allerdings zulasten der Bequemlichkeit.

Dies betrifft insbesondere den Schutz von E-Mail-Inhalten. Wer sichergehen will, dass seine über die Mail-Standards POP3, IMAP und SMTP transportierten Nachrichten nicht abzuhören sind, muss sie auf dem eigenen Rechner selbst verschlüsseln und gewährleisten, dass nur der gewollte Empfänger den Gegenschlüssel hat („Ende-zu- Ende-Verschlüsselung“). Nach gegenwärtigem Stand ist dazu PGP die sicherste Methode. Dieser Verschlüsselungsstandard erfordert allerdings ein wenig Know-how (siehe Seite 82), ist wenig verbreitet und muss von beiden Kommunikationspartnern gewollt sein.

META-VERRAT

Doch auch die beste Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim Mailen Metadaten anfallen, die auf Sender und Empfänger rückführbar sind.

Weder PGP noch die Alternative S/MIME können den Mail-Header chiffrieren. Verschlüsselt werden nur Inhalt (Body) sowie Dateianhänge. Der Nachrichtentransport via Simple Mail Transfer Protokoll (SMTP) klappt nun einmal nicht ohne Sender- und Empfängerangaben im Klartext.

Wer einen Mail-Account bei Microsoft, Google oder Yahoo hat und seine Mail dort archiviert, kann ausprobieren, wie die Header-Analyse funktioniert: Das am Massachusetts Institute of Technology (MIT) entwickelte Web-Tool Immersion (siehe c't-Link auf der nächsten Seite unten) simuliert eine Geheimdienst-Analyse. Es findet Verbindungen zwischen Kontakten und stellt Beziehungsgeflechte grafisch dar. Einige Redaktionskollegen waren verblüfft, wie klar Immersion beispielsweise anhand der Header-Daten verschiedene Peergroups – etwa Familie, Doppelkopfrunde und Arbeitskollegen – differenziert und darstellt. Und die NSA kann wesentlich mehr.

Immersion zeigt übrigens auch drastisch, was es bedeuten kann, Mails nicht sicher vor Zugriff auf dem eigenen Rechner zu verwahren, sondern sie auf dem Server des Providers zu belassen und dort per IMAP oder über ein Web-Frontend zu verwalten. Daher sollte man überlegen, ob man sie nicht lieber lokal archiviert (siehe Seite 64).

Lauschangriffe auf Mails können an jeder Stelle stattfinden: per Trojaner auf dem Absender- und Empfänger-Gerät, auf den Mail-Relays der Provider und während des Transports durchs Internet. Das durch die Snowden-Dokumente zuerst enthüllte PRISM ist ein Programm, bei dem die Anfragen nach Nutzerdaten an verschiedene IT-Unternehmen automatisiert wurden. Geheimdienstler können unter anderem auf E-Mails zugreifen, die bei Microsoft, Google, Yahoo, und AOL gespeichert sind. Bei einem Programm namens Upstream wird die Kommunikation dagegen an großen Unterseekabeln abgefangen, etwa im Mittelmeer, Nahen Osten und an der britischen Küste. Mail-Metadaten, die die NSA an Glasfaserleitungen abgreift, fließen in eine riesige Datenbank namens „Marina“ und werden dort für mindestens ein Jahr vorgehalten.

Inzwischen ist bekannt, dass auch gezielt Datenleitungen angezapft wurden, über die Rechenzentren großer Mail-Dienste wie Google und Yahoo verbunden sind. Während Nutzer also über eine SSL-verschlüsselte Verbindung auf ihre Mail zugriffen, konnte diese trotzdem abgefangen werden, weil die Dienste den internen Traffic unverschlüsselt abwickelten. Als Reaktion haben mehrere Unternehmen angekündigt, diesen Traffic zwischen ihren Rechenzentren künftig auch zu verschlüsseln. Es gibt auch Mail-Dienste, die Sicherheit zum Grundprinzip erkoren haben (siehe Seite 20). Wie sich der Umzug zu solch einem Dienst bewerkstelligen lässt, steht im Artikel ab Seite 32.

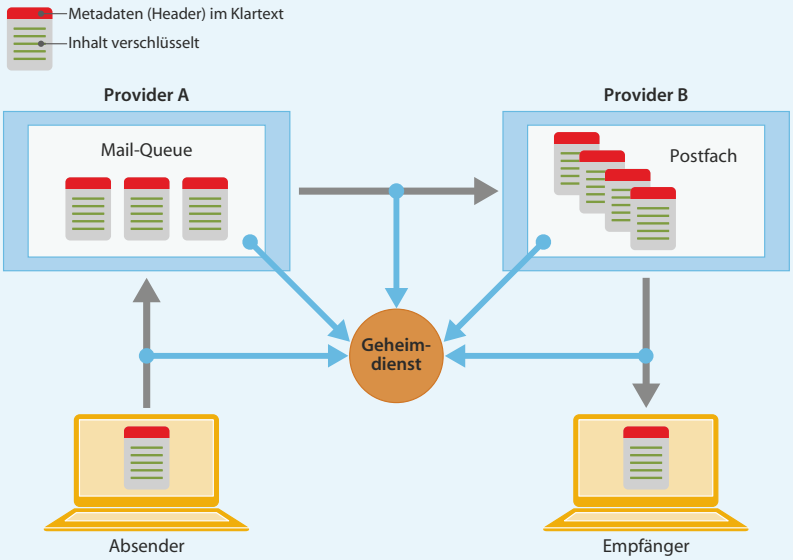
Dabei spricht einiges dafür, einen europäischen Dienstleister zu wählen. Das zeigte der Fall des US-Maildienstes Lavabit. Dessen Betreiber Ladar Levison hatte mit dem Versprechen sicherer Kommunikation sogar Edward Snowden als Nutzer gewonnen. Als dessen E-Mail-Adresse bekannt geworden war, drängten die US-Behörden Levison, ihnen Zugriff auf die gespeicherten Daten Snowdens zu gewähren. Er wehrte sich, wurde aber schließlich gerichtlich zur Herausgabe des SSL-Schlüssels gezwungen, mit dem die Behörden die geschützte Kommunikation zwischen Dienst und Kunden einsehen konnten. Levison schaltete den Dienst daraufhin ab.

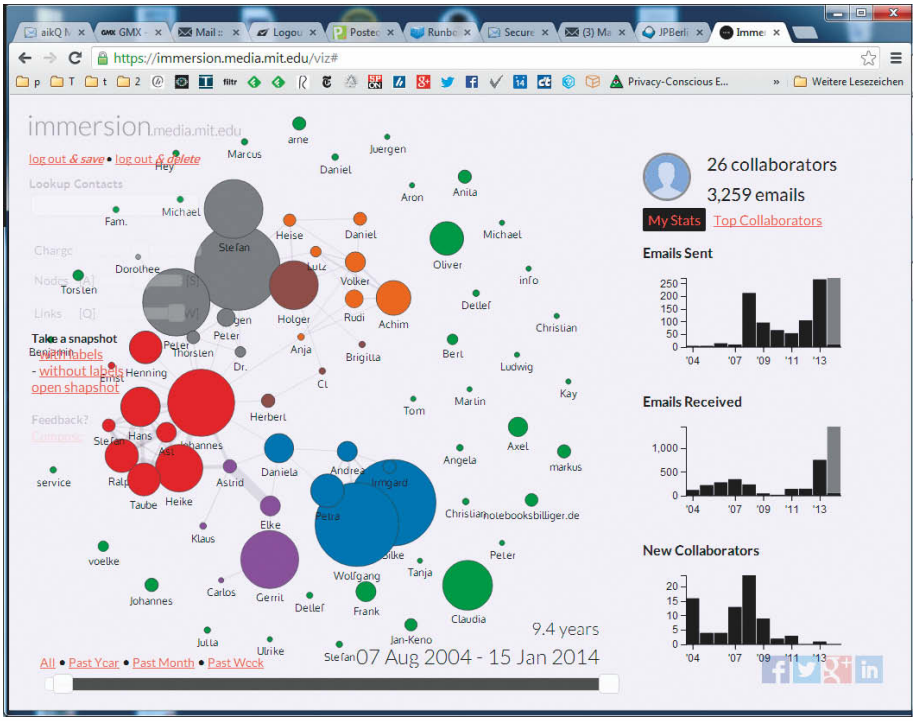
DATENMASSEN

Vor den Snowden-Enthüllungen hätte kaum jemand geglaubt, dass Geheimdienste der USA und ihrer Ver-

Verräterische E-Mail-Metadaten

Auch wenn die Mail-Inhalte beispielsweise mit PGP Ende-zu-Ende-verschlüsselt sind: Metadaten (rot) bleiben unverschlüsselt und verraten eine Menge. Geheimdienste wie BND oder NSA haben heutzutage viele Zugriffspunkte, um Metadaten abzugreifen.





Gewährt man dem Tool Immersion Zugriff auf Header-Daten im Gmail-Account, findet es Beziehungsgeflechte innerhalb der Mail-Kontakte.

bündeten Glasfaser-Backbones anzapfen, um den Datenverkehr zu belauschen. Schließlich geht es hier um riesige Datenmengen. Doch zum Beispiel das Unternehmen Narus ist genau darauf spezialisiert: den Bau von Supercomputern, die für Geheimdienste sogar an 100-GBit-Glasfaser-Leitungen den Datenverkehr mitschneiden und nahezu in Echtzeit filtern können. Das „Narus nSystem“ bietet nach Angaben des Unternehmens eine Komplettlösung inklusive Data-Warehouse, Big-Data-Reduzierung und Forensik-Portal. Narus gehört zur Rüstungssparte des Boeing-Konzerns.

Ein weiterer Zulieferer für Lauschaktionen an Glasfasern dürfte das Unternehmen Glimmerglass sein, denn es warb 2011 damit, dass seine Schnittstellen erfolgreich von US-Geheimdiensten eingesetzt werden. Glimmerglass „CyberSweep“ könne aus IP- und ATM-Datenströmen beispielsweise Gmail-Mails, Facebook-Daten oder Twitter-Tweets in Echtzeit extrahieren und speichern.

In Deutschland ist der in Pullach bei München ansässige Bundesnachrichtendienst (BND) für die „strategische Fernmeldeaufklärung“ zuständig, bei der E-Mail automatisch überwacht wird, die die Landesgrenze überquert. Dazu betreibt der BND bei Providern „Ausl landskopfüberwachung“, lauscht also mit einem Schlüsselwort-Filter an den Servern und Leitungen.

Die Aktivität des BND wird – anders, als es in den USA üblich ist – laufend kontrolliert, und zwar von einem parlamentarischen Kontrollgremium (PKG). Das berichtete, dass 2010 37 Millionen Mails und Telefonate maschinell ausgewertet wurden. Nach PKG-Bericht enthielten lediglich 213 davon verwertbare Hinweise, die zu einem Anfangsverdacht führten. Insgesamt darf der BND gemäß G10-Gesetz höchstens 20 Prozent der Übertragungskapazität ins Ausland dauerhaft belauschen; nach Aussagen aus dem PKG sind es momentan etwa 5 Prozent.

Die Telekommunikations-Überwachungsverordnung (TKÜV) gestattet es Polizei und Staatsanwaltschaft bei Verdacht auf schwere Straftaten gemäß Paragraf 100a Strafgesetzbuch, eine Live-Mail-Überwachung zu starten. Bei jedem Provider, der mehr als 9999 Konten verwaltet, steht dafür eine Schnittstelle bereit. Meist handelt es sich um die sogenannte SINA-Box, die verschlüsselt eine „IP-gestützte Übermittlung der Kopien zur berechtigten Stelle“ ermöglicht. Der Kunde muss über eine solche Überwachungsmaßnahme nicht informiert werden.

Alle Links zum Artikel
www.ct.de/hb1401008

Wer nun meint, mit Verschlüsselung einer solchen Überwachung entgehen zu können, unterschätzt die Möglichkeiten der Ermittler. Seit 2010 ist bekannt, dass hierzulande auch die sogenannte „Quellen-TKÜV“ zum Einsatz kommt, also das Belauschen von Verdächtigen direkt an ihrem Endgerät. Auf diese Weise haben Behörden bereits verschlüsselte Mails nach der Entschlüsselung am PC abgefangen.

WEITERE GEFAHREN

Es sind nicht nur lauschende Geheimdienste, die E-Mail unsicher machen. Das E-Mail-Konto ist der Dreh- und Angelpunkt der digitalen Identität, über den Zugänge bei PayPal, eBay, Amazon, Facebook, Twitter und vielen mehr verwaltet werden. Oft genügt der Zugang zum Mail-Konto, um bei anderen Diensten Passwörter zu ändern. Selbst wenn dabei noch Informationen abgefragt werden, lassen sich diese womöglich anhand von archivierten Mails erraten. In vielen Fällen von Identitätsdiebstahl spielt daher das Kapern des Mail-Kontos eine zentrale Rolle.

Wer nur eine Mail-Adresse nutzt, schafft damit einen gefährlichen Single Point of Failure. Denn gewöhnlich ist dieses nur durch ein einfaches Passwort geschützt. Hat man den Mail-Client falsch eingestellt oder nutzt man den falschen Dienst, wird es unverschlüsselt übertragen. An öffentlichen Hotspots ist es leichte Beute für Kriminelle.

Schadsoftware mit Keylogger-Funktion fängt die Passwörter bereits bei der Eingabe ab, da nützt auch eine SSL-Verbindung nichts. Ironischerweise gelangt Schadsoftware oft per E-Mail auf schlecht geschützte Systeme. Im Januar wurde bekannt, dass deutsche Strafermittler 16 Millionen Datensätze mit so gestohlenen Internet-Zugängen sichergestellt hatten.

Eine weitere Gefahr ist das immer noch betriebene Phishing: Nutzer werden per E-Mail auf gefälschte Webseiten gelockt und sollen dort die Zugangsdaten etwa zu einem Bezahldienst eingeben. Das funktioniert so einfach, weil man die Absenderadresse einer Mail problemlos fälschen kann. Die Fälschung hält aber einer genauen Prüfung nicht Stand (siehe Seite 12).

Und schließlich sind da noch die allgegenwärtigen Werbenetzwerke, die nicht nur unseren Weg durchs Web verfolgen, sondern auch mit präparierten Mails herauszufinden versuchen, wo wir leben und was uns interessiert. Ihr Ziel ist es, uns durch Werbung besser manipulieren zu können. Ob sie es erreichen, hängt vom Mail-Client oder -Dienst ab, den wir verwenden, und von unserem Know-how (siehe Seite 16 und 20). (ad) c't

Betrügerische Mails erkennen

Die Kriminellen lernen dazu. Phishing-Mails lassen sich nicht mehr so einfach enttarnen und die Filter der Mail-Provider halten auch nicht jeden Unrat zurück. Ob die Mails nun mit frohen Botschaften oder mit Druck und Angst arbeiten, wir zeigen, wie Sie Betrugsversuche zuverlässig erkennen.

Von **Kristina Beer**

E-Mail-Betrüger gehen mittlerweile so geschickt vor, dass selbst ausgebuffte Nutzer über die Professionalität neuerer Phishing-Mails ins Staunen geraten. Die Absender wollen ihren Opfern Kreditkartennummern, Pins und Passwörter entlocken, um möglichst viele Konten leerzuräumen.

Die Inhalte und die Optik von Firmen-Mails werden für den Betrug perfekt imitiert. Mit geschickt gewählten Absenderadressen, Domainnamen und exakt nachgebauten Firmen-Homepages versuchen die Betrüger jeden Zweifel an der Echtheit ihrer Phishing-Mails und der Web-Seiten, auf die sie verweisen, zu verwischen. Aber es gibt einfache und schnell anzuwendende Hilfsmittel, mit denen man den Durchblick behält, und ein paar Techniken für die tiefergehende Analyse, die etwas mehr Zeit kosten.

HINWEISE IM TEXT

Phishing-Mails verraten sich oft durch fehlerhafte Grammatik und Orthografie sowie Zeichenkodierungsfehler – vielen merkt man die Google-Übersetzung noch an. Darüber hinaus enttarnen sich manche Phishing-Mails auch durch falsche Ausdrücke; besonders Fachtermini werden häufig in falschen Zusammenhängen gebraucht.

Gerade bei Mails von Unternehmen sollten Sie deshalb immer zunächst auf die Sprache achten. Kundendienste und Werbeagenturen überzeugen zwar auch nicht immer durch fehlerfreies Deutsch, allerdings ist die Fehlerquote dort wesentlich geringer.

„HALLO KUNDE“

Kundendienste personalisieren E-Mails fast immer. Sie werden dort also mit Ihrem richtigen Namen angesprochen – oder zumindest mit dem, den Sie bei der Registrierung angegeben haben. Beginnt die Mail hingegen mit einem allgemeinen „Hallo“ oder „Sehr geehrter Kunde/Kundin“, könnte dies bedeuten, dass der richtige Name dem Absender nicht bekannt ist. Ein eindeutiger Hinweis, dass es sich deshalb um eine Betrugs-Mail handelt, ist das aber nicht. Denn mangels Ausbildung oder Zeit sparen sich einige Kundendienstmitarbeiter diese Mühe.

Dass die Personalisierung Vertrauen schafft, wissen aber natürlich einige Betrüger. So treffen in letzter Zeit auch immer mehr Phishing-Mails ein, bei denen auch die Anrede stimmt. Der zur verwendeten Mail-Adresse gehörende Name stammt dann in der Regel aus Listen, die etwa bei Einbrüchen in Datenbanken von Unternehmen, Online-Shops oder Foren erbeutet wurden. Diese werden auf dem Schwarzmarkt zu höheren Preisen gehandelt als nackte Mail-Adressen.

MAUS VORSCHICKEN

Sind Anrede und Fließtext einwandfrei formuliert, kann man sich die in der Mail enthaltenen Links vornehmen. Auch wenn da „Login bei Ihrem Postbank-Konto“ steht, führt der Link einer Phishing-Mail keineswegs auf den Postbank-Server. Das wahre Ziel enthüllt der Mouse-Over-Test, den alle Mail-Clients wie Outlook und Thun-