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

€ 8,40

Schweiz CHF 12,50 · Österreich, Benelux, Italien, Spanien € 9,40

c't Sichere E-Mail

blackburner 2014

c't wissen • Sichere E-Mail

Heise

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.

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.

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.

EIGENEN SERVER BETREIBEN

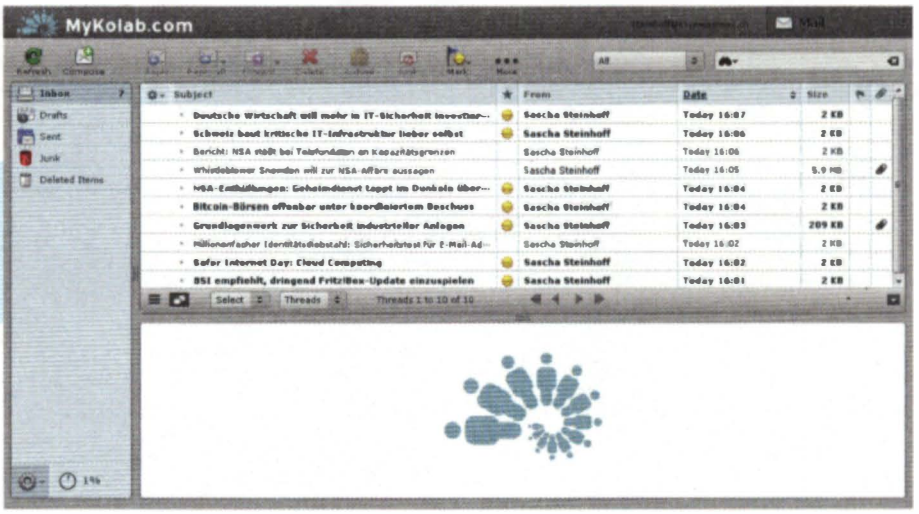
Ein eigener Server entzieht die Mails dem Zugriff der Schnüffler. Er ist schnell und preiswert installiert, bringt aber auch einiges an Verantwortung mit sich.

SICHER VERSCHLÜSSELN

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

ZUM HEFT

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

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).

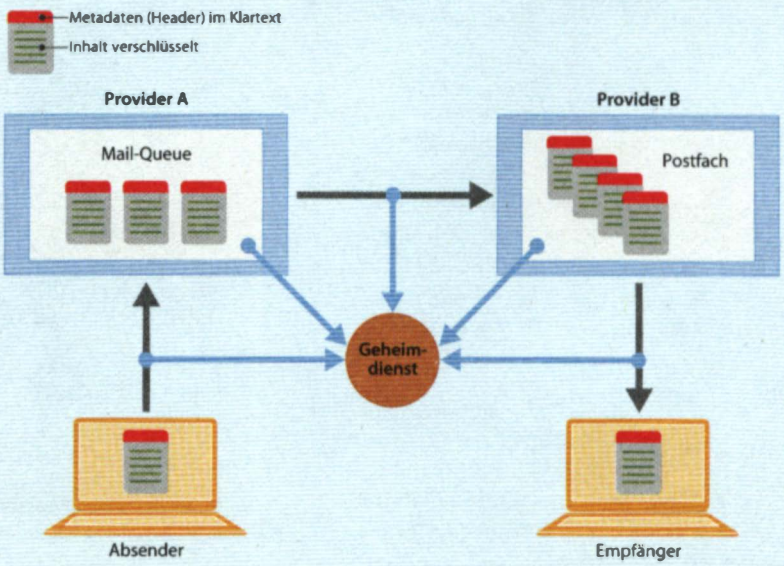
Lauschangriffe auf Mails können an jeder Stelle stattfinden: per Trojaner auf dem Absender- und Empfänger-Gerät, auf den Mail-Relays der Provider und während des Transports durchs Internet. Das durch die Snowden-Dokumente zuerst enthüllte PRISM ist ein Programm, bei dem die Anfragen nach Nutzerdaten 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.

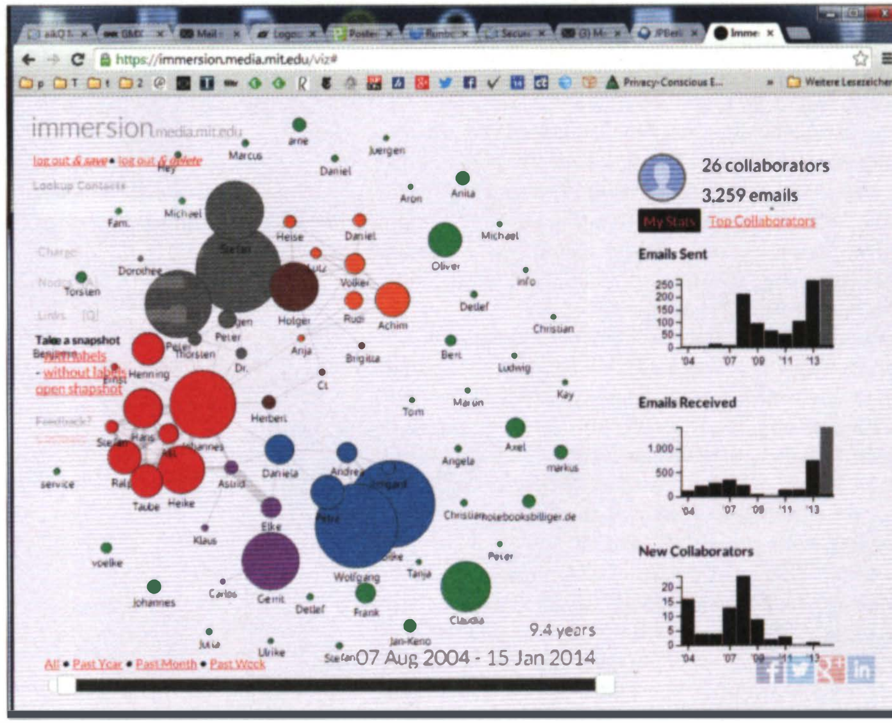
Verräterische E-Mail-Metadaten

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.



DATENMASSEN

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



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 „Auslandskopfüberwachung", 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.

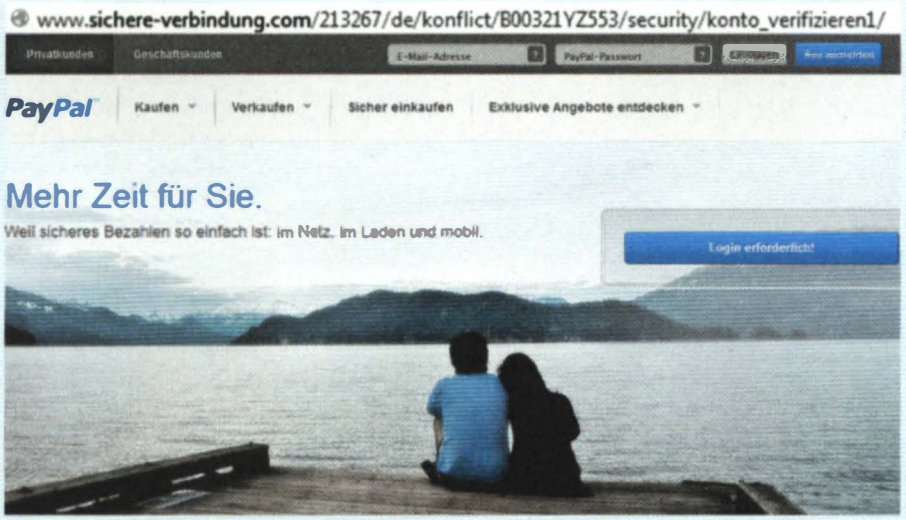
„HALLO KUNDE"

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-



Falsch, weniger Zeit für Sie! Gut gemachte Phishing-Mails stehlen Ihnen Zeit – und wenn Sie darauf hereinfallen, Geld.

derbird - oder bei Web-Mail die Browser - ermöglichen. Wenn man den Mauszeiger auf einen Link schiebt, erscheint in der Statusleiste die komplette URL Das enthüllt dann etwa, dass eine Mail, die angeblich von der Ing-Diba-Bank kommt, zu einer URL wie http://britih.com/_vti_bin/_vti_adm leitet, die dazu nicht passt.

Diesen Test zu machen ist nicht so einfach, wie es klingt, weil Phishing-Mails eigentlich immer mit Druck arbeiten - also Schwierigkeiten oder Notfälle vortäuschen und beispielsweise sofortige Konten-Sperrungen androhen. In der damit erzeugten Hektik neigen selbst besonnene Anwender zu voreiligen Klicks. Deshalb sollte im Umgang mit fordernden und drohenden Mails immer der Grundsatz gelten: Ruhe bewahren - Maus vorschicken.

Aber Achtung: Der Mouse-Over-Trick hilft kaum, wenn sich die Kriminellen mit den Links mehr Mühe gegeben haben. Die zeigen dann zum Beispiel auf: http://ing-diba.de.ht/webkunden/goLogin.do oder http://verifysparkasse.webs.com/ und sind nur noch schwer von den echten zu unterscheiden.

Apropos echte beziehungsweise vertrauenswürdige URLs: Auch die sind oft nicht ohne Weiteres zu erkennen. Immer öfter verwenden Firmen spezielle Domains für Aktionen oder wickeln bestimmte Aufgaben über externe Dienstleister ab. Das Resultat: Die URL steht in keinem offensichtlichen Zusammenhang mit dem Firmennamen.

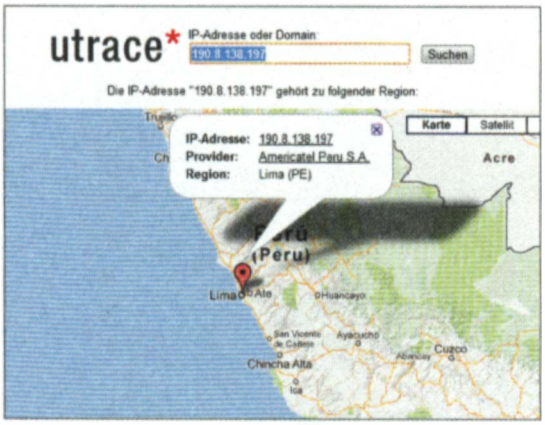
Um sich hier nicht täuschen zu lassen, hilft dann nur ein genauerer Blick auf die Domainnamen. Der Domainname ist der hintere Teil des Server-Namens - also bei http://www.heise.de das „heise.de" und bei dem angeblichen Sparkassen-Link das „webs.com". Wer Zweifel hat, ob das der Sparkasse gehört, kann bei Whois nachsehen, wer diese Domain registriert hat. Das geht zum Beispiel bei heise Netze unter www.heise.de/netze/tools/whois. Dort erfährt man dann, dass „webs.com" zu einem US-amerikanischen Web-Hoster gehört, über den die Sparkasse wohl hoffentlich keine Dienste abwickelt.

IN DEN KOPF GUCKEN

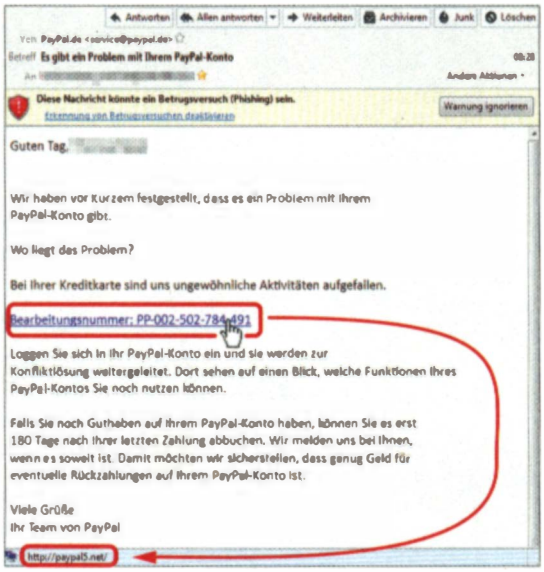
Für weitere Tests lohnt sich ein Blick in den sogenannten Mail-Header. Das sind Verwaltungsinformationen, die unter anderem darüber Auskunft geben, woher eine E-Mail kommt und welchen Weg sie durch das Internet genommen hat.

Normalerweise zeigen Mail-Programme nur ausgewählte Header-Daten an - etwa die Absenderadresse. Doch die lässt sich ganz einfach fälschen und lautet auch bei Phishing-Mails dann etwa „service@postbank.de". Schwerer zu fälschen sind die Informationen, über welche Server die Mail transportiert wurde.

Um den Header vollständig anzuzeigen, wählen Sie in Thunderbird Ansicht/Kopfzeile/Alle. In Outlook findet sich die „Internetkopfzeile" der geöffneten Mail unter Ansicht/Optionen/Nachrichtenoptionen. Die Web-Mailer Web.de und GMX.de erlauben Einblicke über das „i" neben der Datumsanzeige. Yahoo zeigt



Eine E-Mail der Deutschen Post kommt aus Peru? Eher nicht. Anhand der IP-Adresse aus dem Header zeigt Utrace, von wo der vermeintliche Übeltäter aktiv geworden ist.



Da staunte ein Leser nicht schlecht. Die Anrede stimmte, die E-Mail war gut verfasst. Mouse-Over zeigt aber eine verdächtige URL.

den Header, wenn man unter Aktionen den „gesamten Kopfbereich" anwählt. Bei Gmail kommen Sie mit „Original anzeigen" (im Aufklappmenü rechts vom Absender) zum Ziel.

Die interessanten Informationen finden sich in den Received-Feldern. Sie lassen sich nicht ganz einfach lesen. Eine Received-Zeile hat die folgende Form:

```
Received: from smtp-out-127-10.amazon.com [176.32.127.10]...
  by mx.google.com ...
  for <...@gmail.com>; ...
```

Dabei steht der Name hinter „from" für den anliefernden Server, „by" identifiziert den empfangenden Server. Die interessante Received-Zeile ist die des Mail-Servers Ihres Providers. Dazu müssen Sie den ersten GMX-, T-Online-, Google- oder Web.de-Server finden. Dessen Angaben, von wem er die Mail bekommen hat, können Sie vertrauen. Wenn der dann sagt, dass die Mail von einem Amazon-Mail-Server kommt, ist das ein sehr starker Hinweis darauf, dass die Mail tatsächlich von Amazon stammt.

Wenn der Fall nicht ganz so eindeutig ist, kann man sich etwa von dem kostenlosen Dienst Utrace anzeigen lassen, wo der Server steht, dessen IP-Adresse der empfangende Server gesehen hat. Das Schöne an dem Dienst ist, dass er auf der Weltkarte zeigt, wo der Urheber tatsächlich sitzen könnte. Sie schauen den Betrügern damit zwar nicht direkt in den Vorgarten, können so aber erfahren, dass die angebliche Mail der Deutschen Post nicht aus Bonn, sondern aus Lima, Peru kam. Damit darf diese Mail in den Mülleimer wandern.

Häufig tauchen bei solchen Analysen IP-Adressen aus den DSL-Netzen der Internet-Provider auf. Da hat dann in der Regel gar kein richtiger Server die Mail eingeliefert, sondern ein verseuchter Zombie-PC unter der Kontrolle eines Bot-Netz-Meisters, der auf diesem Weg Geld verdient. Er vermietet dazu sein Bot-Netz als Spam-Schleuder. Die Bot-Netz-Sklaven erhalten dann eine Mail-Vorlage und eine Liste von Tausenden Opfern, an die sie diese verschicken sollen.

Viele Phishing-Mails kommen auch von Freemail-Providern. Bei denen legen sich die Phisher möglichst viele kostenlose Accounts an, die ausschließlich dem Zweck dienen, Spam zu verteilen – bis sie der Mail-Provider wieder sperrt.

SCHUTZANZUG ANZIEHEN

Wenn weder Maus noch Mail-Header, Utrace oder Whois Verdachtsmomente ergeben, können Sie sich weiter nach vorne wagen, den Links in der Mail folgen und der Web-Seite auf den Zahn fühlen.

Das sollten Sie aber nur dann tun, wenn Ihr Rechner ausreichend geschützt ist. Für Windows-PCs heißt das neben der obligatorischen Antiviren-Software auch, dass alle Programme auf dem aktuellen Stand sein sollten. Denn es besteht die Gefahr, dass die Zielseite versucht, Ihnen einen Trojaner unterzujubeln. Die Effi-

zienz der Antivirensoftware können Sie übrigens deutlich steigern, wenn Sie zweifelhafte Mails zunächst ein paar Tage liegen lassen. Damit steigen nämlich die Chancen, dass die Schutzmechanismen greifen.

Bevor Sie auf einer Web-Seite wichtige Daten eingeben, können Sie mit ein paar zusätzlichen Checks überprüfen, ob Sie auch auf dem richtigen Server gelandet sind. Stimmt die in der Adressleiste angezeigte URL? Stimmt das Corporate Design? Gibt es sprachliche Mängel? Wohin führen dort die Links (Mouse-Over)? Und bei wichtigen Daten vor allem: Ist die Seite HTTPS-gesichert und stimmt dann auch das Zertifikat?

Das erkennt man am Schloss-Symbol in der Adressleiste der Browser. Über das bekommt man auch weitere Informationen zum Zertifikat. Bei Bankenseiten kann man sogar ein sogenanntes Extended-Validation-Zertifikat erwarten. Dabei zeigen die Browser dann in der Adressleiste zusätzlich zur URL auch die Firma an, der das Zertifikat ausgestellt wurde, also etwa die Postbank AG. Außerdem werden dann je nach Browser Teile der Adressleiste grün hinterlegt. Rufen Sie testweise mal die Seiten Ihrer Bank auf, um das ganz bewusst zu checken.

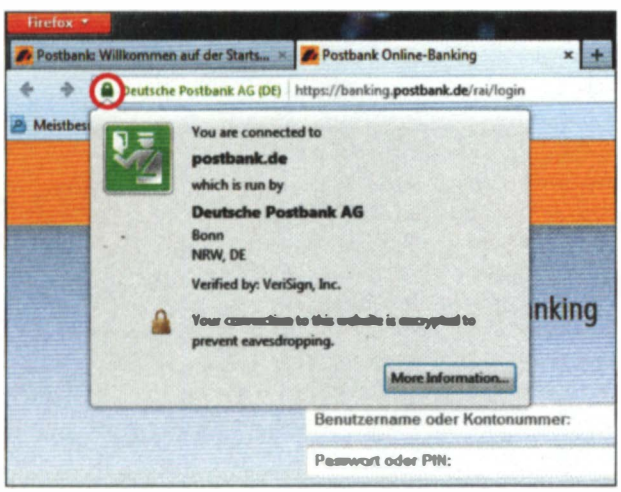
Besondere Gefahr geht von Mail-Anhängen aus, die angeblich neue Geschäftsbedingungen, Rechnungen oder Mahnungen enthalten. Sehr häufig verbergen sich dahinter Trojaner, die beim Öffnen Spionage-Programme auf Ihrem Rechner installieren wollen. Wenn auch nur der geringste Zweifel am Absender einer Mail besteht, sollten Sie die Finger von diesen Anhängen lassen. Wer es sich zutraut, kann mit vorsichtigem Mausfinger über die Eigenschaften den Dateityp überprüfen. Ausführbare Dateien (Endung .Exe, .Com, .Bat, .Cmd, .Vbs, .Js ...) bedeuten höchste Alarmstufe, aber auch Zip-Dateien sind verdächtig, da sie sehr häufig statt des versprochenen PDF-Dokuments eine ausführbare Datei enthalten. Und wird ein Word- oder PDF-Dokument versprochen, muss auch das nicht stimmen. Auch hier schaffen es die Kriminellen, ausführbare Dateien so zu maskieren, dass der nächste Klick völlig harmlos erscheint.

NACHFRAGEN

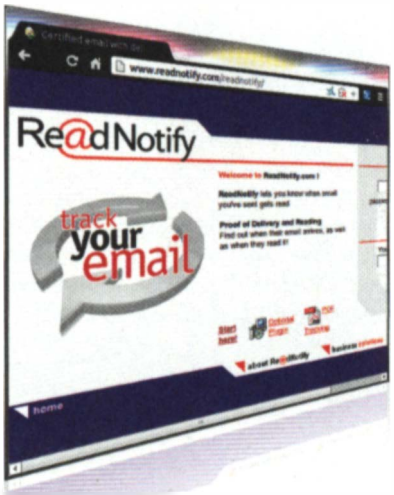
Falls Sie sich bei einer wichtig klingenden Mail immer noch nicht ganz sicher sind, ist es vielleicht das Einfachste, den angeblichen Absender direkt zu fragen. Ein Telefonanruf verschafft schnell Gewissheit. Eine E-Mail-Anfrage beim Kundendienst dauert zwar länger, erspart aber zumindest die Warteschleife der Telefon-Hotline. Wichtig ist, dass Sie nicht die Kontaktadressen aus der vermuteten Phishing-Mail verwenden. Für besonders lukrative Betrugsmaschen betreiben die Cyber-Gangs nämlich sogar schon eigene Callcenter. Gehen Sie also lieber auf die als Lesezeichen gespeicherte Web-Seite der Firma und suchen dort nach einer passenden Kontaktadresse.

Gerade wenn eine E-Mail etwas unter Zeitdruck fordert, sei es die Verifizierung, Bestätigung oder Änderung von Konto- und Kundendaten, oder wenn plötzlich jemand per Mail oder sozialem Netzwerk Hilferufe mit der Bitte um Geldspenden absetzt, sollte man vorsichtig sein. Seriöse Unternehmen setzen Kunden angemessene Fristen und informieren über tiefgreifende Veränderungen mit dem nötigen zeitlichen Vorlauf und ohne sofort Forderungen zu stellen oder Drohungen auszusprechen.

Ärgerlich ist, dass manche Firmen unbedacht E-Mails verschicken, die alle Kriterien für Phishing erfüllen: Schlechtes Deutsch, keine Personalisierung und Links auf dubiose Domains, die irgendwo bei einem Billiganbieter im Ausland gehostet werden. Solche Flüchtigkeitsfehler nerven nicht nur, sondern leisten letztlich Phishing sogar Vorschub. (kbe) c't



Links oben in der Adresszeile ist ein Zettel oder ein Schloss abgebildet. Dort erhält man Auskunft über das Zertifikat der Seite.



Tracking aufspüren und abstellen

Stellen Sie sich vor, Sie öffnen eine E-Mail und im gleichen Moment geht beim Absender ein Alarm los: „Jürgen hat die Mail um 18:53 in Hannover auf seinem iPhone im T-Mobile-Netz geöffnet." Unmöglich? Keineswegs. E-Mail-Tracking gehört längst zum Alltag. Doch Sie können sich schützen.

Von **Jürgen Schmidt**

Nicht hinter jedem Tracking steckt die NSA. Es gibt auch eine andere Art des Trackings, bei der es darum geht, wann eine E-Mail gelesen wird. Und wo. Und womit. Und wie oft. Denn all diese Informationen lassen sich erschreckend einfach ermitteln. Das ist kein theoretisches Szenario, sondern ein sehr reales, auf das sich ein ganzer Geschäftszweig spezialisiert hat.

Fast jeder hat sich schon einmal gewünscht zu sehen, ob beziehungsweise wann eine Mail tatsächlich gelesen wird. Doch die dafür eigentlich vorgesehene optionale Lesebestätigung kann man sich getrost schenken, die klickt ohnehin jeder weg; schließlich geht es keinen was an, wann ich meine Mail lese. Nur die wenigsten lassen sich dabei gern über die Schulter schauen. Viele Programme zeigen die Anfrage nach einer Lesebestätigung deshalb schon gar nicht mehr an.

Vor genau diesem Problem stehen auch viele andere, vom Kleinkriminellen bis hin zum multinationalen Großkonzern. Ein klassisches Beispiel sind Gauner, die durch einen Einbruch ein paar Hunderttausend E-Mail-Adressen ergattert haben, die sie gern zu Geld machen würden. Wenn sie die direkt verkaufen, dann bekommen sie dafür allerdings höchstens ein paar Dollar, denn ein Großteil sind oft nur Dummies oder längst ausrangiert. Wenn sie die Adressen allerdings vorher überprüfen und die validen darunter womöglich sogar mit Zusatzinformationen wie dem Land, in dem der Empfänger wohnt, anreichern können, steigt der Wert ihrer Beute gleich um ein Vielfaches.

Auch die Polizei nutzt das E-Mail-Tracking schon mal, wenn sie etwa gerne wüsste, wo sich ein Verdächtiger gerade aufhält. Oder Werbeagenturen, die ihrem Kunden gegenüber nachweisen müssen, wie erfolgreich sie dessen Botschaft an den Mann oder an die Frau ge-

Es gibt jede Menge E-Mail-Tracking-Dienste im Internet.

bracht haben - und zwar am besten auch in der Region, in der dessen Waren oder Dienstleistungen tatsächlich angeboten werden. Die Interessenten für funktionierendes Tracking stehen also geradezu Schlange.

EINGEBETTET

Prinzipiell lässt sich das auch ganz einfach bewerkstelligen: Sie schicken jemandem eine E-Mail, mit einem Verweis auf etwas, das auf Ihrem Server liegt. Das kann ein Link sein, den der Empfänger dann jedoch anklicken muss. Oder ein Bild, das das Mail-Programm automatisch nachlädt. Dieser Zugriff wird dann in den Log-Dateien des Servers festgehalten. Und damit wissen Sie nicht nur, dass beziehungsweise wann genau die Mail gelesen wurde. Sie sehen noch viel mehr.

Zum Beispiel, dass derjenige in Hannover wohnt, an einem Mac arbeitet - allerdings mit einer etwas veralteten Version von Mac OS X; er ist zwar Telekom-Kunde, hat aber ein iPhone mit Vertrag bei O2. Ort und Provider kann man anhand der IP-Adresse der Zugriffe einfach ermitteln; die eingesetzten Gerätschaften und Programme verrät der sogenannte User-Agent-String, den Programme standardmäßig an den Server schicken.

Diese Problematik ist seit vielen Jahren bekannt. Und wir waren eigentlich auch davon überzeugt, dass Hersteller und Mail-Provider das längst aus der Welt geschafft hätten. Doch weit gefehlt - es ist aktueller denn je. Schon seit Langem haben sich HTML-Mails zumindest so weit als Standard etabliert, dass jedes Mail-Programm sie anzeigen kann. Solche HTML-Mails können dann ähnlich wie Webseiten auch Verweise auf externe Bilder enthalten, die direkt eingebunden werden sollen. Das ist dann ein sogenanntes Image-Tag der Form:

```
<img src="http://www.heise.de/logo.gif">
```

Da der angesprochene Server jeden Zugriff auf ein solches Bild registriert, haben eigentlich alle Mail-Programme - von Outlook Express bis hin zu Thunderbird - dieses automatische Nachladen von Bildern und anderen Elementen abgeschaltet. Statt dessen erscheint immer ein Aktionsknopf wie „Bilder in dieser Mail anzeigen". Das dachten wir zumindest.

Die Beschwerde eines Lesers, dass er in seinem Webmail-Postfach bei GMX keine Möglichkeit hat, das automatische Nachladen von Bildern abzuschalten, machte uns jedoch neugierig. Und unsere daraufhin angestellten Nachforschungen zeigten, dass der Leser nicht nur recht hatte, sondern auf ein sehr viel größeres Problem gestoßen war. Denn die Voreinstellung von GMX war keineswegs ein Einzelfall, sondern zumindest bei Webmail sogar die Regel. Und auch bei einigen richtigen Mail-Programmen und vor allem Smartphone-Apps stellte sich heraus, dass viele Anwender wohl ohne ihr Wissen mehr verraten, als ihnen lieb sein dürfte.

ZURÜCKVERFOLGT

Dieses Tracking ist keineswegs ein theoretisches Problem, das in der Praxis keine Bedeutung hat. Ein Kurztest im Spam-Ordner des Autors zeigte, dass zwar von knapp 10 000 Spam-Mails nur etwa 35 Prozent HTML-Code enthielten. Das ist wahrscheinlich darauf zurückzuführen, dass derzeit viele Spammer versuchen, mit reinen Text-Mails die auf HTML geeichten Spam-Filter auszutricksen. Von den HTML-Mails enthielten dann aber etwa drei von vier auch ein Image-Tag. Und fünf Stichproben zeigten, dass bei jeder Mail mindestens eines davon die charakteristischen Merkmale eines Tracking-Pixels aufwies.

Das sind zum einen die Bildeigenschaften, die darauf ausgelegt sind, das Pixel quasi unsichtbar zu machen: `border="0" height="1" width="1"` ergeben die Minimalgröße von 1×1 Pixel ohne Rand. Dann enthalten die URLs der Bilder immer eine eindeutige Kennung, mit der sie sich nachträglich einer ganz konkreten Mail an eine Adresse zuordnen lassen. Das ist entweder ein Bildname wie „ec28f7710.gif" oder ein angehängter Parameter wie „pixel.gif?token=772ac71...".

Ein besonders aufschlussreiches Beispiel war eine - natürlich nicht angeforderte - Einladung von Charming Events zu einer Weihnachtskreuzfahrt an Bord der „Royal Yacht Britannia". Alle eingebetteten Bilder der Yacht stammten von Systemen aus der Domain charming224.co.uk. Lediglich das unsichtbare 1×1-Tracking-Pixel kam von mylogomail.com, dem Tracking-Server eines Dienstleisters. Die auftraggebende Mitarbeiterin hat allerdings wohl nicht damit gerechnet, dass Mylogomail ihre E-Mail-Adresse paulacreighton@charming-events.co.uk ebenfalls gleich in die Tracking-URL packt - vermutlich, um sich die Auswertung der Spam-Kampagne zu erleichtern. So kann sich das Tracking auch durchaus mal gegen seinen Verursacher richten.

Wie sich weiter herausstellte, enthalten nicht nur Spam-Mails, sondern auch viele offizielle Mails von Firmen, mit denen man in Geschäftsbeziehung steht, solche Tracking-Pixel. So fanden sich etwa in einer echten Telekom-Rechnung gleich zwei davon: eines von „tracking.mlsat02.de" und eines von „statse.webtrendslive. com".

Eine HTML-Mail mit einem solchen Tracking-Pixel zu versehen und die Log-Dateien auszuwerten ist kein Hexenwerk. Das kann jeder mit einem eigenen Web-Server

und ein wenig Hintergrundwissen umsetzen. Firmen, die das Tracking nicht selbst abwickeln wollen, greifen dazu auf die Angebote spezieller Dienstleister zurück. Viele davon bieten einfaches Tracking in kleinen Mengen auch kostenlos an. Somit ist auch persönliche Mail von neugierigen Bekannten keineswegs Tracking-sicher.

DURCHGETESTET

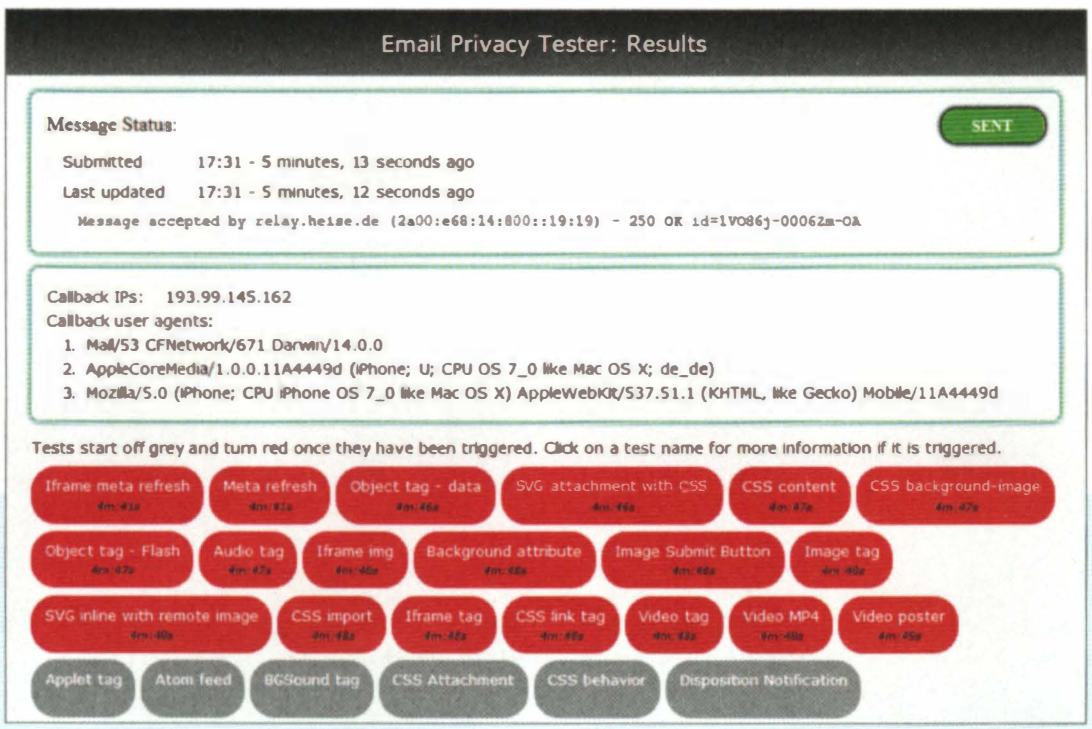
Ob dieses Tracking mit speziellen Zählpixeln dann letztlich auch funktioniert, hängt natürlich von den zum Lesen der Mail eingesetzten Programmen ab. Unsere Tests von über 20 Mail-Clients förderten weitere Überraschungen zutage – viele unangenehmer Natur. Vorbildlich zeigte sich wie erwartet Thunderbird, der ungefragt keine externen Ressourcen nachlud. Outlook Express unter Windows XP verhielt sich genauso brav wie das große Outlook 2012 oder Windows Live Mail unter Windows 7 (Teil der Windows Live Essentials).

Problematisch wurde es schon bei der neuen Mail-App von Windows 8.1. Die lud zwar keine Bilder, versuchte aber schon vor dem Öffnen der Mail im Hintergrund unter anderem auf ein externes Video zuzugreifen. Damit könnte man also nicht das Lesen, aber die Zustellung registrieren. Allerdings sind uns noch keine realen Tracking-Video-Tags in Mails untergekommen.

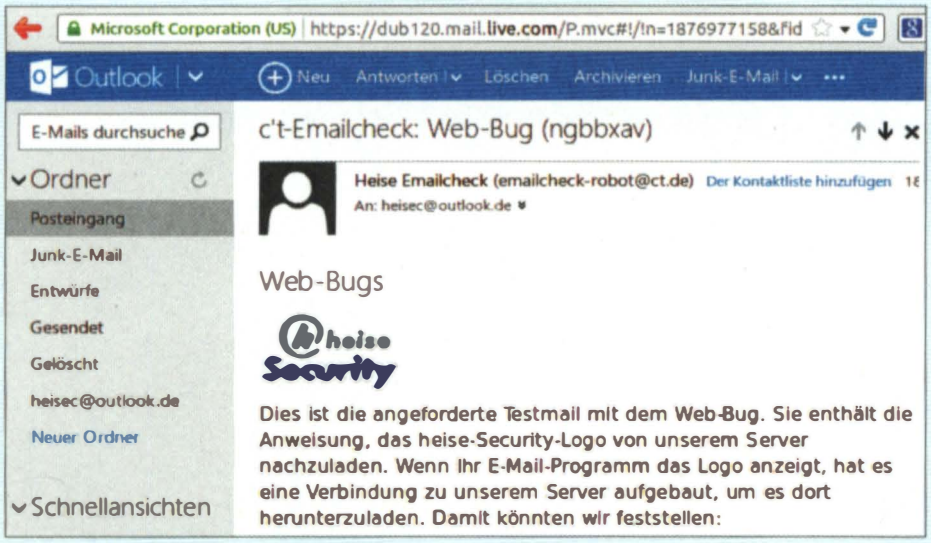
Richtig zur Sache geht es dann jedoch auf dem Mac: Apple Mail unter Mac OS X 10.8 lädt standardmäßig so gut wie alles, was man via HTML einbetten kann: Bilder, Videos, Audiodateien, CSS-Dateien, IFrames und mehr. Wer Wert auf Privatsphäre legt, sollte zumindest unter Darstellung „Nicht lokal gesicherte Bilder in HTML-E-Mails anzeigen" abwählen. Ähnliches gilt übrigens für iPhone- und iPad-Besitzer, die in den Einstellungen unter „Mail, Kontakte, Kalender" die Option „Entfernte Bilder laden" abschalten sollten. Wenn man will, kann man in der Mail immer noch jederzeit „Alle Bilder laden" antippen.

SELBSTSCHUTZ

Wer seinem Mail-Anbieter und den eingesetzten Programmen selbst auf den Zahn fühlen will, der kann sich vom c't-Emailcheck einfach eine Test-E-Mail schicken lassen (www.heise.de/security/dienste/email-check/ oder c't-Link rechts unten). Fordern Sie dort



Alles rot: Ein iPhone lässt sich auf viele Arten tracken. Bei Apple Mail sieht es nicht besser aus.



Mit dem c't-Emailcheck können Sie testen, ob Ihr Mail-Programm wie hier Outlook.de ungefragt Bilder aus dem Internet nachlädt.

unter HTML-Mails eine „Mail mit eingebettetem Bild" an. Sie erhalten zunächst eine Bestätigungs-Mail mit einem Link, nach dessen Aufruf die eigentliche Test-Mail an Sie geschickt wird. Erscheint bei deren Öffnen das heisec-Logo, wurde dieses Bild von unserem Server geladen - aber keine Angst: Wir werten diese Daten nicht aus. Man kann jedoch getrost annehmen, dass das Programm dann alle möglichen Tracking-Pixel ebenfalls lädt.

Nicht immer kann man übrigens aus dem Vorhandensein von Bildern in einer HTML-Mail auf das Nachladen von externen Servern schließen. Es gibt nämlich durchaus die Möglichkeit, die Bilder direkt in die Mail mit reinzupacken. Die werden dann vom Mail-Programm lokal entpackt und direkt in der Mail angezeigt, ohne dass dabei irgendwelche externen Server dies noch mitbekommen. Das Verfahren nennt sich „Inline Images" und ist im Rahmen des MIME-Standards spezifiziert, den alle Mail-Programme und auch Webmailer beherrschen.

Wer noch einen Schritt weiter gehen will, kann auch Datei-Anhänge mit Tracking-Pixeln versehen, die dann beim Öffnen Alarm auslösen. So kann man etwa bei Honeydocs kostenlos Office-Dateien mit eingebetteten Tracking-Pixeln anfordern. Wer dann etwa die Datei „passwords.doc" in LibreOffice oder Word öffnet, löst damit einen „Buzz" auf dem Honeydoc-Server aus.

Um seine Privatsphäre vor Trackern zu schützen, kann man bei manchen Programmen und Apps das Nachladen externer Inhalte abschalten, etwa in iOS oder Apple Mail. Auf dem PC hilft es, Mails statt via Webmailer mit einem Programm wie Thunderbird zu lesen, das diesbezüglich von Haus aus schon sauber voreingestellt ist. Wie mobile Mail-Clients mit Tracking und anderen Sicherheitsproblemen umgehen, lesen Sie ab Seite 50. Immer mehr Anwender wollen auf Webmail-Dienste nicht verzichten. Auch bei diesen gibt es große Unterschiede. Einen Überblick finden Sie ab Seite 20. (ju) c't

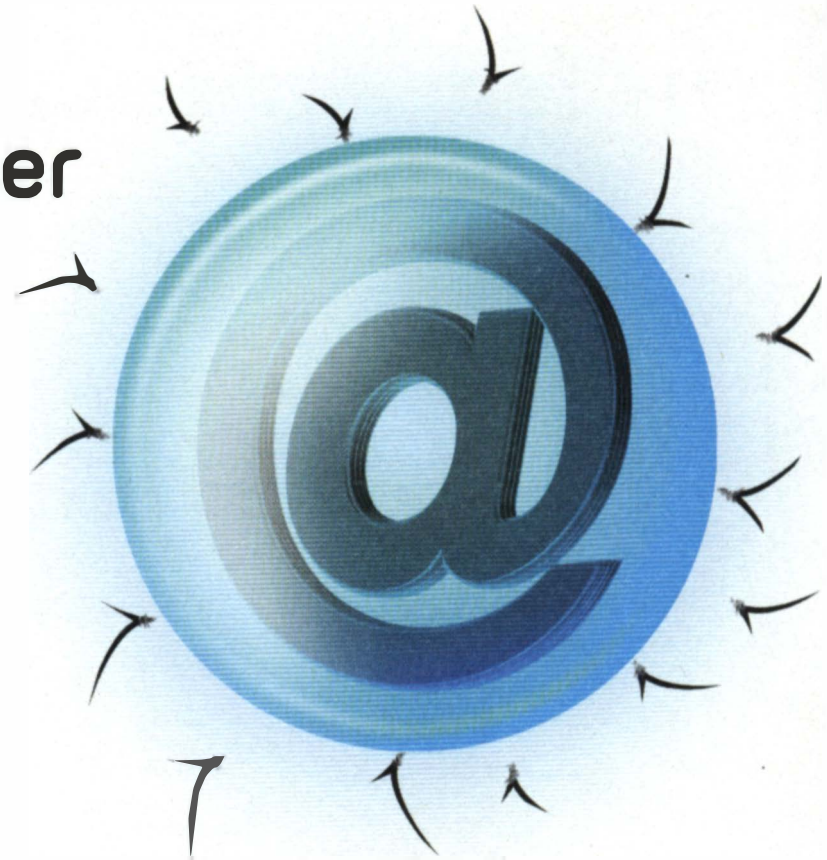
Tracking-Schutz bei Mail-Programmen

Programm	Outlook Express	Outlook	Windows Live Mail	Windows Mail	Apple Mail	Thunderbird
System	Windows XP	Windows	Windows 7	Windows 8.1	Mac OS X 10.8	Linux/Windows/Mac
Tracking-Schutz	○	○	○	○[1]	○[2]	○

[1] lädt Manifest und Video noch vor dem Öffnen im Hintergrund [2] lädt auch Video, Audio, CSS und mehr

Alle Links zum Artikel
www.ct.de/hb1401016

E-Mail-Provider im Test



Vor dem Hintergrund allumfassender Überwachung durch die Geheimdienste haben Mail-Hoster die Themen Sicherheit und Datenschutz als Verkaufsargumente entdeckt. Zeit, sich deren Schutzmaßnahmen einmal genauer anzusehen.

Von **Jo Bager, Jürgen Schmidt**

Kann man sich überhaupt noch E-Mail-Privatsphäre bewahren und sein Postfach gegen Bedrohungen abschotten? Und welchen Beitrag können Mail-Dienstleister dabei leisten? Wir haben uns angesehen, wie E-Mail-Dienstleister ihre Kunden schützen - gegen die Neugier der Geheimdienste, aber auch gegen Schnüffeleien von Werbeunternehmen und andere Bedrohungen.

In unserer Auswahl finden sich große internationale und nationale Provider, im Einzelnen Gmail, Outlook.com und Yahoo sowie GMX, T-Online und Web.de. Daneben positionieren sich kleine Dienstleister als vermeintlich sicherere Alternativen. Wir haben exemplarisch zehn solcher Dienste getestet: aikQ, IPBerlin, MyKolab, mail.de, Posteo, Privat DE Mail, runbox.com, Secure-Mail.biz und VFE Mail.

CLIENT-VERSCHLÜSSELUNG IST PFLICHT

Obwohl die Provider viel zur Sicherheit beitragen können, kommt man für einen wirksamen Schutz seiner Korrespondenz nicht um Verschlüsselung mit dem Client herum. Denn so gut der eigene Provider die Nachrichten schützen mag - man kann sich nicht immer sicher sein, ob dies auch für den Mail-Hoster des Empfängers gilt. Die Nachricht lässt sich also auf ihrem gesamten Weg vom Sender zum Empfänger vor neugierigen Augen nur dann wirksam schützen, wenn der Absender sie verschlüsselt und erst der Empfänger sie entschlüsselt. Dem Thema Ende-zu-Ende-Verschlüsselung im Client widmen wir uns ausführlich ab Seite 82.

Auch wenn ein Mail-Kunde den Inhalt der Nachrichten durch Verschlüsselung vor dem Blick Dritter schützt, befreit das seinen Provider nicht aus der Verantwortung. Denn beim Mail-Versand fallen noch weitere Informationen an, die für Angreifer durchaus interessant sein können. Durch die Enthüllungen von Edward Snowden wurde bekannt, dass sich die Geheimdienste auch dafür interessieren, wer wann mit wem kommuniziert hat. Genau solche Meta-Informationen fallen aber unabhängig von Verschlüsselung an, wenn Mail-Server und -Programme Nachrichten untereinander austauschen.

PSEUDOSICHERHEIT

Die NSA kann auf Basis der Beschlüsse eines Geheimgerichts auf die Mails amerikanischer E-Mail-Dienste zugreifen, ohne dass der Benutzer etwas davon erfährt. Von Gmail, Yahoo und Microsoft weiß man auch, dass es solche Zugriffe in der Vergangenheit bereits gegeben hat. Sollte man daher auf einen Anbieter in einem anderen Land wechseln? So einfach ist das nicht.

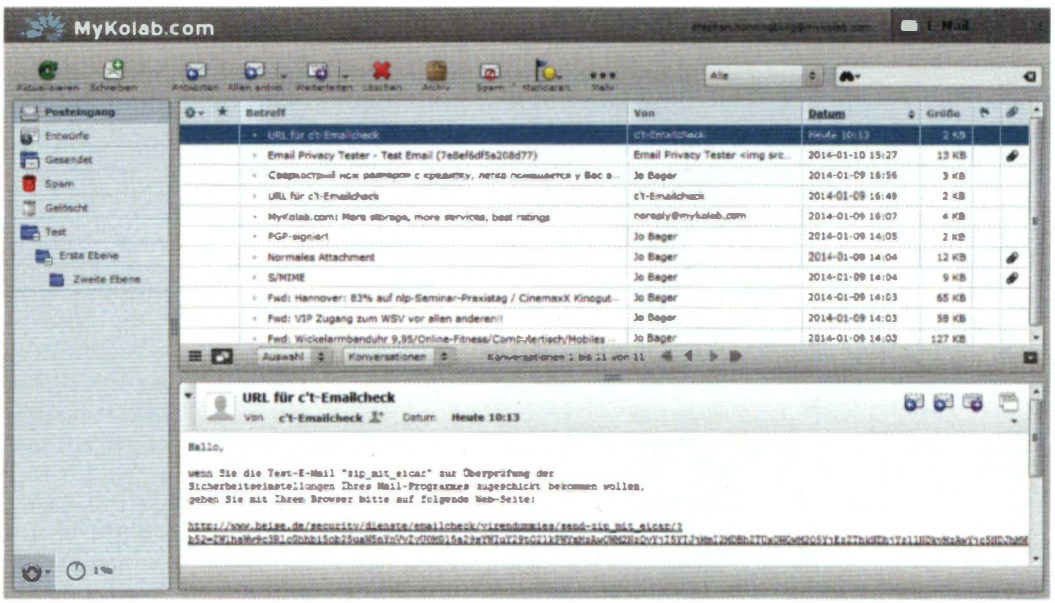
Bei einigen getesteten Diensten ließ sich nicht ermitteln, in welchen Ländern sie sitzen. Davon abgesehen bedeutet der rechtliche Sitz eines Unternehmens nicht unbedingt, dass es seine technische Infrastruktur auch in demjenigen Land betreibt. Bei Privat DE Mail handelt es sich allem Anschein nach um ein deutsches Projekt. Einen Ansprechpartner nennt die Site aber nicht, die Mails lagern offenbar in Ägypten. Die Betreiber begründeten ihre Zurückhaltung auf E-Mail-Nachfrage von c't damit, dass sie sich und ihr Privatprojekt auf diese Weise schützen wollen.

Ebenfalls keine Betreiber nennen Secure-Mail.biz und VFE Mail. Bei diesen Anbietern lagern die Mails in Russland und Island sowie in den USA. Möchte man wirklich seine Nachrichten bei einem Anbieter lagern, der sich nicht zu erkennen gibt und seine Daten in diesen Ländern lagert?

Bei großen Unternehmen wie Google ist der Standort der Server gar nicht zu ermitteln. Solche Riesen betreiben ihr eigenes weltweites Firmennetz; welche IP-Adresse dort zu welchem Land gehört, weiß wohl nur Google selbst. Bei solchen großen Unternehmen muss man außerdem davon ausgehen, dass Kundendaten redundant auf mehreren Servern vorgehalten werden – die dann wieder in unterschiedlichen Ländern stehen können. Soweit möglich, haben wir versucht, den Standort der Server mit Traceroute zu ermitteln und in der Tabelle festgehalten.

Einige E-Mail-Provider werben munter mit den hohen Datenschutzstandards in Deutschland und Europa: GMX, T-Online und Web.de etwa vermarkten ihre Dienste unter dem Label „E-Mail made in Germany". Nachrichten zwischen den Rechenzentren der Unternehmen würden nur verschlüsselt und über deutsche Leitungen übertragen. Bei VFE Mail, der standardmäßig Server in den USA nutzt, kann man in teuren Tarifen seine Mails auch in den Niederlanden lagern lassen.

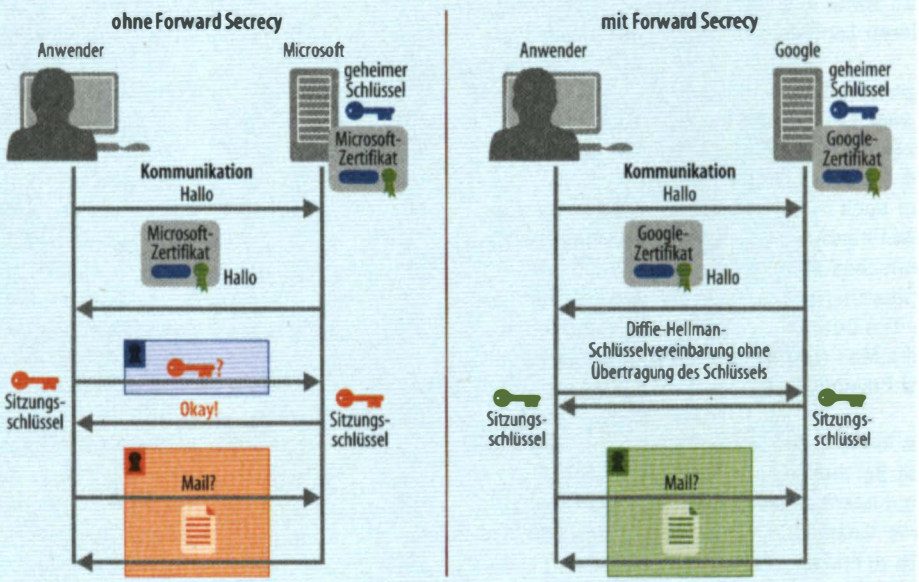
Aber auch hierzulande und in anderen europäischen Ländern kann man sich nicht darauf verlassen, dass staatliche Stellen nicht auf das Postfach zugreifen. Wenn zum Beispiel eine amerikanische Ermittlungsbehörde vor einem US-Gericht einen Durchsuchungsbeschluss für ein in Deutschland beheimatetes E-Mail-Postfach erwirkt, kann es diesen auf dem Weg



MyKolab nutzt das PHP-Mail-Frontend Roundcube, das sich recht bequem bedienen lässt.

SSL-Verschlüsselung mit Forward Secrecy

Bei der Schlüsselvereinbarung mit Diffie-Hellman (rechts) geht der geheime Sitzungsschlüssel nicht über die Leitung. Wer den geheimen Google-Schlüssel klaut, kann deshalb die Mails nicht nachträglich dechiffrieren.



eines Rechtshilfeersuchens an die deutsche Polizei weitergeben, die dann die betreffenden Mails ermittelt. Der Provider muss dann die Inhalte des betreffenden Postfaches herausgeben.

Einige kleinere Provider streuen potenziellen Kunden Sand in die Augen, indem sie beteuern, dass sie ohne das Passwort des Benutzers nicht auf die Mails ihrer Kunden zugreifen können, weil diese verschlüsselt auf ihren Servern gespeichert sind. Das ist aber spätestens zu dem Zeitpunkt ein leeres Versprechen, an dem sich der Benutzer in seinen Account einloggt und seine Nachrichten auf dem Server des Anbieters entschlüsselt werden.

Bei sicheren Mail-Diensten sollte man eigentlich davon ausgehen, dass diese auch Viren ausfiltern können. Wir haben die Virenchecker der Dienste mit einem als Zip-Archiv verpackten Testvirus Eicar auf die Probe gestellt – den eigentlich jeder Virenscanner erkennen sollte. Bei neomailbox.com, Outlook.com, SecureMail.biz und Yahoo ist er dennoch durchgerutscht.

KRYPTISCHES

Ein wichtiger Aspekt unseres Tests war die Konfiguration der Server in Bezug auf Verschlüsselung. Dabei gibt es recht klare Kriterien, an denen man ablesen kann, wie viel Mühe sich der Anbieter gegeben hat, seinen Dienst sicher zu gestalten. Diese lassen sich eindeutig erfassen und bewerten. Sie erlauben dann auch ein qualifiziertes Urteil, das nichts mit gefühlter Sicherheit, irgendwelchen Allgemeinplätzen und Werbebotschaften zu tun hat.

Wir haben uns die Verschlüsselung aller für E-Mail relevanten Server angesehen. Dazu gehört nicht nur

das Web-Mail-Frontend, sondern auch die Server zum Versenden und Lesen von Mails mit einem Mail-Programm. Konkret haben wir mit dem Kommandozeilen-Tool openssl analysiert, welche Verschlüsselungsoptionen die Server für IMAP, POP (Lesen) und für SMTP (Versenden) anbieten. Die gute Nachricht dabei ist, dass man bei allen Anbietern diese Dienste zumindest auch verschlüsselt nutzen kann. Das war noch vor wenigen Jahren keine Selbstverständlichkeit. Bei der Umsetzung gibt es dann jedoch gravierende Unterschiede.

Darüber hinaus haben wir auch gecheckt, mit welchen Verschlüsselungsoptionen uns ein Server des Providers Mails zugestellt hat. Dazu schickten wir über den jeweiligen Dienst E-Mails an eine Adresse wie ju@heisec.de. Der für deren Annahme zuständige Heise-Server protokollierte dabei, ob und wie der anliefernde Server Verschlüsselung aktivierte. Und schließlich überprüften wir auch, ob ein Mail-Server, der Post beim zuständigen Mail-Server des Providers – dem Mail Exchanger (MX) – verschlüsselt anliefern möchte, für dieses Anliegen ein offenes Ohr fand. Schon beim Mail-Transport der Server patzten aikQ und Outlook.com und stellten die Mails im Klartext zu. Da wir mittlerweile wissen, dass NSA, GCHQ und diverse andere Dienste solche Daten an den Backbones fleißig mitlesen, finden sich wohl alle über aikQ und Outlook.com verschickten Mails bereits in deren Archiven. Yahoo änderte dies übrigens erst während unseres Tests.

Bei den Verschlüsselungsoptionen haben wir vor allem auf Kriterien geachtet, die direkte Auswirkungen auf die Abhörsicherheit haben. Das beginnt bei der eingesetzten Protokollversion von Secure Socket Layer (SSL) beziehungsweise Transport Layer Security, geht weiter über die eingesetzten Verschlüsselungsverfahren bis hin zu Zertifikaten der Server. Besonderes Augenmerk legten wir auf die Unterstützung von Forward Secrecy (siehe Grafik links und Kasten auf Seite 25).

Bei den eingesetzten Protokollen gibt es Erfreuliches zu vermelden. Immer mehr Server unterstützen das aktuelle TLSv1.2, das eine Reihe von Problemen aus der Welt schafft, die sich mit den Vorgängern nicht sauber lösen lassen. Der Einsatz von TLSv1 ist zwar kein akutes Sicherheitsproblem; es sollte aber bald durch den immerhin schon 2008 standardisierten Nachfolger abgelöst werden. Richtig blamiert hat sich hier lediglich T-Online mit Servern, die immer noch kein TLS können, sondern auf das veraltete SSLv3 angewiesen sind.

Der magentafarbene Riese schließt bei den eingesetzten Verschlüsselungsverfahren nahtlos an diesen Fauxpas an. Das auf einigen T-Online-Servern immer noch eingesetzte 3DES genügt mit seiner Schlüssellänge von 112 Bit aktuellen Ansprüchen längst nicht mehr und sollte schleunigst ausrangiert werden. Nicht besser macht es Microsoft, dessen Outlook-Server zum Teil ebenfalls noch 3DES einsetzen. Darüber hinaus zeigen die Tests, dass aikQ, GMX, T-Online, Web.de und Yahoo standardmäßig immer noch das fast genauso schlimm einzustufende geknackte RC4 nutzen.

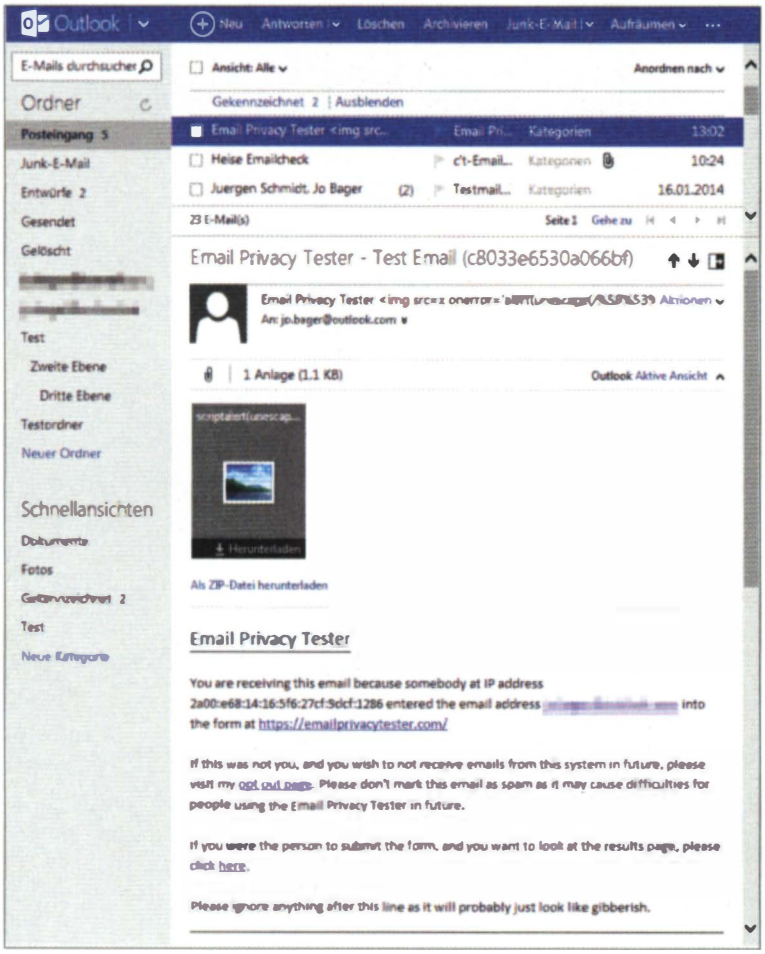
ZUKUNFTSSICHER

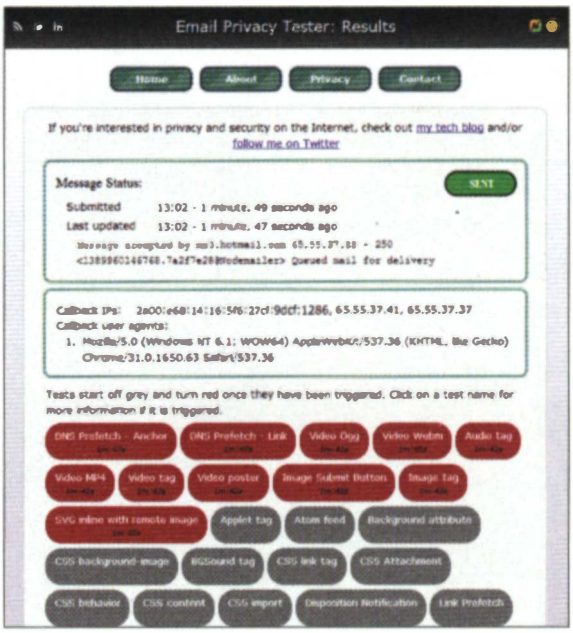
Spätestens seit den Snowden-Veröffentlichungen und den dort dokumentierten Aktivitäten der Geheimdienste ist klar, dass Forward Secrecy kein überflüssiger Krypto-Schnickschnack ist, sondern eine zentrale Sicherheitsfunktion, die man haben will. Doch leider verzichten viel zu viele Provider immer noch darauf, ihre Verschlüsselung damit zukunftssicher zu gestalten. Wer wie aikQ, GMX, Outlook.com, runbox, SecureMail.biz, T-Online, Web.de und Yahoo immer noch die Mehrzahl seiner Server ohne PFS betreibt, hat ganz offensichtlich andere Prioritäten als die Sicherheit.

Wir haben zusätzlich getestet, ob eine verschlüsselte Verbindung zustande kommt, wenn ein Client auf Forward Secrecy insistiert. Das können und sollten Anwender zwar nicht so einstellen, denn Verschlüsselung ohne PFS ist immer noch besser als keine Verschlüsselung oder gar keine Verbindung. Es gibt aber Auskunft darüber, ob der Server das bereits könnte, wenn der Admin wollte oder dürfte.

Auch das Vorhandensein etwas ausgefallenerer Schutzmaßnahmen wie HTTP Strict Transport Security (HSTS) haben wir überprüft und in unseren Ergebnissen festgehalten. Das Fehlen von HSTS ist jedoch nicht in der gleichen Kategorie einzuordnen wie Forward Secrecy, sondern eine eher lässliche Sünde – schon weil es nur die Nutzung des Web-Mail-Frontends betrifft. Trotzdem kann es als Indiz gelten, ob sich der Provider um aktuelle Schutzmaßnahmen bemüht.

Und schließlich haben wir uns auch die eingesetzten Server-Zertifikate angesehen. Auch hier gibt es gute Nachrichten: Alle Zertifikate setzen RSA-Schlüssel mit ausreichender Länge ein; Neomailbox, IPBerlin und Privat DE Mail sogar bereits welche mit zukunftssicheren 4096 Bit. Fast alle Zertifikate enthalten auch eine URL für Statusabfragen (OCSP); lediglich VFE Mail, Neomailbox und Privat DE Mail setzen teilweise auf billige Zertifikate ohne. Privat DE Mail tanzt hier ein bisschen aus der Reihe, weil es sich nicht in das hierarchische Vertrauensmodell von





Der Email Privacy Tester überprüft mit einer Batterie von Tests, ob die Mail-Dienste die Privatsphäre ihrer Kunden schützen.

SSL einordnet, sondern eine eigene Zertifizierungsstelle nutzt.

EINFALLSTOR WEB-MAILER

Alle Mail-Provider außer Privat DE Mail stellen zusätzlich zu den Zugriffsmöglichkeiten für Mail-Clients über die Protokolle IMAP, POP und SMTP auch eine Bedienoberfläche für den Browser bereit. Außer den großen Anbietern GMX, Web.de, T-Online, GMail, Outlook.com und Yahoo unterhalten nur mail.de und runbox eigene Bedienoberflächen. Die restlichen Anbieter setzen auf Standard-Webfrontends auf Basis von PHP, etwa B1gmail, Horde, Roundcube oder Squirrelmail. Dabei betätigt sich MyKolab bei Roundcube als Hauptentwickler. Einige Webdienste stellen sogar mehrere dieser Web-Frontends parallel bereit. Bei VFE Mail etwa kann der Benutzer zwischen Horde5, einer alten Version von Horde sowie Squirrelmail wählen.

Web-Oberflächen sind praktisch. Sie eröffnen dem Benutzer einen zusätzlichen Weg, per Browser auf seine Nachrichten zuzugreifen, wenn mal das E-Mail-Programm außer Reichweite ist. Allerdings stellt jede zusätzliche Möglichkeit, auf den Mail-Bestand eines Mail-Providers zuzugreifen, jede zusätzliche Software-Schicht, ein potenzielles Risiko dar – auch für Nutzer, die gar nicht auf das Web-Frontend zugreifen.

TECHNISCHE ECKPUNKTE FÜR SERVER-VERSCHLÜSSELUNG

SSL/TLS. Die Absicherung von Server-Diensten erfolgt zumeist über Secure Socket Layer (SSL) respektive dessen Nachfolger Transport Layer Security (TLS). Obwohl man immer noch von SSL spricht, sollte man die Protokollversionen SSLv2 und auch SSLv3 nicht mehr einsetzen. Stand der Dinge ist eigentlich TLSv1.2. Die Zwischenversion TLSv1.1 kam nur selten zum Einsatz, viele Server-Betreiber überspringen sie und wechseln direkt auf 1.2. Mehr zu SSL steht im Artikel ab Seite 110.

FS/PFS. Bei Forward Secrecy, manchmal auch als Perfect Forward Secrecy bezeichnet, geht es um zukunftssichere Verschlüsselung. Konkret will man vermeiden, dass ein geklauter oder beschlagnahmter Schlüssel es dem neuen Besitzer ermöglicht, bereits beendete, aber verschlüsselt aufgezeichnete Verbindungen nachträglich zu dechiffrieren. Da man weiß, dass die NSA verschlüsselte Daten vorbeugend aufzeichnet und sich über offizielle Anordnungen zur Herausgabe oder schlichten Diebstahl den Zugang zu geheimen Server-Schlüsseln besorgt, ist Forward Secrecy essenziell. Wurde eine Kommunikation mit Forward Secrecy abgewickelt, kann selbst die NSA nicht rückwirkend alles dechiffrieren, was ihre Horchposten vor den Mail-Servern der Provider vorsorglich schon mal aufgezeichnet haben.

Technisch lässt sich Forward Secrecy bei SSL-Verbindungen durch den Einsatz von Diffie Hellman für den Austausch temporärer Sitzungsschlüssel realisieren. Man erkennt es an dem Vorsatz DHE- oder ECDHE- der Cipher-Suiten in der Tabelle. Dabei einigen sich Client und Server auf ein gemeinsames Geheimnis für die anschließende symmetrische Verschlüsselung etwa mit AES, ohne dass dieses Geheimnis über die Leitung geht. Nach dem Beenden der Verbindung verwerfen die Kommunikationspartner den Schlüssel. Das führt dazu, dass niemand mehr den verschlüsselten Datenverkehr dekodieren kann, ohne AES zu knacken, was derzeit selbst für die NSA aussichtslos sein dürfte.

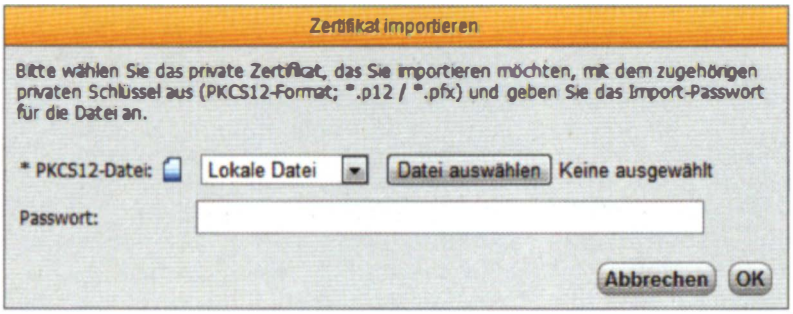
HSTS. Mit HTTP Strict Transport Security (HSTS) kann ein Server dem Browser mitteilen, dass dieser all seine Inhalte – auch zukünftig – über eine verschlüsselte HTTPS-Verbindung abrufen soll. Der Client merkt sich das und wird künftig alle unsicheren Links auf diesen Server in HTTPS-Links umwandeln. Tippt etwa der Benutzer sorglos mail.provider.de in die Adresszeile seines Browsers ein, würde er normalerweise auf der unsicheren Seite http://mail.provider.de landen. Die schickt ihn dann zwar im Idealfall auf die verschlüsselte Seite weiter. Doch ein Man-in-the-Middle kann diese Umleitung verhindern und die im Weiteren unverschlüsselt übertragenen Daten abschnorcheln, indem er alle https-URLs durch gleichlautende http-Links ersetzt.

Hat der Server zuvor jedoch mit einem Header-Feld Strict-Transport-Security HSTS-Unterstützung signalisiert, kontaktiert der Browser direkt die verschlüsselte HTTPS-Seite; der Angreifer bleibt ausgesperrt. Zusätzlich zum Server muss natürlich auch der Browser HSTS unterstützen; derzeit tun das aktuelle Versionen von Firefox, Chrome, Opera und Safari.

RC4: AES/CBC ließ sich eine Zeit lang durch ein Verfahren namens BEAST aushebeln. Das Verschlüsselungsverfahren RC4 ist sehr schnell und galt lange Zeit als gute Alternative zu AES/CBC, um BEAST-Angriffe zu vermeiden. Deshalb wird es gerade von großen Sites häufig eingesetzt; Schätzungen zufolge ist etwa die Hälfte des SSL-verschlüsselten Datenverkehrs mit RC4 gesichert. Allerdings gilt der Algorithmus mittlerweile als geknackt, weil es zumindest unter Laborbedingungen gelungen ist, damit verschlüsselte Daten zu dechiffrieren. Alle Krypto-Experten sind sich einig, dass RC4 der naheliegendste Kandidat für einen Durchbruch der Code-Knacker der NSA ist. Der mit Snowden gut vernetzte Tor-Entwickler Jacob Appelbaum warnt sogar, dass nach seinem Kenntnisstand die NSA RC4 bereits in Echtzeit dekodieren könne.

Da mittlerweile BEAST auch keine Gefahr mehr ist – alle Clients haben Vorkehrungen gegen diese Attacke eingebaut – gibt es auch keinen Grund mehr, RC4 zu verwenden. Stattdessen ist AES mit 128 oder besser noch 256 Bit vorzuziehen.

OCSP: Zertifikate und die zugehörigen Schlüssel können – etwa durch einen Einbruch bei einer CA – gefälscht oder gestohlen werden. Für diesen Fall braucht man eine Möglichkeit, sie für ungültig zu erklären. Das Standardverfahren dazu ist das Online Certificate Status Protocol (OCSP). Dabei trägt der Zertifikatsherausgeber in das Zertifikat einen Server ein, bei dem ein Client nachfragen kann, ob es noch gültig ist. Auch wenn OCSP diverse Probleme hat, ist es das derzeit beste Widerrufsverfahren, das es gibt. Man sollte deshalb nur Zertifikate verwenden, die einen solchen OCSP-Eintrag aufweisen.



Besser nur lokal ablegen: SecureMail.biz will das private S/MIME-Zertifikat auf dem Server speichern.

Das hat sich zum Beispiel bei Roundcube gezeigt. Für das PHP-Paket wurde im Oktober eine Sicherheitslücke bekannt, mit der Angreifer beliebigen Code auf dem angegriffenen Server ausführen und beliebige Dateien auslesen können. Durch einen solchen Angriff könnte der gesamte Mail-Bestand aller Kunden eines Mail-Hosters kompromittiert werden. Der Benutzer kann sich – außer durch Ende-zu-Ende-Verschlüsselung – nicht dagegen schützen, er muss darauf vertrauen, dass sein Mail-Provider solche Lücken bei Bekanntwerden schnell schließt.

Im Großen und Ganzen kann man mit allen Web-Oberflächen vernünftig arbeiten. Nur bei runbox ließen sich Mails nicht per Drag & Drop mit einem aktuellen Chrome-Browser vom Posteingang in einen anderen Ordner verschieben. Die Bedienoberflächen von GMX und Web.de sind ein wenig überladen, was die erste Orientierung ebenso erschwert wie das extrem reduzierte Äußere von Microsofts Mail-Dienst. Alle Dienste sortieren eingehende Nachrichten mit Filtern automatisch in Ordner ein. Die Suchmaschinen von aikQ, GMX, runbox, Secure-Mail.biz und Web.de können nicht die kompletten Inhalte der gespeicherten Mails durchforsten, sondern nur einzelne Header.

Teilweise bieten die Dienste noch Zusatzfunktionen. So gehört zu allen Diensten außer IPBerlin, Privat DE Mail und runbox auch ein Kalender. Die Option, das Adressbuch mit externen Anwendungen zu synchronisieren, bot nur etwa die Hälfte der Dienste. Einige Web-Bedienoberflächen ließen sich nicht gut auf Tablets und Smartphones nutzen, insbesondere die Horde-Oberflächen von neomailbox und VFE Mail. Die für iOS und Android verfügbare authenticator-App von mail.de erzeugt für jeden Login-Vorgang einen zusätzlichen Code und sorgt so für mehr Sicherheit.

SCHNÜFFLER AUSGESPERRT

Einige Dienste unterstützen den Benutzer bei der Zertifikatsverwaltung und Verschlüsselung mit S/MIME und PGP, etwa aikQ, neomailbox, runbox, Secure-Mail.biz, VFE Mail und Web.de. PGP-Signaturen können neomailbox.com und VFE Mail verwalten. Secure-Mail.biz kann sogar ein S/MIME-Zertifikat für das Signieren ausgehender Mails generieren und nutzen oder ein bereits vorhandenes Zertifikat hochladen.

Sobald man aber seine Schlüssel aus der Hand gibt, muss man dem Provider vertrauen. Zertifikatsverwaltung auf dem Server hebelt das Prinzip der Ende-zu-Ende-Verschlüsselung aus. Im Worst Case, etwa wenn der Server des Mail-Betreibers geknackt wird und der private Schlüssel eines Nutzers in die Hände des Angreifers fällt, wären alle Mails des Kunden, auch solche, die vielleicht viel früher einmal abgefangen worden waren, für den Angreifer lesbar. Der private Schlüssel ist die Achillesferse der Ende-zu-Ende-Verschlüsselung und sollte nur auf einem sicheren PC gespeichert werden. Beim Zugriff über das Web-Frontend muss man damit leben, dass man verschlüsselte Nachrichten nicht lesen kann. Wir haben die S/MIME- und PGP-Unterstützung der Web-Frontends in der Tabelle festgehalten, raten aber von ihrer Nutzung ab.

Ein Spam-Filter gehört zum Funktionsumfang aller getesteten Mail-Dienste. Aber einen perfekten Spam-Filter gibt es nicht; überall rutschen mal Nachrichten durch. Und mitunter sind werbliche Mails – etwa der Newsletter vom Online-Händler – ja auch erwünscht. Nichtsdestotrotz sollen solche Nachrichten nicht dazu missbraucht werden können, den Benutzer auszuhorchen. E-Mail-Marketing-Anbieter haben mittlerweile ein großes Instrumentarium entwickelt, durch in

STRATO

KEIN BLABLA

ECHTES HOSTING!
VON PROFIS FÜR PROFIS

NEU!
Verfügbarkeit: Load Balancer bieten maximalen Schutz und 99,94 % Verfügbarkeit durch echte Lastverteilung.

✓ *Hat nicht jeder – bei uns selbstverständlich.*

NEU!
PFS (Perfect Forward Secrecy): Abhörsicherer E-Mail-Verkehr durch PFS-Verschlüsselung.

✓ *Bei uns standardmäßig.*

NEU!
Performance Boost: Jetzt 30 % mehr RAM, SSDs in allen Datenbank-Servern und neue Caching-Technologie.

✓ *Gibt's bei uns on top.*

NEU!
Sicherheit durch SSL: Standard- und Wildcard-Zertifikate einfach per 1-Click verfügbar – mit 256-Bit-Verschlüsselung.

✓ *Bei uns echt günstig.*

Preisaktion bis 31.03.2014!

PowerWeb Plus

6 Monate für

0,– €/Mon.*

Getestet.de Webhosting-Anbieter Testsieger 1,9 (Gut) Test 02 / 2013

TÜV SÜD ISO 27001

HOSTED IN GERMANY 100% Qualität

STRATO.DE

Servicetelefon: 030 - 300 146 - 0

* Aktion bis 31.03.2014: PowerWeb Plus 6 Monate für 0 €/Mon., danach 8,99 €/Mon., Einmalige Einrichtungsgebühr 14,90 €. Mindestvertragslaufzeit 12 Monate. Preise inkl. MwSt. // STRATO AG, Pascalstr. 10, 10587 Berlin

HTML-Mails verborgene Elemente herauszufinden, ob ein Benutzer eine Mail angesehen hat.

Im einfachsten Fall ist das zum Beispiel ein in der HTML-Datei verlinktes, mit einer eindeutigen Kennung versehenes Bild. Ruft der Web-Mailer das automatisch ab, weiß der Werbetreibende, dass der Empfänger die Mail geöffnet hat.

Wichtig ist daher, wie gut Mail-Dienste diese Techniken unterbinden. Immerhin neun Anbieter schaffen es beim Test von emailprivacytester.com, sämtliche Tracking-Tricks ins Leere laufen zu lassen. Bei aikQ und Secure-Mail.biz funktionierten viele Tricks, darunter insbesondere auch Meta Refresh und Meta iFrame Refresh, mit denen sich komplette Webseiten nachladen lassen - fast schon eine Einladung für Angreifer.

ZUGANGSFRAGEN

Alle großen Dienste außer T-Online bieten Apps für den Zugriff von Tablets oder Smartphones an. Das Resümee unseres Tests ab Seite 50: Alle Apps schützen vor Man-in-the-middle-Attacken. Beim Schutz der Privatsphäre mit in HTML-Mails eingebundenen Inhalten ließen sich nur die Android-Apps von Gmail und Web.de nicht austricksen.

Privat DE Mail und VFE Mail haben auch Zugänge via Tor Hidden Services eingerichtet. Ob das wirklich einen Sicherheitsgewinn bringt, ist zu bezweifeln - eher im Gegenteil: Man muss davon ausgehen, dass ein wesentlicher Teil der Tor-Exit-Knoten von NSA und Co. betrieben wird. Wer seine Nachrichten also über das vermeintlich sicherere Netz versendet, spielt am Ende den Nachrichtendiensten in die Hände.

Die Anbieter haben sehr unterschiedliche Geschäfts- und Abrechnungsmodelle. So muss man sich bei neomailbox gleich für ein Jahr binden und mindestens 50 US-Dollar ausgeben. Fairer sind die Preismodelle zum Beispiel von aikQ und Posteo. Sie berechnen für ein Postfach, das für viele Zwecke völlig ausreicht, einen Euro pro Monat, bei einem Monat Kündigungsfrist. Wer bei Posteo mehr will, etwa zusätzlichen Speicherplatz oder weitere Alias-Adressen, kann diese Zusatzfunktionen dazubuchen.

Eine Sonderstellung nimmt das Projekt Privat DE Mail ein, das nichts kostet, aber auch nur sehr eingeschränkte Accounts bereitstellt. So lassen sich maximal 100 Mails pro Tag versenden. Mails können maximal 10 MByte groß sein, auf dem Server stehen pro Postfach maximal 500 MByte Speicherplatz zur Verfügung. Wer sich 90 Tage nicht per IMAP oder POP3 einloggt, dessen Account wird gelöscht. Bei einer ganzen Reihe von Diensten kann der Kunde anonym bezahlen, wobei der Grad der Anonymität variiert: Posteo verspricht, Bezahlvorgänge von Postfächern abzukoppeln. Bei aikQ kann man Geld per Brief einsenden.

Mail-Dienste – Überblick

Name	aikQ	GMX	Google Mail	JPBerlin	mail.de	MyKolab	Neomailbox
URL	http://aikq.de	www.gmx.de	http://mail.google.com	www.jpberlin.de	https://mail.de	https://mykolab.com	http://neomailbox.com
Firmenstandort	Deutschland	Deutschland	USA	Deutschland	Deutschland	Schweiz	Seychellen
Server-Standort (IMAP)	Deutschland	Deutschland	k. A.	Deutschland	Deutschland	Schweiz	Schweiz
Kosten, Vertrag							
Preis	1 €/ Monat	4,99 €/Monat	kostenlos	1 €/ Monat	kostenlos	40,44 €/ Jahr	49,95 US-$/ Jahr
kostenloser Test-Account	✓ (1 Monat)	✓ (1 Monat)	–	✓	✓	–	–
Zahlungsverfahren	PayPal, Überweisung, Brief	Bankeinzug, Überweisung	–	Vorabüberweisung, Bankeinzug, Rechnung, Bargeld	PayPal, PayOne, BitPay	PayPal, Bitcoin, Überweisung	pecunix, Kreditkarte, PayPal, Bitcoin
anonyme Zahlung	✓	–	–	✓	✓	✓	✓
Vertragslaufzeit	1 Monat	12 Monate	–	6 Monate	12 Monate	monatlich	12 Monate
Kündigungsfrist	monatlich	4 Wochen zum Ablauf der Vertragslaufzeit	–	1 Monat	1 Monat	1 Monat	– (muss nicht gekündigt werden)
Zusatzoptionen / andere Tarife	SMS versenden (10 Cent/Stück), Faxe versenden (ab 12 Cent/ Seite)	u. a. FreeMail: kostenlos/werbefinanziert, bis zu 1,5 GByte Speicherplatz; ProMail: 2,99 €/Monat	Google Apps u. a. für Unternehmen: ab 4 €/Nutzer, Monat	Accounts mit Webhosting, eigenen Domains und unlimitierten Mail-Adressen ab 7 €/Monat	u. a. PlusMail: werbefrei, 1,99 €/Monat	u. a. 1 GByte zusätzlicher Speicherplatz: 0,42 €/Monat, Synchronisation: 0,83 €/ Monat	5 GByte: 79,95 US-$/Jahr, 10 GByte: 109,95 US-$/Jahr

[1] siehe Text [2] nach 90 Tagen ohne Login wird der Account gelöscht ✓ vorhanden – nicht vorhanden k. A. keine Angabe

FAZIT

Wer seine Privatsphäre gegen übergriffige Staatsmacht oder andere Angreifer schützen will, sollte verschlüsseln. Denn alles, was im Klartext übers Netz geht, ist leichte Beute und kann von Geheimdiensten und anderen analysiert und ausgewertet werden. Das heißt dann aber auch: Wer Wert auf Sicherheit und Privatsphäre legt und die Mail-Dienste von aikQ oder Microsofts Outlook.com nutzt, sollte sich dringend nach Alternativen umsehen. E-Mail-Provider, die heute noch E-Mails im Klartext transportieren, signalisieren damit ganz deutlich, dass man auf sie beim Schutz seiner Privatsphäre nicht zählen darf. Aber auch die großen Provider Yahoo, T-Online, Web.de und GMX setzen Verschlüsselung eher schlecht als recht um und leisten sich viele Patzer, die sich dann auch in entsprechend schlechter Bewertung widerspiegeln.

Demgegenüber stehen mehrere kleinere Dienstleister, die sich erkennbar und vor allem erfolgreich bemühen, Sicherheit in den Mittelpunkt zu stellen. An der Verschlüsselung der Server von MyKolab, Posteo und Privat DE Mail sieht man deutlich, dass „sichere E-Mail" hier kein bloßes Lippenbekenntnis ist. Bei jeder einzelnen getesteten Option wurde hier das heute sinnvolle Optimum an Sicherheit umgesetzt. Privat DE Mail verwendet für seine Homepage allerdings nur ein selbstsigniertes Zertifikat. Dort überlässt man, ebenso wie bei Secure-Mail.biz und VFE Mail, seine E-Mails einem Anbieter, der sich nicht zu erkennen gibt.

Nur Posteo, Privat DE Mail und Secure-Mail.biz unterstützen HSTS beim Web-Mailer, um auch wirklich sicherzustellen, dass der Benutzer automatisch auf eine verschlüsselte Seite geleitet wird, wenn er aus Versehen beim Web-Frontend eine unverschlüsselte Adresse angegeben hat.

Alles in allem sollte aber, wer vertrauliche Nachrichten sendet, den Web-Mailer höchstens im Ausnahmefall nutzen. Ein Maximum an Sicherheit erreichen Sie, wenn Sie Ihre Mails auf dem PC verschlüsseln und der Empfänger sie auf seinem PC entschlüsselt. Verschlüsselung beim E-Mail-Dienstleister hebelt das Prinzip der Ende-zu-Ende-Verschlüsselung dagegen aus.

Auch wenn es unseren Test erschwert hat, stellten wir erfreut fest, dass in puncto Mail-Sicherheit etwas in Bewegung gekommen ist. So haben Yahoo und mail.de bereits während des Tests einzelne Server auf sichere Verfahren umgestellt. Einige kleinere Provider wie MyKolab und IPBerlin griffen unsere Kritikpunkte spontan auf und haben ihre Server-Einstellungen geändert. GMX, Web.de und die Telekom wollen bis zum Frühjahr reagieren und unter anderem die fehlende Forward Secrecy nachrüsten. Sollten Sie darauf nicht warten wollen, weil Sie die Notwendigkeit erkannt haben, Ihren Mail-Anbieter zu wechseln, finden Sie im Beitrag ab Seite 32 eine Anleitung dazu. (jo)

Alle Links zum Artikel
www.ct.de/hb1401020

Outlook.com	Posteo	Privat DE Mail	runbox	Secure – Mail.biz	T-Online	VFEmail	Web.de	Yahoo
www.outlook.com	https://posteo.de	https://privatdemail.net/de	https://runbox.com	https://secure-mail.biz	https://email.t-online.de/ipad/	https://www.vfemail.net	https://web.de	https://mail.yahoo.com
USA	Deutschland	Deutschland	Norwegen	k. A.	Deutschland	k. A.	Deutschland	USA
k. A.	Deutschland	Ägypten[1]	Norwegen	Russland/Island	Deutschland	USA	Deutschland	k. A.
kostenlos	1 €/ Monat	kostenlos	14,95 €/ Jahr	3,33 € monatlich	kostenlos	kostenlos	5 €/ Monat	kostenlos
✓	✓	✓	✓	✓ (FreeMail)	✓	✓ (Copper Account)	✓ (FreeMail)	✓
–	bar, Überweisung, PayPal	–	bar, Überweisung, PayPal, Kreditkarte	PayPal, WebMoney, Perfect Money, paysafecard	–	Kreditkarte, PayPal, Bitcoin	Lastschrift, Kreditkarte, Überweisung	–
–	✓	–	✓	✓	–	✓	–	–
–	1 Monat	–	1 Jahr	1 Monat, 3 Monate	–	Monat/ Jahr	1 Jahr	–
–	14 Tage	–[2]	– (muss nicht gekündigt werden)	– (muss nicht gekündigt werden)	–	– (muss nicht gekündigt werden)	1 Monat vor Ablauf	–
Office 365: ab 10 €/Monat für private Nutzung	0,25 €/zus. GByte Speicherplatz, Monat; 10 Cent/zus. Alias, Monat; 10 Cent/zus. Kalender, Monat	–	1 GByte zus. Speicherplatz: 12,95 €/Jahr; E-Mail-Domain: 4,95 €/Jahr	FreeMail: 45 MByte Speicherplatz, kostenlos; TopMail: 5 GByte Speicherplatz, 25 €/Jahr	Mail & Cloud M: 15 GByte Speicherplatz, 50 Frei-SMS	u. a. Silber: 3 GByte Speicherplatz, Server in den Niederlanden, 10 US-$/Jahr	FreeMail: 1024 MByte E-Mail-Speicherplatz, kostenlos	Ad Free: 34,99 €/Jahr, bezahlbar mit PayPal oder Kreditkarte

Mail-Dienste – Testergebnisse

Name	aikQ	GMX	Google Mail	JPBerlin	mail.de	MyKolab	Neomailbox
Basis-Funktionen							
getesteter Tarif	Paket Q	TopMail	Einheitstarif	JustMail	FreeMail	Lite (mail only)	Offshore Secure Email
POP3 / IMAP	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	–/✓	✓/✓
Inklusiv-Adressen	10	50 + 20 FunDomain	1	1	11	20	1
Adresse unter eigener Domain möglich?	✓	–	–	–	✓	✓ (12 CHF/Jahr)	✓
Inklusiv-Speicherplatz	10 GByte	10 GByte[1]	15 GByte	1 GByte	2 GByte	2 GByte	1 GByte
maximale Größe der Mails	50 MByte	100 MByte	25 MByte	58,5 MByte	60 MByte	50 MByte	50 MByte
Web-Mailer / eigene App / Tor Hidden Service	✓/✓/–	✓/✓/–	✓/✓/–	✓/–/–	✓/–/–	✓/–/–	✓/–/–
Basis-Sicherheitsfunktionen							
maximale Passwortlänge	18+	18+	18+	18+	18+[12]	18+	18+
Spamfilter	✓	✓	✓	✓	✓	✓	✓
Malware-Schutz: Eicar geblockt?	✓	✓	✓	✓	✓	✓	–
Verschlüsselung							
SMTP: Cipher	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1.2 AES128	TLSv1 AES256	TLSv1 AES256 /	TLSv1.2 AES256	TLSv1.2 AES256
SMTP: PFS / PFS erzwungen	–/–	✓/✓	✓/✓	✓/✓	✓/✓[9]	✓/✓	✓/✓
POP: Cipher	TLSv1.2 AES256	TLSv1 AES256	TLSv1.2 AES128	TLSv1 AES256	TLSv1.2 AES128	TLSv1.2 AES256	TLSv1.2 AES256
POP: PFS / PFS erzwungen	–/–	–/–	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
IMAP: Cipher	TLSv1.2 AES256	TLSv1 AES256	TLSv1.2 AES128	TLSv1 AES256	TLSv1.2 AES128	TLSv1.2 AES256	TLSv1.2 AES256
IMAP: PFS / PFS erzwungen	–/–	–/–	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
SMTP-Auslieferung[4]: Cipher	–	TLSv1.2 AES128	TLSv1 ARCFOUR[4]	TLSv1 AES256/	TLSv1.1 AES256	TLSv1.2 AES256	TLSv1.2 AES256
SMTP-Auslieferung[4]: PFS	–	✓	–[4]	✓	✓[11]	✓[11]	✓[10]
SMTP-Eingang (MX, starttls): Cipher	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1.2 AES128	TLSv1 AES256	TLSv1.1 AES256	TLSv1.2 AES256	TLSv1.2 AES256
SMTP-Eingang (MX): PFS / PFS erzwungen	–/–	✓/✓	✓/✓	✓/✓	–/–	✓/✓	–/–
HTTPS: Cipher	TLSv1 RC4-SHA	TLSv1 RC4-SHA	TLSv1.2 AES128	TLSv1 AES256	TLSv1.2 AES128	TLSv1.2 AES256	TLSv1.2 AES256
HTTP: PFS / PFS erzwungen	–/✓	–/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Web-Mailer: Datenschutz und Sicherheit							
HSTS	–	–	–	✓[9]	✓[9]	–	–
Extended Validation	–	–	–	–	–	–	–
RSA-Schlüssel (Länge/Bit)	2048	2048	2048	2048/4096	2048	2048	2048/4096
OCSP	✓	✓	✓	✓	✓	✓	–[5]
Tracking-Test / ggf. Anzahl nicht bestand. Tests	–/8[3]	✓	–/3	✓	✓	✓	✓
blockiert externe Bilder / Proxy	✓/–	–/–	–/✓	✓/–	✓/–	✓/–	✓/–
PGP: erkennen / nutzen	–/–	–/–	–/–	–/–	–/–	–/–	✓/✓
S/MIME: Erkennen / nutzen	✓/✓	–/–	–/–	–/–	–/–	–/–	✓/–
Web-Mailer: sonstige Funktionen							
verwendete Web-Mailer-Software	b1gMail	eigene	eigene	Roundcube	eigene	Roundcube	Horde
Web-Mailer mit Smartphone / Tablet nutzbar	✓/✓	✓/✓	✓/✓	–/✓	–/✓	–/✓	–/–
IMAP-Ordner / 3 Ebenen	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Filter	✓	✓	✓	✓	✓	✓	✓
Volltextsuche auf dem Server	–	–	✓	✓	✓	✓	✓
Adressbuch / -Sync	✓/✓ (beta)	✓/–	✓/✓	✓/–	✓/✓	✓/✓	✓/–
Kalender / Online-Festplatte	✓/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓	✓/–
Sonstiges	Aufgabenverwaltung, Notizen, RSS-Reader	Media-Center, SMS-Versand, Fax etc.	alle Google-Dienste	–	–	Groupware, Active-Sync-Synchronisation	RSS-Reader
Bewertung							
Basis-Sicherheitsfunktionen	⊕⊕	⊕⊕	⊕⊕	⊕⊕	⊕⊕	⊕⊕	○
sichere Verschlüsselung	⊖⊖	⊖	⊕	⊕⊕	⊕	⊕⊕	⊕
Datenschutz und Sicherheit beim Web-Mailer	⊖	⊕	○	⊕	⊕	⊕	⊕

[1] 100 MByte/ Monat zusätzlich [2] kein Web-Mailer [3] darunter Meta Refresh und Meta iFrame Refresh [4] evtl. durch den Heise-Server beschränkt [5] IMAP, POP, SMTP, HTTPS [6] IMAP, POP, SMTP

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden k. A. keine Angabe = schlecht = gefährlich

Outlook.com	Posteo	Privat DE Mail	runbox	Secure – Mail.biz	T-Online	VFEmail	Web.de	Yahoo
Einheitstarif	Postfach	Privat DE Mail	Micro	ProMail	Freemail	Copper Account	Web.de Club	Einheitstarif
✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
> 5	3	1	11	6	10	1	20	1
–	–	–	✓ (69,95 €/Jahr)	–	–	✓	✓ (0,99 €/Monat)	–
7 GByte	2 GByte	500 MByte	1 GByte	15 GByte	1 GByte	50 MByte	unbegrenzt	1 TByte
50 MByte	50 MByte	10 MByte	100 MByte	15 MByte	32 MByte	50 MByte	50 MByte	50 MByte
✓/✓/–	✓/–/–	✓/–/✓	✓/–/–	✓/–/–	✓/–/–	✓/–/✓	✓/✓/–	✓/✓/–
<= 16	18+	18+	18+	18+	<=16	18+	18+	18+
✓	✓	✓	✓	✓	✓	✓	✓	✓
–	✓	✓	✓	–	✓	✓	✓	–
TLSv1 3DES	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 AES256	TLSv1.2 AES256	SSLv3/TLSv1 3DES	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 RC4
–/–	✓/✓	✓/✓	✓/✓	–/–	–/–	–/–	✓/✓	–/–
TLSv1 3DES	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1.2 AES256	SSLv3 3DES	TLSv1 AES256/✓/✓	TLSv1 AES256	TLSv1 RC4
–/–	✓/✓	✓/✓	–/–	–/–	–/–	✓/✓	–/–	–/–
TLSv1 AES128	TLSv1.2 AES256	TLSv1.2 AES2564	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 AES256	TLSv1 AES256	TLSv1 AES256	TLSv1 RC4
–/✓	✓/✓	✓/✓	–/–	–/–	–/–	✓/✓	–/–	–/–
–[11]	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 AES256	TLSv1.2 AES256	TLSv1.0 AES256	TLSv1 AES256/	TLSv1.2 AES128	TLSv1AES256
–	✓	✓	–	✓	–	✓[10]	✓[11]	✓
–	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 AES256	TLSv1.2 AES256	SSLv3/TLSv1 3DES/AES	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 CAMELLIA256
–/–	✓/✓	✓/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓	✓/✓
TLSv1 AES128	TLSv1.2 AES128	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1.2 AES256	TLSv1 RC4	TLSv1.2 AES256	TLSv1 RC4	TLSv1.2 AES256
–/✓	✓/✓	✓/✓	✓/✓	✓/✓	–/✓	✓/✓	–/✓	✓/✓[9]
–	✓	✓	–	✓	–	–	–	–
✓	✓	–[8]	✓	–	–	–	–	–
2048	2048	4096	2048	2048	2048	2048	2048	2048
✓	✓	–[6]	✓	✓	✓	–[7]	✓	✓
–/11	✓	–[2]	–/1	–/9[3]	–/8	✓	✓	✓
–/✓	✓/–	–/–[2]	✓/–	✓/–	✓/–	✓/–	✓/–	✓/–
–/–	–/–	–/–[2]	–/–	–/–	–/–	✓/✓	–/–	–/–
–/–	–/–	–/–[2]	✓/–	✓/✓	–/–	✓/–	✓/✓	–/–
eigene	Roundcube	–	eigene	b1gmail	eigene	Horde	eigene	eigene
✓/✓	–/✓	–/–[2]	–/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓
✓/✓	✓/✓	–/–[2]	✓/✓	✓/✓	✓/✓	✓/✓	✓/–	✓/✓
✓	✓	–[2]	✓	✓	–	✓	✓	✓
✓	✓	–[2]	–	–	–	✓	–	✓
✓/✓	✓/✓	–/–[2]	✓/–	✓/–	✓/–	✓/–	✓/–	✓/✓
✓/✓	✓/–	–/–[2]	–/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/–
Office Web-Apps, Chat per Skype	–	–	–	Aufgabenverwaltung, Notizen	–	Aufgabenverwaltung, Notizen	Office, Club-Rabatte, Prämien, werbefrei	alle Yahoo-Dienste
⊖	⊕⊕	⊕⊕	⊕⊕	○	⊕	⊕⊕	⊕⊕	○
⊖⊖	⊕⊕	⊕⊕	⊖	○	⊖⊖	○	⊖	⊖⊖
○	⊕	–	○	⊖	○	○	⊕	⊕

[7] HTTPS [8] eigene CA, deshalb Zertifikatswarnung [9] während des Tests umgestellt [10] nur SMTPS, kein starttls [11] nur starttls, kein SMTPS [12] zusätzlich per App

c't

E-Mails und Kontakte umsiedeln

Stellt sich der Mail-Anbieter als unsicher heraus, sollte man sein elektronisches Postfach schleunigst zu einem anderen Dienst umziehen. Für die Flucht nach vorn gibt es verschiedene Strategien, die wir hier mit Tipps und Tricks vorstellen.

Von **Daniel Berger**

Besonders einfach gestaltet sich der Umzug, wenn Ihre Mails auf einem Mailserver liegen und der neue Anbieter über einen Sammeldienst verfügt: Dieser ruft die alten Konten ab und lädt deren Inhalte ins neue Postfach. Der Nutzer kann einstellen, ob sie dabei auch gleich vom alten Mailserver gelöscht werden sollen.

Neue Mails landen ebenfalls im Posteingang: Der Sammeldienst von Posteo etwa ruft alle 30 Minuten drei Monate lang Mails von den Fremd-Accounts ab. Diese Frist kann man wiederholt um drei Monate verlängern. Ähnlich funktionieren auch die Sammeldienste beispielsweise von aikQ, Yahoo Mail, Outlook.com, Web.de oder GMX. GMail schaufelt aus bis zu fünf Accounts Nachrichten ins Postfach, der Abruf erfolgt mit POP3. Google bietet zudem ein kleines Windows-Programm, das Nachrichten, Kontakte sowie Termine aus Outlook zu GMail transferiert (siehe c't-Link am Ende des Artikels).

KOMFORT KOSTET

Einige Dienstleister haben sich auf die Mail-Migration spezialisiert und erledigen gegen ein Entgelt die Fleißarbeit. Eines dieser Umzugsunternehmen ist Audriga aus Karlsruhe, das für knapp 12 Euro einen Mail-Account dupliziert. Die Übertragung wird mit SSL verschlüsselt – sofern die verwendeten Mail-Provider das unterstützen. Für seinen Umzugsdienst nutzt Audriga die Infrastruktur externer Anbieter; derzeit sind das Amazon mit Servern in Irland sowie domainFactory aus Deutschland. Die Daten werden von einem Server abgerufen und direkt auf einen anderen kopiert, wobei die Quelldaten auf dem Ausgangsserver bleiben. Das hat den Vorteil, dass Sie sich das Hochladen über die eigene Leitung sparen. Testweise kann man kostenlos Mails der vergangenen zehn Tage übertragen lassen, wobei das Datenlimit bei 20 MByte liegt.

Für den bequemen Umzug müssen Sie Audriga Ihre Zugangsdaten anvertrauen. Das Unternehmen verspricht, diese verschlüsselt zu speichern und nach der erfolgreichen Mail-Übertragung zu löschen. Wenn Sie ganz sichergehen wollen, sollten Sie Ihr Mail-Passwort nach abgeschlossenem Transfer ändern.

Die Handhabung gestaltet sich sehr einfach: Eine Schritt-für-Schritt-Anleitung führt den Nutzer durch den Umzugsprozess, der komplett online abgewickelt wird; eine Software-Installation entfällt. Aus zwei Listen wählen Sie die Anbieter aus oder tragen die Server- und Zugangsdaten selbst ein. Audriga verrät dann die geschätzte Umzugsdauer. Laut eigener Angaben liegt der Datendurchsatz zwischen 0,25 und 1 GByte pro Stunde. Ein Protokoll informiert über den Verlauf der Übertragung. Möglich ist auch der parallele Umzug mehrerer Accounts sowie deren Zusammenführung in ein Postfach.

Konkurrierende Anbieter wie MigrationWiz, YippieMove oder MoveMyMail sind bei ähnlichem Funktionsumfang zwar billiger als Audriga, haben ihren Sitz aber in den USA. Vor der neugierigen NSA sind Ihre Mails dort schlechter geschützt als hierzulande.

MAILER UND SAMMLER

Mehr Kontrolle über die Migration haben Sie, wenn Sie den Umzug selber in die Hand nehmen. Deshalb lohnt sich die Installation eines Mail-Clients, selbst wenn Sie Ihr Mail-Konto gewöhnlich über eine Weboberfläche verwalten. Der digitale Umzug fällt nämlich mit einem Mail-Programm wie Outlook, Opera Mail oder Thunderbird unkompliziert aus: Per Drag & Drop schieben Sie Mails und Ordner aus Ihrem alten

Account einfach in den neuen - sofern Ihr neuer Mailanbieter den Zugriff per IMAP anbietet. Ein Abruf über dieses Protokoll belässt die Mails auf dem Server; außerdem ermöglicht IMAP im Gegensatz zu POP3 auch den Upload von Nachrichten. Der große Vorteil von IMAP ist zudem, dass Sendedatum sowie der Status einzelner Mails beim Kopieren nicht verloren gehen: Gelesene, weitergeleitete und beantwortete Nachrichten bleiben als solche gekennzeichnet.

Um E-Mails zwischen Konten hin- und herzubewegen, legen Sie in Thunderbird einfach den neuen Account parallel zu Ihrem alten Postfach an: „Datei/Neu/Existierendes E-Mail-Konto".

Statt Mails zu verschieben, können Sie die Nachrichten auch kopieren - dann verbleiben sie zusätzlich in Ihrem alten Account. Markieren Sie dazu die Mails, die Sie kopieren möchten; mit STRG+A selektieren Sie sämtliche Nachrichten in einem Ordner. Über einen Rechtsklick und „Kopieren in/neue@mailadresse.de/Posteingang/" klonen Sie die Nachrichten in ein anderes Postfach. Ordner können Sie auf diese Weise mit Thunderbird allerdings nicht direkt duplizieren: Zuerst müssen Sie manuell alle Verzeichnisse im neuen Account anlegen, um anschließend Mails hineinzukopieren. Diese Methode kostet etwas Zeit, bietet aber immerhin den Anlass, das eigene Postfach von Werbemüll und traurigen Liebes-Mails zu befreien.

Thunderbird überträgt die Nachrichten samt ihrer Anhänge auf den neuen Mailserver. Das kann, je nach Umfang des Postfachs und Verbindungsgeschwindigkeit, eine Weile dauern. Bei einem umfangreichen Postfach ist es daher sinnvoll, nicht gleich alle Ordner und Nachrichten auf einmal zu verschieben, damit es nicht zu Problemen wie einem Time-out kommt. GMail etwa beschränkt die Datenmenge, die man täglich über IMAP absaugen kann - bietet dafür aber die Möglichkeit, das komplette Postfach mit Google Takeout im mbox-Format herunterzuladen. Für den Upload einer solchen Mailbox reicht der Funktionsumfang von Thunderbird leider nicht aus.

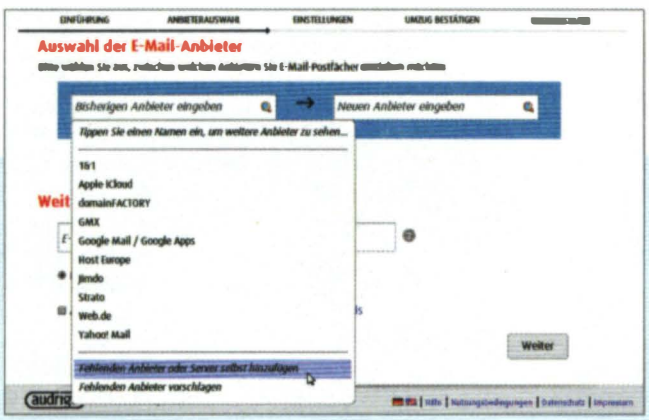
SPEZIALISTEN

Zusammengefasste Mailboxen im mbox-Format kriegen Sie mit einem Spezialprogramm wie IMAPSize in Ihr neues Postfach. Das Tool beherrscht zudem den Upload von Einzel-Mails im eml-Format. Außerdem ist der Umzug mit diesem kostenlosen Windows-Programm ein Stück bequemer: Das Tool zieht den kompletten Inhalt eines Postfachs auf den Rechner und lädt ihn von dort in den neuen Account. IMAPSize eignet sich nicht nur als Backup-Programm, Sie können damit auch einzelne Dateianhänge löschen, um Ihren Mail-Account zu entschlacken.

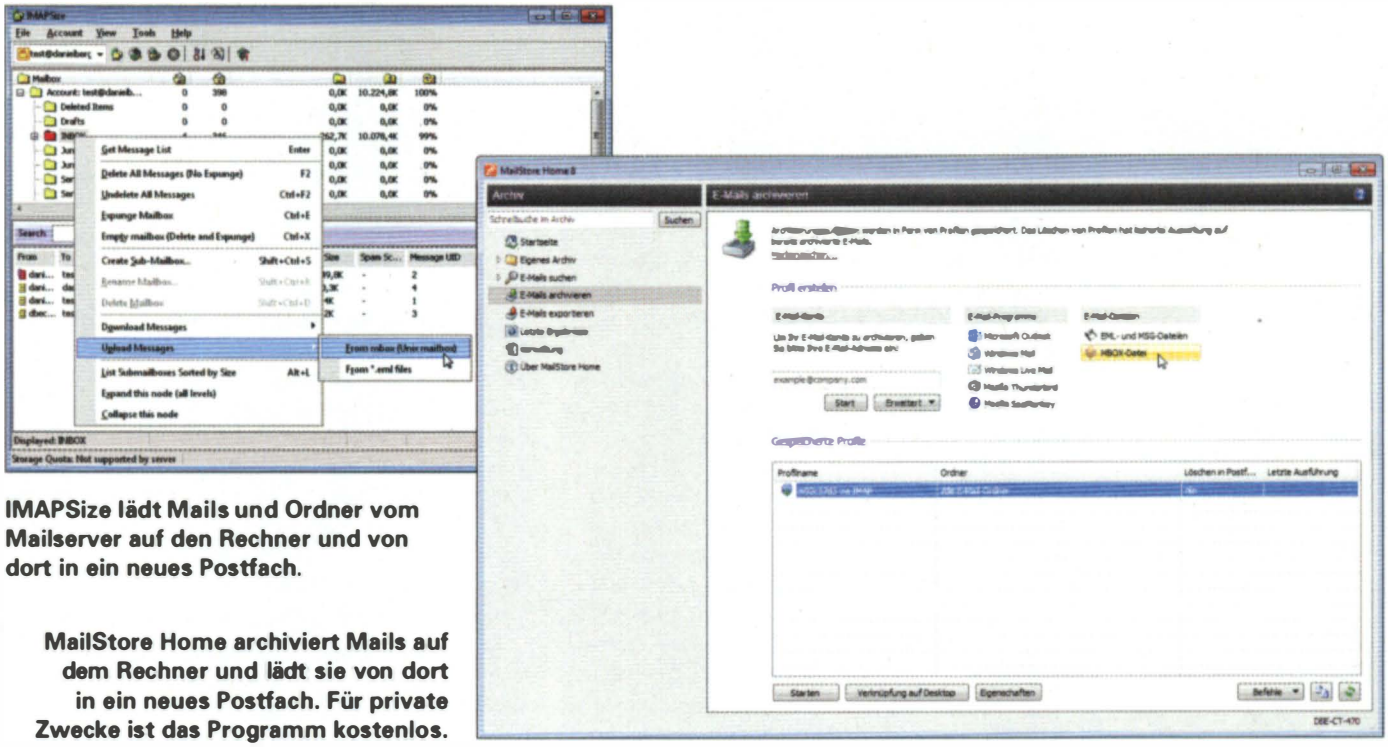
Ein anderer Spezialist, der Mails direkt von Server zu Server kopiert, ist das Perl-Skript imapsync von Gilles Lamiral. Die Bedienung läuft über die Kommandozeile und ist deshalb nicht so komfortabel wie mit einer grafischen Oberfläche. Dafür punktet das Kopierskript mit einem großen Funktionsumfang. In der einfachsten Form sind drei Zeilen nötig, um zwei Accounts zu synchronisieren:

```
imapsync \
--host1 imap.anbieter1.de --user1 dbe1 --password1 12345 \
--host2 imap.anbieter2.de --user2 dbe2 --password2 56789
```

Den IMAP-Server bestimmen Sie mit host und die Zugangsdaten mit user sowie password. Lamiral stellt auf seiner Webseite Anleitungen für Installation und Betrieb seines Tools zur Verfügung und gibt Hinweise zur Sicherheit (s. c't-Link). Wer das volle Potenzial von imapsync ausschöpfen will, muss etwas herumprobieren.



Die bequemste Variante: Schritt für Schritt führen Anbieter wie Audriga durch den Umzugsprozess. Der Nutzer spart sich so den Upload über die eigene Leitung.



IMAPSize lädt Mails und Ordner vom Mailserver auf den Rechner und von dort in ein neues Postfach.

MailStore Home archiviert Mails auf dem Rechner und lädt sie von dort in ein neues Postfach. Für private Zwecke ist das Programm kostenlos.

Die Einarbeitung lohnt aber nur für Mail-Nomaden, die öfter umziehen, zumal das Skript 50 Euro kostet.

Wer es eilig hat und eine bequemere Lösung sucht, schaut sich MailStore Home an: Die Software sichert Mail-Postfächer als zentrales Archiv auf dem Windows-PC und ist für private Anwender gratis. Die heruntergeladenen Mails kann man verwalten, durchsuchen und in ein anderes IMAP-Postfach exportieren (siehe Seite 64).

POP! POP!

Wenn Sie Ihre Mails mit POP3 abholen, werden sie im Normalfall vom Mailserver gelöscht – wenn man das Mail-Programm nicht angewiesen hat, sie dort zu belassen. Sie existieren dann lediglich lokal auf Ihrer Festplatte. Verfügt Ihr neuer Anbieter über einen IMAP-Zugang, können Sie die Nachrichten aus Ihrem Mail-Programm einfach in den neuen Account schieben oder kopieren. Oder Sie verwenden das bereits erwähnte MailStore Home, das lokale Mails von Outlook, Windows Mail, Live Mail sowie Thunderbird ausliest und sie dann in ein Mail-Konto lädt.

Bietet Ihr neuer Anbieter allerdings nur einen POP3-Zugang, erschwert das den Umzug: Sie können nicht einfach mittels Mail-Programm Nachrichten verschieben oder kopieren, weil POP3 keinen Upload von E-Mails ermöglicht. Einen Workaround bieten Add-ons wie etwa Mailredirect für Thunderbird (siehe c't-Link). Mit der Erweiterung können Sie Mails an den neuen Account umleiten („bouncen"), ohne dass Sendedatum, Mailheader oder Absenderadresse verfälscht werden – beim normalen Weiterleiten wäre das der Fall. Outlook und Apple Mail haben eine solche Umleitungsfunktion bereits eingebaut. Ansonsten kann MailStore Home die Mails via SMTP in einen Mail-Account ohne IMAP schicken – wobei der Posteingangsserver eventuell die Verbindung kappt, wenn er zu viele Mails in einem Rutsch erhält.

Alle Links zum Artikel
www.ct.de/hb140132

KONTAKTE UND ADRESSEN

Die meisten Mail-Anbieter mit Webmailer verwalten auch Adressbücher und können diese in der Regel im- und exportieren. Für Kontaktinformationen haben sich das CSV- sowie das vCard-Format etabliert.

Der Nachteil von CSV ist allerdings die fehlende Standardisierung: Weder die Feldbezeichnungen noch die Reihenfolge der Felder ist festgelegt, weshalb Sie beim Einpflegen in ein Adressbuch nachhelfen müssen. Das allerdings ist beim Import über das Webinterface der Mail-Anbieter selten möglich. Man muss also darauf hoffen, dass die Konvertierung fehlerlos klappt – was aber oft genug nicht der Fall ist. Weniger

Probleme bereitet das standardisierte vCard-Format. Thunderbird bietet während des Imports von CSV-Dateien („Extras/Importieren") einen kleinen Editor, mit dem Sie die Adressbuchfelder zuordnen. Setzen Sie Häkchen bei den Feldern, die befüllt werden sollen. Mit den Schaltflächen „Nach oben" und „Nach unten" verschieben Sie nun die Angaben, bis etwa „Primäre Mail-Adresse" mit der jeweiligen Mail-Adresse korrespondiert. Diese Zuordnung kann eine ziemlich pfriemelige Arbeit sein. Hilfreich ist da ein Blick in die CSV-Datei mit Excel, um den Feldern die korrekten Namen zuzuordnen. Outlook.com, GMX und Web.de rücken Kontakte allerdings nur im CSV-Format heraus. Die großen US-Anbieter GMail und Yahoo Mail exportieren auch im vCard-Format. Der Import von korrekten vCards klappt über das Frontend der Mail-Anbieter sowie mit Thunderbird problemlos und schnell. Um Thunderbird Adressen als vCards zu entlocken, benötigen Sie die Erweiterung MoreFunctionsForAddressBook.

Einige Anbieter wie Posteo oder GMail ermöglichen die Synchronisation zwischen Ihren Online-Adressbüchern und denen der Mail-Programme über den CardDAV-Standard. Sie können Ihre Kontakte mit der komfortablen Import-Funktion über das Webinterface des Mail-Anbieters einlesen und die Adressen dann mit Ihrem Mail-Programm abgleichen. Sie müssen dazu lediglich das passende Plug-in installieren: Für Outlook gibt es iCal4OL von Roland Scherrer und für Thunderbird SOGo Connector (siehe c't-Link).

Haben Sie Mails und Kontakte in Ihren neuen Account übertragen, sollten Sie in der Übergangsphase einen „Nachsendeauftrag" bei Ihrem alten Provider einrichten, der Mails an die neue Adresse weiterleitet. Ein solches E-Mail-Forwarding können Sie bei allen großen Anbietern einrichten. Zusätzlich können Sie eine automatische Abwesenheitsnachricht konfigurieren und darin über Ihre neue Mail-Adresse informieren. (dbe)

Import- und Export-Funktionen erleichtern den Umzug von Adressbüchern – hier bei MyKolab. ct

Alternativen zur E-Mail

Das technische Konzept von E-Mail bietet sehr viele Angriffspunkte. Daher liegt es nahe, sich nach einem anderen, besser geschützten Kommunikationsmittel umzusehen. Wir haben uns die Alternativen De-Mail und den E-Postbrief, aber auch Exotisches wie Bitmessage und Dark-Mail genauer angesehen.

Von **Holger Bleich, Axel Kossel**

Dem System E-Mail schenkt man in Deutschland traditionell kaum Vertrauen, wenn es ernst wird: Behördengänge lassen sich rechtlich nicht dadurch ersetzen, der Austausch vertraulicher Informationen, beispielsweise Patientendaten, via Mail ist tabu. Der Einsatz von qualifizierter Verschlüsselung für Bürger-Amt-Kommunikation scheiterte an hohen gesetzlichen Hürden und damit verbundenen Kosten.

Inzwischen sind die Ansprüche an Sicherheit und Vertraulichkeit aber gesunken. Ein Beispiel ist das De-Mail-Gesetz, das die Rahmenbedingungen für rechtssichere und vertrauliche Kommunikation auf elektronischem Weg vorgibt. De-Mail-Dienste müssen sich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizieren lassen. Per De-Mail verschickte Nachrichten ersetzen unterschriebene Schriftstücke, die als Brief, Einschreiben oder eigenhändige Sendung ausgeliefert werden.

Hartnäckig hält sich das Gerücht, dass Inhaber eines De-Mail-Kontos verpflichtet seien, dieses ebenso wie den Briefkasten regelmäßig auf eingegangene Nachrichten zu prüfen. Sonst drohe Ärger, wenn man ein wichtiges Schreiben übersehe. Das stimmt so nicht. De-Mail ersetzt den herkömmlichen Zustellweg nur, wenn man das mit dem jeweiligen Kommunikationspartner, also etwa einer Behörde, explizit vereinbart hat. Dann gilt allerdings die sogenannte „Zustellfiktion": Eine im Postfach eingegangene De-Mail gilt als formell zugestellt.

PAY-MAIL

Zertifizierte De-Mail-Anbieter sind die Deutsche Telekom, 1&1 mit GMX und Web.de sowie Mentana Claimsoft. Die Deutsche Post war mit ihrem E-Postbrief vorgeprescht, hat aber bis heute keine De-Mail-Zertifizierung.

Beide Systeme verlassen den standardisierten Austausch mit SMTP und setzen stattdessen jeweils auf eine zur konventionellen E-Mail inkompatible Infrastruktur. Das heißt: Mails lassen sich nur jeweils zwischen De-Mail-Kunden oder E-Post-Kunden austauschen. Übergänge zwischen den Systemen oder zu E-Mail gibt es nicht. Bis auf eine Ausnahme: Möchte ein E-Post-Kunde einen Empfänger außerhalb erreichen, druckt die Post die Nachricht aus und stellt sie als Papierbrief zu.

Dieser Service ist vielleicht das beste Argument für den Post-Service, bei dem ansonsten zumindest Privatpersonen trotz der laut Post siebenstelligen Nut-

zerzahlen kaum Kommunikationspartner finden. Dass die Briefe zunächst elektronisch an das dem Absender nächstgelegene Briefzentrum übertragen werden, hält den Zustellweg für den physischen Brief kurz. Die Zustellung am Folgetag ist daher die Regel.

Ein solcher Brief mit maximal drei Seiten kostet 60 Cent Porto. Dasselbe bezahlt man für die elektronische Zustellung eines maximal 20 MByte großen E-Postbriefs. Und hier liegt das Problem: Trotz teurer Werbeaktionen ist es der Post nicht gelungen, das Bezahlen für elektronische Post in die Köpfe der Verbraucher zu bekommen.

Mit De-Mail kommen zumindest Privatkunden günstiger weg. Bei Web.de und GMX dürfen sie 10 De-Mails im Monat kostenlos versenden, jede weitere kostet ab 39 Cent. Services wie eine Empfangsbestätigung werden wie beim E-Postbrief extra berechnet. Die Telekom bietet De-Mail bis Januar 2015 kostenlos an. Danach sollen ab der vierten Nachricht im Monat 39 Cent fällig werden. Mentana Claimsoft nimmt für jede Nachricht mindestens 58 Cent.

VERTRAUENSSACHE

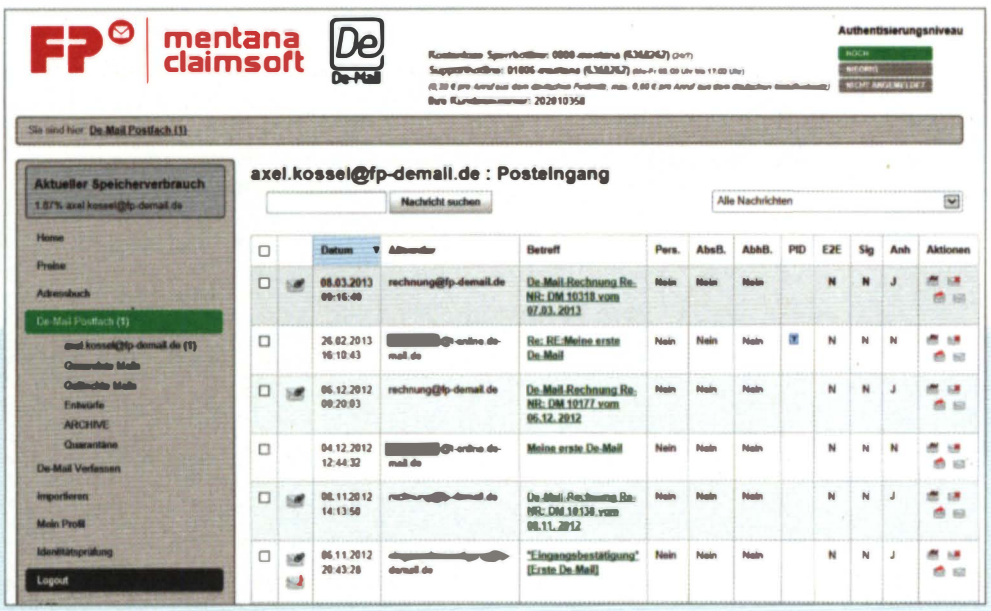
Zu den Konzepten von De-Mail und E-Post gehört die sichere Authentifizierung aller Teilnehmer. Das soll die Vertrauenswürdigkeit gegenüber der gewöhnlichen E-Mail erhöhen und unschönen Dingen wie Spam oder Phishing einen Riegel vorschieben.

Bei E-Post wird die Identität des Nutzers mit Post-Ident geprüft, die De-Mail-Provider schicken entweder einen Mitarbeiter des Dienstleisters Sign Today vorbei, der den Ausweis prüft, oder bitten die Kunden, dazu in einem Telekom- beziehungsweise Hermes-Paket-Shop vorbeizukommen. Bei der Telekom und bei Mentana Claimsoft kann man sich auch bequem mit der eID-Funktion des Personalausweises anmelden, der dann auch den Zugang zum Webinterface sichert. Die Post nutzt das Handy als zweiten Faktor, um die E-Post-Konten vor Passwortdieben zu schützen.

Nachrichten von E-Post und De-Mail-Kunden verlassen die jeweiligen Zustellsysteme nicht - es findet kein Routing durchs Internet statt. So soll sichergestellt sein, dass an keiner Stelle Inhalt von externer Seite abgegriffen werden kann. Alle Server sprechen SSL-verschlüsselt miteinander.

Doch bei beiden Systemen kann von Vertraulichkeit gegenüber dem Dienst dennoch keine Rede sein: De-Mails werden zwar verschlüsselt, doch der Schlüssel liegt bei den Anbietern. Laut De-Mail-Gesetz muss das zum Schutz der Kunden so sein, damit jede Nachricht auf dem Transportweg entschlüsselt und auf Viren hin gecheckt werden kann.

Privatkunden, die auf eine Ende-zu-Ende-Verschlüsselung Wert legen, müssen die Daten etwa mit PGP entweder auf Dateiebene verschlüsseln und als Dokument anhängen oder in der Zwischenablage verschlüsseln und ins Webfrontend kopieren. Für Firmen



Obwohl dieses De-Mail-Konto selten genutzt wurde, gingen regelmäßig Rechnungen ein. Für E-Mail-Nutzer ist das sehr gewöhnungsbedürftig.

bietet Mentana Claimsoft De-Mail-Gateways an, die von Gerät zu Gerät verschlüsseln. Das funktioniert aber nur, wenn beide Seiten die Hardware dieses Anbieters nutzen.

Die Post verzichtet gleich ganz auf Verschlüsselung. Zwar gibt es seit Sommer 2013 mit dem sogenannten „E-Postbrief End-To-End" die angebliche „Lösung für die digitale Kommunikation mit allen Berufsgeheimnisträgern". Doch was die Post verspricht, hält sie nicht, denn auch hier liegt der Schlüssel für die Chiffrierung der Nachrichten beim Betreiber, der die Nachrichten in der Browser-Oberfläche entschlüsselt anzeigt oder sogar ausgedruckt zustellt.

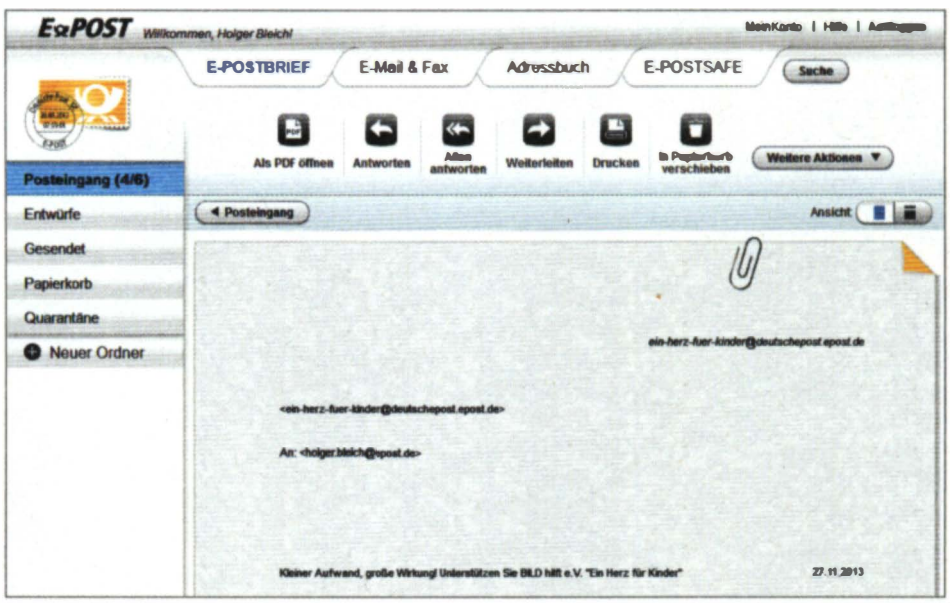
Sichere Ende-zu-Ende-Verschlüsselung bleibt also bei beiden Systemen Aufgabe des Nutzers. Wie bei der E-Mail muss er die Schlüssel selbst verwalten. Er zieht dabei keinen Vorteil aus der Tatsache, dass alle Teilnehmer von De-Mail und E-Postbrief bei der Anmeldung identifiziert wurden. Auch wer mit wem kommuniziert, wird in den Systemen nicht verschleiert. Für die Nachrichten gilt nicht das Brief-, sondern das Fernmeldegeheimnis. De-Mail und E-Postbrief sind der E-Mail in puncto Vertraulichkeit nicht überlegen.

VERSCHLÜSSELUNGSHIMMEL

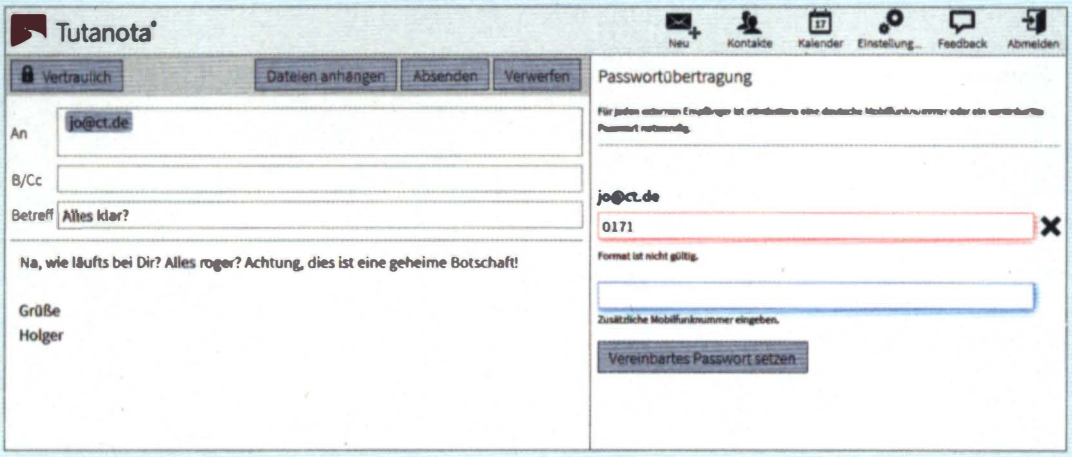
Die Idee eines hermetischen – und zu E-Mail inkompatiblen – Nachrichten- und Speichersystems mit integrierter Ende-zu-Ende-Verschlüsselung ist keineswegs neu. Bereits seit 2002 bietet der kanadische Provider CryptoHeaven eine Infrastruktur, in der echte Ende-zu-Ende-Verschlüsselung funktioniert. Meldet sich der Nutzer dort erstmalig an, generiert er sich wie bei PGP (siehe Seite 82) ein Paar aus öffentlichem und geheimem Schlüssel (RSA mit bis zu 4096 Bit Länge). Der öffentliche Schlüssel landet bei CryptoHeaven, der geheime bleibt auf dem lokalen Rechner oder wird auf ausdrücklichen Nutzerwunsch mit Passphrase gesichert hochgeladen, um überall verfügbar zu sein.

CryptoHeaven-Mails liegen verschlüsselt auf den kanadischen Servern des Anbieters. Der Nutzer verwaltet sie mit Open-Source-Clients, die für Windows, Mac OS und Linux verfügbar sind. Diese Clients sind mit Java realisiert, was alle sicherheitsbewussten Anwender zunächst aufschreien lässt. Allerdings beruhen sie auf einer angepassten Runtime, die sie selbst mitbringen und die unabhängig von einem unsicheren Java läuft, das vielleicht auch auf dem Rechner installiert ist. Alternativ greift der Kunde über ein Web-Frontend auf seinen Account zu. Diese Oberfläche benötigt allerdings eine aktuelle Java-Runtime, von deren Installation als Browser-Plug-in wir aus Sicherheitsgründen dringend abraten.

CryptoHeaven versteht sich nicht nur als abhörsicherer Mail- und Messaging-Service, sondern dient auch als Online-Speicher. Außerdem deuten ein rudi-



Beim E-Postbrief soll es keine Spam-Nachrichten geben, dennoch kommt Werbung an.



Schreibt man jemanden über Tutanota an, kann man dessen Mobilnummer angeben. Er erhält dann die Passphrase, die zum Entschlüsseln nötig ist, per SMS.

mentäres, gruppenfähiges Office-Tool sowie die Preisstruktur darauf hin, dass der Dienst eher für Unternehmen denn für Privatpersonen konzipiert ist. Es ist zwar möglich, aber nicht praktikabel, Nachrichten mit herkömmlichen E-Mail-Nutzern auszutauschen. Eine Metadaten-Analyse des internen Mail-Verkehrs kann nur stattfinden, wenn CryptoHeaven mitspielt und Zugriff auf die Server gibt.

Im Kurztest machte der Service einen ausgereiften, sicheren Eindruck. In den 14 Jahren des Bestehens sind bei CryptoHeaven unseres Wissens keine Sicherheitslücken aufgetreten. Das Konzept trägt, beruht auf quelloffener Software und ist damit überprüfbar. Für ansprechendes Design haben die Kanadier allerdings kein Händchen: Der Web-Auftritt des Unternehmens wirkt abschreckend und alles andere als vertrauenerweckend. Auch die Clients sind nicht sehr hübsch, dafür aber stabil und praktisch. Privatpersonen sind ab 8 US-Dollar monatlich dabei, dafür gibt es allerdings gerade mal ein 200 MByte großes Postfach. Eine kostenlose Trial-Phase lädt zum ersten Probieren ein.

KANALWECHSEL

Eine interessante Methode, vertrauliche Mails verschlüsselt zu übermitteln, hat das deutsche Start-up Tutao entwickelt. Dessen Service Tutanota setzt auf den Austausch von symmetrisch verschlüsselten Nachrichten, die mit einer Passphrase gesichert sind, wel-

che nur den Kommunikationspartnern bekannt ist. Schreibt man an Partner, die keine Tutanota-Nutzer sind, kann man diesen automatisch die Passphrase zum Entschlüsseln der Mail per SMS zuschicken. Die Mail können sie über einen Weblink abrufen.

Derzeit läuft die Betaphase von Tutanota, in der man den Service ausprobieren kann (Links zu allen Services finden Sie unten auf dieser Seite). Die Mails lassen sich nicht per Client abrufen, sondern nur über ein Browser-Frontend verwalten, das auch die Ver- und Entschlüsselung auf dem lokalen Rechner ausführt. Sämtliche Aktionen laufen über ein Web-API, mit dem sowohl das Frontend als auch ein ebenfalls verfügbares Outlook-Add-in für Tutanota kommuniziert.

Bei der Erstanmeldung generiert Tutanota zuerst einen öffentlichen und einen geheimen Schlüssel im Browser. Tutao nutzt RSA mit einer Länge von 2048 Bit, was als sicher gilt. Der öffentliche Schlüssel wird hochgeladen und im Tutanota-System an die Mail-Adresse gebunden, sodass er von anderen Nutzern automatisch verwendet wird. Der private Schlüssel erhält als Passphrase das Nutzer-Passwort für den Dienst und kommt ebenfalls auf die Tutanota-Server.

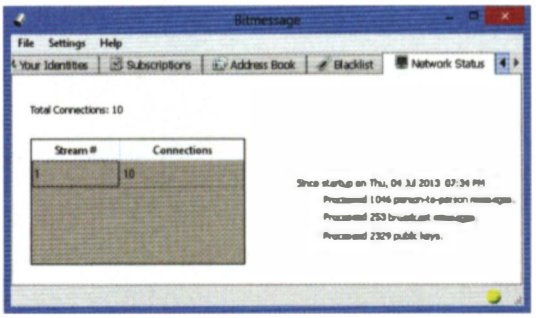
Und hier liegt die Schwäche des Konzepts: Nur das Dienstepasswort schützt vor Lauschangriffen des Services selbst oder Dritter, die sich Zugriff verschaffen. Der Kunde muss darauf vertrauen, dass Tutao die Passwort-Datenbank für den Service gut absichert und gegen Angriffe schützt.

P2P-MAIL

Obwohl viel Hirnschmalz drinsteckt, dürften kleine Insellösungen wie Tutanota wohl kaum an der beherrschenden Position der gängigen Mail-Standards kratzen. Ein großer Wurf bleibt weiter aus. Viele Experten halten es für unmöglich, auf Basis der bestehenden Protokolle IMAP und SMTP einen abhörsicheren, leicht zu bedienenden Mail-Service hinzubekommen, der noch dazu keine Metadaten generiert. Als einzige Alternative gilt unter einigen Mail-Experten derzeit der Umstieg hin zu verschlüsselter Peer-to-Peer-Vernetzung aller Kommunikationsteilnehmer.

Ein „Proof of Concept" existiert mit Bitmessage bereits seit 2012. Die Idee hinter dem Konzept, das aus der Bitcoin-Szene entstanden ist: Verschlüsselte Nachrichten gehen nicht nur an den Empfänger, sondern an alle Teilnehmer des P2P-Netzes. Wer die Nachricht entschlüsseln kann, für den ist sie gedacht. Gehen alle Nachrichten nach dem Broadcast-Prinzip an alle, fallen keine Metadaten an, die die Kommunikationsrichtung und das Ziel verraten.

Bei Bitmessage geht jede Nachricht an viele Empfänger, doch nur der Adressat hat den Schlüssel, um sie zu öffnen. Schnüffler erfahren jedoch nicht, wer das ist.



Dies gelänge umso besser, je mehr Verkehr im Netzwerk herrscht. Allerdings ist bei Bitmessage das Problem der Skalierbarkeit eines solchen Netzes noch ungelöst: Wenn alle Welt Bitmessage statt E-Mail benutzte, wäre das Datenaufkommen unvorstellbar. Protokoll und Client enthalten daher Vorkehrungen, damit sich das Netz bei hohem Aufkommen in mehrere kleinere Netze teilen kann. Man hat das in der Praxis aber noch nicht funktionieren gesehen.

In der gut funktionierenden Referenzimplementierung des bitmessage.org-Clients gilt bislang, dass Nachrichten nach zwei Tagen vom P2PClient automatisch gelöscht werden. Das im (Python-)Quelltext und als Windows-Binary herunterladbare Programm ist noch recht rudimentär. Nachrichten bestehen aus nacktem Text ohne Formatierung und ohne die Möglichkeit von Anhängen. Man müsste einen leistungsfähigen E-Mail-Client hernehmen und auf Bitmessage als Transportmedium umrüsten, um eine gleichwertige Alternative zur Mail zu schaffen. Vorkehrungen und Bestrebungen dazu gibt es bereits.

Den Nachrichteninhalt schützt Bitmessage durch asymmetrische Verschlüsselung: Jeder Teilnehmer erzeugt ein Schlüsselpaar aus geheimem und öffentlichem Schlüssel. Aus Letzterem leitet sich die Bitmessage-Adresse ab. Eine Sicherheitsprüfung durch anerkannte Experten fehlt allerdings noch und im Bitmessage-Forum werden etliche Angriffsszenarien diskutiert. Es ist sicherlich noch zu früh, seine ganze Hoffnung auf dieses System zu setzen.

MAIL 3.0

Der Fall Edward Snowden hat zwei bis dahin fast unbekannte Mail-Provider in den Focus gerückt: Lavabit und Silent Circle. Beide waren mit dem Verspre-

Alle Links zum Artikel
www.ct.de/hb1401036

chen angetreten, verschlüsselte Mail-Übertragung ohne Metadaten anzubieten. Doch die Konzepte hatten Schwächen. Dies bekam besonders Lavabit-Chef Ladar Levison zu spüren, der unter seinen Kunden auch Snowden verzeichnete. Levison wurde vom FBI so stark unter Druck gesetzt, dass er Lavabit Mitte 2013 dichtmachte und die Kundendaten vernichtete. Kurze Zeit später schloss auch Silent Circle, an dem PGP-Erfinder Phil Zimmermann beteiligt ist.

Lavabit und Silent Circle gaben aber nicht auf, sondern stellten der überraschten Öffentlichkeit im vergangenen Oktober ihre Dark-Mail-Initiative vor. Die Dark Mail Alliance habe ein fertiges Konzept für „E-Mail 3.0" in der Tasche, teilte Levison mit. Man wolle bald ein Protokoll und eine Architektur liefern, die eine voreingestellte Ende-zu-Ende-Verschlüsselung ermöglichen, ohne dass Metadaten anfallen. Die Bestandteile dieser Architektur sollen auf Open-Source-Füßen stehen.

Mit diesem nebulösen Versprechen und ohne konkrete technische Details, etwa ein Whitepaper, sammelte Levisons Allianz immerhin mehr als 200 000 US-Dollar auf der Crowdfunding-Plattform Kickstarter ein. Im zweiten Quartal 2014, sollen erster Quellcode und ein Whitepaper erscheinen, versprach er. Fest steht, dass als Protokoll eine Weiterentwicklung des Instant-Messaging-Standards XMPP zum Einsatz kommen soll, und zwar das „Silent Circle Instant Messaging Protocol" (SCIMP). Die erste Implementierung werde „Silent Mail" heißen.

Die Nachrichten sollen auf Servern bei Providern verschlüsselt gespeichert und via SCIMP abrufbar sein, ohne dass Metadaten anfallen. Levison verspricht außerdem eine Open-Source-Komplettlösung für Provider namens „Magma". Sie besteht demnach aus einem JavaScript-Webfrontend sowie einem mit JSON realisierten API zum verschlüsselten Mail-Zugriff. Ein Gateway soll die Verbindung zur klassischen SMTP/IMAP/HTTPS-Infrastruktur beim Provider schaffen können.

In der Mail-Branche herrscht bezüglich Dark Mail eher Skepsis. Viele bezweifeln, dass tatsächlich eine relevante Zahl von Providern Dark Mail implementieren würde. Brian Spector, Chef des Security-Unternehmens CertiVox, glaubt, kein großer Provider tue sich „diesen Stress" an. Als Mail-Hoster habe man sofort die Regierungen auf dem Hals, wenn man keine Kommunikationsdaten herausrücken könne. Dark Mail sei, wie alle alternativen Konzepte, eher etwas für Internet-Freiheitskämpfer, die nicht logisch denken. (hob) c't

Thunderbird statt Webmail

In der indigenen Mythologie fungierte der zornige Donnervogel als Götterbote. Heute kümmert er sich in Form des nach ihm benannten Mail-Clients um die tägliche Nachrichtenflut. Das macht er schon ganz gut – und mit einigen Tipps und Add-ons sogar noch viel besser.

Von **Daniel Berger**

Thunderbird erfreut sich über Windows hinaus großer Beliebtheit. Seine größten Konkurrenten sind nicht unbedingt andere Mail-Clients, sondern die per Browser besuchten Web-Frontends der Mail-Dienste. Viele Nutzer nämlich verwalten ihre Mails ausschließlich darüber. Die Weboberflächen sehen attraktiv aus und sind komfortabel zu bedienen. Warum also überhaupt noch Thunderbird auf dem Rechner installieren? Sicher, der Komfort ist vielleicht einen Tick größer als bei Web-Interfaces. Doch der größte Vorteil ist die Unabhängigkeit: Mit Thunderbird, einer eigenen Domain und Mail-Adresse sind Sie ein Stück autonomer und sicherer vor neugierigen Geheimdiensten. Die großen Mail-Anbieter Gmail oder Yahoo speichern die Nachrichten oft auf ausländischen Servern, wo sie gründlich durchleuchtet werden, um personifizierte Werbung anzuzeigen.

Zusätzliche Verschlüsselung stärkt die Privatsphäre und schützt vor Wortfiltern des BND und neugierigen Werbevermarktern. Mit Thunderbird chiffrieren Sie lokal auf dem eigenen Rechner – mit dem richtigen Add-on ist das ganz unkompliziert. Und eine eigene Domain samt Mail-Adresse gibt es bereits für wenige Euro im Monat. Dank IMAP und POP haben Sie ebenfalls von überall Zugriff auf Ihre Mails. Thunderbird Portable lässt sich sogar auf einem USB-Stick installieren, der sich leicht mitnehmen lässt – nur für das Smartphone gibt es Thunderbird bisher leider nicht.

Den meisten Nutzern reichen die Basisfunktionen, sagt Mozilla. Doch das Programm kann viel mehr, kann inzwischen außer Newsgroups und Feeds auch Facebook- und Twitter-Chats verwalten. Weitere nützliche Funktionen sind oft verborgen, wodurch das Potenzial des Mail-Clients nicht auf den ersten Blick erkennbar ist. Doch mit ein paar Handgriffen spreizt Thunderbird seine heiligen Schwingen.

MULTIPLE PERSÖNLICHKEITEN

In Thunderbird können Sie mehrere Mail-Konten einrichten. Mittels Profilen lassen sich diese auch komplett getrennt voneinander verwalten. Sinnvoll ist das bei privaten und beruflichen Mail-Konten oder wenn mehrere Familienmitglieder denselben PC nutzen.

Um in den Profilmanager zu gelangen, muss man Thunderbird mit dem Parameter „-p" starten. Legen Sie auf dem Desktop eine Verknüpfung an, in deren Eigen-

schaften Sie unter „Ziel" ein -p mit führendem Leerzeichen hinter das letzte Anführungszeichen setzen. Auch in Mac OS und Linux müssen Sie den Parameter anhängen.

Wichtig ist, dass Sie im Profilmanager das Häkchen bei „Beim Starten nicht nachfragen" entfernen, damit das Programm eben doch nachfragt, welches Profil geladen werden soll. Der Zugang zu den Einzelprofilen lässt sich in Thunderbird unter „Einstellungen/Sicherheit" mit einem Passwort schützen. Dieses muss bei jeder Sitzung einmal eingegeben werden. Die aktuelle Version von Thunderbird öffnet beim Start nicht mehr die Standard-Mailbox, sondern merkt sich die Ansicht beim Schließen und stellt diese wieder her. Wie im Browser lassen sich die Posteingänge auch parallel in Tabs öffnen: Rechtsklick auf die Mailbox, dann „In neuem Tab öffnen". So lässt sich schnell von einer in die andere Mailbox springen. Wer so viele Mail-Adressen hat, dass es eng wird, kann statt eines Tab auch ein neues Fenster öffnen - genau so wie bei Firefox.

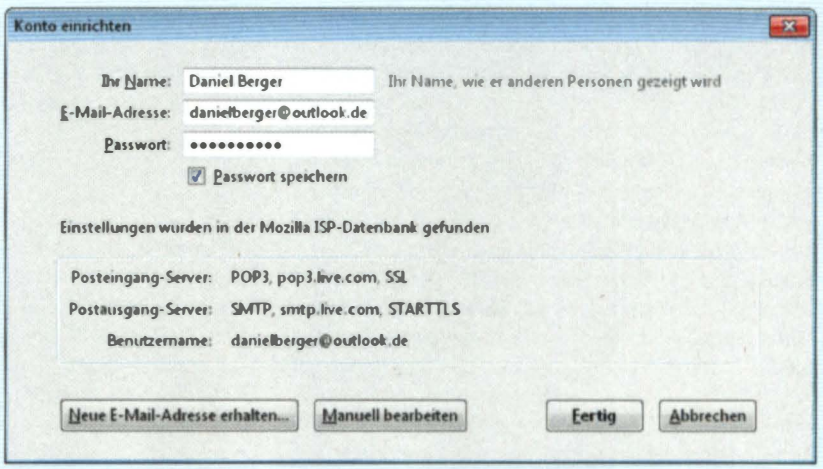
Eine interessante Alternative ist die Unified Mailbox - oder auf Deutsch: der gruppierte Posteingang. Dieser bündelt mehrere Mailboxen; so muss nicht mehr hin und her geklickt werden, wenn im fünften Account eine neue Mail eintrudelt - alles landet an einem Ort. Beim Beantworten einer Mail verwendet das Programm den Ausgangsserver, der für die Empfängerbox angegeben ist. Die zusammengelegte Mailbox versteckt sich unter: „Ansicht/Ordner/Gruppiert".

KONTAKT AUFNEHMEN

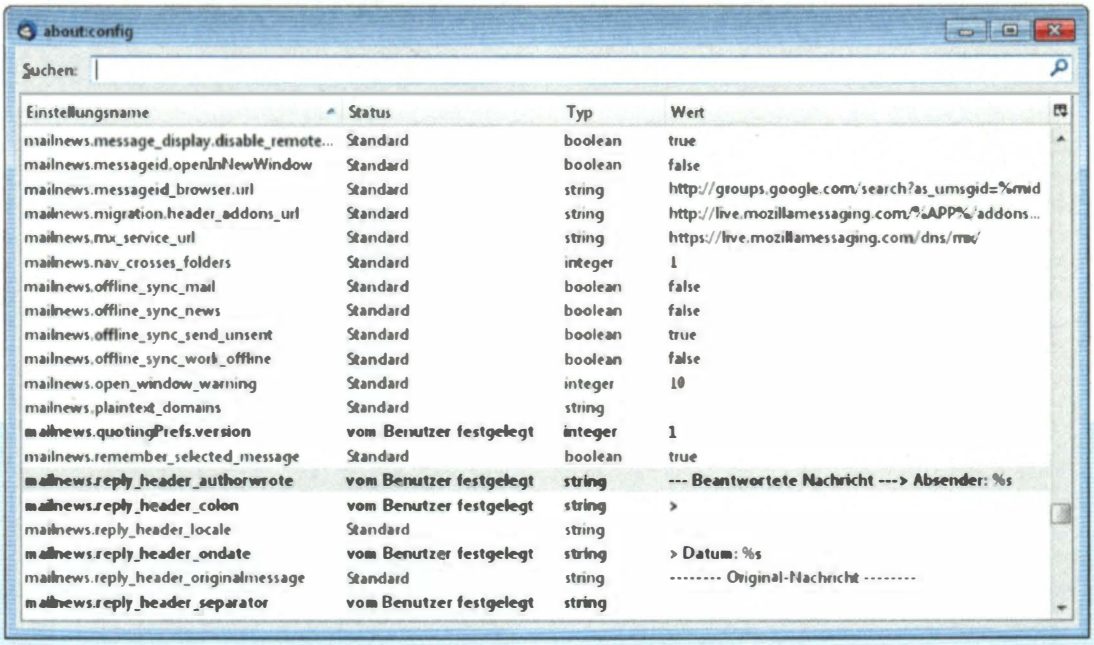
Neuerdings kann Thunderbird auch von Microsofts Exchange-Servern Mails abrufen und darüber Kontakte synchronisieren - dank der Erweiterung ExQuilla von James R. Kent (siehe c't-Link am Artikelende). Ansonsten sei die Verwendung von IMAP empfohlen: Die Mails bleiben auf dem Server und auch die Ordnerstruktur wird dort gespeichert. So kann Thunderbird auf mehreren Rechnern installiert sein und beim Abrufen der Mails werden die jeweiligen Ordner samt Inhalt vom Server übernommen. Die Inhalte bleiben dadurch immer synchron und der Zugriff gestaltet sich komfortabel wie beim Abrufen über ein Web-Interface.

Mails von Gmail lassen sich via IMAP auch mit Thunderbird abrufen und verwalten: Dazu muss IMAP bei Gmail über das Web-Interface aktiviert werden: „Einstellungen/POP/IMAP". Dort sind dann auch alle erforderlichen Zugangsdaten aufgeführt. Einfacher geht die Einrichtung direkt im Thunderbird: Gehen Sie auf „Datei/Neu/Existierende Mail" und tragen Ihre Zugangsdaten ein. Die passenden Server-Daten fischt Thunderbird aus einer Datenbank, in der alle großen Mail-Anbieter vorhanden sind. Die Einrichtung klappt in der Regel wunderbar.

Auch eine GMX-Adresse richtet der Assistent zügig ein, wobei aber nur Premiumkunden auf ihre Nachrichten via IMAP zugreifen können. Kostenlose Konten lassen sich lediglich mit POP abrufen. Dabei belässt Thun-



Mit dem Assistenten geht die automatische Einrichtung von Gmail, Yahoo, GMX und Co. in Thunderbird sehr zügig.



Unter dem Gefieder von Thunderbird können in der about:config viele Einstellungen vorgenommen werden.

derbird die Originalnachricht zwar ebenfalls auf dem Server, löscht diese aber nach 14 Tagen von dort. In den Konten-Einstellungen lässt sich diese Säuberung unter „Server-Einstellungen" abschalten.

Bei eigenen Mail-Domains versagt die automatische Einrichtung gern, weil die individuellen Serverdaten nicht in der Datenbank enthalten sind. Thunderbirds erratener Vorschlag muss deshalb oft händisch korrigiert werden. Denken Sie abschließend daran, die SSL-Verschlüsselung zwischen Mail-Client und Server zu aktivieren.

Sind Konten und Profile eingerichtet und der Erstkontakt mit dem Mail-Server hergestellt, kann es an das Feintuning von Thunderbird gehen. Zunächst sollten Sie entscheiden, ob Sie Mails im HTML- oder im Textformat versenden wollen – Letzteres ist sicherlich unaufdringlicher. Puristen, die auf jede Text-Verschönerung durch HTML verzichten möchten, müssen an zwei Orten Änderungen vornehmen: Im Konten-Menü unter „Verfassen & Adressieren" deaktivieren Sie die Option „Nachrichten im HTML-Format verfassen". Diese Option müssen Sie für jedes einzelne Mail-Konto ändern. Wenn Sie jetzt noch in den allgemeinen Einstellungen unter „Verfassen" die Sende-Optionen zu „Nachrichten in reinen Text konvertieren" ändern, verschickt Thunderbird alle Nachrichten befreit von Formatierungen und bunten Spielereien.

Ähnlich nervig wie grelle HTML-Mails sind lästige Nachfragen bei Empfangsbestätigungen. Diese können in den Einstellungen unter „Erweitert" kaltgestellt werden. In den Konten-Einstellungen lassen sich für einzelne Mailboxen aber auch Ausnahmen von der globalen Regelung bestimmen.

SCHNELLER LOSLEGEN

Bei der Einrichtung kann sich unter Umständen das Deaktivieren der globalen Suche und Indexierung empfehlen – andernfalls lädt sich Thunderbird auch aus einem IMAP-Account alle Mails herunter, speichert sie lokal und beginnt, diese zu indexieren. Das kann eine Weile dauern, je nach Umfang des Posteingangs inklusive seiner Unterordner. Im Gegenzug geht das Finden von Nachrichten dann schneller. In den Konten-Einstellungen können Sie unter „Synchronisation

& Speicherplatz" begrenzen, wie viele Nachrichten lokal gespeichert werden.

Lahmt Thunderbird im Laufe der Zeit, kann das am zu groß eingestellten Cache-Speicher liegen, den Thunderbird bei jedem Start komplett inhaliert und aktualisiert. Den sollte man unter einem Gigabyte halten: „Einstellungen/Erweitert/Netzwerk & Speicherplatz". Hier lässt sich der Cache auch leeren. Ebenfalls können Sie dort die Komprimierung aller Ordner aktivieren. Das erhöht die Geschwindigkeit und entschlackt die lokal gespeicherten Mailboxen, indem längst gelöschte Nachrichten rausgeschmissen werden. Auch auf dem Server lässt sich diese Entschlackung veranlassen: Dazu in den „Server-Einstellungen" die Option „Expunge" aktivieren. Sie sorgt dafür, dass gelöschte Nachrichten nicht nur markiert werden, sondern wirklich aus dem Posteingang verschwinden. Diese Funktion gilt nur für IMAP-Server.

BESSER ANTWORTEN

Je nach Vorliebe lässt sich genau einstellen, wie Thunderbird Antwort-Mails gestaltet. Soll beispielsweise die eigene Antwort über dem zitierten Text erscheinen, lässt sich dies unter „Verfassen & Adressieren" einstellen. Auch der Kopf über der beantworteten Nachricht kann verändert werden: Beispielsweise lässt sich das unnötige Komma vor „schrieb" entfernen. Dazu müssen Sie unter das Gefieder des Thunderbird schauen, wo sich weitere Justierungen in der sogenannten about:config verbergen: „Einstellungen/Erweitert/Konfiguration bearbeiten". In diesem Editor lassen sich unzählige Anpassungen vornehmen. Das überflüssige Komma findet sich im Eintrag mailnews.reply_header_separator, wo es sich durch ein Leerzeichen ersetzen lässt. Und keine Angst: Änderungen lassen sich im Kontextmenü (Rechtsklick) zurücksetzen.

Zusätzlich lässt sich im Antwortkopf hinter der Uhrzeit noch das Wort „Uhr" einfügen. Geben Sie beim Parameter mailnews.reply_header_ondate einfach „Am %s Uhr" ein. Künftig steht dann über von mir beantworteten Mails beispielsweise: „Am 17.01.2014 10:31 Uhr schrieb Daniel Berger". Ein Komma zwischen Datum und Uhrzeit lässt sich leider nicht einfügen.

Der Antwortkopf kann auch komplett umgebaut werden, zum Beispiel in den mehrzeiligen Stil von Outlook. Eine Änderung in der about:config reicht nicht aus, weil dort der Zeilenumbruch \n ignoriert wird. Deshalb müssen Sie im Profilordner die Datei user.js anlegen. Wechseln Sie unter Windows in den Explorer zu „%appdata%\Thunderbird\Profiles". Im jeweiligen Profilordner (zumeist wird nur „default" zu finden sein) legen Sie die Datei an. Die dortigen Einstellungen werden beim nächsten Start von Thunderbird von user.js in die pref.js übernommen – vor dem Experimentieren sollten Sie davon besser eine Sicherheitskopie anlegen. In die user.js tragen Sie nun folgende Zeilen ein:

```
user_pref("mailnews.reply_header_type", 3);
user_pref("mailnews.reply_header_authorwrote", "- - Beantwortete
                                    Nachricht - -\n> Absender: %s");
user_pref("mailnews.reply_header_ondate", "> Datum: %s Uhr");
user_pref("mailnews.reply_header_separator", "\n");
user_pref("mailnews.reply_header_colon", "\n> ");
```

Künftig sieht der Kopf dann so aus:

```
- - Beantwortete Nachricht - -
> Absender: Daniel Berger
> Datum: 17.01.2014 10:31 Uhr
> ...
```

Erleichterung beim Schreiben der Antwort verschafft das Add-on Quicktext von Emil Hesslow. Mit ihm lassen sich oft verwendete Floskeln („Schönen Gruß", „Gute Besserung") als Textbausteine anlegen, die per Knopfdruck in Nachrichten eingefügt werden.

Eine Mail im Originalzustand weiterschicken („bouncen") können Sie mit dem Add-on Mail Redirect von Pawel Krzesniak und Onno Ekker. Anders als beim Weiterleiten wird die Absenderkennung der Nachricht nicht verändert. Auch eine Konvertierung etwa von HTML nach Text, die beim Weiterleiten „im Text" passiert, unterbleibt.

Abgeschlossen wird eine Mail oft von einer Signatur. Diese können Sie in den Konten-Einstellungen eintragen; pro Mail-Adresse ist eine Signatur vorgesehen. Wenn Sie mehrere verschiedene verwenden möchten, hilft das Add-on Signature Switch von Achim Seufert. Hier lassen sich Filter definieren, sodass bei Firmen-Mails immer eine bestimmte Signatur angehängt wird, bei Ihrer privaten Mail-Adresse eine andere oder keine.

Große Anhänge hängt Thunderbird ab: Die Funktion Filelink schiebt auf Wunsch Dateien zum Hosting-Dienst, sobald diese eine bestimmte Größe überschreiten. Diese können Sie in den allgemeinen Einstellungen unter „Anhänge" festlegen. Die Mail enthält dann nur noch einen Link und keinen Anhang mehr, der kleine Mailboxen verstopft. Gratisspeicher im Filelink bieten derzeit die Anbieter Ubuntu One (5 GByte), box.com (10 GByte) und Hightail (2 GByte). Zusätzlich lässt sich aber auch die Dropbox (bis zu 18 GB) verwenden, wofür das Add-on Dropbox for Filelink nötig ist. Bei der Autorisierung muss Thunderbird noch der Zugriff erlaubt werden, dann kann in den Einstel-

lungen unter „Anhänge/Hinzufügen" auch Dropbox ausgewählt werden.

Zur Rechtschreibkontrolle bietet Thunderbird auch ein Wörterbuch. Weil das unter einer anderen Lizenz als Thunderbird veröffentlicht wird, muss dieses nachinstalliert werden. Unter „Einstellungen/Verfassen/Rechtschreibung" findet sich ein Link zu „weiteren Wörterbüchern". Es können durchaus mehrere Wörterbücher installiert werden.

Im Rechtschreibungsmenü lässt sich auch die sofortige Prüfung während des Schreibens aktivieren. Notorische Vertipper können zusätzlich einstellen, dass eine Mail vor dem Versenden automatisch gegengelesen wird.

Das Standard-Wörterbuch für Deutsch leidet allerdings unter einem beschränkten Wortschatz: Anfangs kennt es einige einfache Vokabeln nicht, beispielsweise „Einmaleins". Das muss Thunderbird erst noch lernen: Mittels Rechtsklick werden unbekannte Wörter schnell hinzugefügt. Die individuell aufgenommenen Begriffe werden lokal im erwähnten Profilordner in der Datei persdict.dat gespeichert. Hier entfernt man auch versehentlich hinzugefügte Wörter („Einmaleis"). Um auf die Datei zuzugreifen, muss Thunderbird geschlossen sein.

Eine Synchronisation zwischen Wörterbüchern auf mehreren Rechnern gibt es leider nicht. Da bleibt nur das manuelle Kopieren der Datei von einem auf den anderen PC. Manchmal hilft es, eine geschriebene Mail erst einmal liegen zu lassen und später noch einmal drüber zu lesen. Eine Nachricht wird mit Strg + S in den Entwürfen gespeichert. Thunderbird bietet zusätzlich die Funktion „Später senden" (Strg + Shift + Enter): Die Mail wird dann in den Postausgang gelegt. Beim Schließen fragt das Mail-Programm nach, ob die Nachricht versendet werden soll. Erweitert wird diese Funktion durch das Add-on Send Later von Jonathan Kamens. Hier lässt sich ein genauer Zeitpunkt festlegen, an dem die Mail versendet wird. So kann man eine Geburtstags-Mail vorschreiben, die dann pünktlich verschickt wird.

Für zeitversetztes Senden muss Thunderbird laufen, was auch das große Problem bei Abwesenheits-Mails ist: Damit der Mail-Client eintreffende Nachrichten während eines Urlaubs mit einer definierten Vorlage automatisch beantwortet, darf der PC nicht ausgeschaltet sein. Für viele Nutzer dürfte das keine akzeptable Lösung sein.

Ungleich einfacher gestaltet sich die Sache bei Anbietern wie Gmail, Yahoo oder GMX, bei denen sich Abwesenheitsmeldungen vom Server über die Weboberfläche aktivieren lassen. Eine Lösung könnte also sein, seine Mails temporär zu einem solchen Anbieter umzuleiten, der diese dann automatisiert beantwortet.

VERSCHLÜSSELT SCHREIBEN

Persönliche Nachrichten sollten verschlüsselt versendet werden (siehe Artikel ab Seite 78). S/MIME ist bei Thunderbird bereits integriert, OpenPGP kann mit dem Add-on Enigmail von Patrick Brunschwig nachgerüstet werden. Außerdem muss GnuPG auf dem Rechner installiert werden: Für Windows gibt es dafür Gpg4Win und für Mac OS GPGTools, womit sich die Einrichtung komfortabel erledigen lässt. Ist das getan und Enigmail installiert, findet sich in Thunderbirds Menüleiste der Punkt „OpenPGP". In den dortigen Einstellungen muss eventuell der Pfad zur gpg.exe nachgetragen werden. Bei der weiteren Anpassung hilft der OpenPGP-Assistent, der ebenfalls über das OpenPGP-Menü aufzurufen ist. Weil längst nicht alle Mail-Nutzer Nachrichten auch entschlüsseln können, sollten Sie die Option „Nein, ich möchte in Empfängerregeln festlegen, wann verschlüsselt werden soll" auswählen.

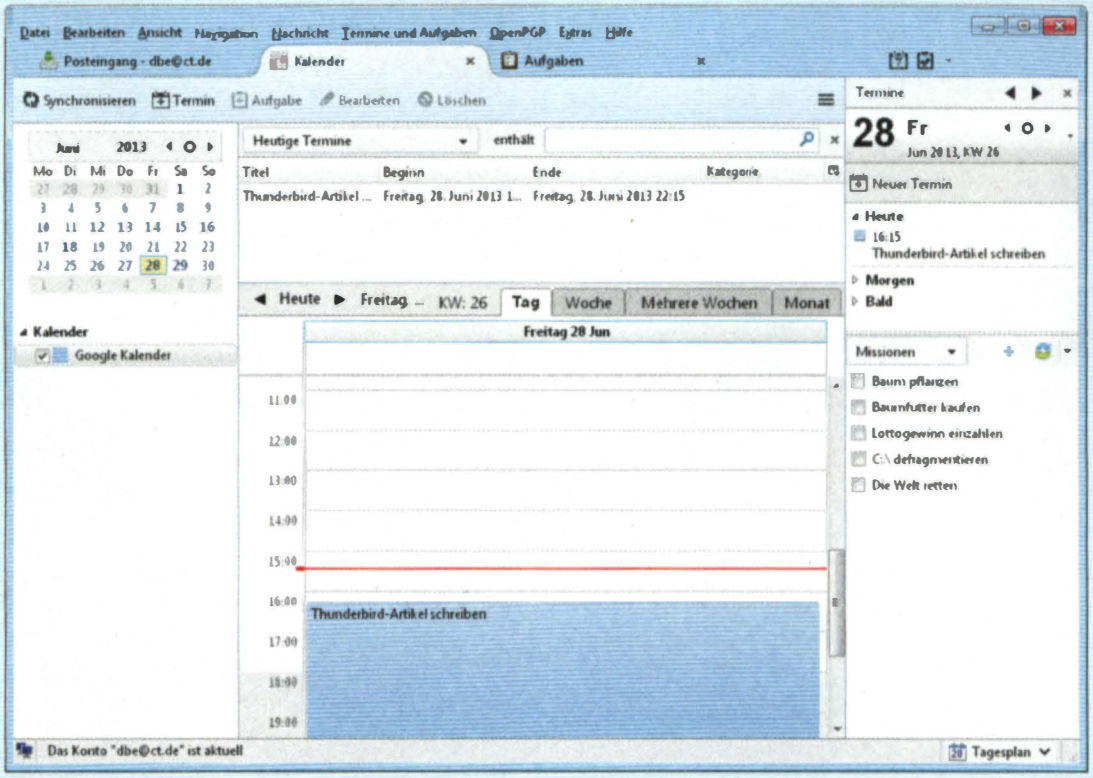
Der Assistent bietet zum Schluss an, ein Schlüsselpaar zu erzeugen, bestehend aus einem geheimen und einem öffentlichen Schlüssel. Das Prinzip lässt sich mit einem Vorhängeschloss vergleichen: Der öffentliche Key ist das Schloss, mit dem Nachrichten an Sie gesichert werden; den Schlüssel zur Entsperrung haben nur Sie.

Zur Absicherung des privaten Schlüssels empfiehlt sich die Festlegung einer Passphrase. Das kann und soll durchaus ein kompletter Satz sein (und nicht nur ein einzelnes Passwort), idealerweise mit exotischen Sonderzeichen garniert. Enigmail erzeugt nicht nur das Schlüsselpaar, sondern auch das passende Widerrufszertifikat, womit kompromittierte Schlüssel entwertet werden. Den öffentlichen Schlüssel können Sie anschließend verteilen und auf einen Schlüssel-Server wie sks-keyservers.net laden, wo andere ihn herunterladen können.

Um aus einer Mail eine Geheimbotschaft zu machen, rufen Sie in der Einzel-Mail-Ansicht den Menüpunkt „OpenPGP/Nachricht verschlüsseln" (Strg + Shift + E) auf. Bedenken Sie, dass Sie den öffentlichen Schlüssel des Empfängers benötigen. Auch angehängte Dateien wie vertrauliche Dokumente können auf Wunsch gleich mitverschlüsselt werden. Große Anhänge sollten aber lieber als verschlüsseltes ZIP-Archiv verschickt werden - so kann man nämlich auch Filelink verwenden.

SONDERAUSSTATTUNG

Ohne Blitz kein Donner: Vollständig wird Thunderbird eigentlich erst durch die Erweiterung Lightning - einem Kalender, der aus dem Mail-Programm ein kleines



Durch Lightning verwaltet Thunderbird nicht nur Mails, sondern auch Termine und Aufgaben. Die Synchronisation mit Google ist mit den richtigen Add-ons auch kein Problem.

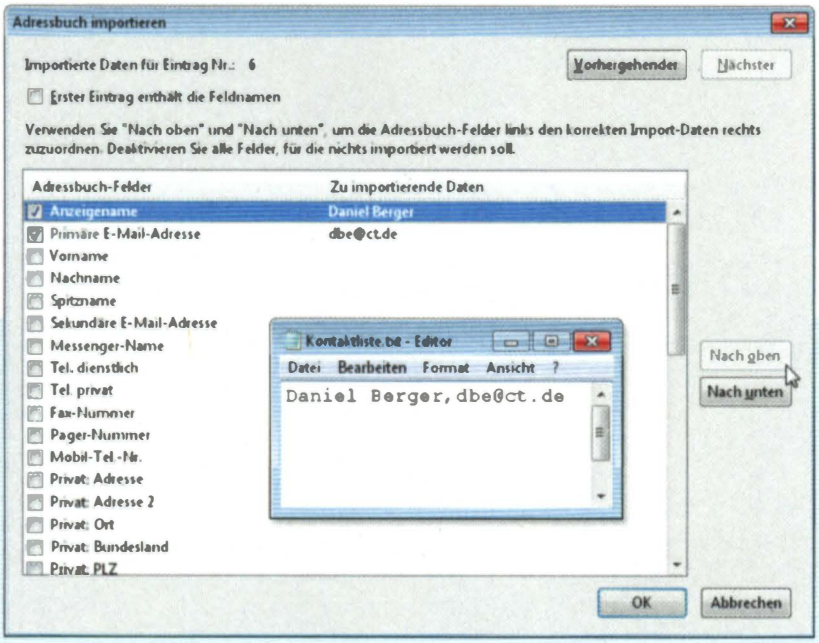
Outlook macht. Außer Terminen lassen sich damit auch Aufgaben verwalten. Vergessliche Nutzer werden durch eine Popup-Meldung an ihre Verabredungen erinnert.

Lightning lässt sich über die XML-Schnittstelle auch mit dem Google-Kalender synchronisieren und mit dessen Terminen befüllen. Hierzu nötig ist die Erweiterung Provider for Google Calendar von Philipp Kewisch. Leider unterstützt das Add-on Googles Aufgaben-Planung bisher nicht – der Entwickler verweist auf Probleme mit dem API. Bis diese gelöst sind, schafft der Pole Tomasz Lewoc mit Google Task Sync Abhilfe: Ist es installiert, müssen Sie dem Add-on nur noch den Zugriff auf Ihren Google-Account erlauben. Die Verwaltung der Aufgaben läuft über ein kleines Fenster, das sich nahtlos in den Lightning-Kalender einbettet, aber nicht über den eigentlichen Menüpunkt „Aufgaben" erreichbar ist. Der bleibt weiterhin Lightnings eigener To-do-Liste vorbehalten. Diese Aufgabenteilung ist vielleicht nicht die eleganteste Lösung, aber doch benutzbar.

Mit dem Add-on Zindus von Leni Mayo lassen sich dann noch die Kontakte aus Google und Zimbra-Konten mit dem lokalen Adressbuch von Thunderbird abgleichen: entweder mit dem persönlichen Standard-Adressbuch oder einem eigenen, das exklusiv mit den Google-Kontakten befüllt wird. Leider hat der Entwickler angekündigt, Zindus nicht weiterzuentwickeln. Immerhin verspricht er, Sicherheits-Updates zu liefern, sollte dies nötig sein. Dank Adressbuch, dem nachgerüsteten Kalender und der Aufgabenverwaltung mutiert der Mail-Client zu einem recht ordentlichen Personal Information Manager (PIM) im Stil von Outlook.

SICHER IST SICHER

Auch wenn die Mails sicher auf einem IMAP-Server liegen, möchte man sich vielleicht eine lokale Sicherheitskopie anlegen. Dafür gibt es das Programm MozBackup von Pavel Cvrcek, das nicht nur die Mails sichert, sondern auf Wunsch auch sämtliche Einstellungen, Passwörter, Adressbücher und so weiter. Eine rechtssichere Archivierung ersetzt das aber nicht. MozBackup erzeugt ein Archiv, das sich als normale Zip-Datei auch entpacken lässt. Dazu muss einfach die Dateiendung .pcv in .zip umbenannt werden. Vorgesehen ist aber, dass MozBackup das erstellte Archiv in ein (frisches) Thunderbird importiert – ein manuelles Entpacken also gar nicht nötig ist. Einzelne Mails lassen



Kontakte können auch gesammelt via Textdatei ins Adressbuch importiert werden.

sich in Thunderbird übrigens ganz simpel mit Strg + S als HTML- oder Textdatei auf Festplatte speichern.

MAILING-LISTEN MIT THUNDERBIRD

Mit Thunderbird lassen sich einfache Rundschreiben versenden, beispielsweise an die Großfamilie (um dadurch einem persönlichen Treffen aus dem Weg zu gehen). Mailing-Listen werden in Thunderbirds Adressbuch (Strg + Shift + B) angelegt.

Der besseren Übersicht halber empfiehlt sich die Einrichtung eines neuen Adressbuches über „Datei/Neu/Adressbuch". Dort können Sie verschiedene Mailing-Listen anlegen. Die erste soll an alle gehen: Rechtsklick auf das eben angelegte Adressbuch, „Neue Liste", und diese dann „Familie-alle" nennen. Bereits in anderen Adressbüchern vorhandene Familienmitglieder können schon mal per Drag and Drop in die Mailing-Liste geschoben werden. Der Rest (also Schwiegermutter und der knurrige Onkel aus Südbayern) müssen erst noch ins Adressbuch importiert werden. Das ist durchaus fummelig und bei großen Listen muss man aufpassen, dass beim Drag and Drop keine Kontakte verloren gehen.

Als Szenario denkbar wäre, dass die zahlreichen Mail-Adressen der Verwandten aus verschiedenen Quellen zusammengetragen wurden. Diese zunächst in einer Textdatei zu bündeln, erspart beim Import ins Adressbuch das mühsame Einpflegen jedes einzelnen Kontaktes. Für einen problemlosen Import sollte in jeder Zeile der Textdatei ein Kontakt stehen. Getrennt werden die Angaben durch ein Komma, woraus sich folgendes Zeilenschema ergibt: Anzeigenname,Mail. Wer sämtliche Felder in Thunderbirds Adressbuch füllen möchte, muss wie folgt erweitern: Anzeigenname,Mail, Vorname,Name und so weiter. Leider lassen sich die einzelnen Posten beim Import nicht doppelt zuordnen: Der Vorname kann also im Adressbuch nicht die Felder „Vorname" *und* „Anzeigenname" befüllen – sondern nur eines der beiden. Deshalb müssten Sie beide Angaben in der Textdatei hinterlegen. Für eine Mailing-Liste reichen jedoch die beiden Angaben „Anzeigenname" und „Primäre Mail" völlig aus.

Die Textdatei mit den Kontakten lesen Sie anschließend im Adressbuch über „Extras/Importieren" ein. Mit den Schaltflächen „Nach oben" und „Nach unten" müssen Sie die Adressbuch-Felder so anordnen, bis es passt: „Primäre Mail-Adresse" korrespondiert mit der jeweiligen Mail-Adresse und der Name mit dem Feld „Anzeigenname". Thunderbird importiert die Daten in ein neues Adressbuch. Die Kontakte darin ziehen Sie einfach in das bereits angelegte Adressbuch, damit alle Kontakte an einem Ort gesammelt sind.

Um eine Nachricht an eine Mailing-Liste zu schicken, tragen Sie einfach deren Namen als Empfänger ein. Wählen Sie dabei „BCC" aus, bleiben die Adressen den einzelnen Empfängern verborgen. (Damit der Onkel aus Bayern die anderen nicht auch noch nervt.) (dbe) c't

Alle Links zum Artikel
www.ct.de/hb1401042

heise Security

Sichere Kommunikation trotz Überwachung und Spionage

Firmen-IT, E-Mail und Smartphones sinnvoll schützen

Die heise Security Tour 2014

Foto: © Jakub Jirsak + violetkaipa – Fotolia.com

Das Jahr 2013 war geprägt vom Abhörskandal der Geheimdienste. Auf der renommierten *heise Security Tour* geben Ihnen unsere Experten Hilfestellung, wie Sie insbesondere sensible Geschäftsdaten noch besser schützen.

Die Vorträge aus dem Umfeld der Unternehmenspraxis und der Forschung zeigen Ihnen Probleme sowie Risiken auf und geben Ihnen adäquate Lösungsvorschläge zum Schutz von Unternehmens-IT und -Kommunikation an die Hand.

Jetzt 15% Frühbucherrabatt sichern!

TERMINE: **8. Mai,** Hamburg • **13. Mai,** Nürnberg • **15. Mai,** Stuttgart • **21. Mai,** Köln

PROGRAMMAUSZUG

- **Risiken und Auswirkungen von PRISM – Cloud-Dienste, Kryptographie und Schlüsselmanagement,**
  Christoph Wegener, wecon.it-consulting
- **Sichere Verschlüsselung für Server-Dienste: SSL in der Praxis – Der Leitfaden für Nicht-Krytoplogen**
  Jürgen Schimdt, Heise Zeitschriften Verlag
- **Von der Prävention zur Detektion: Firmen-Netze vor Cyber-Angriffen schützen und Einbrüche erkennen**
  Wilhelm Dolle, KPMG AG

- **100% unabhängig**
- **hochkarätige Referenten**
- **Praxisrelevanz der Vorträge**
- **hervorragende Plattform zum Networking und Erfahrungsaustausch**
- **begleitende Ausstellung mit Informationen über die neuesten IT-Lösungen & -Produkte**

Frühbuchergebühr: 485,- Euro (inkl. MwSt.)
Standardgebühr: 570,- Euro (inkl. MwSt.)

Eine Veranstaltung von: heise Security

Organisiert von: heise Events

Weitere Infos und Anmeldung unter: **www.heise-events.de/securitytour2014**

Test: E-Mail-Apps für Android und iOS

Für den schnellen Mailcheck unterwegs reichen die Beigaben der Mobilsysteme oft noch aus. Was aber, wenn man länger auf Tour ist, oder das Postfach vom Smartphone und Tablet aus organisieren will? Unser Test prüft die Beigaben und Alternativen.

Von **Jo Bager, Holger Bleich**

Mails unterwegs zu bearbeiten kann zur Qual werden: Eine kleine Smartphone-Tastatur, das Minidisplay und die vermaledeite Autokorrektur vermiesen den Spaß. Die bordeigenen Mail-Apps unterstützen lediglich rudimentär. Gefragt sind frische Bedienkonzepte, die diesen Mankos begegnen.

Bei Android gab es vom Start weg reichlich alternative Mail-Apps. Apple dagegen hatte anfangs bei iOS die Hand drauf und schützte die Monopolstellung der Mail-Anwendung, in dem es andere Apps schlicht untersagte. Dieses Verbot existiert nicht mehr, und so warten im App Store mittlerweile einige interessante Alternativen darauf, ausprobiert zu werden. Dennoch: Mail bleibt Standard-Handler, etwa, wenn man aus Apps heraus Texte oder Bilder verschicken will.

Gerne hätten wir auch Mail-Apps unter Windows Phone getestet, aber hier existieren noch keine Alternativen zum bordeigenen Client. Das dürfte sich erst ändern, wenn der Marktanteil des Microsoft-Betriebssystems wächst. Insgesamt 22 Apps haben wir getestet, 13 für Android, 9 für iOS. Sofern nicht anders erwähnt, sind die vorgestellten Apps gratis.

ORGANISATIONSFÄHIGKEITEN

Mobile Mail-Nutzung bedeutet vor allem: begrenzte Ressourcen. Auf Smartphones und Tablets steht Mail-Apps weniger Platz für die Darstellung zur Verfügung als auf dem heimischen 24-Zöller. Wir haben daher ausprobiert, ob die Apps den zur Verfügung stehenden Platz sinnvoll ausnutzen – und zwar im Hoch- wie im Querformat.

Um möglichst schnell den Posteingang zu überblicken, ist es hilfreich, Mails nach Datum, Betreff und Absender zu sortieren und zu einer Unterhaltung (Thread) gehörende Mails zusammenfassen zu können. Eine Favoriten-Markierung ermöglicht, einzelne Mails einfach wiederzufinden; Tags helfen, verschiedene zu einem Projekt gehörende Nachrichten zusammenzufassen.

Die Kür sind individuelle Filter, die die Nachrichten vorsortieren. Eine Suchfunktion dagegen ist Pflicht. In der Regel werden nicht alle auf dem Server lagernden Mails mit auf das Mobilgerät geladen. Daher sollte die Suche den Server durchforsten, sofern dieser die Option bietet.

Begrenzt ist unterwegs auch das Download-Volumen – wer will schon das Datenkontingent seines Mobilfunkvertrages ausschöpfen, nur weil der Mailer jede noch so unwichtige Nachricht inklusive aller Attachments komplett herunterlädt? Intelligenter ist es, von jeder Nachricht automatisch nur die wichtigsten Metadaten und vielleicht ein paar KByte Text holen zu lassen – den Rest lädt man nach, wenn man ihn tatsächlich benötigt.

Apropos intelligentes Herunterladen: Die meisten Mailer stellen neue Nachrichten via Push fast in Echtzeit zur Verfügung, sobald diese auf dem Server vorliegen. Per akustischem Alarm, blinkender Geräte-LED und unter Android mit Widgets informieren sie den Benutzer über eintreffende Nachrichten.

Genauso segensreich kann es aber sein, wenn der Mailer Ruhe gibt, Bandbreite und Akku schont – etwa nachts. Einige Apps bieten daher ein sehr ausgefeiltes Empfangsmanagement: Der Anwender kann festlegen, wie viele Mails sie wie oft zu welcher Tageszeit laden sollen – und ob überhaupt.

PROTOKOLLFRAGEN

Wir haben uns sowohl speziell auf Mail-Dienste zugeschnittene als auch universell einsetzbare Apps angeschaut. Bei letzteren legten wir besonderes Augenmerk auf die Implementierung des IMAP4-Protokolls. POP3 ist für den mobilen Zugriff von mehreren Geräten aus kaum geeignet, weil es nur Kopien aus der Inbox, nicht aber aus vorsortierten Ordnerstrukturen ziehen kann. Außerdem bietet es – anders als IMAP mit der Idle-Funktion – keine Möglichkeit, Nachrichten vom Server zum Client zu „pushen".

Einige Apps im Testfeld beherrschen darüber hinaus Microsofts proprietäres Active-Sync-Protokoll, das auch als Exchange ActiveSync (EAS) bekannt ist und zur Kommunikation mit Exchange-Servern dient. ActiveSync wurde lange Zeit von Google für den unmittelbaren Austausch (Direct Push) der Mail-, Kalender- und Kontaktdaten unterstützt. Im Juli hat Google diese Funktion abgeschaltet. Das dürfte dazu führen, dass ActiveSync als Mail-Protokoll künftig an Bedeutung verlieren wird.

Ein Pin-Code bietet einen Grundschutz für den Fall, dass das Gerät in falsche Hände gerät. Als Maßnahme gegen Nutzer-Tracking und Sicherheitsprobleme sollten E-Mail-Programme HTML beim Mail-Empfang abschalten können. Die Apps mussten Testmails des Online-Dienstes Email Privacy Tester abarbeiten, die eine ganze Batterie von Schnüffeltricks ausprobieren. Besonders schwer wog dabei, wenn eine Mail per Meta Refresh eine Webseite aufrief: Das ist fast schon eine Einladung, Schadcode per Browser-Bug auszuführen.

Zum Schutz vor Mitlesern sollten Apps Nachrichten verschlüsseln und den Übertragungsweg per SSL absichern. Wie sorgfältig sie letzteres bewerkstelligen, haben wir mit einem manipulierten Übertragungsweg untersucht. Wir probierten, den Apps per Man-in-the-Middle-Angriff einen kompromittierten Server unterzuschieben, der den Datenverkehr mitlesen könnte.

ANDROID

AQUA MAIL

Aqua Mail zählt zu den vielseitigeren Mail-Apps – auch wenn es keine Exchange-Accounts unterstützt. In den Tiefen der Optionen lassen sich sehr viele Details des Nachrichtenabrufs und der Darstellung feintunen. Dazu gehört, wie viele Mails pro Ordner die App maximal vorhalten, wie sie unter welchen Netzwerkbedingungen mit Anhängen umgehen, wann sie wie über eintreffende Nachrichten informieren und welche Details sie in Mail-Listen anzeigen soll. Mit den Lauter/Leiser-Tasten des Geräts lässt sich die Schrift vergrößern und verkleinern.

Die „Smart Inbox" fasst neue, ungelesene Nachrichten vorgegebener Ordner zusammen. Zwei Widgets

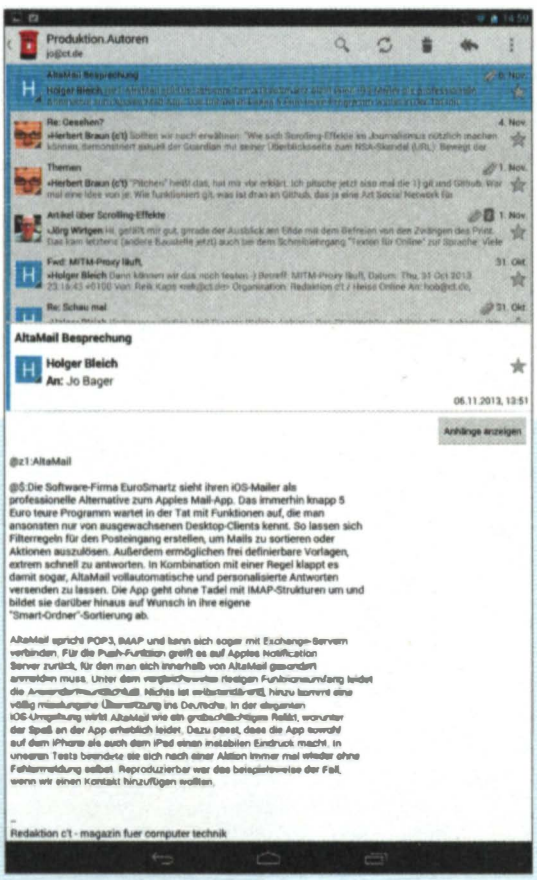
Praktisch für den schnellen Mail-Check: Die Smart Inbox von Aqua Mail zeigt neue, ungelesene Nachrichten vorgegebener Ordner an.

zeigen entweder die neuesten Nachrichten oder die Anzahl ungelesener Nachrichten an. Aqua Mail ist gut im Android-Ökosystem verankert. Es gibt Add-ons unter anderem für das Automatisierungstool Tasker, diverse Launcher und mehrere Sony-Smartwatches. Das Preismodell ist fair: Die kostenlose Version unterstützt nur zwei Accounts, hängt einen Werbetext an versendete Nachrichten an und bietet keine Identitäten, mit denen der Anwender mehrere Signaturen nutzen kann. Für knapp vier Euro fallen diese Einschränkungen.

E-MAIL

Die Standard-Mail-App von Android ruft Nachrichten per POP3, IMAP und ActiveSync ab, bei letzteren beiden Protokollen beherrscht es Push. Ebenfalls keine Selbstverständlichkeit: Bei IMAP- und Exchange-Accounts durchsucht die App außer den heruntergeladenen Nachrichten auch den Datenbestand auf dem Server im Volltext. Textbausteine erleichtern die schnelle Antwort.

Die Optionen zur Darstellung und Feinjustierung sind dagegen nicht so vielseitig wie bei anderen Mail-Apps. Bei der Einrichtung von Accounts bietet die App an, beliebige Zertifikate zu akzeptieren. Diese Option kann dann nötig sein, wenn der Mail-Server unterschiedliche Zertifikate hat oder diese oft wechselt (was allerdings nicht im Sinne einer sicheren SSL-Implementierung ist). Man sollte darauf achten, das Häkchen nur in speziellen Fällen zu setzen, da die Option auch jeden Schutz gegen Man-in-the-Middle-Attacken aushebelt.



Alternative Ansicht: Wer's mag, kann Kaiten das Fensterlayout auch horizontal aufteilen lassen.

GMAIL

Die Gmail-App spricht nur mit dem Google-eigenen Mail-Service. Sie bildet ausschließlich die wesentlichen Funktionen von Gmail auf dem Mobilgerät ab. Der Benutzer findet seine Nachrichten im „sortierten" Posteingang vor, bei dem Google Nachrichten aus sozialen Netzen, Werbung, „Benachrichtigungen" und Foren in eigene Ordner vorsortiert. Alternativ lässt sich aber auch der klassische Eingang mit allen Nachrichten öffnen. Google hält Labels zwischen Web-Frontend und App immer synchron.

Gmail unterstützt keine Verschlüsselung einzelner Nachrichten und lässt sich nicht mit einer PIN schützen. Dafür war es die einzige Mail-App, die sich bei den Sicherheitstests keine Panne erlaubte. Obwohl sie HTML-Mails darstellt, lädt sie keine Elemente von fremden Servern nach, über die sich der Benutzer von kommerziellen Anbietern rückverfolgen lässt. HTML-URLs zeigt die App an, wenn man für längere Zeit drauftippt – ohne sie direkt aufzurufen.

GMX/WEB.DE

Die Apps von GMX und Web.de kommen offensichtlich aus derselben Schmiede: Sie gleichen sich in der Versionsnummer, dem Veröffentlichungsdatum, der Größe und dem Namen der Installation. Der Funktionsumfang unterscheidet sich nur minimal.

Beide Apps sind nicht auf die Dienste ihrer Anbieter eingeschränkt. Außer GMX- und Web.de-Accounts lassen sich auch beliebige andere POP3- oder IMAP-Konten nutzen. Ein praktisches Detail hilft, volle Postfächer schnell aufzuräumen: Wischt man eine Nachricht in der Übersicht zur Seite, löscht die App die Mail.

Der einzige wesentliche Unterschied zwischen den Apps von GMX und Web.de zeigte sich beim Daten-

schutztest: Während die GMX-App beim Abruf der Mail von Email Privacy Tester nachvollziehbar drei Elemente abrief und dann auch noch abstürzte, machte die App von Web.de alles richtig – und lief stabil.

OUTLOOK.COM

Die App für Microsofts Dienst ist eine reine Smartphone-App. Auf dem Tablet verschwendet sie zu viel Platz, weil eine Zweispaltenansicht fehlt. Außer Mails synchronisiert die App auch Kontakte und Kalender zwischen genau einem Outlook.com-Konto und dem Gerät. Dabei kann der Benutzer eine Ruhezeit festlegen, bei der die App nicht synchronisiert.

Die Outlook.com-App ist sehr stylish im Metro-Design gehalten; ein Widget für den Android-Desktop bietet sie auch. Sie durchsucht nicht nur den lokalen Nachrichtenstamm, sondern auch den Server. Unter den Android-Apps hat Outlook.com die mit Abstand schlechteste Gesamtbewertung im Play Store; Anwender bemängeln insbesondere immer wieder Probleme bei der Anmeldung. Wir konnten diese Kritik nicht nachvollziehen.

K-9/KAITEN

K-9 gehört zu den meistinstallierten Mailern für Android. Das hat unter anderem damit zu tun, dass das Open-Source-Programm rege weiterentwickelt wird. K-9 beherrscht POP und IMAP und kann auch Mails von Exchange-Servern abrufen. Letzteres wickelt K-9 aber per WebDAV ab, nicht per ActiveSync. Deshalb steht Push für solche Konten nicht zur Verfügung.

Es gibt sehr viele Einstellungsmöglichkeiten, um den Mail-Abruf und die Darstellung auf die individuellen Notwendigkeiten anzupassen. So fasst die „gemeinsame Inbox" die ungelesenen Nachrichten der Eingangsordner aller Accounts sowie beliebiger anderer IMAP-Ordner zusammen. Die Lauter/Leiser-Tasten des Geräts kann man umfunktionieren, um damit zur vorherigen oder nächsten Nachricht zu wechseln. Über sogenannte Identitäten lassen sich mehrere Signaturen verwenden. Einige Optionen sind aber unnötig kompliziert.

K-9 und sein Bruder Kaiten sind die einzigen E-Mailer, die PGP unterstützen – die zusätzliche App APG vorausgesetzt. Auch per Man-in-the-Middle-Angriffen ließen sie sich nicht austricksen. Sie bemängelten Probleme bei der Verifikation der Server während der Einrichtung.

In der Beschreibung von Kaiten steht, dass die App auf K-9 „basiere". Häufig wird sie auch als Weiterentwicklung von K-9 beschrieben. Ganz falsch ist beides nicht. De facto ist aber Kaiten fast ein Klon von K-9. Es stammt von zwei federführenden K-9-Entwicklern, die damit offensichtlich ein paar Dollar dazuverdienen wollen. Anders als K-9 ist der Client nicht werbefrei. Möchte man die Banner loswerden, sind knapp 4 Euro im Play Store fällig.

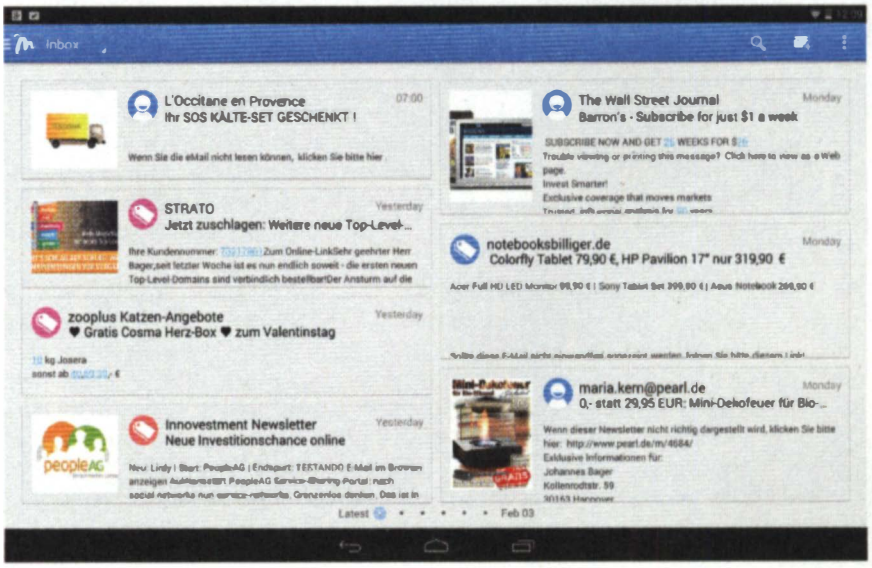
Es gibt nur wenige Unterschiede zu K-9. So präsentiert Kaiten seine Mails in Listen mit farbigen Icons ein wenig schicker. Auch bietet Kaiten mehr Optionen, wenn man Nachrichtenlisten und einzelne Mails gemeinsam anzeigen will: K-9 teilt das Display nur horizontal auf. Bei Kaiten kann man dagegen für Hoch- und Querformat getrennt festlegen, ob es Mail-Listen und einzelne Nachrichten horizontal oder vertikal trennen soll.

MAILDROID

MailDroid beherrscht POP, IMAP und Exchange via WebDAV. Seine große Stärke ist die sehr gelungene IMAP-Implementierung. So zeigt MailDroid die Ordner-Hierarchie als einklappbaren Baum an – praktisch insbesondere bei Firmen-Servern mit Dutzenden von Ordnern. Man kann Ordner auch umbenennen, löschen und neu anlegen.

Einzelne Ordner lassen sich als Lesezeichen ablegen, woraufhin MailDroid sie auf dem Startbildschirm ablegt. Große Ordner kann man gezielt mit Filtern

Unter den Android-Mailern stellt MailDroid hierarchische IMAP-Ordnerhierarchien am besten dar.



Frischer Wind für Android-Tablets: Molto präsentiert den Posteingang magazinartig in zwei Spalten.

durchforsten. Man kann über Regeln sehr detailliert festlegen, was neue Mails bewirken sollen, abhängig vom Account, dem Absender, dem Betreff, dem Wochentag und der Uhrzeit. Die Verbindungsverwaltung legt ebenso fein granuliert fest, an welchen Tagen, zu welcher Zeit und bei welchem Verbindungstyp MailDroid überhaupt Nachrichten abrufen soll.

Die App lässt dem Anwender sehr viele Freiheiten beim Layout. So kann er zum Beispiel Nachrichten im Vollbildmodus ansehen. Sogenannte Schnellantworten liefern häufig benutzte Textbausteine. Alles in allem ist MailDroid ein Arbeitstier – das aber seinen Preis hat. Entweder akzeptiert man die Bannerwerbung der kostenlosen Version oder man bezahlt etwa 14 Euro für die Pro-Version, die unter anderem zusätzlich zwei Widgets mitliefert. Ein Spam-Plug-in gibt es gegen eine monatliche oder jährliche Gebühr.

MOLTO

Das nur für Tablets verfügbare Molto geht bei der Darstellung eigene Wege. Die App läuft stets im Querformat und zeigt die Nachrichten jeweils eines Ordners zweispaltig in Form von Anrissen an. Dabei präsentiert sie neben dem Text auch Bilder oder Bildausschnitte aus der Mail. Teils wertet sie auch Links in den Mails aus und lädt Bilder von den verlinkten Websites nach, um das Layout aufzulockern.

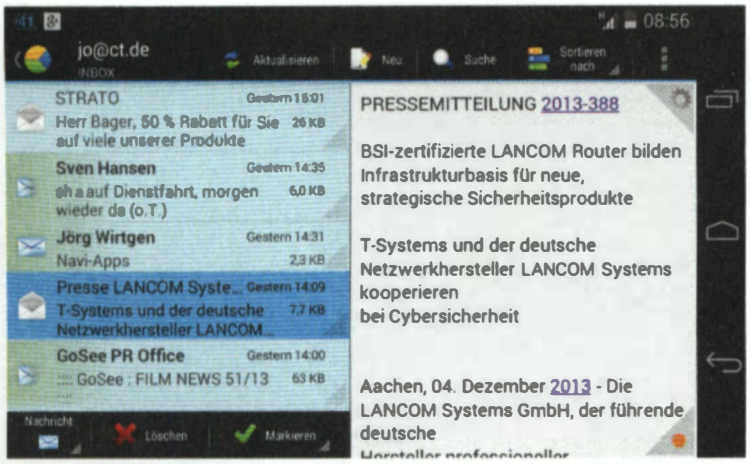
Bei nicht gespeicherten Nachrichten dauert das ein paar Sekunden länger als bei anderen Clients – und es benötigt auch erheblich mehr Bandbreite, weshalb man Molto besser nur im WLAN betreiben sollte. Abschalten lässt sich dieses Verhalten nicht, weshalb es auch nicht verwundert, dass Molto eines der schlechtesten Ergebnisse des Datenschutztests erzielt.

Miniaturen der Kontakte holt die App aus den Gerätekontakten. Wer will, kann Molto mit Facebook verknüpfen, um auch von dort die Porträts der Kontakte einzubetten. Alles in allem ergibt das ein sehr schickes, fast magazinartiges Layout. Man kann direkt in den Mail-Teasern scrollen, um die Mails komplett zu lesen.

Neben Gmail beherrscht Molto beliebige IMAP-Accounts. Die Ordnerliste sieht weniger schick aus als die der Nachrichten: Jeden IMAP-Ordner listet es mit seinem vollen Pfadnamen, einklappen lässt sich die Liste nicht. Im Test verhaspelte sich die Beta-Software mit der Darstellung, und bei einigen Textkodierungen stellt sie Umlaute nicht richtig dar.

PROFIMAIL GO

ProfiMail Go stammt ursprünglich aus der Symbian- und Windows-Mobile-Welt; um Android-Standards zu genügen, haben seine Entwickler den POP- und IMAP-Client aber komplett neu entwickelt. Die Oberfläche von ProfiMail Go ist besonders vielseitig konfigurierbar. So blendet ProfiMail Go in Mail-Listen auf dem Smartphone bei Bedarf die Vorschau einer Nachricht



ProfiMail Go stellt die zweigeteilte Ansicht auch auf einem Smartphone im Querformat vernünftig dar.

ein, und es stellt sogar die vom PC gewohnte dreigeteilte Ansicht mit Ordnerliste, Inhalt eines Ordners und einzelner Mail dar. Der Benutzer kann sehr detailliert vorgeben, wann ProfiMail Go welche und wie viele Mails herunterladen soll, und aus einer IMAP-Hierarchie Ordner auswählen, deren Nachrichten die App in einem Sammelordner aggregiert.

Regeln helfen, Nachrichten automatisiert zu bearbeiten. Will man seine Mails vorgelesen bekommen, kann ProfiMail Go sie an Androids Text-to-Speech-Engine durchreichen lassen. ProfiMail Go beherrscht S/MIME für die Verschlüsselung von Mails und digitale Signaturen. Unkonventionell ist das Preismodell: Die App kostet nichts, solange man sie nur für einen E-Mail-Account einsetzt. Wer seine Nachrichten auf mehreren Accounts verwalten möchte, zahlt eine monatliche Gebühr von 89 Cent oder 5,90 Euro im Jahr.

TOUCHDOWN

Touchdown, beziehungsweise Touchdown HD für Tablets, spielt in einer anderen Liga als die restlichen E-Mailer für Android. Die App unterstützt nur Exchange, aber nicht POP und IMAP. Das beschränkt den Einsatzzweck auf Unternehmens-Mail, wie auch seine vielfältigen Sicherheitsfunktionen belegen. So kommuniziert Touchdown verschlüsselt und legt seine Daten verschlüsselt auf der SD-Karte des Geräts ab. Die App lässt sich auch aus der Ferne warten: Geht das Smartphone verloren, lassen sich die darauf liegenden Daten aus der Ferne löschen. Die App kostet knapp 16 Euro.

TouchDown bietet viele nützliche Funktionen für die tägliche Mailbearbeitung. Man kann zum Beispiel die Schaltflächen auf der E-Mail-Symbolleiste frei definieren oder festlegen, was ein Rechts-Wisch auf eine E-Mail bewirken soll. Die Gerätekontakte bezieht es bei der Adressvervollständigung nicht mit ein, stattdessen nutzt es das eigene Adressbuch.

YAHOO MAIL

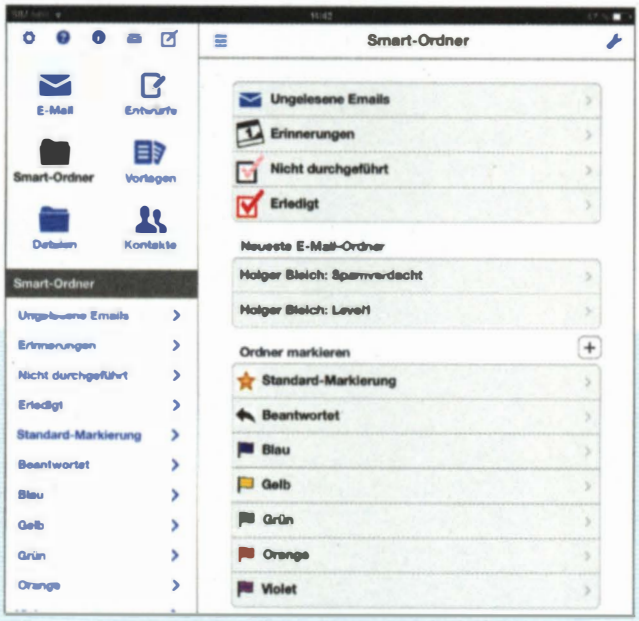
Mit Yahoos App lassen sich nur Nachrichten von Accounts bei dem Online-Dienst verwalten. Wie beim Web-Frontend kann der Anwender auf die automatisch geführten Ordner mit bekannten Kontakten und Mails mit Anhängen zugreifen sowie auf alle selbst angelegten Ordner. Die Volltextsuche fahndet auch auf dem Server. Die sehr schick gehaltene App orientiert sich vom Design her ein wenig an Windows 8. HTML lässt sich bei empfangenen Mails nicht abschalten. Dennoch schneidet Yahoo beim Datenschutztest noch glimpflich ab.

iOS

ALTAMAIL

Das gerade mal knapp 5 Euro teure Programm wartet mit Funktionen auf, die man ansonsten nur von ausgewachsenen Desktop-Clients kennt. So lassen sich Filterregeln für den Posteingang erstellen, die Mails sortieren, Aktionen auslösen oder Nachrichten zur späteren Erinnerung zurückstellen. Außerdem ermöglichen frei definierbare Vorlagen, extrem schnell zu antworten. In Kombination mit einer Regel kann AltaMail sogar vollautomatische und personalisierte Antworten versenden. Die App geht ohne Tadel mit IMAP-Strukturen um und bildet sie darüber hinaus auf Wunsch in ihre eigene „Smart-Ordner"-Sortierung ab.

AltaMail spricht POP, IMAP und kann sich mit Exchange-Servern verbinden. Unter dem vergleichsweise riesigen Funktionsumfang leidet die Anwenderfreundlichkeit. Nichts ist selbsterklärend, hinzu kommt eine völlig misslungene Übersetzung ins Deutsche. In der eleganten iOS-Umgebung wirkt AltaMail wie schlampig hinkodiert. Dazu passt, dass die App sowohl auf dem iPhone als auch dem iPad einen instabilen Eindruck macht. In unseren Tests schloss sich der Client immer mal wieder ohne Fehlermeldung selbst. Positiv hingegen: AltaMail ließ sich von unseren SSL-Manipulationen nicht überlisten.



AltaMail bietet jede Menge Sortieroptionen. Leider sorgen diese Möglichkeiten aufgrund der unübersichtlichen Darstellung eher für Verwirrung.

INBOX PRO OUTLOOK EDITION

Inbox Pro kommuniziert ausschließlich mit Exchange-Accounts. Dabei nutzt die App nicht ActiveSync, sondern greift via HTTPS auf Outlook Web Access (OWA) des Exchange Servers zu. Im Grunde genommen bildet Inbox Pro also nur den Teil der Funktionen ab, die Exchange-Nutzer mit OWA ohnehin nutzen können. Dies erledigt die App aber sehr elegant, ganz im neuen iOS-7-Look. Der Hersteller Code Before Dawn wirbt damit, dass Inbox Pro auch mit „schwierigen" Exchange-Umgebungen klarkomme und problemlos über VPNs von Außendienstlern laufe. Von dem Betrieb im geschäftlichen Umfeld können wir indes nur abraten: Leiteten wir bei Inbox Pro den Datenverkehr über unseren SSL-Proxy, konnten wir den verschlüsselten Datenverkehr sogar im Klartext mitlesen, ohne ein falsches Zertifikat unterzuschieben - der „worst case" also.

GMAIL

Die Gmail-App ist wie unter Android voll auf die Funktionen von Googles Mail-Service zugeschnitten. Sie stellt den vom Anbieter vorsortierten Posteingang und die über Label geregelte Ordnerstruktur sowohl auf dem iPhone als auch auf dem iPad übersichtlich dar. Die App verwaltet mehrere Gmail-Konten parallel. Außerdem kann der Nutzer über das Web-Frontend die Konten vieler anderer Services einbinden und dann ebenfalls über die App einsehen. Ein nettes Gimmick: Per Fingertipp kann der Nutzer ein Skribble zeichnen und direkt versenden. Aktive Inhalte in Mails sowie nachzuladende Elemente blockiert die Gmail-App - wie unter Android - gut.

GMX/WEB.DE

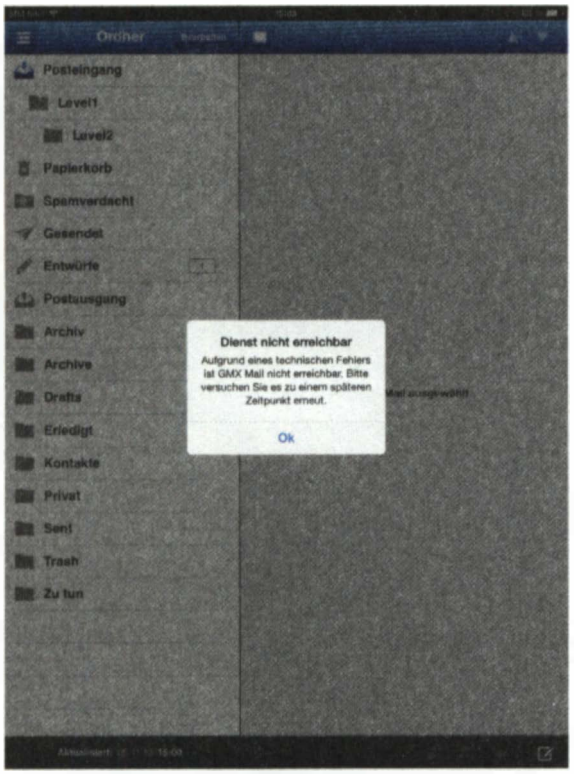
Die iOS-Mail-Apps der Provider der beiden United-Internet-Töchter GMX und Web.de unterscheiden sich von den Android-Pendants, untereinander tragen sie aber dieselbe Versionsnummer und wirken optisch identisch. Sie gewähren einen schnörkellosen, schnellen Zugriff auf den Mail-Account. Mit horizontalen Wischgesten kann der Nutzer schnell zwischen Ansichts-Modi wechseln und Ordnung ins Postfach bringen. In der Vorschau etwa streicht er quer nach links über die Mail, um sie zu markieren, in die Gegenrichtung zum Löschen. Drückt er länger auf die Vorschau, kann er die Mail in einen anderen Ordner verschieben.

Die Einstellmöglichkeiten bieten wenige, aber sinnvolle Optionen. Auf Wunsch benachrichtigen die Apps nicht nur über in der Inbox angekommene Mails, sondern auch über solche in wählbaren anderen Ordnern. Wie auch bei den Android-Apps reagierten die Anwendungen unterschiedlich auf unseren Privacy-Test, allerdings genau umgekehrt: Die GMX-App erlaubte sich kaum Blößen, die Web.de-App schützte schlechter.

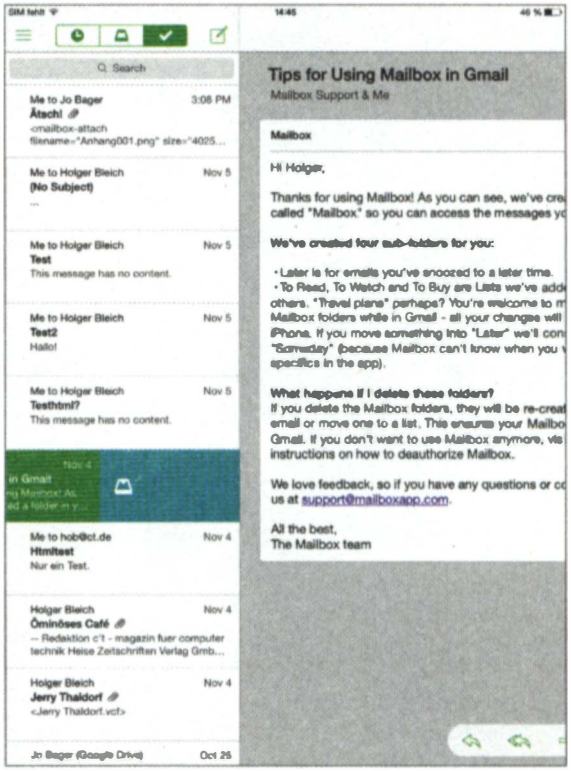
MAIL

Die Einstellungen für Apples Standard-Client finden sich nicht in der App selbst, sondern in den iOS-Einstellungen. Apple Mail spricht POP, IMAP und ActiveSync (Exchange). IMAP-Ordnerstrukturen bildet der Client immer vollständig und aufgeklappt ab. Eine Möglichkeit, Ordner zu wählen oder ein- und auszublenden existiert nicht. So kann es schnell unübersichtlich werden. Threads fasst die App zusammen, auch eine Sammel-Inbox für mehrere Accounts bietet sie an.

Standardmäßig sammelt die App alle Infos zur ersten Account-Einrichtung selbst ein, wählt als Standard-



Gut: Die GMX-App baut keinen Kontakt zum Server auf, wenn die SSL-Verbindung kompromittiert wurde. Weniger gut: die unspezifische Fehlermeldung.



Mailbox bricht die HTML-formatierte Mail in der Vorschau nicht korrekt um. Ein Wisch befördert sie aus dem Posteingang ins Archiv.

protokoll aber nicht IMAP, sondern POP. Um einen Account manuell einrichten zu können, muss man bewusst falsche Daten eingeben, um damit ein Scheitern der Automatik zu forcieren. In unserem Privacy-Test scheiterte die App krachend und tappte in fast sämtliche Tracking-Fallen. Dafür verhielt sie sich beim SSL-Test vorbildlich.

MAILBOX

Mailbox soll dem Nutzer dazu verhelfen, mit einigen Wischgesten und organisatorischen Kniffen schnell zur „Zero Inbox" zu kommen, also zur Ordnung im Posteingang. Ein kurzer Wisch nach links in der Mailvorschau öffnet die Snooze-Option, damit lassen sich die Nachrichten zur Wiedervorlage wegsortieren, beispielsweise mit „Later Today", „Tomorrow" oder zu einem bestimmten Datum. Ein langer Wisch bringt Listenordner zum Vorschein, so kann die Nachricht in Ordner namens „To Read" oder „To Watch", oder auch in einen selbst definierten Listenordner geschoben werden. Gelesene Mails wandern automatisch ins Archiv.

Die App leitet alle Mails über Dropbox-Server. Diese fungieren als eine Art transparenter Cache, ohne dass die Nutzer das mitbekommen – aus Datenschutzsicht inakzeptabel. Bislang kann der Dropbox-Dienst offensichtlich nur mit Gmail umgehen, andere Accounts verwaltet Mailbox nämlich nicht. Irgend-

Molto besticht in der iPhone-Version schon vom Start weg mit guten Tutorials und Erläuterungen und macht den Einstieg leicht.

wann soll die App auch mit IMAP-Konten klarkommen, erklärten die Entwickler. Im Privacy-Test schnitt Mailbox akzeptabel ab. Sehr gut gefiel, dass unsere SSL-Manipulationen an dem Client abprallten: Er verweigerte die Kommunikation mit kompromittierten Gegenstellen.

MOLTO

Molto, das ehemals Incredimail hieß, nutzt die Mail-Engine von iOS und beherrscht daher sowohl IMAP als auch ActiveSync. Als Standard-Mailer darf es sich allerdings dennoch nicht in iOS einklinken. Während die iPad-Version ähnlich gestaltet ist wie die für Android-Tablets, ist die iPhone-Variante bereits sehr gut ans iOS-7-Design angepasst.

Mails bereitet Molto in der Vorschau grafisch wie das Android-Pendant auf und fügt beispielsweise Profilbilder aus den Gerätekontakten oder auch aus Facebook hinzu. Ein Filter sortiert die Inbox in Smart Folders vor, zu denen ein Wisch nach unten führt. Die IMAP-Struktur stellt Molto vollständig ausgeklappt dar. Mails können parallel an mehrere Kontakte mit einer Art Verteiler geschrieben werden. In Sachen Datenschutz ist Molto hingegen schwach: Die App war außerstande, gängige Tracking-Attacken abzuwehren. Wie unter Android ließ sich die SSL-Verbindung sogar belauschen, ohne dem Client ein gefälschtes Zertifikat unterschieben zu müssen.

Alle Links zum Artikel
www.ct.de/hb1401050

YAHOO MAIL

Die schmale App dient auch unter iOS ausschließlich dem Zugriff auf Yahoo-Konten. Sie zeigt die Ordnerstruktur, lässt den Nutzer mit Wischgesten verschiedene Aktionen in der Mail-Vorschau ausführen (beispielsweise Spam-Markierung oder Tags setzen) und wirkt optisch schlicht und elegant. Auffällig war, dass der Zugriff auf Mails bisweilen arg langsam vonstatten ging, insbesondere bei Anhängen.

FAZIT

Als Allzweck-Client für Gelegenheitsmailer verrichtet die zu Android gehörende Mail-App gute Dienste. Unter den Apps der Mail-Betreiber stechen nur die Outlook-App hervor, die neben den Mails auch Kalender und Kontakte synchronisiert, sowie die Gmail-App, weil sie sich als einziges Programm mit Datensammler-Maschen nicht austricksen lässt. AquaMail, ProfiMail und K-9/Kaiten bieten mehr an individuellen Einstellungsmöglichkeiten als die Provider-Apps.

MailDroid und TouchDown sind Spezialisten: TouchDown funktioniert nur mit einem Exchange-Server, MailDroid spielt seine Stärken vor allem mit einem IMAP-Server aus. Molto geht neue Wege der E-Mail-Aufbereitung: schön anzusehen, aber ziemlich datenintensiv.

Molto ist auch unter iOS ein echter Hingucker, der noch dazu kostenlos ist und einiges kann. Mailbox besticht durch seine ausgefeilte Gestenbedienung und innovative Funktionen. Allerdings handhabt die App bislang nur Gmail-Konten und leitet darüber hinaus alle Mails durch die Dropbox-Cloud.

Apples bordeigene iOS-Mail-App ist besser als ihr Ruf und für Gelegenheitsmailer ausreichend. Wer einen iOS-Client sucht, dessen Funktionsumfang an den eines Desktop-Programms heranreicht, liegt bei AltaMail richtig. Doch gerade diese App belegt anschaulich, wie wenig Sinn es ergibt, mobile Clients mit Optionen zu überfrachten. Der Anwender muss sich lange einarbeiten; darunter leiden die Übersicht und damit auch der Spaß.

In puncto Sicherheit konnte keine App vollends überzeugen – vertrauliche E-Mails bearbeitet man besser auf dem PC. (jo)

E-Mail-Apps für Android

Name/Version	AquaMail 1.2.5.5	E-Mail 4.1	Gmail 4.6	GMX 1.56.6	K-9 4.409	Kaiten 2.014
Darstellung Smartphone: hoch/quer	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Darstellung Tablet: hoch/quer[4]	✓/✓	✓/✓	✓/✓	–/–	✓/✓	✓/✓
Accounts/Abholen						
automatische/manuelle Einrichtung	✓/✓	✓/✓	✓/–	✓/✓	✓/✓	✓/✓
Multi-User/-Account	–/✓	–/✓	–/✓	–/✓	–/✓	–/✓
POP3/ IMAP4/ ActiveSync (EAS)	✓/✓/–	✓/✓/✓	–/–/–	✓/✓/–	✓/✓/–[3]	✓/✓/–[3]
Push: IMAP/ EAS	✓/–	✓/✓	✓/–	✓/–	✓/–	✓/–
Größenbegrenzung beim Download	✓	–	–	✓	✓	✓
Zeitabschnitt/Anzahl abzuholender Mails	5 Min. – tägl. / 15 bis 5000	5 Minuten – stündlich	beliebig viele Tage	1 Minute – alle 24 Stunden	jede Minute – alle 24 Stund.	jede Minute – alle 24 Stund.
Adressen						
Nutzt Gerätekontakte/Adressimport aus …	✓/–	✓/–	✓/–	✓/GMX	✓/–	✓/–
Vcard-Unterstützung	–	–	–	–	✓	✓
korrekte Darstellung von Sonderzeichen	✓	✓	✓	✓	✓	✓
Absender ins Adressbuch übernehmen	✓	–	✓	–	✓	✓
Verteilerlisten	–	–	–	–	–	–
Ordner-Organisation (z. B. IMAP)						
Mails in andere Ordner verschieben	✓	✓	✓	✓	✓	✓
alle Ordner/nur abonnierte anzeigen	–/✓	–/✓	✓/✓	✓/–	–/✓	–/✓
Struktur bearbeiten/Namen änderbar	–/–	–/–	✓/–	✓/✓	–/–	–/–
Ordner einklappbar/freie Auswahl möglich	✓/✓	✓/–	–/–	–/–	✓/✓	–/✓
Organisieren/Lesen						
Sammel-Eingangsordner	✓	✓	✓	✓	✓	✓/–
Widget(s)	4×2, 1×1	3×2, 1×1	3×3	4×1[7]	1×1	1×1
Dauer für „Gelesen"-Markierung einstellbar	✓	–	–	–	–	–
Mail als Favorit/ungelesen markieren	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Sortierung nach Datum/Absender/Betreff	✓/✓/✓	✓/–/–	✓/–/–	✓/✓/✓	✓/✓/✓	✓/✓/✓
Thread-Darstellung	–	–	✓	–	✓	✓
Filter/Suche lokal/ auf dem Server	–/✓/–	–/✓/✓	–/✓/✓	–/✓/–	–/✓/✓	–/✓/✓
Rückkehr zur Mail nach Klick auf Links	✓	✓	✓	✓	✓	✓
Tags vergeben/als Spam markieren	–/–	–/–	✓/✓	–/✓	–/–	–/–
mehrere Mails in einem Vorgang löschen	✓	✓	✓	✓	✓	✓
alle Mails in Ordner löschen	✓	–	–	✓	✓	✓
Schreiben/Adressieren/Versenden						
Mail als Entwurf speichern	✓	✓	✓	✓	✓	✓
Versand als Klartext/HTML/wahlweise	✓/✓/–	✓/–/–	✓/–/–	✓/✓/–	✓/✓/✓	✓/✓/✓
Rechtschreibkorrektur	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]
Adressiervervollständigung aus Kontakten/ benutzten Adressen	✓/✓	✓/–	✓/✓	✓/–	✓/–	✓/–
Multi-Signatur	–	–	–	–	✓	✓
Datenschutz und Sicherheit						
In-App-PIN-Schutz	✓	–	–	✓	–	–
HTML abschaltbar bei empfangenen Mails	–	–	–	–	–	–
E-Mail-Privacy-Tests bestanden	– (14 nicht)	– (2 nicht)[2]	✓	– (3 nicht)	– (2 nicht)[2]	– (2 nicht)[2]
kein Nachladen der Bilder/abschaltbar	✓/✓	✓/✓	✓/✓	✓/–	✓/–	✓/✓
Links in HTML-Mails im Klartext sichtbar	–	–	✓	–	✓	✓
SSL-Sessionverschlüsselung	✓	✓	✓	✓	✓	✓
Schutz vor Man in the Middle-Attacken: ohne Zertifikat/ mit Zertifikat	✓/✓	✓/✓	✓/–	✓/✓	✓/✓	✓/✓
S/MIME/ PGP	–/–	–/–	–/–	–/–	–/✓[5]	–/✓
Bewertung						
Accounts/Adressen	○	○	○	○	⊕	⊕
Organisieren/Lesen	⊕	○	⊕	○	⊕	⊕
Schreiben/Adressieren/Versenden	⊕	○	⊕	○	⊕	⊕
Datenschutz und Sicherheit	○	⊖	⊕	○	⊖	⊖
Preis	kostenlos: 2 Accounts, Vollversion: 3,77 €	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos: Werbung, Vollversion: 3:99 €

[1] Systemfunktion [2] darunter Meta refresh [3] WebDAV-Zugriff auf Exchange: ✓ [4] IMAP geht durch, SMTP nicht [5] mit APG [6] sinnvolle Darstellung [7] je nach Gerät 3 × 1

	MailDroid 3.27	Molto 1.0.7 beta (engl.)	Outlook.com 7.8.2.12	ProfiMail Go 4.14.00	TouchDown (HD) 8.3.00036	Web.de 1.56.6	Yahoo Mail 3.0.5.1311380
	✓/✓	–/–	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
	✓/✓	–/✓	–/–	✓/✓	✓/✓	–/–	✓/✓
	✓/✓/–[3]	–/✓/–	–/–/–	✓/✓/–	–/–/✓	✓/✓/–	–/–/–
	✓/–	–/–	✓/–	✓/–	–/✓	✓/–	✓/–
	✓	–	✓	–	✓	✓	–
	beliebig	–/–	1 Tag – unbegrenzt	15 Minuten	jede Min. – 4 Std., benutzerdef.	1 Minute – alle 24 Stunden	–/–
	✓/–	✓/–	✓/Outlook.com	✓/–	–/Exchange	✓/Web.de	✓/Yahoo
	–	–	–	–	✓	–	–
	✓	✓	✓	✓	✓	✓	✓
	–	–	✓	✓	–	–	–
	✓	–	–	–	✓	–	–
	✓	✓	✓	✓	✓	✓	✓
	✓/✓	✓/–	✓/–	✓/✓	–/✓	✓/–	✓/✓
	✓/✓	–/–	–/–	–/–	–/–	✓/✓	✓/✓
	✓/✓	–/–	–/✓	✓/✓	✓/✓	–/–	–/–
	✓	✓	✓	✓	–	✓	–
	3×2, 1×1	–	4×2	3×2	4×3, 3×2, 2×2	4×1[7]	–
	–	–	–	✓	–	–	–
	✓/✓	✓/✓	✓/✓	✓/✓	–/✓	✓/✓	✓/✓
	✓/✓/✓	✓/–/–	✓/–/–	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/–/–
	✓	✓	✓	✓	✓	–	✓
	✓/✓/✓	–/✓/–	–/✓/✓	✓/✓/–	✓/✓/✓	–/✓/–	–/✓/✓
	✓	✓	✓	✓	✓	✓	✓
	–/✓	–/–	–/✓	–/–	✓/–	–/✓	–/✓
	✓	✓	✓	✓	✓	✓	✓
	✓	–	–	✓	✓	✓	✓
	✓	✓	✓	✓	✓	✓	✓
	✓/✓/✓	–/✓/–	✓/–/–	✓/✓/✓	✓/✓/–	✓/✓/–	✓/✓/–
	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]
	✓/–	✓/–	✓/–	✓/–	✓/–	✓/–	✓/–
	✓	–	–	✓	–	–	–
	✓	–	✓	–	–	✓	–
	–	–	✓	✓	–	–	–
	– (7 nicht)[2]	– (15 nicht)[2]	– (11 nicht)[2]	✓	– (3 nicht)	✓	– (4 nicht)
	✓/✓	–/–	–/✓	✓/–	–/✓	✓/–	✓/✓
	–	–	✓	–	✓	–	✓
	✓	✓	✓	✓	✓	✓	✓
	✓/✓	✓/✓	✓/–	✓/✓	✓/–	✓/✓	✓/–
	–/–	–/–	–/–	✓/–	✓/–	–/–	–/–
	⊕	○	○	⊕	○	○	○
	⊕⊕	⊖	○	⊕	⊕	○	○
	⊕⊕	○	○	⊕	○	○	○
	○	⊖⊖	○	⊕	⊕	⊕	○
	kostenlos: Werbung; Pro-Version: 14 €	kostenlos	kostenlos	kostenlos: 1 Account, mehrere 5,90 /Jahr€	15,96 €	kostenlos	kostenlos

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden k. A. keine Angabe

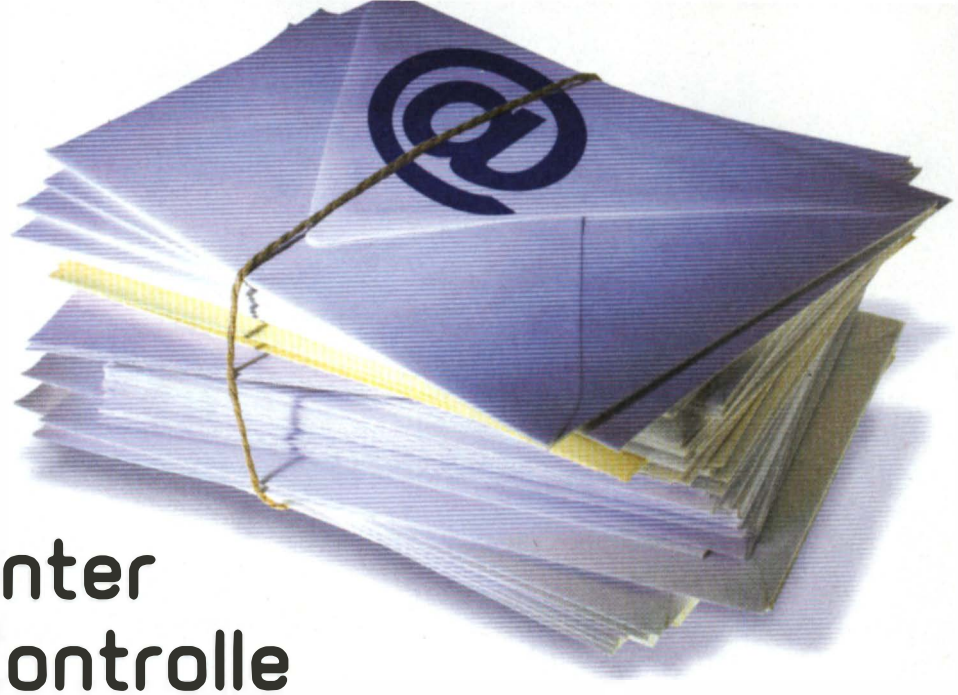
E-Mail-Apps für iOS

Name/Version	AltaMail 5.2	Inbox Pro Outlook Edition 3.1 (engl.)	Gmail 2.4.3	GMX 2.36.1
Darstellung Smartphone: hoch/quer	✓/✓	✓/✓	✓/✓	✓/✓
Darstellung Tablet: hoch/quer[1]	✓/✓	✓/✓	✓/✓	✓/✓
Accounts/Abholen				
automatische/manuelle Einrichtung	✓/✓	✓/–	✓/–	✓/–
Multi-User/-Account	–/✓	–/✓	–/✓	–/–
POP3/ IMAP4/ ActiveSync (EAS)	✓/✓/✓	–/–/–	–/–/–	–/✓/–
Push: IMAP/ EAS	✓/✓	–/–	–/–	✓/–
Größenbegrenzung beim Download	–	–	–	–
Zeitabschnitt/Anzahl abzuholender Mails	✓/–	–/✓	–/–	–/–
Adressen				
Nutzt Gerätekontakte/Adressimport aus …	✓/–	✓/Exchange	✓/Gmail	✓/–
Vcard-Unterstützung	–	✓	✓	–
korrekte Darstellung von Sonderzeichen	✓	✓	✓	✓
Absender ins Adressbuch übernehmen	–	✓	–	–
Verteilerlisten	✓	–	–	–
Ordner-Organisation (z. B. IMAP)				
Mails in andere Ordner verschieben	✓	✓	✓	✓
alle Ordner/nur abonnierte anzeigen	✓/–	✓/✓	✓/–	✓/–
Struktur bearbeiten/Namen änderbar	✓/✓	–/–	–/–	✓/✓
Ordner einklappbar/ freie Auswahl möglich	✓/✓	–/✓	–/–	–/–
Organisieren/Lesen				
Sammel-Eingangsordner	✓	✓	✓	–
Dauer für „Gelesen"-Markierung einstellbar	–	–	–	–
Mail als Favorit/ungelesen markieren	✓	–/✓	–/–	✓/–
Sortierung nach Datum/Absender/Betreff	✓/✓/✓	✓/✓/✓	✓/–/.0	✓/–/–
Thread-Darstellung	✓	–	✓	–
Filter/Suche lokal/ auf dem Server	✓/✓/✓	–/✓/–	–/✓/–	–/✓/–
Rückkehr zur Mail nach Klick auf Links	✓	✓	✓	–
Tags vergeben/als Spam markieren	✓	–	✓	✓
mehrere Mails in einem Vorgang löschen	✓	✓	✓	✓
alle Mails in Ordner löschen	✓	–	–	✓
Schreiben/Adressieren/Versenden				
Mail als Entwurf speichern	✓	✓	–	✓
Versand als Klartext/HTML/wahlweise	✓/–/–	✓/–/–	–/✓/–	✓/–/–
Rechtschreibkorrektur	✓	–	–	–
Adressiervervollständigung aus Kontakten/ benutzten Adressen	✓/✓	✓/✓	✓/✓	✓/–
Multi-Signatur	–	–	–	–
Datenschutz und Sicherheit				
In-App-PIN-Schutz	✓	✓	–	✓
HTML abschaltbar bei empfangenen Mails	–	–	–	✓
E-Mail-Privacy-Tests bestanden	– (18 nicht)[2]	✓ (2 nicht)	✓ (2 nicht)	✓ (2 nicht)
kein Nachladen der Bilder/abschaltbar	–/–	–/–	–/–	–/–
Links in HTML-Mails im Klartext sichtbar	–	–	✓	–
SSL-Sessionverschlüsselung	✓	✓	✓	✓
Schutz vor Man in the Middle-Attacken: ohne Zertifikat/ mit Zertifikat	✓/✓	–/–	✓/–	✓/–
S/MIME/ PGP	–/–	–/–	–/–	–/–
Bewertung				
Accounts/Adressen	⊕	○	⊕	○
Organisieren/Lesen	○	○	⊕	⊕
Schreiben/Adressieren/Versenden	⊕	⊕	⊕	○
Datenschutz und Sicherheit	○	⊖	⊕	⊕
Preis	4,49 €	4,49 €	kostenlos	kostenlos

[1] sinnvolle Darstellung [2] darunter Meta refresh

Mail App iOS 7.0.3	Mailbox 1.6.3 (engl.)	Molto 2.0.1	Web.de 2.36.1	Yahoo Mail 2.0.2
✓/✓	✓/✓	–/–	✓/✓	✓/✓
✓/✓	✓/✓	–/✓	✓/✓	✓/✓
✓/✓	✓/–	✓/–	✓/–	✓/–
–/✓	–/✓	–/✓	–/–	–/✓
✓/✓/✓	–/–/–	–/✓/–	–/–/–	–/–/–
–/✓	–/–	–/–	✓/–	–/–
–	–	–	–	–
–/✓	–	–/–	–/–	–/–
✓/–	✓/Gmail	✓/–	✓/–	✓/–
✓	✓	✓	–	–
✓	✓	✓	✓	✓
✓	–	✓	–	✓
–	–	–	–	–
✓	–	✓	✓	✓
✓/–	–/–	✓/–	✓/–	✓/–
✓/✓	–/–	–/–	✓/✓	–/–
–/–	–/–	–/–	–/–	–/–
✓	✓	✓	–	✓
–	–	–	–	–
✓/–	✓/✓	✓/✓	✓/–	✓/✓
✓/–/–	✓/–/–	✓/–/–	✓/–/–	✓/–/–
✓	✓	✓	–	✓
–/✓/–	–/✓/–	–/✓/–	–/✓/–	–/–/✓
–	–	✓	–	–
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✓	✓	–	✓	–
✓	–	✓	✓	✓
✓/–/–	–/✓/–	–/✓/–	✓/–/–	✓/–/–
–	–	–	–	–
✓/✓	✓/✓	✓/✓	✓/–	✓/–
–	–	–	–	–
–	–	–	✓	–
–	–	–	✓	–
– (19 nicht)[2]	– (3 nicht)	– (17 nicht)[2]	– (4 nicht)	– (4 nicht)
–/✓	–/–	–/–	–/–	–/–
–	–	–	–	–
✓	✓	✓	✓	✓
✓/✓	✓/✓	–/–	✓/–	✓/–
✓/–	–/–	–/–	–/–	–/–
⊕	○	⊕	○	○
○	⊕⊕	○	⊕	○
⊕	⊕	⊕	○	○
○	○	⊖⊖	○	⊕
Bestandteil von iOS	kostenlos	kostenlos	0,89 €	kostenlos

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden k. A. keine Angabe c't



E-Mails unter eigener Kontrolle archivieren

Noch lange werden die meisten E-Mails unverschlüsselt bleiben. Riesige Mengen persönlicher Daten lagern daher als einfach lesbare Textdateien auf den Servern von Google, Microsoft und anderen Providern. Diesen muss man vertrauen – oder seine Mails nach Hause holen.

Von **Axel Kossel, Peter Siering**

Wichtige Mails wie Rechnungen, Anmeldebestätigungen oder Antworten auf Hotline-Anfragen sollte man aufbewahren. Eigentlich lohnt sich die Mühe des Löschens nur bei Nachrichten mit großen Anhängen, etwa Fotos, die man nur einmal anschaut oder anderswo speichert. Aus allem Übrigen wächst über die Jahre ein Archiv heran, das viel über den Inhaber der E-Mail-Adresse verrät.

Webmail-Dienste speichern diese Archive gerne und verwöhnen ihre Kunden daher gigabyteweise mit Speicher. Auch wenn man mit einem IMAP-Client darauf zugreift, verbleiben die Nachrichten auf dem Server. Google und Yahoo etwa versichern, die Mails nur automatisch nach Stichwörtern zu durchsuchen, um passende Werbung schalten zu können. Doch es ist mittlerweile kein Geheimnis mehr, dass US-Behörden sich einfach Zugang zu Daten verschaffen können, die bei US-Unternehmen lagern. Und bei deutschen Diensten ist man nicht vor Pannen gefeit, die zu Indiskretion oder Datenverlust führen.

NACH HAUSE

Es spricht also vieles dafür, das Mail-Archiv nicht beim Provider, sondern unter eigener Kontrolle zu lagern. Solange Sie nur einen Computer nutzen, ist das ganz einfach: Installieren Sie einen E-Mail-Client wie Thunderbird (siehe Seite 42) so, dass er die E-Mails mit dem Protokoll POP3 vom Server holt und dort löscht. Soll das sofort geschehen, müssen Sie bei Thunderbird unter „Extras/Konto-Einstellungen/Server-Einstellungen" die standardmäßig gesetzte Option „Nachricht auf dem Server belassen" deaktivieren.

In der Standardeinstellung belässt Thunderbird die Mails nach dem Abruf per POP3 noch 14 Tage lang auf

dem Server, ehe er sie löscht. Damit funktioniert dieses Konzept auch dann, wenn man mit verschiedenen Geräten E-Mail liest: Vom Smartphone, Tablet oder Notebook aus greift man per IMAP auf die Mail zu und bekommt alles, was neu eingegangen ist, sowie die Mails der letzten Tage zu sehen. Ältere, gelesene Nachrichten verschwinden nach dem Abruf mit dem PC, der als Archiv dient, aus Webmailer und Mobil-Clients. Die Frist, nach der auf dem Server gelöscht wird, können Sie unter Server-Einstellungen Ihren Bedürfnissen anpassen.

Über ein zweites Thunderbird-Konto, das parallel zum ersten per IMAP auf die Mailbox zugreift, lässt sich auf dem Server ein Ordner für Mails anlegen, die man mobil länger im Zugriff haben möchte. Thunderbird kann in diesen Ordner auch Nachrichten zurückkopieren, die bereits per POP3 abgeholt und auf dem Server gelöscht wurden. Etwa der IMAP-Client des Smartphones hat dann dauerhaft Zugriff darauf, vielleicht aber auch die NSA.

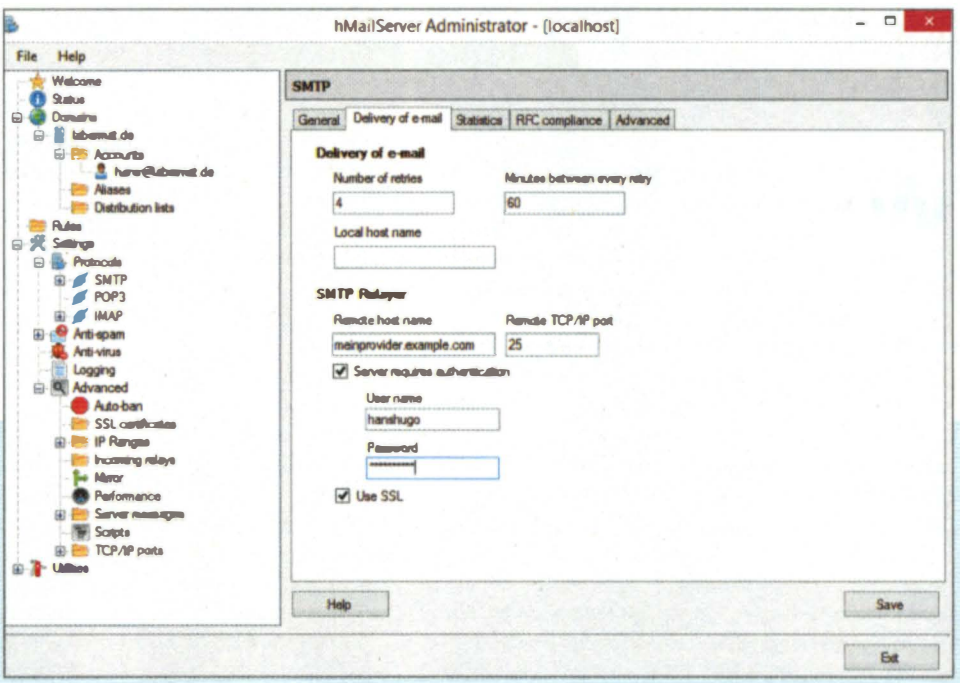
IN SICHERHEIT

Für das lokale Mailarchiv benötigen Sie eine Backup-Strategie. Dazu könnten Sie das Verzeichnis, in dem Thunderbird die heruntergeladenen Mails lagert, mit einem Backup-Programm regelmäßig auf einen externen Datenträger schreiben. Welches Verzeichnis das ist, steht in den Server-Einstellungen unter „Lokaler Ordner".

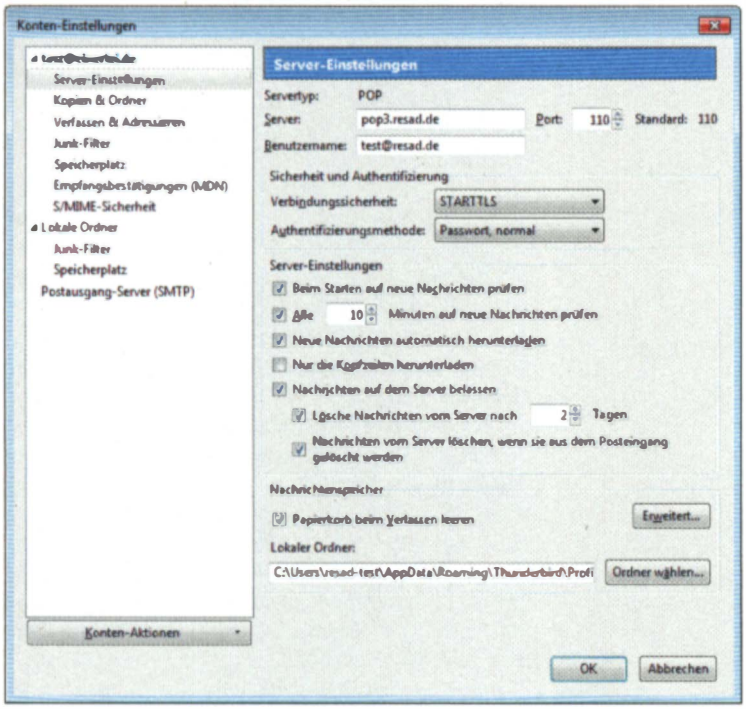
Allerdings speichert Thunderbird im MBOX-Format, sodass alle Nachrichten aus einem Mail-Ordner in eine Textdatei geschrieben werden. Diese Dateien werden mit der Zeit sehr groß und müssen bereits nach Eingang einer kleinen Mail komplett neu gesichert werden. Das kostet Zeit und Speicherplatz. Außerdem ist es nicht möglich, einzelne Mails wieder herzustellen, ohne die gesamte MBOX-Datei und den dazugehörigen Index zu überschreiben.

Daher ist es eleganter, die Mail-Ordner von Thunderbird mit Mailstore Home in ein Archiv zu schreiben. Dieses Programm ist für private Anwender kostenlos. Es erzeugt für jede archivierte Nachricht eine .eml-Datei. Außerdem besitzt Mailstore Home eine sehr gute Suchfunktion für archivierte Mails und kann versehentlich gelöschte auch wieder in Thunderbird zurückschreiben.

Nach der Installation geben Sie unter „Verwaltung/E-Mails und Einstellungen" das Verzeichnis an, in dem das Archiv angelegt werden soll. Das kann eine externe Festplatte sein oder ein Ordner auf der internen, dessen Inhalt dann zum Beispiel über ein Hybrid-Backup verschlüsselt und verteilt gesichert wird.



Der lokale E-Mail-Server (hier hMailServer) holt die Mails per POP3 beim Provider ab und übergibt ausgehende Nachrichten an dessen SMTP-Relay.



Thunderbird lädt E-Mails per POP3 komplett herunter und löscht sie zwei Tage später vom Server. Danach kann man mit Smartphone & Co. nicht mehr darauf zugreifen.

Für die Archivierung der Mails müssen Sie unter „E-Mail archivieren" ein Mailstore-Profil erstellen. Dabei wählen Sie „Mozilla Thunderbird" als Quelle in der Liste der E-Mail-Programme aus. Im nächsten Fenster bestimmen Sie, aus welchem Thunderbird-Profil die Ordner archiviert werden sollen. Falls Sie im Client nicht verschiedene Benutzer angelegt haben, die unter einem Windows-Konto arbeiten, ist „default" richtig, andernfalls wählen Sie den Benutzer.

Als Nächstes können Sie das Archivieren auf bestimmte Ordner oder ältere Mails einschränken; hier sind keine Änderungen nötig. Damit ist das Profil für die Sicherung angelegt und kann durch Doppelklick auf den neuen Eintrag in der Tabelle „Gespeicherte Profile" gestartet werden.

Allerdings sollte so eine Sicherung automatisch ablaufen, was die Home-Version von Mailstore leider nicht unterstützt. Sie müssen daher die Aufgabenverwaltung von Windows zu Hilfe nehmen. Zunächst klicken Sie aber in Mailstore das eben gespeicherte Profil mit der rechten Maustaste an und wählen „Verknüpfung auf dem Desktop erstellen". Über diese Verknüpfung startet das Programm und archiviert die neuen Mails in Thunderbird.

Nun rufen Sie unter „Systemsteuerung/System und Sicherheit/Verwaltung" die Aufgabenplanung auf. Hier klicken Sie im Frame „Aktionen" auf „Einfache Aufgabe erstellen", geben einen Namen für die automatische Archivierung ein und wählen als Aufgabentrigger beispielsweise „Täglich". Den nächsten Dialog können Sie überspringen, dann wählen Sie „Programm starten" und über Durchsuchen die auf dem Desktop erzeugte Verknüpfung aus.

Dabei wird allerdings der Aufrufparameter nicht übernommen. Klicken Sie daher mit der rechten Maustaste auf die Verknüpfung, wählen „Eigenschaften" und kopieren die Zeichen aus der Zeile „Ziel", die hinter dem letzten Anführungszeichen stehen. Das sollte in etwa so aussehen: /c archive –id="1" und wird ins Feld „Argumente hinzufügen" der Aufgabenerstellung kopiert. Im letzten Dialog können Sie die Aufgabe dann „Fertig stellen". Mailstore sichert von nun an täglich die neuen Mails in Thunderbird.

SELBST BEDIENT

Sollen doch alle E-Mails von mehreren Geräten aus zugänglich sein, brauchen Sie einen eigenen E-Mail-Server. Dafür muss man keinen dicken Rechner anschaffen; schon ein kleines NAS genügt. Oder ein Desktop-PC erledigt die Aufgabe zusätzlich. Selbst ein Raspberry Pi ist der Aufgabe gewachsen (siehe Seite 68).

Für das sichere Aufbewahren der Mails genügt es, wenn der Server neue Nachrichten regelmäßig per

LITERATUR

[1] Johannes Endres, **E-Mail-Server unter Windows**, Poststelle für den Home Server, www.ct.de/-1484479

[2] Reiko Kaps, **Zugangsticket**, Kostenlose DynDNS-Dienste, c't 7/13, S. 108

Alle Links zum Artikel
www.ct.de/hb1401064

POP3 vom Provider holt und dort löscht. Die Clients lässt er dann per IMAP darauf zugreifen. Der Weg, auf dem gesendet wird, spielt dabei keine Rolle. Die Clients können Nachrichten entweder weiterhin direkt über den Server des Providers verschicken oder über den eigenen, der sie dann am SMTP-Relay des Providers abliefert.

Den passenden Server gibt es mit Dovecot als Open Source für Linux (und diverse NAS) und mit hMailServer [1] als Freeware für Windows. Wer sich nicht die Einrichtung der diversen Einzelteile eines E-Mail-Servers unter Linux zutraut, dem hilft iRedMail bei der Konfiguration und bringt obendrein Roundcube mit, ein Web-Frontend für den Mail-Zugriff.

Um es Dritten nicht allzu leicht zu machen, die E-Mail mitzulesen, und vor allem um sicherzustellen, dass die für den Zugriff auf den E-Mail-Server oder das SMTP-Relay nötigen Passwörter nicht in falsche Hände geraten, ist es Pflicht, alle Verbindungen zu verschlüsseln, also nur POP3S, IMAPS und SMTP mit SSL oder TLS zu verwenden.

OFFENE TÜR

Steht der Mail-Server hinter einem DSL-Router, soll aber auf dem Smartphone auch aus dem Internet erreichbar sein, müssen Sie zwei Dinge tun. Erstens besorgen Sie sich ein Konto bei einem Dyn-DNS-Anbieter [2] und richten Ihren Router so ein, dass er es benutzt. Dadurch können Sie Ihren Server über einen Namen weltweit erreichen; der Router meldet seine Adresse beim Neuverbinden dorthin.

Zweitens müssen Sie Ihrem Router gestatten, aus dem Internet eingehende Anfragen, etwa die Zugriffe auf den IMAPS-Dienst an den E-Mail-Server weiterzuleiten. Diese Port-Weiterleitung brauchen Sie nur für eingehende, nicht aber für ausgehende Verbindungen. Sie müssen nicht den Standard-Port, etwa 993 für IMAPS nutzen, sondern können einen beliebigen (maximal 65535) nehmen – der Router schreibt die Zugriffe geeignet um. Der Client muss freilich die Konfiguration eines Ports erlauben.

Wer sein E-Mail-Archiv auf diese Weise öffnet, muss sich darüber im Klaren sein, dass er Risiken eingeht: Die Server-Software selbst könnte Sicherheitslücken aufweisen, etwa E-Mails preisgeben oder ein Sprungbrett für Angriffe ins interne Netz sein. Aufwendig, aber sicherer ist ein VPN-Zugang (siehe Seite 72, „Zugang von außen"). Letztlich sollte man die direkte Verbindung mit dem Internet nur wagen, wenn ein regelmäßiger Blick in die Protokolldateien der Software Bestandteil der Routine wird. (ad)

Raspberry Pi als privater Server

Der Inhalt privater E-Mails ist viel zu persönlich, um sie auf Dauer einem Fremden anzuvertrauen. Zu groß ist die Versuchung, den Inhalt zu Werbezwecken auszuwerten oder an Big Brother weiterzugeben. Unser Vorschlag: Ein eigener Mail-Server auf Basis des stromsparenden Raspberry Pi kostet Sie nicht einmal 60 Euro.

Von **Mirko Dölle, Axel Kossel**

Mit einem eigenen IMAP-Server, der die E-Mails für Sie abruft, lokal aufbewahrt, beim Provider löscht und für den PC und die mobilen Geräte bereitstellt, holen Sie Ihre digitale Post nach Haus. Zudem soll der Server E-Mails von Geräten aus dem lokalen Netz entgegennehmen, was für Multifunktionsgeräte mit Scan-to-Mail-Funktion äußerst praktisch ist, da die gescannten Dokumente keinen Umweg mehr über das Internet machen müssen. Ein Web-Frontend für einen einfachen Zugriff auf die E-Mail-Konten komplettiert den Server und bringt nebenbei noch einen Apache-Webserver inklusive SSL-Verschlüsselung, PHP und einer MySQL-Datenbank mit. So wird der Server zu einem vollwertigen LAMP-Server (Linux, Apache, MySQL, PHP) inklusive IMAP.

Auch wenn die Versuchung groß sein mag, eignen sich alte Rechner für dieses Vorhaben nicht, denn ein IMAP-Server läuft üblicherweise im Dauerbetrieb. Bei einer Leistungsaufnahme von 30 Watt und mehr verursachen selbst sparsame ältere Rechner Stromkosten von über 75 Euro pro Jahr. Daher empfehlen wir als Server-Hardware den Raspberry Pi, den Sie inklusive Netzteil, Gehäuse und Speicherkarte schon für unter 60 Euro bekommen. Damit amortisiert sich das Rechnerchen schon im ersten Jahr allein über den geringeren Stromverbrauch.

RASPBIAN INSTALLIEREN

Als Betriebssystem kommt die Debian-Variante Raspbian zum Einsatz, das Image des aktuellen Stable Release Wheezy finden Sie in komprimierter Form als sogenanntes Raw Image auf raspberrypi.org zum Download (siehe c't-Link). Haben Sie das Speicherkarten-Image aus dem Zip-Archiv entpackt, übertragen Sie es auf die Speicherkarte. Dazu öffnen Sie unter Linux ein Terminal und geben folgenden Befehl ein:

```
dd if=2013-05-25-wheezy-raspbian.img of=/dev/sdX bs=4M
```

Welchen Gerätenamen (/dev/sdX) Ihre Speicherkarte hat, finden Sie unter Linux am einfachsten mit Hilfe des Partitionierungsprogramms GParted heraus. Windows-Anwender können das Image mit dem Win32 Disk Imager (siehe c't-Link) auf die Speicherkarte übertragen und müssen nicht erst ein Live-Linux booten. Das Raspbian-Image würde mit einer Größe von nicht einmal 2 GByte auf eine 2-GByte-SD-Karte passen, Sie benötigen jedoch noch Speicherplatz für zusätzliche Pakete und Ihre E-Mails - Speicherkarten unter 4 GByte sind also völlig ungeeignet; bei Karten mit 16 GByte oder mehr sind Sie auf der sicheren Seite.

Der Bootvorgang von Raspbian endet mit dem Start des Konfigurationsprogramms raspi-config auf der Textkonsole. Der erste Schritt ist, das nicht einmal

2 GByte große Raspbian-Image auf die ganze Speicherkarte auszudehnen, um den zusätzlichen Platz überhaupt nutzen zu können. Dazu wählen Sie im Konfigurationsprogramm gleich den ersten Menüpunkt „Expand Filesystem". Anschließend sollten Sie noch im Menü „Internationalisation Options" die Zeitzone und die Tastaturbelegung anpassen, mit „Change User Password" das Standard-Passwort „raspberry" für den Benutzer „pi" ändern und schließlich im Menü „Advanced Option" SSH aktivieren, damit Sie die weitere Einrichtung per Fernzugriff erledigen können. Mit „Finish" schließen Sie die Erstkonfiguration ab, woraufhin der Raspberry Pi neu startet.

Im nächsten Schritt müssen Sie die Netzwerkkonfiguration anpassen. Raspbian verwendet standardmäßig nur IPv4 und konfiguriert den Netzwerkanschluss per DHCP. Für den Server-Betrieb ist es allerdings sinnvoll, dem Minirechner eine feste IP-Adresse zuzuweisen – schließlich müssen Sie diese IP-Adresse auch bei Ihren mobilen Geräten eingeben, um auf Ihre E-Mails zugreifen zu können. Ein Wechsel der IP-Adresse wäre insofern unpraktisch. Welche IP-Adresse der Raspberry Pi erhalten hat, erfahren Sie übrigens am Ende des Bootvorgangs in der letzten Systemmeldung.

Da Raspbian praktisch vollständig kompatibel zu Debian GNU/Linux ist, ist die Einrichtung einer statischen IP-Adresse für Debian-erfahrene Anwender nicht weiter schwierig. Dazu editieren Sie lediglich die Datei /etc/network/interfaces als Root-Benutzer. Um Root zu werden, geben Sie nach der Anmeldung als Benutzer pi das Kommando „sudo su -" im Terminal ein oder verwenden „sudo", um ein Programm mit Root-Rechten zu starten. Als Editor zum Bearbeiten der Netzwerkkonfiguration können Sie zum Beispiel pico verwenden:

```
sudo pico /etc/network/interfaces
```

Die DHCP-Konfiguration der Netzwerkschnittstelle versteckt sich hinter folgender Konfigurationszeile:

```
iface eth0 inet dhcp
```

Für eine statische IP müssen Sie „dhcp" in „static" ändern und dann die IPv4-Konfigurationsdaten in weiteren Zeilen angeben, hier ein Beispiel für die IP-Adresse 192.168.178.2:

```
iface eth0 inet static
  address 192.168.178.2
  netmask 255.255.255.0
  gateway 192.168.178.1
```

Die IP-Adresse des Nameservers tragen Sie direkt in der Datei /etc/resolv.conf ein:

```
nameserver 192.168.178.1
```

Mit „sudo reboot" starten Sie den Raspberry Pi neu, anschließend erreichen Sie ihn unter der neuen IP-Adresse.

Ziel ist es, den Raspberry Pi zu einem LAMP-Server mit IMAP und Web-Mail aufzurüsten, wozu Sie mehrere Dienste einrichten müssen: den Apache Webserver, PHP, die MySQL-Datenbank, den lokalen Mail-Server Exim, den IMAP-Server Dovecot und Roundcube als Web-Mail-Frontend.

Zunächst installieren Sie Exim 4, das als MTA (Mail Transfer Agent) für die Zustellung von E-Mails im System zuständig ist:

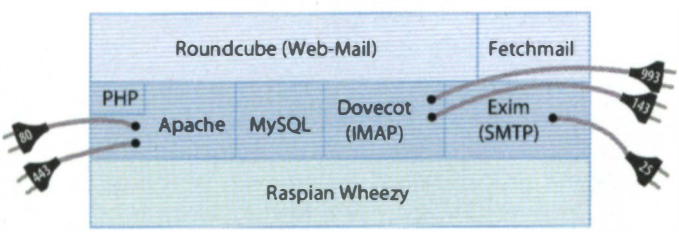
```
sudo aptitude install exim4
```

In der Standardkonfiguration stellt Exim die E-Mails entweder lokal zu, wenn sie zum Beispiel an den Standard-Benutzer pi gerichtet sind, und versucht ansonsten, die Mails direkt an den Mail-Server des Empfängers auszuliefern. Das klappt aufgrund der heutigen Spam-Abwehr in der Regel nicht mehr: Die IP-Adressbereiche von DSL-Anschlüssen stehen bei den Mail-Servern der Provider üblicherweise auf einer Blacklist. Daher benötigen Sie in der Praxis weiterhin ein Postfach bei einem Provider, über das Exim die E-Mails verschicken kann.

Die Konfiguration von Exim erledigen Sie menügeführt im Terminal mit dem Kommando:

```
sudo dpkg-reconfigure exim4-config
```

Wichtig ist, dass Sie als Adressen für eingehende SMTP-Verbindungen sowohl 127.0.0.1 als auch die IPv4-



Damit IMAP-Server, Web-Mail und Mail-Abholung funktionieren, müssen Sie den Raspberry Pi erst zum LAMP-Server aufrüsten.

Adresse des Raspberry Pi, im Beispiel 192.168.178.2, angeben. Als Trennzeichen zwischen beiden Adressen verwenden Sie ein Semikolon. Damit Exim als sogenannter Smarthost arbeitet und auch E-Mails aus dem lokalen Netz entgegennimmt, müssen Sie außerdem bei „Machines to relay mail for" das gesamte Subnet eintragen, etwa „192.168.178.0/24". Schließlich erfragt der Konfigurationsassistent noch den Namen des Mail-Servers Ihres Providers, an den Exim ausgehende E-Mails weiterleiten soll, und das Format, in dem lokale E-Mails gespeichert werden sollen. Behalten Sie bei Letzterem die Standard-Einstellung „mbox format in /var/mail/" bei, da sonst das Einsortieren von E-Mails bestehender Mail-Konten mit Fetchmail nicht klappt.

Die Zugangsdaten für Ihr E-Mail-Postfach für den Versand hinterlegen Sie in Form einer Konfigurationszeile in der Datei /etc/exim4/passwd.client. Hier das Format:

```
mail.example.com:username:password
```

Um Ihr Passwort, wie heute üblich, verschlüsselt an den Mail-Server zu übertragen, müssen Sie noch die Datei /etc/exim4/exim4.conf.localmacros mit folgendem Inhalt anlegen:

```
MAIN_TLS_ENABLE = 1
```

Ob der Mail-Versand einwandfrei funktioniert, testen Sie direkt im Terminal des Raspberry Pi:

```
echo "Smarthost-Test" | mail -s Smarthost-Test user@example.com
```

Selbstverständlich müssen Sie die E-Mail-Adresse gegen Ihre eigene austauschen. Die Smarthost-Funktion des Raspberry Pi ist übrigens nicht dafür gedacht, dass lokale PCs, Smartphones und Tablets ihre E-Mails nun erst zum Raspberry Pi schicken: Die Benutzer können Ihre E-Mails weiterhin direkt beim Provider abliefern und sich den Umweg über den Raspberry Pi sparen – nützlich ist die Smarthost-Funktion vor allem für Multifunktionsgeräte mit Scan-to-Mail-Funktion, damit eingescannte Dokumente für lokale Anwender nicht erst einen Umweg über das Internet machen.

IMAP MIT DOVECOT

Bevor Sie Dovecot als IMAP-Server installieren, müssen Sie das Kernel-Modul ipv6 nachladen:

```
sudo modprobe ipv6
sudo aptitude install dovecot-imapd
```

Hintergrund ist, dass Dovecot standardmäßig für IPv4 und IPv6 konfiguriert ist, Raspbian aber nur für IPv4. Ohne IPv6-Unterstützung würde die Dovecot-Installation fehlschlagen. Um die IPv6-Unterstützung von Dovecot abzuschalten, müssen Sie in der Konfigurationsdatei /etc/dovecot/dovecot.conf folgende Zeile ergänzen:

```
listen *
```

Alternativ können Sie bei Raspbian die IPv6-Unterstützung aktivieren, indem Sie das Modul ipv6 in die Konfigurationsdatei /etc/modules eintragen, sodass es bei jedem Start automatisch geladen wird.

Damit ist Dovecot schon einsatzbereit und Sie können auf Ihrem PC etwa in Thunderbird ein neues Mail-Konto für den Benutzer pi Ihres Raspberry Pi einrichten. Das Mail-Passwort von „pi" ist dasselbe, mit dem Sie sich als Benutzer beim Raspberry Pi anmelden. Als IMAP-Server tragen Sie einfach die IP-Adresse des Raspberry Pi ein. Da Dovecot auch SSL unterstützt, können Sie neben dem unverschlüsselten Port 143 auch den SSL-Port 993 für die Mail-Abfrage verwenden. Allerdings erhalten Sie bei SSL die Warnung, dass Thunderbird die Authentizität des Zertifikats nicht überprüfen kann. Da es sich um ein selbst erstelltes Zertifikat handelt, ist das normal – Sie sollten zur Sicherheit aber den Fingerabdruck des Dovecot-Zertifikats überprüfen. Auf dem Raspberry Pi rufen Sie ihn folgendermaßen ab:

```
openssl x509 -fingerprint -in /etc/dovecot/dovecot.pem -noout
```

Sollen mehrere Benutzer ihre Mails auf dem Raspberry Pi speichern, müssen Sie für jeden ein eigenes Linux-Benutzerkonto auf dem Miniaturrechner einrichten. Das geht sehr leicht mit dem Kommando useradd, anschließend richten Sie mittels passwd das Passwort ein:

```
sudo useradd -m mmuster
sudo passwd mmuster
```

Genauso einfach ist es, den Benutzer mmuster wieder zu löschen:

```
sudo userdel -r mmuster
```

Vorsicht, dabei gehen sämtliche E-Mails und das Home-Verzeichnis des Benutzers auf dem Raspberry Pi verloren!

Mit der bisherigen Dovecot-Konfiguration haben Sie aufgrund des Mbox-Dateiformats für Ihre E-Mails (siehe Exim-Konfiguration) keine Möglichkeit, Unterordner im Posteingang anzulegen, um Ihre E-Mails sortieren zu können. Indem Sie Dovecot vom Dateiformat Mbox auf Maildir++ umstellen, lösen Sie das Problem elegant. Sie finden die Option in der Datei /etc/dovecot/conf.d/10-mail.conf:

```
mail_location = mbox:~/mail:LAYOUT=maildir++:INBOX=↵
                /var/mail/%u:CONTROL=~/mail/control
```

Mit dem Web-Mailer Roundcube können Sie auch von unterwegs auf Ihre E-Mails zugreifen – natürlich über eine verschlüsselte Verbindung.

Anschließend müssen Sie Dovecot neu starten:

```
sudo service dovecot restart
```

Damit verwendet Dovecot weiterhin eine Datei im Mbox-Format pro Mail-Ordner, erlaubt aber über den Dateinamen eine hierarchische Anordnung. Der Posteingang bleibt bei dieser Konfiguration weiterhin /var/mail/pi für den Standard-Benutzer pi, alle anderen E-Mails landen in Dateien unterhalb des Verzeichnisses mail im Home-Verzeichnis von pi. Den Papierkorb finden Sie zum Beispiel unter ~/mail/.Trash. Legen Sie etwa mit Thunderbird im Posteingang den Unterordner Gmail an, so speichert Dovecot die E-Mails dieses Unterordners in der Datei ~/mail/.INBOX.Gmail.

MAIL-KOLLEKTOR FETCHMAIL

Diese Dateihierarchie eignet sich optimal, um E-Mails mittels Fetchmail von mehreren externen Mail-Konten einzusammeln und in separaten IMAP-Unterverzeichnissen abzuspeichern. Dazu müssen Sie lediglich die Pakete fetchmail und procmail nachinstallieren:

```
sudo aptitude install fetchmail procmail
```

Die Konfiguration von Fetchmail nimmt jeder Benutzer selbst vor, indem er eine Konfigurationsdatei .fetchmailrc in seinem Home-Verzeichnis auf dem Raspberry Pi speichert. Hier ein Beispiel für den Mail-Abruf bei Google Mail via IMAP:

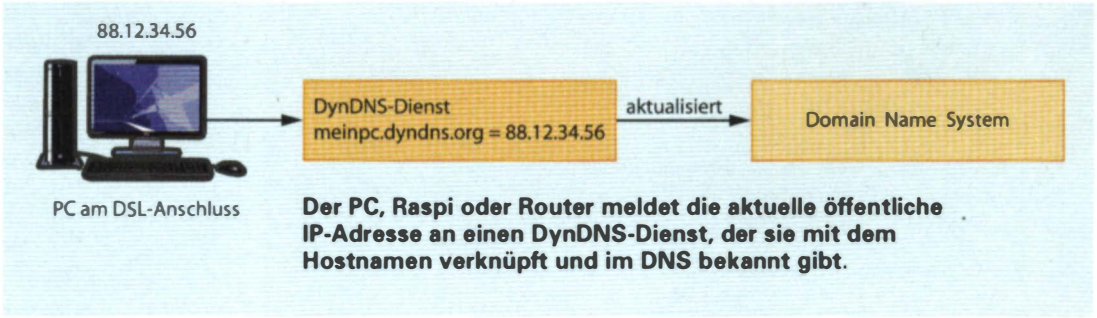
```
poll imap.gmail.com
  protocol IMAP
  user 'maxmuster@googlemail.com'
  is mmuster
  pass '123456'
  folder INBOX
  ssl
  mda 'formail -c >> ~/mail/.INBOX.Gmail'
  keep
```

Sie müssen lediglich die Zugangsdaten für Ihren Google-Mail-Account eintragen und den Namen des Benutzers auf dem Raspberry Pi, im Beispiel mmuster, gegen den korrekten Benutzernamen austauschen. Der Clou steckt in der vorletzten Zeile: Dort wird das Programm formail verwendet, um die abgerufenen E-Mails in der Datei mail/.INBOX.Gmail zu speichern. Da formail lediglich das Mbox-Format unterstützt, war das der entscheidende Grund für die Wahl dieses Dateiformats für Exim und Dovecot.

Nachdem Sie die Konfigurationsdatei mit dem Befehl chmod 600 .fetchmailrc vor neugierigen Blicken anderer Benutzer geschützt haben, rufen Sie Fetchmail von Hand auf, um die Funktion zu überprüfen:

```
fetchmail -v
```

Die Option keep am Ende der Fetchmail-Konfiguration sorgt dafür, dass zunächst keine E-Mail von den Google-Servern gelöscht wird - also nichts verloren geht, sollten Sie ein Problem entdecken. Diese Option sollten Sie erst entfernen, wenn Sie den Raspberry Pi einige Tage verwendet haben. Müssen Sie noch einmal alle E-Mails abrufen, so starten Sie Fetchmail mit dem Parameter -a. Funktioniert die Fetchmail-Konfiguration, legt jeder Benutzer selbst einen Cron-Job an. Dazu loggt er sich per SSH ein und gibt den Befehl



Der PC, Raspi oder Router meldet die aktuelle öffentliche IP-Adresse an einen DynDNS-Dienst, der sie mit dem Hostnamen verknüpft und im DNS bekannt gibt.

crontab -e zum Editieren der Cron-Konfiguration ein. Am Dateiende fügt man dann an:

```
0,15,30,45 * * * * /usr/bin/fetchmail -s
```

Damit schaut der Raspberry Pi alle vollen 15 Minuten nach neuen E-Mails.

WEB-MAILER MIT SSL

Um auch unterwegs von einem fremden PC aus in die E-Mails schauen zu können, ohne erst ein E-Mail-Programm installieren zu müssen, ist der Web-Mailer Roundcube eine gute Wahl. Wichtig ist allerdings, dass auch hier die Datenübertragung per SSL verschlüsselt erfolgt. Dazu müssen Sie zunächst Apache, PHP und MySQL nachinstallieren:

```
sudo aptitude install apache2 mysql- client mysql-server php5-mysql
```

Damit Apache auch SSL unterstützt und nutzt, müssen Sie noch ein eigenes Zertifikat erstellen und SSL aktivieren. Dies erledigen Sie mit den folgenden Befehlen:

```
sudo mkdir /etc/apache2/ssl
sudo make-ssl-cert /usr/share/ssl-cert/7
                                ssleay.cnf /etc/apache2/ssl/apache.pem
sudo a2ensite default-ssl
sudo a2enmod ssl
```

Kontrollieren Sie nun mit einem Browser, ob Sie Ihren Raspberry Pi nun sowohl per HTTP als auch per HTTPS erreichen können. Beim Zugriff via HTTPS warnt der Browser vor einem unbekannten Zertifikat, genau wie Thunderbird beim ersten Zugriff auf Dovecot. Auch hier sollten Sie den Fingerabdruck des Zertifikats überprüfen:

```
openssl x509 -fingerprint -in /etc/apache2/ssl/apache.pem -noout
```

Anschließend geht es an die Einrichtung von Roundcube:

```
sudo aptitude install roundcube-core roundcube-mysql
```

Während der Konfiguration startet ein Assistent, der verschiedene Parameter für Roundcube abfragt. Wichtig ist, dass Sie als Datenbank MySQL auswählen, ansonsten übernehmen Sie die Standardeinstellungen. Ist die Roundcube-Installation abgeschlossen, müssen Sie noch zwei Alias-Angaben in der Datei /etc/apache2/conf.d/roundcube eintragen:

```
Alias /roundcube/program/js/tiny_mce/ /usr/share/tinymce/www/
Alias /roundcube /var/lib/roundcube
```

Nach einem Neustart von Apache mittels `sudo service apache2 restart` können Sie dann Roundcube unter https://192.168.178.2/roundcube aufrufen. Für den Zugang von außen aktivieren Sie eine Port-Weiterleitung von Port 443 auf den Raspberry Pi, womit wiederum nur verschlüsselte Aufrufe möglich sind. Natürlich können Sie Apache auch dafür nutzen, um eine Homepage mit dem Raspberry Pi bereitzustellen - in diesem Fall sollten Sie auch für den Port 80 noch eine Weiterleitung in Ihrem DSL-Router einrichten.

ZUGANG VON AUSSEN

Um von unterwegs auf den Raspi zugreifen zu können, müssen Sie die IP-Adresse kennen, die der Provider Ihrem DSL-Router zugeteilt hat. Da diese sich üblicherweise täglich ändert, sollten Sie einen dynamischen Domain Name Service (DynDNS) nutzen. Diesem teilt Ihr Router die aktuelle IP-Adresse mit, damit der Dienst sie einer statischen Klartextadresse zuordnet. Letztere nutzen Sie dann im Browser oder Mobil-Client.

Die Router-Hersteller AVM und D-Link stellen ihren Kunden DynDNS kostenlos zur Verfügung (siehe c't-Link). Aber auch viele andere Router enthalten einen DynDNS-Client. Damit sollten sich auch kostenlose

Dienste wie Afraid.org (auch IPv6), SPDNS oder Two-DNS nutzen lassen. Sie müssen dort ein Konto anlegen, eine Klartextadresse (Hostname) wählen und die Zugangsdaten anschließend im Router eintragen.

Falls sich Ihr Router nicht zum Zusammenspiel mit dem Dienst bewegen lässt, können Sie auch auf dem Raspi einen DynDNS-Client installieren:

```
sudo aptitude install ddclient
```

Nach der Installation startet der Konfigurationsclient. Um zum Beispiel SPDNS zu nutzen, wählen Sie als Anbieter „anderer", als Server „www.spdns.de „ und als Protokoll „dyndns2". Dann müssen Sie den Benutzernamen angeben, unter dem Ihr Konto bei SPDNS läuft, sowie das Passwort. Als Nächstes geben Sie die Netzwerkschnittelle des Raspi an (eth0) und den Hostnamen, den Sie bei SPDNS angelegt haben. Danach wird ddclient gestartet und meldet alle 5 Minuten die aktuelle IP-Adresse an den Dienst. Sie müssen die dazugehörige Konfigurationsdatei aber noch bearbeiten:

```
sudo nano /etc/ddclient.conf
```

Ersetzen Sie die Zeile mit „eth0" durch folgende beiden:

```
use=web, web=myip.spdns.de
if=eth0
```

Über den Hostnamen erreichen Sie jetzt den Router. Um zum Mail-Server durchzudringen, können Sie alle Anfragen an den zum Dienst gehörigen Port – also 443 für Webmail oder 993 für IMAP über SSL – zur internen IP-Adresse (zum Beispiel 192.168.178.2) des Raspi durchleiten. Diese Portfreigaben lassen sich im Setup-Menü des Routers einfach einstellen. Dann kann aber auch jeder andere aus dem Internet auf Ihren Mail-Server zugreifen und ihn auf Sicherheitslücken abklopfen. Das wird passieren – und wehe, Sie haben einen Fehler gemacht!

Prinzipiell könnten Sie auch für Port 25 von Exim eine Port-Weiterleitung einrichten. Damit könnten Sie dann Ihre E-Mails direkt empfangen, wenn Sie zum Beispiel eine eigene Domain besitzen und dort den dynamischen Hostnamen als MX (Mail Exchanger) eintragen. Wir raten allerdings dringend davon ab: Dynamische Hostnamen könnten missbraucht werden oder in fremde Hände fallen, womit Ihre E-Mails dann beim falschen Server landen würden. Zudem würde bei den häufig auftretenden Spam-Attacken Ihre DSL-Leitung ausgelastet. Zuverlässiger ist es, zumindest ein Konto bei einem Provider einzurichten und dieses, wie für Google Mail gezeigt, per Fetchmail auszulesen. Auf die Privatsphäre hat das keinen Einfluss, denn E-Mails werden ohnehin im Internet offen befördert und schon ein einfaches DNS-Spoofing würde dafür sorgen, dass Big Brother Ihre Mails vor Ihnen erhält.

Alle Links zum Artikel
www.ct.de/hb1401068

PRIVATWEG

Sicherer als die Port-Weiterleitung, aber auch aufwendiger ist es, die Authentifizierung und Verschlüsselung auf ein vorgeschaltetes Virtual Private Network (VPN) zu verlagern. Viele DSL-Router enthalten VPN-Lösungen. Damit bauen Sie erst einen verschlüsselten Tunnel in ihr Heimnetz auf und können darüber dann auf den Raspi zugreifen. Der Vorteil dieser Lösung: Nur wer sich erfolgreich beim VPN anmeldet, kommt an Ihren E-Mail-Server ran. Sie ist ideal, wenn Sie mit eigenen Mobilgeräten auf den Server zugreifen wollen. An fremden PCs werden Sie hingegen meist keinen VPN-Client einrichten können.

Das Einrichten des VPNs am Router ist je nach Modell und Verfahren unterschiedlich; manche Router bringen mehr als ein VPN-Verfahren mit. Zu den gängigen gehören IPSec, L2TP over IPSec und SSL-VPNs wie OpenVPN. Viele Router haben auch noch das längst geknackte PPTP an Bord, das nicht genug Schutz bietet – lassen Sie also die Finger davon.

Ein Sonderfall ist die IPSec-Lösung älterer FritzBoxen, die mit spezieller Software arbeitet. Sie ist auf dem VPN-Service-Portal von AVM gut dokumentiert. Bei der FritzBox 7490 geht AVM neue Wege bei der VPN-Einrichtung. Mehr darüber erfahren Sie über den c't-Link unten. Bei anderen Routern ist das sichere und komfortabel einzurichtende L2TP over IPSec eine gute Wahl. Denn Windows, Mac OS X, Android und iOS haben L2TP ab Werk an Bord. Auch auf der Router-Seite ist dessen Einrichtung unkompliziert – folgen Sie der Dokumentation, schalten Sie den Dienst ein und fügen Sie die Konten der VPN-Nutzer hinzu. Passwörter (Preshared-Keys, PSK) vereinfachen gegenüber den SSL-Zertifikaten die Authentifizierung zwischen den Gegenstellen. Verwenden Sie dafür eine möglichst lange, nicht leicht nachvollziehbare Kombination aus Buchstaben und Ziffern; vermeiden Sie aber Sonderzeichen.

Bauen Sie dann eine VPN-Verbindung auf, beispielsweise per Smartphone über Mobilfunk. Um den Zugang zu testen, können Sie zum Beispiel mit dem Kommando „ping" den Raspi über seine interne IP-Adresse (192.168.178.2) ansprechen oder gleich auf den E-Mail-Server zugreifen. (mid) c't

Rechtlicher Rahmen für Mailserver

Hat man den eigenen Nachnamen endlich als Domain ergattert, wollen oft auch Verwandte unter dieser eine E-Mail-Adresse haben. Doch egal ob auf einem selbst betriebenen Mail-Server oder beim Provider: Wer anderen ein Postfach einrichtet, wird zum Telekommunikationsanbieter und muss strenge gesetzliche Vorgaben beachten.

Von **Joerg Heidrich**

Eine von mehreren Familienmitgliedern genutzte Mail-Adresse, ein Server in der WG oder gar ein gemeinsames Netz mit den Nachbarn: Die Möglichkeiten, sich einen Mailserver zu teilen, sind vielfältig. Nicht anders als in einem Unternehmen oder bei einem Provider unterliegt jedoch der Administrator dieses geteilten Angebots rechtlichen Vorgaben. Vor allem darf er nicht uneingeschränkt auf an andere gerichtete Nachrichten zugreifen, um diese zu lesen, zu verändern oder zu löschen.

Ausgangspunkt der gesetzlichen Regelungen ist Paragraf 88 des Telekommunikationsgesetzes (TKG). Darin wird festgelegt, dass jeder „Diensteanbieter" zur Wahrung des Fernmeldegeheimnisses verpflichtet ist. Unter den Begriff des Diensteanbieters fällt jedes Unternehmen und jede Privatperson, soweit diese „ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken".

GESCHÄFTSMÄSSIG

Das klingt ganz so, als ob diese Vorschrift nur dann anwendbar wäre, wenn jemand mit seinen Mail-Diensten ein Geschäft macht und Geld verdient. Aber das Gesetz versteht unter dem Merkmal der Geschäftsmäßigkeit das „nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht". Es macht also aus juristischer Sicht keinen Unterschied, ob jemand für das Betreiben des Mailservers Geld verlangt oder nicht.

Daher fallen darunter auch nichtkommerzielle Angebote im Familien- und Bekanntenkreis wie das Bereitstellen von E-Mail-Zugängen, sofern das Ange-

bot über einen gewissen Zeitraum zur Verfügung steht und nicht lediglich einmalig erfolgt. Ausgenommen sind nur solche Zugänge, die für eigene Zwecke und eben nicht für Verwandte und Freunde bereitgehalten werden.

Darüber hinaus gilt das Fernmeldegeheimnis auch für Personen, die an der Erbringung von E-Mail-Zugängen mitwirken. Für den privaten Bereich bedeutet dies, dass die gesetzlichen Regelungen nicht nur gelten, wenn man einen eigenen Mail-Server betreibt, sondern auch für Postfächer, die man für Familienmitglieder und Bekannte bei einem Provider einrichtet und verwaltet.

FERNMELDEGEHEIMNIS

Kern des Fernmeldegeheimnisses ist das sogenannte Kenntnisnahmeverbot, das sowohl für den Inhalt von Mails als auch die „näheren Umstände" der Telekommunikation gilt. Unter die näheren Umstände fällt insbesondere die Frage, wer an einem Telekommunikationsvorgang beteiligt ist oder war. Allerdings kann man kaum einen Mailserver verwalten, ohne zumindest gelegentlich Adressfelder zu sehen und in Einzelfällen sogar auf die Inhalte von Nachrichten zugreifen zu müssen.

Diesem Umstand trägt der Gesetzgeber dadurch Rechnung, dass er die Kenntnisnahme ausnahmsweise erlaubt, wenn sie zur Erbringung des Dienstes und zum Schutz der technischen Systeme erforderlich ist. Für Daten, auf die unter diesen Gesichtspunkten zugegriffen wird, gilt dann eine strenge Zweckbindung: Sie dürfen ausschließlich für Administrationszwecke genutzt und insbesondere nicht weitergegeben werden.

Leider regelt der Gesetzgeber aber nur ansatzweise, unter welchen Umständen genau der Admin auf vertrauliche Daten zugreifen darf. Ein Ausgangspunkt dafür sind die Bestimmungen über den Datenschutz und die Bestimmungen über die öffentliche Sicherheit im TKG, die aber auf größere Provider ausgelegt sind. Für einen privaten Mail-Besorger im Familien- und Freundeskreis ergibt sich daraus, dass ein Zugriff auf fremde Mails in der Regel für ihn tabu ist. Eine Ausnahme liegt etwa dann vor, wenn er Anhaltspunkte dafür hat, dass eine Mail Schadsoftware enthält.

CYBER-ATTACKEN

Eine weitere wichtige Ausnahme der engen Zugriffsvoraussetzungen liegt dann vor, wenn der Mail-Empfänger explizit zugestimmt hat. In der Praxis wäre dies zum Beispiel der Fall, wenn er den Admin darum bittet, für ihn eine bestimmte Mail herauszusuchen oder zu löschen. Eltern agieren als gesetzliche Stellvertreter des minderjährigen Nachwuchses und dürfen als solche in dessen Mails schauen.

Auch dürfte dann ein ansonsten unzulässiger Zugriff auf Mails und deren Inhalte ausnahmsweise erlaubt sein, wenn der Mailserver Ziel eines Online-Angriffs ist, etwa durch ein Mail-Bombing, und der Admin Maßnahmen ergreifen muss, um das Funktionieren des gesamten Systems zu erhalten. Das betrifft nicht nur den selbst betriebenen Server, sondern auch Postfächer beim Provider, wenn beispielsweise der freie Speicher zur Neige geht.

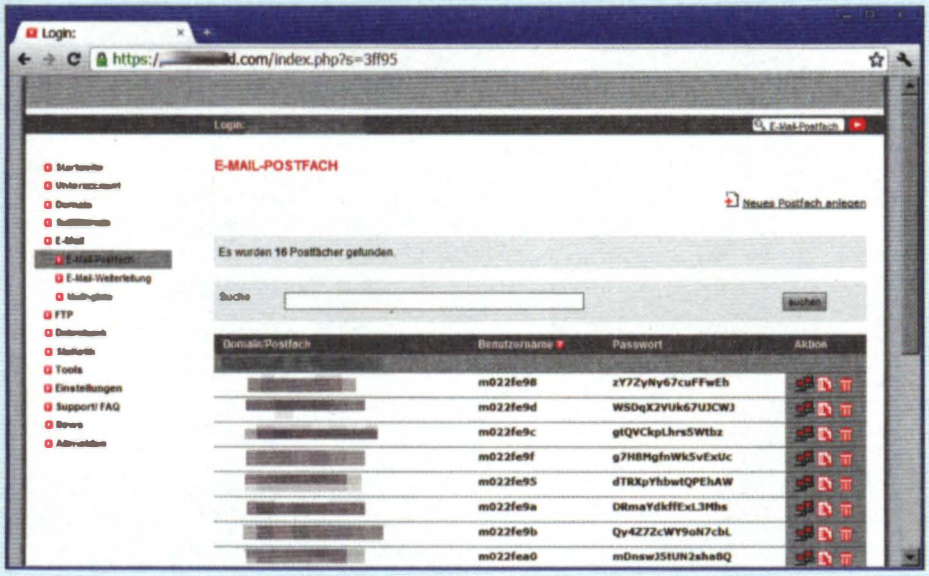
Im gesamten Bereich von potenziell strafbaren Handlungen ist auch der Betreiber eines privaten E-Mail-Servers - nicht anders als ein professioneller Provider - verpflichtet, mit den Strafverfolgungsbehörden zu kooperieren. Zwar besteht keine Pflicht zur Datenspeicherung auf Vorrat. Auf Anfrage von Polizei, Staatsanwaltschaft und Co. muss der Anbieter jedoch die angeordnete Überwachung und Aufzeichnung der Telekommunikation ermöglichen. Zudem muss er gegebenenfalls gegenüber den Behörden Auskunft über die anfallenden Daten erteilen und diese herausgeben.

Schließlich sind private ebenso wie hauptberufliche Admins verpflichtet, im Rahmen ihrer Tätigkeit auch zufällig erlangte Kenntnisse über schwere Straftaten bei der Polizei anzuzeigen. Unterlassen sie dies, so droht ihnen nach Paragraf 138 des Strafgesetzbuchs (StGB) selbst eine Freiheitsstrafe von bis zu fünf Jahren oder eine Geldstrafe. Allerdings gilt diese Vorschrift nur für Kapitalverbrechen wie Mord, Raub oder Geldfälschung. Nicht erfasst sind zum Beispiel Verstöße gegen das Urheberrecht, für die keine Pflicht zu einer Anzeige besteht.

SCHADENSERSATZ UND UNTERLASSUNG

Wer als Betreiber eines privaten Servers gegen die Vorgaben des Fernmeldegeheimnisses verstößt, muss mit unangenehmen Folgen rechnen. Möglich sind vor allem Schadensersatz-, aber auch Unterlassungsansprüche, die mit teuren Abmahnungen geltend gemacht werden können.

In schweren Fällen, etwa wenn ein Admin intime Mail-Inhalte wie Krankenberichte oder Aktfotos weitergibt, die dann in Blogs oder auf Facebook auftauchen, kann ein Mail-Nutzer ihm sogar einen immateriellen Schaden in Rechnung stellen. Das mag



Bekommt der Mail-Admin wie hier alle Zugangsdaten im Klartext angezeigt, kann er auch E-Mails unter fremden Namen versenden. Falls dann etwa Beleidigungen über einen Account verschickt wurden, kommt er als Urheber infrage.

zunächst unwahrscheinlich klingen, aber auch ein unbegründeter Verdacht kann für viel Verdruss sorgen. Letztlich hängt es von der Streitbarkeit der Verwandten und Freunde ab, ob der Admin mit Ärger rechnen muss. Spätestens bei Zerwürfnissen und Trennungen zahlt es sich aus, wenn man eine schriftliche Vereinbarung abgeschlossen hat.

Sie sollte die Haftung des Admins für fahrlässige Handlungen beschränken und die Fälle, in denen er ausnahmsweise auf Mails zugreifen darf, genau regeln. Ausgangspunkt für solche Vereinbarungen können zum Beispiel die allgemeinen Geschäftsbedingungen von E-Mail-Providern sein. Ein vorsätzlicher Missbrauch von Admin-Rechten wie im genannten Beispiel lässt sich aber nicht durch einen Haftungsausschluss legitimieren.

HAFTUNGSRISIKEN

Jenseits einer Verletzung des Fernmeldegeheimnisses stellt sich die Frage, wer zivil- und strafrechtlich für Rechtsverletzungen haftet, die über die bereitgestellten E-Mail-Zugänge begangen werden. Im Bereich des Strafrechts könnten dies zum Beispiel per Mail versandte Beleidigungen oder falsche Bestellungen sein.

Dabei wird der ahnungslose Betreiber des Servers im Normalfall keine Verurteilung zu befürchten haben. Wie auch im Bereich von geteilten WLAN-Zugängen werden sich die Strafverfolgungsbehörden bei ihren Ermittlungen allerdings erst einmal an den Inhaber der IP-Adresse oder der Mail-Domain wenden. Dies kann unangenehm genug sein, etwa wenn in Fällen schwerer Kriminalität eine Hausdurchsuchung stattfindet.

Der Admin wird dann im Zweifelsfall nachweisen müssen, dass nicht er die besagte Nachricht verschickt hat, sondern dies über einen von ihm betreuten Account geschah. Dazu sollte er glaubhaft machen können, dass er die Zugangsdaten nicht kannte, die zum Versand der Nachricht notwendig waren.

MÜLL ENTSORGEN

Im Bereich der Unternehmenskommunikation und bei Providern regelmäßig problematisch ist die Filterung von E-Mails auf Schadsoftware und Spam. Das Aussortieren von Viren, Würmern und Co. erachten die meisten Juristen als grundsätzlich zulässig. Dies gilt zumindest dann, wenn Software die Mails automatisch prüft, ohne dass im Normalfall ein Admin die Mails manuell öffnet. In diesem Fall geht man davon aus, dass die Schadsoftware eine akute Gefahr für die IT-Sicherheit der eigenen Systeme darstellt und daher sogar eine Löschung von verseuchten eingehenden Nachrichten ohne Kenntnis und Zustimmung des betroffenen Empfängers möglich ist.

Dies gilt sicher auch im Bereich von privaten Mailservern. Auch hier darf man davon ausgehen, dass eine mutmaßliche Einwilligung des Empfängers in Antiviren-Maßnahmen vorliegt, die eine Löschung auch hinsichtlich möglicher strafrechtlicher Konsequenzen rechtfertigt. Hierfür muss der Admin also keine Zustimmung einholen.

Anders sieht es bei der Filterung der eingehenden elektronischen Post auf Spam aus. Dies liegt vor allem daran, dass es keine allgemeingültige Definition von Spam für alle Empfänger gibt, sondern die Frage nach dem Charakter der einzelnen Mail immer individuell zu beurteilen ist. Denn was für den einen ungewollten Werbemüll darstellt, ist für den anderen unter Umständen eine hoch willkommene Information. Daraus resultiert der Grundsatz, dass der Betreiber eines Mailservers niemals ohne Wissen und Zustimmung des Empfängers an diesen gerichtete Nachrichten löschen, blocken oder aussortieren sollte.

Wie bei professionellen Anbietern empfiehlt es sich auch im Privatbereich, die Zustimmung der Empfänger zum automatischen Filtern und Löschen eingehender Mails vorab einzuholen, am besten schriftlich oder zumindest per Mail. Nicht nötig ist diese Prozedur nur dann, wenn die Spam-Filterung nicht zentral, sondern erst beim Empfänger geschieht. Ebenfalls zulässig ist das automatische Umsortieren von Mails, bei dem die Nachrichten nicht gelöscht, sondern lediglich markiert und in ein Spam-Postfach verschoben werden.

Für private Mail-Administratoren gibt es zumindest eine gute Nachricht: Professionelle Anbieter von E-Mail-Konten und auch Unternehmen verletzen beim unerlaubten Löschen von E-Mails ohne Wissen und Zustimmung des Empfängers das Post- oder Fernmeldegeheimnis nach Paragraf 206 StGB und machen sich damit strafbar. Private Betreiber müssen hier dagegen keine strafrechtliche Verfolgung fürchten. Denn diese Vorschrift gilt nach ihrem Wortlaut nur für „Inhaber oder Beschäftigte eines Unternehmens, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt".

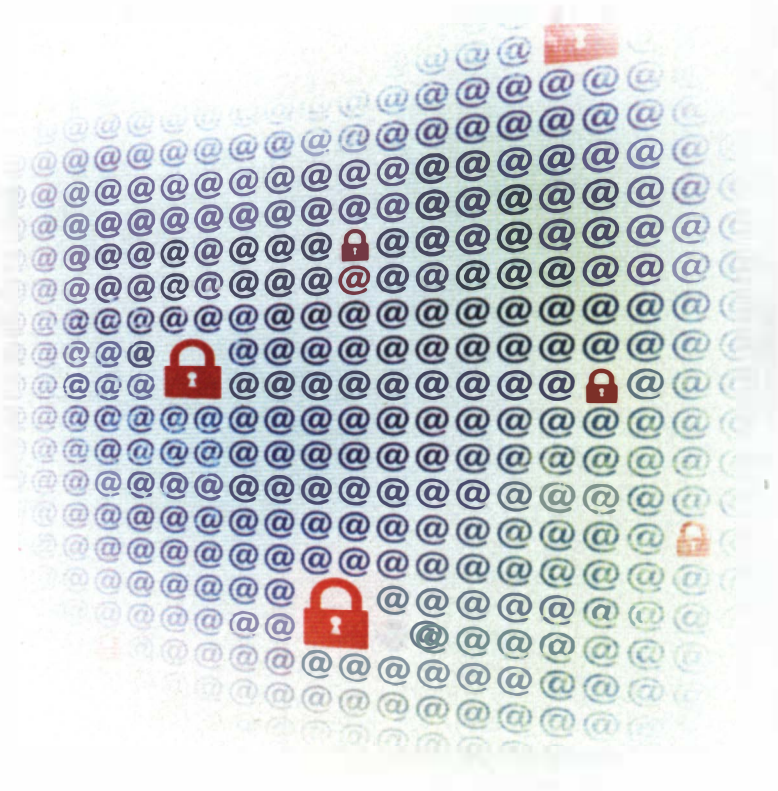
FAZIT

Wer im Familien-, Freundes- oder Bekanntenkreis einen gemeinsam genutzten E-Mail-Server betreibt, unterliegt wie auch ein professioneller Anbieter den Vorgaben des Fernmeldegeheimnisses. Danach ist ein Zugriff auf den Inhalt von Mails ebenso wie auf die beim Transport anfallenden Daten im Normalfall nur dann erlaubt, wenn dies für den Betrieb des Dienstes notwendig ist.

Verstößt der Admin gegen diese Vorgaben, so riskiert er eine eigene Haftung auf Unterlassung und Schadenersatz. Insoweit empfiehlt es sich gerade bei Nutzern außerhalb des engsten Familienkreises, eine kurze Vereinbarung zu schließen, die die Rechte und Pflichten des Admins regelt und die dessen Haftung für fahrlässige Handlungen ausschließt. Diese Vereinbarung sollte zudem noch einen Passus enthalten, der die Filterung von E-Mails nach Schadsoftware und Spam durch den Admin ausdrücklich erlaubt. (ad)

Joerg Heidrich ist Justiziar des Heise Zeitschriften Verlags und Rechtsanwalt in Hannover. c't

Vertraulich kommunizieren



Wenn der E-Mail- und Messaging-Verkehr privat bleiben soll, kann man auf vielfältige Methoden zurückgreifen. Manche dieser Verfahren erweisen sich aber bei näherem Hinsehen als unzureichend, andere als zu aufwendig. Eine Handvoll Faustregeln genügt jedoch, um das der jeweiligen Situation Angemessene zu finden.

Von **Dušan Živadinović**

Wenn man die Privatheit von elektronischen Nachrichten gewährleisten will, kann man prinzipiell zwei Szenarien unterscheiden: Im einfachen Fall geht es darum, den Inhalt der ausgetauschten Nachrichten für Dritte unzugänglich zu halten. Dafür gibt es eine Reihe etablierter Verfahren, die aber allesamt noch Spuren hinterlassen (z. B. Absender- und Empfängeradressen, Uhrzeiten, IP-Adressen ...). Wenn man auch noch anonym bleiben will, muss man den Aufwand erhöhen und auf weniger gängige Programme ausweichen. Ganz spurlos lassen sich Mails und Instant Messages aber nicht versenden.

Zu den neuralgischen Punkten zählen Mail-Server, die mit gesetzlich angeordneten oder heimlich eingerichteten Abhörschnittstellen ausgerüstet sind. Außerdem sollte man die Mail-Server von US-Firmen wie Google, Yahoo oder Hotmail möglichst meiden und zur Kommunikation mit engen Freunden eigene Server aufsetzen. Solche dezentralen Strukturen sind sehr viel schwieriger zu belauschen als die großen Mail-Zentralen. Dieser Tipp gilt besonders für Büros und kleine Firmen, deren Mitarbeiter bei der internen Kommunikation über öffentliche Mail-Server womöglich ungewollt Vertrauliches preisgeben.

Wirklich vertraulich sind aber erst verschlüsselte Nachrichten. Aktuelle Verschlüsselungsverfahren setzen auf die asymmetrische Kryptografie, bei der jeder Teilnehmer selbst ein Schlüsselpaar aus privatem und öffentlichem Key lokal erzeugt. Die Technik schließt Mitleser aus und gewährleistet zugleich die Authentizität des Absenders. Sie gilt als sicher, solange der private Schlüssel geheim bleibt. Wer den öffentlichen Key eines Empfängers hat, kann ihm damit verschlüsselte Nachrichten senden, die nur der Empfänger lesen kann - weil sie sich nur mit seinem privaten Schlüssel entschlüsseln lassen.

MAILS ABHÄRTEN

Um beim Mail-Verkehr die Privatheit zu gewährleisten, genügen schon die gängigen Verfahren PGP und S/MIME, die den Inhalt der Nachrichten verschlüsseln. Programme gibt es für alle aktuellen Betriebssysteme, auch für Android und iOS. Wie man PGP und S/MIME einrichtet, haben wir ausführlich ab Seite 82 und 92 beschrieben. Ab Seite 42 lesen Sie, wie man PGP in Thunderbird nachrüstet. Beide Verfahren gründen auf asymmetrischen kryptografischen Schlüssel-

paaren; jeder Teilnehmer hat einen öffentlichen und einen privaten Schlüssel. Die Verfahren gelten so lange als sicher, wie Dritte keinen Zugriff auf die privaten Schlüssel haben. PGP bringt einen größeren Funktionsumfang, S/MIME gilt als komfortabler und besser in Betriebssysteme und Mail-Clients eingebunden.

MEHR VERSCHLÜSSELUNG

Wer unerkannt E-Mails versenden will, muss außer PGP und S/MIME weitere Techniken suchen, denn bei beiden bleiben die Kopfzeilen der Mails (Header) unverschlüsselt. So liegen Betreffzeilen, Absender- und Empfänger-IP-Adressen, aber auch Uhrzeiten und diverse andere Details offen.

Ein vom Konzept her einfacher Weg besteht darin, eigene Mail- und VPN-Dienste (Virtual Private Network) aufzusetzen. Alle vertrauenswürdigen Mail-Teilnehmer bekommen Zugang zum VPN und die Mail-Clients nutzen für den vertraulichen Verkehr ein separates Konto. Dieses Konto greift nur via VPN auf den Mail-Server zu, der von außen nicht erreichbar ist. Zu den gängigen VPN-Verfahren gehört IPSec, das einige Router und alle aktuellen Betriebssysteme an Bord haben.

Die Einrichtung und Verwaltung eines VPN ist aber nicht jedermanns Sache und wenn sich die Mail-Partner nicht kennen und keinen Weg haben, Zugangsdaten zum VPN sicher auszutauschen, kommt die Technik nicht in Frage.

REMAILER

Eine Alternative können Remailer-Dienste sein. Dabei handelt es sich um anonymisierende Internet-Dienste, die E-Mails annehmen, die ursprünglichen Header entfernen und den Rest zum Ziel weiterleiten. Der Empfänger bekommt nur die IP-Adresse des Remailers zu sehen; die IP-Adresse des Absenders bleibt geheim. So kann man unerkannt Nachrichten absenden. Wenn man eine Antwort haben will, kann man natürlich seine Mail-Adresse in den Mail-Inhalt schreiben und diesen verschlüsseln.

Angreifer können aber aus der Beobachtung des ein- und ausgehenden Remailer-Verkehrs dennoch Rückschlüsse darüber ziehen, wer mit wem kommuniziert. Dagegen haben Remailer-Entwickler mehrere Strategien entworfen, unter anderem die Verschlüsselung der gesamten Mail vor dem Versand, das zeitversetzte Weiterversenden oder auch die Verkettung von mehreren Remailern.

Remailer haben aber wie gewöhnliche Mail-Dienste eine zentralisierte Struktur, bei der man dem Anbieter vertrauen muss. Außerdem bleiben bei diesem Verfahren die Empfänger nicht anonym.

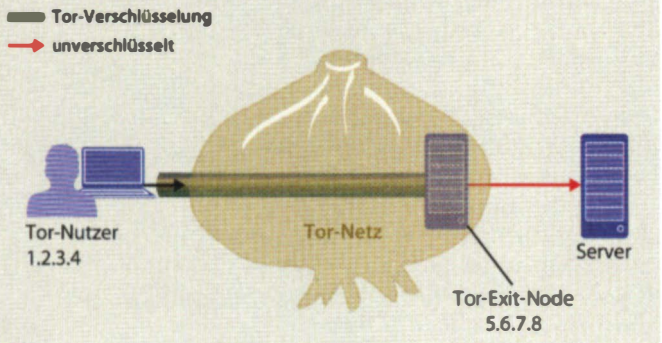
ANONYMES MAILEN

Wenn man das Anonymisierungsnetz Tor verwendet, können beide, Sender und Empfänger, anonym bleiben. Tor verschleiert den IP-Verkehr über diverse Verfahren und führt ihn an nicht vorhersehbaren Punkten ins Internet. Wenn man sich per Tor bei einem Mail-Anbieter einbucht, bleibt also unklar, woher der Zugriff stammt. Auf dem Weg durch das Tor-Netz werden die Daten verschlüsselt. Diese Verschlüsselung endet am Exit-Node. Der Absender muss daher den Inhalt der Mail zusätzlich verschlüsseln (siehe Seite 82), um ihn vor Mitlesern zu schützen. Gehen beide Mail-Partner so vor, bleiben sie unbelauscht und anonym.

Mittels GPG verschlüsselte Mails lassen sich auf allen gängigen Betriebssystemen erzeugen und versenden.

Tor als Anonymisierungsdienst

Für den Server sieht es so aus, als spräche er mit der Tor-Exit-Node. Deren Betreiber kann den kompletten Verkehr mitlesen.



Eine Variante des Tor-Zugriffs besteht darin, beliebige öffentlich zugängliche Server, zum Beispiel Cloud-Dienste, zu verwenden und dort Nachrichten zu hinterlassen; dann freilich nicht als Mail-, sondern etwa als verschlüsselte Text-Dokumente. Voraussetzung dafür ist, dass sich die Kommunikationspartner die Zugangsdaten zum jeweiligen Dienst teilen.

MESSAGING OHNE MITHÖRER

Auf Instant-Messaging-Nachrichten lässt sich die asymmetrische Kryptografie ebenfalls anwenden. Viele Messaging-Clients verschlüsseln den Verkehr bereits. Die besonders häufig eingesetzten gelten jedoch als kompromittiert (z. B. das Skype-Messaging).

Es gibt aber diverse weitere Messaging-Clients, die die Privatheit gewährleisten. Das trifft auf iMessage von Apple zu, das den Datenverkehr verschlüsselt. iMessage ist in Mac OS X und iOS eingebaut. Wenn eine Nachricht nicht übers Internet zugestellt werden kann, weil der Empfänger nicht im Internet eingebucht ist, stellt das Programm den Text per SMS zu – und die kann an den Mobilfunkschnittstellen von Dritten gelesen werden. Die SMS-Zustellung lässt sich aber abschalten.

Ähnlich vertrauenswürdig erscheint der Messaging-Dienst Threema. Clients gibt es bisher nur für Android und iOS. In Apples App Store und über Google Play ist das Programm für unter 2 Euro erhältlich. Es setzt ebenfalls auf die asymmetrische Kryptografie, erzeugt also einen privaten und einen öffentlichen Schlüssel. Den öffentlichen Schlüssel zeigt es als QR-Code an. Den kann man dann Gesprächspartnern persönlich aushändigen, die ihn vor Gebrauch mit der Smartphone-Kamera einlesen.

Alle Links zum Artikel
www.ct.de/hb1401078

OTR-MESSENGER

Einen Schritt weiter gehen Messaging-Programme, die das OTR-Protokoll einsetzen (Off The Record). Es verschlüsselt Nachrichten und wahrt gegenüber Lauschern die Anonymität der Teilnehmer. Dazu erzeugt es mehrere private Schlüssel und nutzt unterschiedliche für die Authentifizierung der Teilnehmer untereinander und die Verschlüsselung. Die zur Nachrichtenverschlüsselung eingesetzten werden später verworfen, sodass keine Rückschlüsse auf den Absender möglich sind und die für die Authentifizierung übertragenen Elemente werden veröffentlicht, sodass jeder Teilnehmer sie genutzt haben könnte. Mit OTR übertragene Nachrichten lassen sich später mangels der Schlüssel nicht mehr lesen.

Derzeit wird OTR vorwiegend zusammen mit dem Messaging-Protokoll XMPP eingesetzt. Die Verschlüsselung lässt sich aber auch prima mit OSCAR (ICQ, AIM) und Microsofts MSN-Protokoll kombinieren. Voraussetzung ist ein Client, der OTR unterstützt. In Pidgin (Windows, Mac OS X, Linux) und Miranda (Windows) lässt es sich als Plug-in nachrüsten, andere wie Adium (Mac OS X) unterstützen es direkt. (dz) c't

Der Messenger Threema versendet Nachrichten Ende-zu-Ende-verschlüsselt.

Des Apfels Kern.

6 x im Jahr das Neueste von Mac & Co.
Abo-Dankeschön gratis.
Alle Vorteile genießen.

Gefällt mir!

Ihre Vorteile im Abo:

- Über 10% Preisvorteil
- Touch Screen Handschuhe gratis
- Portofreie Lieferung an Ihre Wunsch-Adresse

Bestellen Sie jetzt Ihr Abo!

www.mac-and-i.de/geschenk
040 300 735 25 Bitte Bestellcode MCP13131 nennen.
leserservice@heise.de

Verschlüsseln und signieren mit PGP

Noch können auch die Geheimdienste nicht überall mithören. Wenn Sie Ihre digitale Kommunikation wirksam vor Zugriff schützen wollen, steht dafür eine effektive und kostenlos nutzbare Technik bereit – Pretty Good Privacy (PGP). Hier erfahren Sie, wie es geht.

Von **Holger Bleich**

Es war ein Offenbarungseid der Bundesregierung auf dem Höhepunkt des NSA-Spähskandals. Der damalige Innenminister Hans-Peter Friedrich erklärte für selbstverständlich, dass alle Daten der Bürger von Dritten mitgelesen werden. Seine Konsequenz daraus: Jeder müsse mit technischen Maßnahmen selbst dafür sorgen, dass seine Daten vor fremdem Zugriff geschützt seien, sagte er Mitte Juli 2013. CSU-Innenpolitiker Hans-Peter Uhl assistierte: „Wem Daten wichtig sind, der muss sie verschlüsseln und darf nicht auf den eigenen Nationalstaat hoffen." Lächerlich mache sich dagegen, wer glaube, dass die Kanzlerin da zuständig sei.

Da war es also raus: Datenschutz ist Privatsache. Uns ist es selbst überlassen, ob und wie wir für die Sicherheit unserer Kommunikation sorgen. Der Staat fördert lediglich Scheinsicherheit, etwa im Fall von De-Mail, wo wirksame Verschlüsselung nur suggeriert wird. In Wirklichkeit zwingt das zugehörige Gesetz Provider dazu, die Mail auf ihren Servern zu entschlüsseln, um einen Virenscan durchzuführen (siehe Seite 36).

Vom Staat ist – das zeigt De-Mail deutlich – keine Unterstützung mehr zu erwarten. Tatsächlich sollten die Bürger ihre Kommunikation selbst verschlüsseln, wenn sie sie vor Zugriff schützen wollen. Doch aus Bequemlichkeit tun das noch zu wenige. Dies sorgt absurderweise sogar dafür, dass die wenigen, die Verschlüsselung im Alltag einsetzen, auffallen wie bunte Hunde, und vielleicht gerade deshalb in Verdacht geraten.

Daraus folgt: Je mehr Menschen sichere Verschlüsselungstechnik einsetzen, desto sicherer ist der Einzelne vor falschen Verdächtigungen. Die Snowden-Enthüllungen zu Lauschaktionen der NSA haben immerhin bewirkt, dass sich so viele Nutzer mit dem Thema beschäftigen wie noch nie zuvor – und das trotz aller Unkenrufe, E-Mail-Verschlüsselung sei schwer zu verstehen und im Tagesbetrieb viel zu unbequem einzusetzen.

UNKEN TROTZEN

Wer unkt, liegt falsch. Sichere Verschlüsselung kann jeder – zumindest auf dem heimischen Desktop – ohne nennenswerten Komfortverlust in seinen Mail-Alltag integrieren. Dies gilt für Privatpersonen genauso wie für kleine Unternehmen. In den großen Konzernen sor-

gen ohnehin die Admins für die Mitarbeiter dafür, dass vertrauliche Daten niemals im Klartext durch die Leitungen rauschen.

Das Verschlüsselungskonzept Pretty Good Privacy (PGP) erlebt zurzeit eine Renaissance – Vertrauenswürdigkeit von Kommunikation wird hier nicht von übergeordneten Instanzen beglaubigt, die kompromittiert sein könnten, sondern von allen Teilnehmern untereinander. Den nötigen Unterbau liefert seit Jahren das Open-Source-Projekt GnuPG mit der gleichnamigen Software, derzeit in Version 2.0.21.

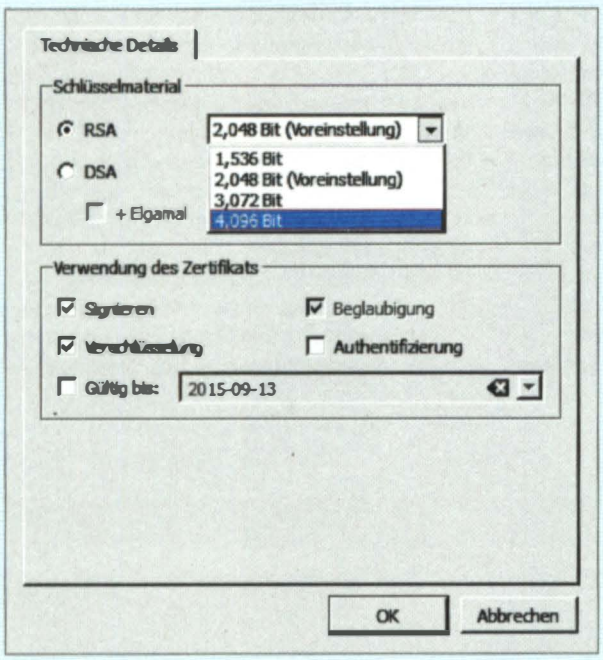
Eine Reihe von Tools bieten grafische Oberflächen für GnuPG, erläutern die Optionen und erleichtern damit im Alltag den Umgang mit PGP enorm. Zum Einstieg sollten Sie eine Variante wählen, die GnuPG gleich mitinstalliert. Für Windows empfiehlt sich Gpg4win, für Mac OS PGPTools (siehe c't-Link am Ende des Artikels). Beide sind kostenlos und besitzen einen komfortablen Installer. Linux-Nutzer haben je nach Distribution und Desktop die Wahl zwischen mehreren GUIs (siehe Liste auf gnupg.org).

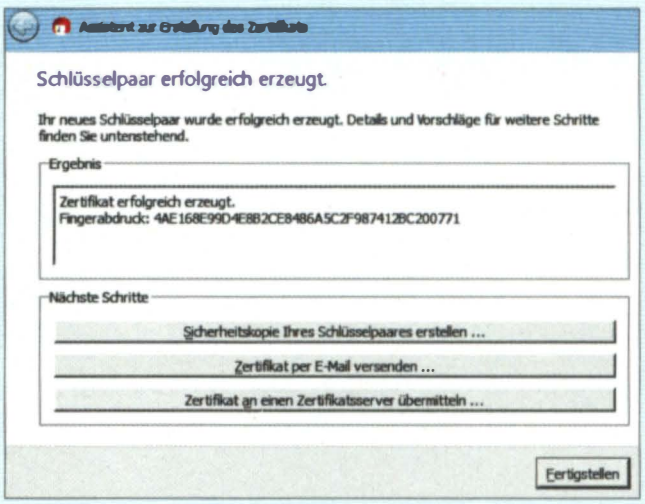
Sofern Sie noch kein Schlüsselpaar besitzen, sollten Sie als Erstes eines generieren. Bei Gpg4win etwa wählen Sie die Option „Neues Zertifikat …" im Datei-Menü. Lassen Sie sich nicht verwirren: Der Begriff „Zertifikat" stammt aus der S/MIME-Welt und bedeutet in PGP übersetzt „Schlüssel". Viele PGP-Tools – wie auch GnuPG mit Gpg4win – beherrschen sowohl die Verwaltung von OpenPGP-Schlüsseln als auch von S/MIME-Zertifikaten und halten die Begriffe nicht auseinander.

SCHLÜSSELSCHUTZ

Bevor Sie ein Paar aus privatem und öffentlichem Schlüssel erzeugen, müssen Sie Angaben zu den damit verbundenen Mail-Adressen machen. Verlassen Sie sich bei der Schlüssellänge (in Gpg4win unter „Erweiterte Einstellungen …") nicht auf die Vorgaben, sondern wählen Sie mindestens eine Länge von 2048 Bit, besser 4096: Je länger der Schlüssel ist, desto schwerer lässt er sich knacken. Zurzeit gilt 1024 Bit als gerade noch sicher, aber angesichts der weiter steigenden Rechenleistung könnte sich das ändern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) etwa prognostiziert in seiner offiziellen technischen Richtlinie 2013, dass RSA-Schlüssel von 2048 Bit Länge bis mindestens 2019 unknackbar sein sollten.

Unter gestandenen PGP-Nutzern gehen die Meinungen darüber auseinander, ob man seine Schlüssel





Schlüsselerzeugung mit Gpg4win: Der Schlüssel sollte eine Minimallänge von 2048 Bit haben. Nach der Herstellung fertigen Sie am besten eine Kopie an und verwahren sie sicher.

WARUM SIE MIT PGP AUF DER SICHEREN SEITE SIND

Pretty Good Privacy (PGP) gilt seit seiner Erfindung 1991 durch Phil Zimmermann als sicheres Verschlüsselungskonzept. In seiner kommerziellen Variante spielt es heute aber kaum noch eine Rolle. An seine Stelle ist seit 1998 das erweiterte Verfahren OpenPGP getreten, das als RFC 4880 standardisiert wurde. Der Einfachheit halber lautet das Sammel-Akronym in diesem Artikel dennoch „PGP". Seit 1999 existiert der quelloffene „GNU Privacy Guard" (GnuPG), der OpenPGP umsetzt und für alle gängigen Desktop-Betriebssysteme verfügbar ist. Die Software bietet nur Kommandozeilen-Steuerung und ist für wenig erfahrene Nutzer nicht zu empfehlen.

PGP beruht auf dem Prinzip der asymmetrischen Verschlüsselung. Der Absender chiffriert seine Kommunikation – etwa den Inhalt einer Mail – mit dem öffentlichen Schlüssel des Empfängers. Nur der Empfänger ist in Besitz des geheimen Gegenstücks, mit dem sich die Mail wieder in Klartext wandeln lässt. Technisch gesehen stimmt das nicht hundertprozentig, denn genau genommen mischt PGP aus Performance-Gründen symmetrische und asymmetrische Verschlüsselung zu einem Hybridverfahren: Es verschlüsselt den Mail-Inhalt mit einem hierfür erzeugten symmetrischen Sitzungsschlüssel. Anschließend wird nur dieser Schlüssel mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.

Außer der sicheren Verschlüsselung bietet OpenPGP noch eine weitere Funktion: E-Mails lassen sich unterschreiben, um ihre Echtheit zu beglaubigen. Dazu erstellt die Software eine eindeutige Prüfsumme (Hash) über den Inhalt einer Mail. Anschließend zertifiziert der Nutzer diesen Hash mit seinem geheimen Schlüssel. Der Empfänger erstellt nun mit derselben Methode und demselben Algorithmus ebenfalls einen Hash, entschlüsselt den beim Sender erstellten Hash mit dem öffentlichen Schlüssel und vergleicht beide. Stimmen sie überein, hat er Gewissheit darüber, dass der Sender authentisch ist und der Mail-Inhalt auf dem Sendeweg nicht manipuliert wurde.

S/MIME: Schwachstelle Vertrauenskonzept

Nennenswert verbreitet sind derzeit zwei Verfahren zur Mail-Verschlüsselung: S/MIME und PGP. Die Funktionsweise sowie die Vor- und Nachteile von S/MIME sind im Artikel ab Seite 92 beschrieben. Die Enthüllungen rund um den NSA-Skandal haben das Vertrauen in S/MIME erschüttert. Das Problem bei S/MIME ist das strikt hierarchische Vertrauenskonzept, dessen Basis – die Zertifizierungsstellen, denen die Programme vertrauen – als kompromittiert gelten müssen. Ein Geheimdienst, der Google, Microsoft und Apple zur Zusammenarbeit zwingen kann, wird nicht vor Zertifizierungsstellen wie Verisign halt machen.

Man muss also davon ausgehen, dass die NSA zumindest eine eigene intermediäre Zertifizierungsstelle betreibt. Mit der kann sie sich dann Zertifikate auf beliebige Namen und Adressen ausstellen, denen dann Browser und Mail-Programme vertrauen. Damit kann der Geheimdienst immer noch nicht Ihre S/MIME-verschlüsselte Mail lesen, denn die dazu nötigen Schlüssel befinden sich im Idealfall nur auf Ihrem PC. Aber die Geheimdienste könnten Mails in Ihrem Namen verschicken und unterschreiben. Der Empfänger sieht ein allem Anschein nach gültiges Zertifikat und schickt unter Umständen auch damit verschlüsselte Mails, die die NSA dann entschlüsseln kann. Darüber hinaus ist auch nicht auszuschließen, dass die kommerziellen S/MIME Implementierungen Hintertüren enthalten, die bislang noch nicht aufgeflogen sind.

Demgegenüber steht das nicht hierarchische Vertrauensmodell von PGP, das mangels Angriffshebel schwerer kompromittierbar ist. Anders als in den Medien mitunter dargestellt, ist es ja keineswegs so, dass die NSA jegliche Verschlüsselung knacken kann. Starke Verschlüsselung ist nach wie vor sicher – und alle Experten sind sich einig, dass die bei PGP eingesetzten Verfahren dazugehören. PGP-Erfinder Phil Zimmerman hält PGP nach wie vor für sicher und auch Edward Snowden – der es noch am ehesten wissen müsste, wenn die NSA PGP-Verschlüsselung knacken könnte – vertraute PGP sein Leben an, indem er noch vor seinem Coming-out verschlüsselte Mails mit Journalisten austauschte. (ju/hob)

mit einem Verfallsdatum versehen sollte. Einige halten das für sicherer. Ihr Argument: Sollte der Schlüssel in fremde Hände geraten oder der Besitzer ihn nicht mehr nutzen können, weil er das Passwort dazu vergessen hat, bleibt er nicht endlos gültig. Andererseits ist es lästig, regelmäßig das Procedere der Schlüsselerzeugung und -weitergabe neu zu vollziehen. Im Grunde genommen spricht nichts dagegen, das Schlüsselpaar nicht mit einem Ablaufdatum zu versehen, solange Passwort und Widerrufsmöglichkeit gesichert sind. Ein Limit können Sie übrigens auch nachträglich einbauen.

Besonderes Augenmerk sollten Sie auf die Wahl des Passworts – bei PGP auch „Passphrase" oder „Mantra" genannt – legen. Nur die Passphrase schützt den geheimen Schlüssel vor Missbrauch. Umgekehrt: Ohne Kenntnis der Passphrase ist der Schlüssel unbrauchbar. Gerät dieser in fremde Hände, kann der Dieb aber eine unlimitierte Brute-Force-Attacke starten. Wie man ein wirklich sicheres Passwort wählt, hat c't zuletzt in [1] erläutert. Bedenken Sie aber auch, dass Sie die Passphrase oft nutzen werden – eventuell auch auf Smartphone-Touch-Tastaturen eingeben wollen. Eine 30-stellige Passphrase ist zwar nicht zu knacken, dafür aber praxisuntauglich. Keine Sorge: Genau wie das Verfallsdatum lässt sich auch die Passphrase später noch ändern.

SCHLÜSSEL-RÜCKRUF

Die beiden generierten Schlüssel stellen sich nach dem Export als Textdateien in Blockformatierung dar, in denen scheinbar nur Wirrwarr steht. Eine Kopie des geheimen Schlüssels sollten Sie auf ein sicheres Medium, etwa einen USB-Stick – exportieren und den Datenträger für Fremde unzugänglich aufbewahren. Wenn Sie ganz sichergehen wollen, drucken Sie ihn zusätzlich aus und verwahren das Papier unzugänglich, beispielsweise in einem Tresor. Den öffentlichen Schlüssel dagegen sollten Sie an Ihre Kommunikationspartner verteilen. Dazu gleich mehr.

Aus gutem Grund fordert Gpg4win direkt nach der Schlüsselerzeugung dazu auf, ein sogenanntes Widerrufszertifikat (revocation certificate) zu generieren. Nur mit einem solchen „Gegenschlüssel" lässt sich auch ohne Passphrase ein veröffentlichter PGP-Schlüssel als ungültig markieren, etwa, wenn er kompromittiert ist oder die Passphrase zum geheimen Gegenstück vergessen wurde. Kleopatra, das Frontend von Gpg4win zur Schlüsselverwaltung, kann leider selbst kein Widerrufszertifikat erzeugen. Dazu weisen Sie GnuPG auf Kommandozeilenebene an:

```
gpg --output Widerruf_<Schlüssel-ID>.asc
    --gen-revoke <Schlüssel-ID>
```

Alternativ nutzen Sie dazu das Thunderbird-Add-on Enigmail, welches im Kontextmenü seiner Schlüsselverwaltung die Option bietet, auch ohne Kommandozeile Widerrufszertifikate zu erzeugen. Auf Enigmail geht dieser Artikel später noch ausführlicher ein.

Das Beispiel oben enthält die Schlüssel-ID, also die Kennung des Schlüssels. Jedem Schlüsselpaar wird eine solche ID vergeben, die aber nicht einmalig sein muss. Unverwechselbar wird das Paar nach außen hin erst durch seine Fingerabdrücke (Fingerprints), die aus kryptografischen Hashes sowie der Schlüssel-ID zusammengesetzt sind. Anhand des Fingerabdrucks kann jeder einen öffentlichen Schlüssel zweifelsfrei seinem Besitzer zuordnen, wenn dieser – beispielsweise am Telefon – die Ziffern und Buchstaben vorliest. Viele PGP-Nutzer hängen den Fingerabdruck ihres öffentlichen Schlüssels als 40-stellige Hexadezimalzahl an ihren E-Mail-Footer, damit der Empfänger die Möglichkeit zur Validierung hat.

HALLO PGP-WELT!

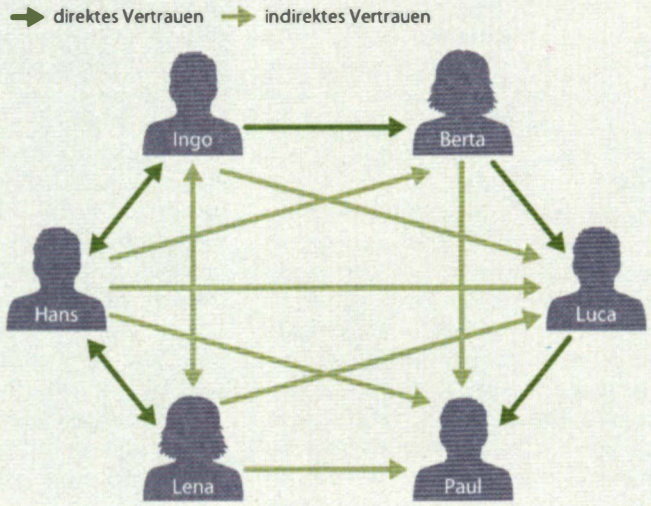
Nachdem die Schlüsselerzeugung abgeschlossen ist, wird der öffentliche Schlüssel digital unterschrieben (signiert) und damit seine Echtheit für Fremde bestätigt. In Gpg4win etwa wählen Sie dazu „Zertifikat beglaubigen" im Kontextmenü zum eigenen Schlüssel. Dort werden Sie feststellen, dass Sie die Zugehörigkeit für jede angegebene E-Mail-Adresse zum Schlüssel einzeln bestätigen müssen. Das hat seinen Grund: Nicht nur Sie, sondern auch jeder andere PGP-Nutzer darf Ihren öffentlichen Schlüssel mit seiner digitalen Unterschrift beglaubigen und ihm damit mehr Glaubwürdigkeit verleihen. Er sollte aber nur jene Zugehörigkeiten bestätigen, deren er sich auch sicher ist. Kennt er eine Mail-Adresse von Ihnen nicht, kann er sie bewusst ausklammern.

Ist der öffentliche Schlüssel beglaubigt, können Sie beginnen, ihn unter die Leute zu bringen. Eine Möglichkeit ist natürlich, den kompletten Public-Key-Textblock als Footer unter die Mails zu hängen. Besser aber, Sie veröffentlichen den Key irgendwo im Web, etwa auf Ihrer Homepage, und hängen in Mails nur die URL dorthin sowie den Fingerprint an. Die gängigste Methode, den Schlüssel zu veröffentlichen, ist aber, ihn auf einen Keyserver hochzuladen.

Keyserver speichern und publizieren öffentliche Schlüssel sowie zugehörige Beglaubigungen. Die meisten gängigen Keyserver laufen mittlerweile unter

Web of Trust (WoT)

Ingo und Hans haben gegenseitig ihre PGP-Schlüssel signiert. Ingo kennt Berta, Berta traut Ingo aber nicht. Hans kann dennoch indirekt darauf vertrauen, dass Luca nicht schwindelt.



der Software „Synchronizing Key Server" (SKS), sind auf dieser Basis miteinander vernetzt und tauschen über ein eigenes Protokoll ihre Daten aus. Für den PGP-Nutzer bedeutet das: Wenn er seinen öffentlichen Schlüssel oder die Beglaubigung eines fremden Schlüssels zu einem SKS-Server überträgt, spiegelt dieser die Daten an alle anderen Server weiter. Oft dauert es allerdings bis zu einem Tag, bis Änderungen alle Server im Verbund erreicht haben.

Alle gängigen PGP-Frontends bieten Schnittstellen zum SKS-Verbund (sks-keyservers.net), dessen Server sie bevorzugen sollten. Gpg4win etwa schlägt automatisch vor, den neu generierten Schlüssel zum voreingestellten SKS-Server hochzuladen. Liegt der öffentliche Schlüssel eines fremden Empfängers nicht vor, hilft vielleicht eine Suche auf dem Keyserver. Wichtig ist, dass Sie öfter einmal Ihre Sammlung von öffentlichen Schlüsseln (public keyring) mit dem Keyserver synchronisieren (in Gpg4win: „Aktualisieren"). Auf diesem Weg erhalten Sie neue Beglaubigungen genauso wie Schlüsselwiderrufe.

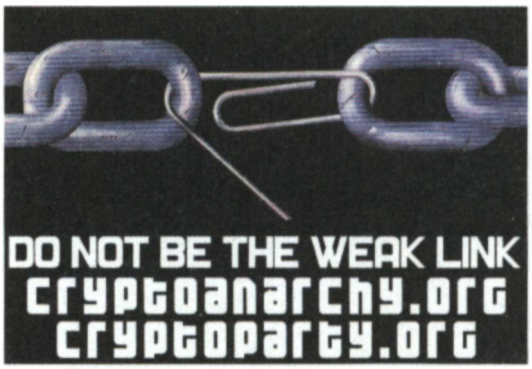
Beachten Sie, dass alle Aktionen, die Sie lokal mit GnuPG oder dem zugehörigen Frontend vornehmen, erst einmal lokal bleiben. Wenn Sie beispielsweise den öffentlichen Schlüssel eines Freundes beglaubigen, gilt diese Signatur nur für Ihren lokalen Schlüsselspeicher. Erst wenn Sie bestätigen, dass die Signatur zum Keyserver geladen wird, bekommen alle anderen PGP-Nutzer mit, dass Sie dem Schlüssel des Freundes voll vertrauen. Ein öffentlicher Schlüssel, der einmal in den SKS-Verbund geladen ist, lässt sich übrigens nie wieder entfernen. Allerdings kann man ihn mit Hilfe des eingangs erwähnten Widerrufszertifikats öffentlich für ungültig erklären. Auch hier gilt: Zuerst müssen Sie dieses Zertifikat lokal mit Ihrem Schlüssel verbinden und dann den Schlüssel erneut hochladen.

VERTRAUENSNETZ

Während bei S/MIME die Vertrauenswürdigkeit eines Schlüssels von einer zentralen Instanz (Certification Authority, CA) bestätigt wird, beruht PGP auf gegenseitigen Vertrauens- oder Misstrauensbekundungen der Nutzer untereinander. Vertrauen bei PGP bedeutet, dass man sicher sein kann: Der öffentliche Schlüssel, mit dem ich diese geheimen Informationen verschlüssele, gehört garantiert der Person, an die ich sie schicke.

Vertrauen bekunden PGP-Nutzer, indem sie mit einer PGP-Signatur am öffentlichen Schlüssel versichern, dass der Schlüssel zum darin angegebenen Besitzer gehört. Dabei können sie in die Signatur einflie-

Die Cryptoparty-Bewegung ruft Netznutzer dazu auf zu verschlüsseln und zu beglaubigen, statt weiterhin ein unsicheres Glied im Web of Trust zu sein.



ßen lassen, wie die Prüfung erfolgt ist. Zur Wahl steht „gar nicht", „nur einfach", oder „sehr genau". Diese Grade sind recht unpräzise, und genau darin liegt eine Schwäche des PGP-Konzepts: Der eine Nutzer versteht unter „nur einfach", dass er sich telefonisch den Fingerabdruck vorlesen ließ, der andere wählt dieselbe Stufe, verlangt aber eine Ausweiskopie des angeblichen Schlüsselbesitzers. Doch auf diesen Angaben beruht eben auch das abgeleitete Vertrauen Dritter.

Wenn man den Schlüssel selbst geprüft hat, heißt das hergestellte Vertrauen in der PGP-Welt „direct trust". Außerdem lässt sich die Vertrauenswürdigkeit von Personen (owner trust) auf einer Skala von 0 (Vertrauen unbekannt) bis 5 (absolutes Vertrauen) festlegen und im Schlüsselbund abspeichern. Die höchste Stufe sollten Sie nur dem eigenen Schlüssel zuweisen. Das Besitzervertrauen können Sie meist in der Schlüsselverwaltung des GnuPG-Frontends im Kontextmenü für die einzelnen Schlüssel einstellen.

Wozu nun das Ganze? Aus den gegenseitigen Bekundungen entsteht nach dem PGP-Konzept ein Netzwerk des gegenseitigen Vertrauens, das sogenannte „Web of Trust" (WoT). Wenn ein PGP-Nutzer einen Schlüssel selbst nicht einschätzen kann, hilft ihm dieses Netz bei der Bewertung, ohne dass es einer zentralen Instanz bedarf. Dazu überprüft er, wie andere, für ihn vertrauenswürdige Nutzer den Schlüssel und den Besitzer bewerten. So kennt Hans in der Grafik auf Seite 86 Berta nicht und möchte ihr eine verschlüsselte Mail schreiben. Ingo, ein Freund von Hans, kennt dafür Berta und hat ihren Schlüssel bereits geprüft. Weil Hans Ingos Urteil vollständig traut, kann er Bertas Schlüssel vom Keyserver laden und bedenkenlos nutzen.

Diese Einschätzung kann manuell erfolgen, wird aber im Normalfall von GnuPG im Hintergrund erledigt. Die Software ermittelt einen „Key-Legitimacy"-Wert. Ist beispielsweise ein öffentlicher Schlüssel von mindestens zwei PGP-Nutzern signiert, denen „gering" vertraut wird, gilt er per GnuPG-Voreinstellung als vertrauenswürdig. Bei „vollem Vertrauen" genügt bereits eine Beglaubigung. Auch unter diesem Aspekt erweist es sich als sinnvoll, den eigenen Schlüsselbund oft mit einem Keyserver zu synchronisieren. Fördert das Update zutage, dass ein Schlüssel in der Vertrauenskette widerrufen wurde, entfällt dessen Glaubwürdigkeit und die Kette reißt.

Das WoT-Konzept birgt im Vergleich zu S/MIME mit den zentralen Vertrauensinstanzen Vor- und Nachteile. Ein Plus ist, dass PGP-Nutzer trauen können, wem sie trauen wollen. Der NSA-Skandal hat zutage gebracht, dass der US-Nachrichtendienst bestrebt ist, CAs unter Kontrolle zu bringen, sich Vertrauen zu erschleichen, um verschlüsselte Kommunikation zu kompromittieren. Das ist bei PGP nicht möglich. Dafür müssen PGP-Nutzer permanent am Ball bleiben, ihr Vertrauensnetz kontrollieren und mit Beglaubigungen selbst dazu beitragen.

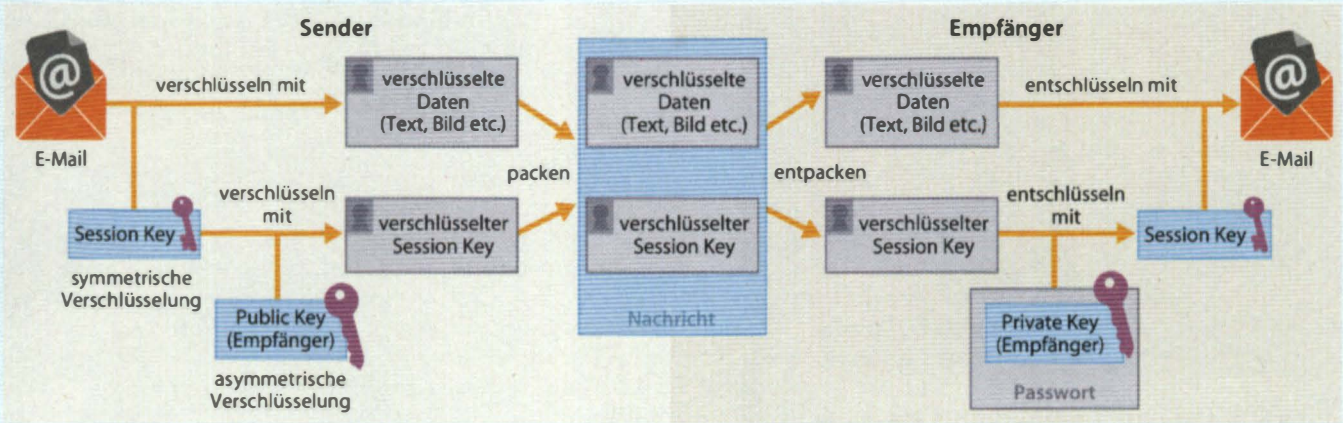
Der Aufbau dieses Netzes kann aber auch Spaß machen: Seit etwa einem Jahr feiert die Cryptoparty-Bewegung ihre Auferstehung. Auf zwanglosen Treffen erklären PGP-Nerds Anfängern Schritt für Schritt, wie sie sicher verschlüsseln können und richten die nötigen Komponenten auf den mitgebrachten Notebooks bei Bedarf auch gleich ein. Fester Bestandteil ist das gegenseitige Keysigning, bei dem sich jeder von der Vertrauenswürdigkeit der anderen überzeugt und deren Schlüssel unterschreibt.

Wenige Instanzen sind angetreten, um PGP-Schlüssel mit ihrem guten Namen zu stärken. Dazu gehört CAcert (cacert.org), vor allem aber die c't. Weil wir die Verschlüsselung mit PGP fördern wollten, haben wir

Funktionen von OpenPGP

Verschlüsseln

Beim Verschlüsseln von Mails wird die Nachricht mit einem Session Key symmetrisch chiffriert. Danach verschlüsselt PGP diesen Key mit dem öffentlichen Schlüssel des Empfängers (Hybridverschlüsselung).



1997 die c't-CA aus der Taufe gehoben (www.ct.de/pgp). Seitdem beglaubigen wir öffentliche Schlüssel, nachdem wir den Ausweis des Besitzers vor Ort geprüft haben. Der Clou dabei: Unsere Signatur lässt sich leicht überprüfen, weil der Fingerprint unseres Signierschlüssels in jedem c't-Impressum unveränderbar veröffentlicht ist. Die Möglichkeit, kostenlos diesen Service zu nutzen, besteht meist auf unseren Messeständen, außerdem mittwochs von 16:30 bis 17:30 Uhr im Heise Verlag (siehe Impressum).

SOFTWARE-KOMBI

Oft wird gesagt, die Software-Unterstützung für PGP und seine Derivate sei mangelhaft. Das gilt heutzutage aber längst nicht mehr. Wer PGP-verschlüsseln will, hat zumindest auf dem Desktop viele Möglichkeiten. Alles, was Sie dazu benötigen, ist ein E-Mail-Account, der mit den Mail-Protokollen POP3/IMAP und SMTP ansprechbar ist. Sollte Ihnen ein Mail-Dienst anbieten, über sein Web-Frontend zu verschlüsseln, nehmen Sie davon Abstand. Denn eine sichere Ende-zu-Ende-Übertragung kann damit nicht gewährleistet werden.

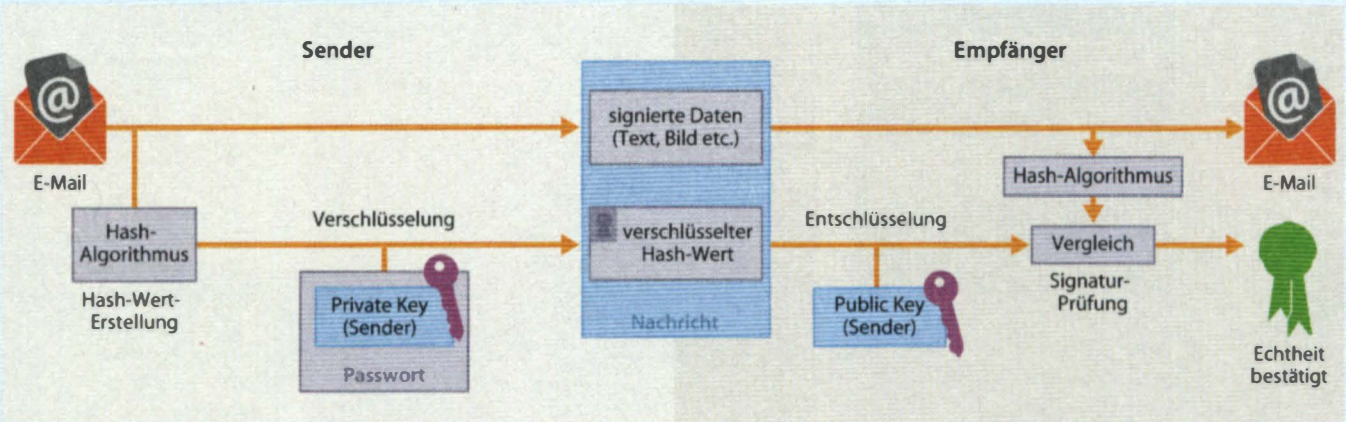
Besser ist es, auf dem Desktop eine Kombination aus GnuPG, Frontend und Mail-Programm zu wählen. Bewährt hat sich der Mozilla-Mailer Thunderbird in Verbindung mit dem Verschlüsselungs-Add-on Enigmail. Diese Kombination lässt sich auf allen Desktop-Plattformen nutzen, weil Thunderbird sowohl für Windows als auch für Mac OS und Linux verfügbar ist. Weil Enigmail selbst kein GnuPG mitbringt, sollte dies vor der Installation vorhanden sein, beispielsweise in der Version von Gpg4win (Windows) oder den GPGTools (Mac OS). In Linux-Distributionen ist GnuPG in aller Regel bereits enthalten.

Enigmail erkennt, dass ein GnuPG installiert ist und greift automatisch darauf zu. Das Tool bietet außer der Signier- und Verschlüsselungslogik inzwischen eine ausgereifte Schlüsselverwaltung und kann auch Schlüssel generieren. Damit macht es unter Windows das Verwaltungswerkzeug Kleopatra von Gpg4win prinzipiell überflüssig. Doch einiges lässt sich mit Kleopatra noch bequemer regeln, insbesondere der Zugriff auf die Grundeinstellungen über den GPG-Agent von GnuPG.

Ein Beispiel: GnuPG hält die einmal eingegebene Passphrase zum geheimen Schlüssel für eine bestimmte Zeit in seinem Cache, damit sie nicht jedes Mal neu eingegeben wird. Der Cache-Timeout steht per Voreinstellung auf drei Minuten – was viele Nut-

Signieren

Die PGP-Signatur einer Mail enthält einen mit dem geheimen Schlüssel des Senders beglaubigten Hash-Wert. Der Empfänger kann die Signatur entschlüsseln und feststellen, ob die Mail unangetastet und der Sender authentisch ist.



zer für viel zu kurz halten, weil sie ständig die Passphrase neu eintippen müssen. Zwar bietet Enigmail in den PGP-Einstellungen an, den Timeout-Wert frei zu wählen, meldet dann aber, dass dies gar nicht geht, weil Enigmail keinen Zugriff auf den GPG-Agent in GnuPG hat. Sie können die Änderung des Timeouts auf GnuPG-Kommandozeile vermeiden, wenn sie in Kleopatra im Menü „GPG Agent" unter „Optionen zum GnuPG System" den gewünschten Wert im Feld „Lasse PINs im Cache nach N Sekunden verfallen" eintragen. Warum die Passphrase hier verwirrenderweise plötzlich als PIN bezeichnet wird, bleibt allerdings das Geheimnis der Entwickler von Pgp4win.

Die Stärke des Add-ons Enigmail liegt in seiner nahtlosen Integration ins Mailprogramm Thunderbird. Die OpenPGP-Informationen zu jeder Mail zeigt es in der dreigeteilten Mail-Ansicht direkt über den Header-Informationen. Der Nutzer erfährt über Signalfarben, wie GnuPG die Vertrauenswürdigkeit der Nachricht beurteilt. Rot bedeutet, dass kein Vertrauen vorhanden ist, weil der Schlüssel nicht gefunden wurde oder nicht korrekt ist. Ein blasses Grün signalisiert, dass die Verschlüsselung und Signierung auf Absenderseite korrekt gelaufen ist, aber dem Gegenüber nur mäßig getraut wird. Das sattere Grün bedeutet volles Vertrauen, das beispielsweise durch ein „direct trust" bestätigt ist. Einziges Manko: Bisweilen scheint Enigmail die Sicherheitsinfos zu cachen, sodass es beim Abruf der nächsten Mail erst mal den Status zur vorherigen Mail zeigt. Hier ist Vorsicht angebracht.

Manche Voreinstellungen von Enigmail stören viele PGP-Nutzer. So verschlüsselt das Add-on Kopien von gesendeten Nachrichten erst einmal nicht mit dem eigenen, sondern nur mit dem öffentlichen Schlüssel des Empfängers. Das bedeutet, dass man die Kopien seiner eigenen Mails nicht mehr lesen kann. Im Reiter „Senden" unter „OpenPGP-Einstellungen" finden Sie die Option „Zusätzlich mit eigenem Schlüssel verschlüsseln". Die sorgt dafür, dass die Kopie mit dem eigenen öffentlichen Schlüssel verschlüsselt wird und damit für Sie lesbar bleibt.

In der Voreinstellung signiert Enigmail Nachrichten im Inline-Modus, das heißt, die PGP-Informationen finden sich direkt im Mail-Body und können Nicht-PGP-Nutzer verwirren. Wenn Sie das lästig finden, nutzen Sie die Möglichkeit, Signaturen als MIME-Anhang zufügen zu lassen. Wenn Sie eine neue Mail verfassen, wählen Sie das „OpenPGP"-Menü am oberen Fensterrand und wählen dort die Option „PGP/MIME verwen-

Die Android-App APG importiert Schlüsselringe, die zuvor in den USB-Speicher des Smartphones geladen wurden.

den" – verschlüsselte Inhalte und Signaturen landen dann im MIME-Anhang.

So manchen Nutzer nervt es, wenn er in der Thunderbird-Vorschau schnell über seine Mails blättert und jedes Mal, wenn er über eine PGP-Nachricht scrollt, zur Eingabe der Passphrase aufgefordert wird. Dies lässt sich unterbinden: Im „OpenPGP"-Menü der Thunderbird-Leiste findet sich die Option „Automatisch entschlüsseln/überprüfen", die per Voreinstellung aktiviert ist. Entfernen Sie das Häkchen, bleibt Enigmail zunächst inaktiv, wenn es auf eine verschlüsselte oder signierte Nachricht trifft. Es zeigt dann lediglich an, dass die Mail PGP-Code enthält, und schlägt in der Statuszeile vor, aktiv zu werden.

OUTLOOK & CO.

Gab es lange gar keine PGP-Unterstützung für Microsofts Mailer Outlook, existieren nun immerhin zwei rudimentäre Plug-ins, die beide eine Installation von GnuPG voraussetzen. Eines davon heißt GpgOL und kommt mit Gpg4win. Ende August wurde das Plug-in runderneuert und läuft nun auch mit Outlook 2010 und 2013, außerdem auch auf 64-Bit-Varianten von Windows. Die Autoren des kostenlosen Tools bedauern selbst, dass GpgOL nur in der Lage ist, inline zu verschlüsseln und zu signieren, die Unterstützung für PGP/MIME fehle bis auf Weiteres, weil dafür „eine Finanzierung fehle".

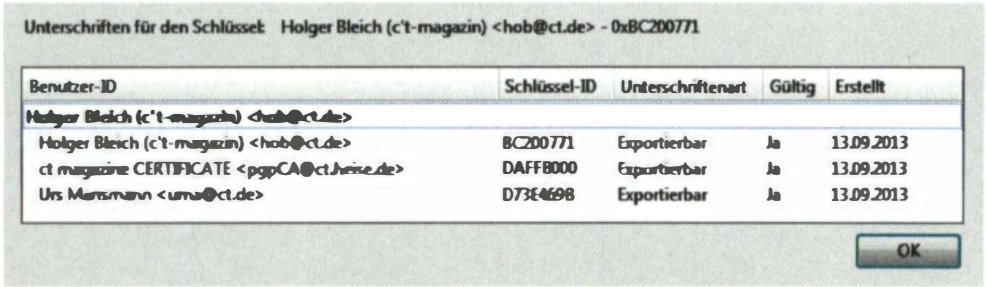
Die zweite Möglichkeit, mit Outlook OpenPGP zu nutzen, bietet das noch als Beta vertriebene kostenlose Tool „Outlook Privacy Plugin" der Firma Deja-vu-Security. Es fügt sich nahtlos in die Menüleiste von Outlook ein und macht einen stabilen Eindruck. Seine Fähigkeiten sind noch begrenzt, sollen aber nach dem Willen der Entwickler ausgebaut werden. Zurzeit (Beta 34) kann es mit verschlüsselten und/oder signierten Mails umgehen. Auch mit verschlüsselten Anhängen kommt es klar. Allerdings ist es genau wie GpgOL nicht in der Lage, PGP/MIME zu versenden. Das sei aber geplant, versichern die Entwickler auf der Homepage des Projekts.

Apple-Nutzer müssen unter Mac OS keineswegs von ihrem geliebten Apple-Mail zu Thunderbird umsteigen, um PGP nutzen zu können. Die GPGTools liefern mit „GPG for Mail" ein Plug-in für den Standard-Mailer mit, das einwandfrei seinen Dienst verrichtet und überaus leicht zu bedienen ist. Leider kommen die Entwickler von GPGTools nicht immer mit dem Rhythmus der Betriebssystem-Updates hinterher. Beim Umstieg zu Mac OS X 10.8 (Mountain Lion) beispielsweise dauerte es Monate, bis eine GPG-for-Mail-Version herauskam, die mit den Änderungen in Apple Mail klarkam. Wer vorher ein Update installiert hatte, war so lange ohne PGP unterwegs.

PGP MOBIL

Möchten Sie PGP auch unterwegs auf dem Tablet oder Smartphone nutzen, lichten sich die Software-Optionen. Auf mobilen Endgeräten ist Mail-Verschlüsselung nach wie vor eine frickelige Angelegenheit. Das liegt schon daran, dass es einen zur Weißglut treiben kann, für jede Ver- oder Entschlüsselung die Passphrase auf der virtuellen Tastatur am Touchscreen einzutippen. Möchten Sie Ihren Bund öffentlicher Schlüssel nutzen, müssen Sie ihn regelmäßig und aufwendig importieren. Wenigstens sind die erwähnten Apps in der Lage, auf SKS-Keyserver zuzugreifen und unbekannte Schlüssel nachzuladen.

Tragen Sie das Gerät mit sich herum, gelten andere Sicherheitsmaßstäbe als beim Desktop-PC zu Hause oder im Büro. Denken Sie daran, dass der geheime Schlüssel im Klartext im Speicher liegt. Ein hinreichender Zugangsschutz, etwa per PIN, ist folglich Pflicht. Das Gerät sollte so gesichert sein, dass keine Zugriffsmöglichkeit besteht, wenn es verloren geht. Es verbietet sich von selbst, dass der geheime Schlüssel via Klartext-E-Mail ins Gerät importiert wird. Ab Seite 92



Ein Klick auf den importierten Schlüssel zeigt konkret, wer ihn bislang beglaubigt hat.

haben wir ausführlich sichere Importmöglichkeiten für Schlüssel auf Android- und iOS-Geräten beschrieben.

Android-Nutzer greifen auf die App APG und den Mailer K-9 oder dessen kommerziellen Ableger Kaiten zurück. Dieses Gespann lässt sich einigermaßen leicht bedienen und bietet alle für den Nachrichtenaustausch nötigen Features. Achtung, bei der Installation kommt es auf die Reihenfolge an: Erst muss APG installiert werden, dann K9. Haben Sie beide Programme installiert, richten Sie zunächst den oder die E-Mail-Accounts in K9 ein und importieren anschließend die dazu passenden privaten Schlüssel in APG.

Zwar ist APG auch in der Lage, Schlüsselpaare zu erzeugen, im Vergleich zu PC-Tools wie Kleopatra bietet es aber wenig Komfort. Besser und sicherer ist es, das Schlüsselpaar am PC zu erzeugen und anschließend auf das Mobilgerät zu übertragen. Hat man schon eine Schlüsselsammlung aus öffentlichen Schlüsseln, die man für die Kommunikation benötigt, packt man diese am besten gleich dazu.

Nach dem Export in der PC-Schlüsselverwaltung legen Sie alle Dateien, die auf dem Mobilgerät zu importierende öffentliche und private Schlüssel enthalten, in einem Verzeichnis auf dem Mobilgerät ab.

Das Ver- und Entschlüsseln von Nachrichten geht auch mit schwachbrüstigen Prozessoren recht schnell. Allerdings scheitert K9, wenn der Absender das Chiffrat nicht inline, sondern per PGP/MIME verschickt hat. Dann hilft nur noch das Abspeichern der angehängten PGP-Datei und deren anschließendes Entschlüsseln, was APG immerhin beherrscht.

Mehr Komfort als APG bietet unter Android OpenPGP Keychain, eine komplette und leicht zu bedienende Open-Source-Schlüsselverwaltung. Dieses Tool erlaubt sogar den Tausch von Schlüsseln per QR-Code und NFC. Allerdings arbeitet die Alpha-Version noch nicht mit K-9 zusammen, sodass alle Ent- und Verschlüsselungen über Dateioperationen und Cut & Paste erfolgen müssen. Der Entwickler verspricht, diese K9-Integration nachzuliefern, es lohnt sich also, mitunter im Play Store vorbeizuschauen und nach einer neuen Version zu suchen.

Für iOS existiert nur eine halbwegs praktikable PGP-App, die für Privatanwender in Frage kommt. iPGMail (1,79 Euro) ist mangels Schnittstellen in iOS nicht in die bordeigene Mail-App integriert. Möchte man Mails dechiffrieren, heißt es, sie per Cut & Paste in iPGMail zu importieren. Möchte man selbst Mails verschlüsseln, klappt das direkt in iPGMail. Geheime Schlüssel und öffentliche Schlüsselbunde lassen sich via USB und iTunes importieren. Vorsicht: Einmal entschlüsselte Nachrichten speichert die App im Klartext, außerdem bietet sie noch die Möglichkeit, Texte und Schlüssel beispielsweise in die iCloud zu laden. Selbstredend, dass sie dort nichts verloren haben.

Wer - etwa im Urlaub - an fremden PCs ver- und entschlüsseln will, kann auf die kostenlose Thunderbird-Portable-Distribution des GnuPT-Projekts zurückgreifen, die von einem USB-Stick läuft. Das Installer-Verzeichnis müssen Sie zunächst auf die heimische Festplatte entpacken. Von dort aus gestartet, fragt der Installer, welche Version von Thunderbird installiert werden soll. Als Ort sollten Sie den eingesteckten USB-Stick angeben. Der Installer besorgt sich die angegebene Version sowie das aktuelle Enigmail und konfiguriert das Paket auf dem Stick vor. Er bietet sogar die Möglichkeit, ein Profil inklusive Mails und PGP-Konfiguration von Thunderbird auf der Festplatte zu importieren - bequemer geht es kaum.

Doch auch hier gilt: Passen Sie unterwegs gut auf Ihren Stick auf. Die kleinen Teile gehen leicht verloren, und mit ihnen dann vielleicht extrem vertrauliche Informationen und geheime Schlüssel. Am besten, Sie verschlüsseln die gesamte Stick-Partition mit einem Tool wie Truecrypt, bevor Sie sich auf die Reise machen. Es wäre paradox, wenn Sie Wert darauf legen, sicher digital zu kommunizieren und dabei den Grundschutz vergessen. (hob) c't

LITERATUR

[1] Jürgen Schmidt, **Passwort-Schutz für jeden**, Sicherheit mit System und trotzdem unberechenbar, c't 3/13, S. 88

Alle Links zum Artikel
www.ct.de/hb1401082

Verschlüsseln mit S/MIME

Viele Internet-Nutzer scheuen E-Mail-Verschlüsselung, weil sie die Technik dahinter für kompliziert halten und deshalb einen Komfortverlust befürchten. Wenige wissen, dass auf ihren Rechnern und Smartphones längst alles fürs manipulationssichere Mailen vorbereitet ist. Nur wenige Arbeitsschritte fehlen, um mit S/MIME verschlüsselt zu kommunizieren.

Von **Holger Bleich** und **Sven Neuhaus**

Wer mailt, muss stets im Hinterkopf behalten, dass die Inhalte der Nachrichten wenig vertrauenswürdige Zwischenstationen passieren und vielleicht sogar der Empfänger kompromittiert ist. Umgekehrt ist auch bei empfangener Mail Misstrauen angebracht.

Mitte 2012 etwa kaperten Unbekannte Tausende Nutzerkonten beim Mail-Provider GMX und versandten von dort Links zu Malware-Webseiten. Vertrauten die Empfänger auf die Integrität der Mail-Adresse und öffneten den Link, hatten sie einen Trojaner auf dem Rechner. Hätten sie auf signierte Mails bestanden, wäre das nicht passiert. Der private Schlüssel, den der Absender dafür benötigt, ist in den gekaperten Webmail-Konten nicht verfügbar.

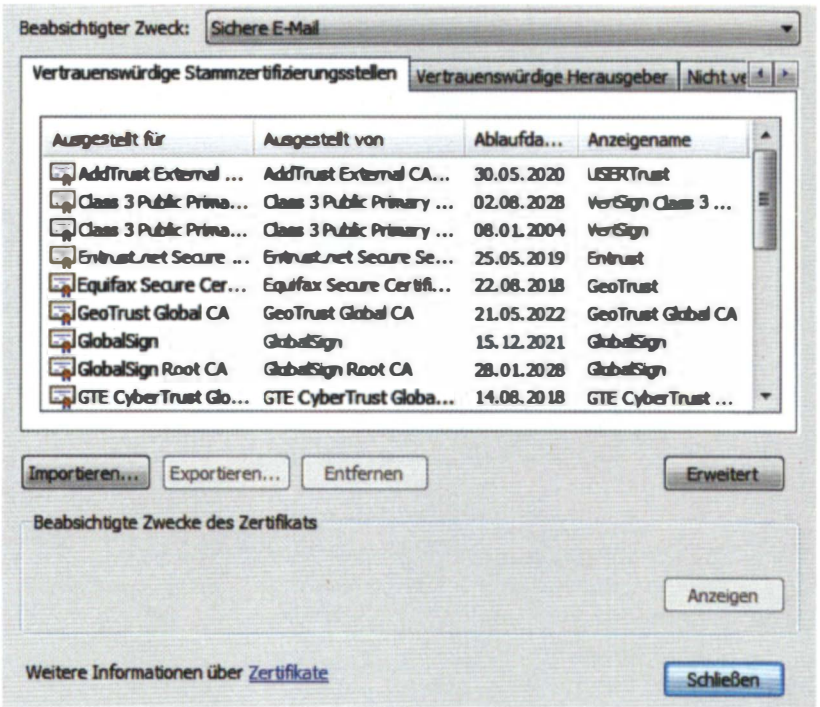
Mit S/MIME kann man heute relativ leicht seine Mail-Kommunikation absichern. Alles, was man prinzipiell dazu benötigt, ist eine Kombination aus dem privaten Schlüssel in Form einer Datei sowie einem öffentlichen Schlüssel mit einem Zertifikat, mit dem eine glaubwürdige Instanz diesen beglaubigt.

Das Prinzip der zentralen CAs macht S/MIME praktikabel, bildet aber auch die Schwachstelle des strikt hierarchischen Vertrauenskonzepts: Ein Geheimdienst wie die NSA, der Google, Microsoft und Apple zur Zusammenarbeit zwingen kann, wird nicht vor Zertifizierungsstellen wie Verisign halt machen. Es ist derzeit zwar unwahrscheinlich, aber nicht gänzlich auszuschließen, dass S/MIME kompromittiert werden kann (siehe Seite 84).

ZERTIFIZIERUNG

Mit dem öffentlichen Schlüssel chiffriert man die Mails. Lesbar machen lassen sie sich dann nur wieder mit dem geheimen Gegenstück. Den öffentlichen Schlüssel darf man also frei verteilen, und wer ihn hat, kann an den Besitzer Nachrichten schicken, die dann wirklich nur dieser lesen kann.

Zu wem ein solcher öffentlicher Schlüssel gehört, steht im Zertifikat. Es enthält den Namen des Besitzers, dessen E-Mail-Adresse sowie den öffentlichen Schlüssel



Via Internet Explorer lassen sich die in Windows installierten Zertifikate einsehen und verwalten.

selbst und ist vom Aussteller digital signiert. Bei S/MIME geben zentrale Organe, die Certificate Authorities oder kurz CAs, die Zertifikate aus. Das Format der S/MIME-Zertifikate lautet gemäß einem ITU-Standard „X.509v3".

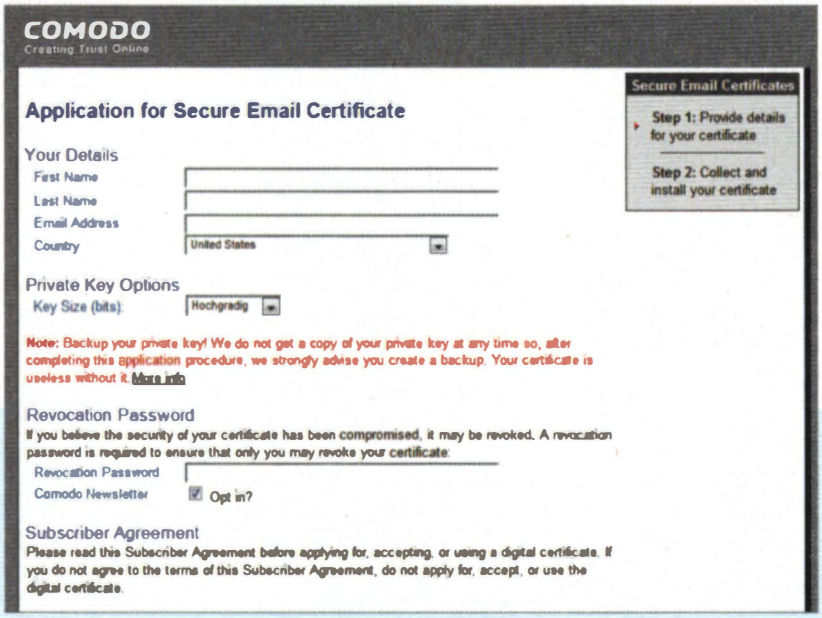
Jeder, der mitmachen will, muss sich bei einer der Zertifizierungsstellen melden. Die CA beglaubigt die Schlüssel des Kunden und stellt ihm als Beleg ein digitales Zertifikat aus. Kompromittierte Zertifikate veröffentlicht die CA in einer „revocation list". Anwendungen, etwa Mail-Clients, können diese Liste abfragen und so unsichere Kandidaten erkennen. Die Richtlinien, nach denen Zertifikate ausgestellt oder eingezogen werden, kann man online in der „certification policy" der Zertifizierungsstelle nachlesen.

Die meisten CAs bieten ihre Zertifikate in mehreren Qualitätsstufen an. Sie unterscheiden sich durch die Gründlichkeit der Prüfung des Antragstellers – je umfangreicher die Prüfung, desto mehr Vertrauen kann man dem Zertifikat entgegenbringen und umso höher sein Preis. Klasse-1-Zertifikate haben die geringste Vertrauenswürdigkeit, werden dafür aber mitunter sogar kostenlos angeboten (siehe Tabelle „Gratis-Zertifikate").

IDENTITÄTSKONTROLLE

Bei den Klasse-1-Zertifikaten erfolgt keine echte Identitätsprüfung, sondern lediglich eine mehr oder weniger gründliche Plausibilitätsprüfung der Adressdaten, und zwar ausschließlich online und voll automatisiert. Der Antragsteller bekommt einen Freischaltcode unverschlüsselt per E-Mail zugeschickt. Den muss er auf der Webseite der CA eingeben und erhält dann sein Zertifikat. So wird sichergestellt, dass der Antragsteller Zugriff auf das E-Mail-Postfach hat, für welches das Zertifikat gelten soll.

Ob er wirklich die Person ist, die er vorgibt zu sein, lässt sich damit nicht belegen: Jeder, der auch nur vorübergehend einen Mail-Account kontrolliert, kann sich ein solches Zertifikat besorgen. Gebunden ist die Echtheitsurkunde nur an die E-Mail-Adresse, nicht aber an den Namen des Besitzers, da dieser gar nicht über-



CAs wie comodo bieten kostenlose S/MIME-Zertifikate zur Mail-Verschlüsselung an, die allerdings nur 12 Monate gültig sind und dann oft kostenpflichtig werden.

Ein S/MIME-Zertifikat kann man via Mail-Anhang in iOS 7 importieren. Dafür legt iOS ein neues Profil an.

prüft wurde. Entsprechend sind damit verschlüsselte Mails nur unter Bekannten wirklich vertrauenswürdig. Kostenlose Klasse-1-Zertifikate sind maximal ein Jahr gültig.

SCHLÜSSELDIENST

Für unser Beispiel haben wir das kostenlose StartSSL-Home-Zertifikat der Klasse 1 von StartCom gewählt. Der Ablauf ist aber bei anderen Anbietern ähnlich. Wählen Sie auf der Homepage von StartCom den Menüpunkt „Registrierungsprozess" und füllen Sie das Formular für ein „StartSSL-Free"-Zertifikat aus. Bestätigen Sie, dass Sie Ihre Daten korrekt eingegeben und die Nutzungsbedingungen gelesen haben. Sie erhalten per Mail einen Freischaltcode, den Sie auf der Webseite von StartSSL eingeben müssen.

Anschließend erfolgt eine Überprüfung durch StartSSL, die nach Angaben des Unternehmens bis zu sechs Stunden dauern kann, in den meisten Fällen aber nach wenigen Minuten abgeschlossen ist. Daraufhin erhalten Sie eine weitere E-Mail mit einer Freischalt-URL und einem weiteren Code. Durch einen Klick auf die URL haben Sie nachgewiesen, dass Sie Kontrolle über das angegebene E-Mail-Postfach haben.

Nun können Sie ein Schlüsselpaar erstellen. Das erzeugt nicht die CA, sondern ein Kryptomodul Ihres Browsers, was den Vorteil hat, dass Ihr privater Schlüssel gar nicht erst durchs Internet muss. Wählen Sie die maximale und damit sicherste Schlüssellänge aus (2048 Bit). Nachdem die Schlüssel generiert wurden, können Sie sie zusammen mit Ihrem Zertifikat über den Install-Button installieren.

Haben Sie die Schlüssel mit Firefox erzeugt, landen sie inklusive Zertifikat in dessen Zertifikatsverwaltung. Einsehbar sind sie im Zertifikat-Manager unter den Verschlüsselungseinstellungen. Der Internet Explorer führt sie unter den Internetoptionen im Menüpunkt Inhalte, die Zertifikate selbst verwaltet in diesem Fall aber das Betriebssystem Windows. Safari unter Mac OS übergibt die Zertifikatsdatei automatisch an das Betriebssystem, von dem man sie mit der Schlüsselbund-Anwendung auslesen kann. Sollten Sie mehr als einen Schlüsselbund besitzen, platzieren Sie den neuen Schlüssel im Anmelde-Schlüsselbund.

Auch Chrome legt die Zertifikate in der Windows-Verwaltung beziehungsweise im Schlüsselbund ab, das Vorgehen ist deshalb identisch. Sofern Sie einen anderen Browser verwenden, müssen Sie zunächst das Zertifikat aus dem Browser exportieren und es per Doppelklick im Schlüsselbund importieren.

Sollte der Schlüssel des Empfängers noch nicht vorliegen, so erscheint der Name des Empfängers in Hellrot mit einem geöffneten Vorhängeschloss.

Das Zertifikat und die Schlüssel gelangen in einer Datei verpackt auf andere Rechner oder ein mobiles Gerät. Übernimmt der Browser die Zertifikatsverwaltung, ist er auch für den Export zuständig. Bei Firefox finden Sie in den erweiterten Einstellungen unter „Verschlüsselung/Zertifikate anzeigen/Ihre Zertifikate" den Punkt „Sichern...". Hier lassen sich die Dateien schnüren, mit einem Passwort versehen und exportieren. In Opera verstecken sich die Zertifikate in den erweiterten Einstellungen unter Sicherheit/Zertifikate verwalten..." im Reiter „Persönliche".

An die von Windows verwalteten persönlichen Zertifikate gelangen Sie am schnellsten über den Internet Explorer („Internetoptionen/Inhalte"). Hier lässt sich das Zertifikat mitsamt dem privaten Schlüssel in eine PKCS12-Datei exportieren. Mac-Anwender holen die Zertifikate aus dem Schlüsselbund. Öffnen Sie dazu die Schlüsselbundverwaltung und wählen Sie die Rubrik „Meine Zertifikate". Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie „<Zertifikat> exportieren".

Sichern Sie die Dateien an einem Ort außerhalb Ihres Rechners, etwa auf einem Stick, den Sie geschützt verwahren. Mit ihm können Sie die Schlüssel auch sicher auf andere Rechner transportieren. Auf Geräten, auf denen Sie Ihren privaten Schlüssel nicht installiert haben oder nicht installieren wollen (etwa im Internet-Café), können Sie chiffrierte Nachrichten nicht lesen. Der private Schlüssel existiert nur auf Ihrem Rechner (und nun auch auf dem Stick) und kann nicht erneut erzeugt oder irgendwo heruntergeladen werden.

SIGNIEREN UND VERTEILEN

Nachdem nun die Grundlagen geschaffen sind, kann das neue Schlüsselpaar mitsamt dem X.509-Zertifikat in E-Mail-Programmen zum Einsatz kommen. Sämtliche gängigen Clients für den Desktop beherrschen S/MIME. Ob Nachrichten stets signiert und/oder verschlüsselt werden sollen, lässt sich in der Regel in den globalen Sicherheitseinstellungen bestimmen. Möchte man nur einzelne Mails mit S/MIME versehen, wählt man dies beim Verfassen aus.

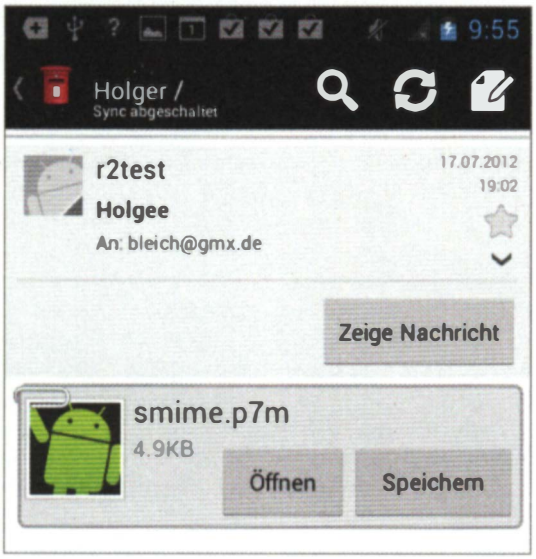
Um eine Mail zu verschlüsseln, benötigen Sie den öffentlichen Schlüssel des Empfängers. Auch wenn Sie bislang noch nicht mit S/MIME gearbeitet haben, haben Sie vermutlich bereits den einen oder anderen öffentlichen Schlüssel gesammelt. Der wird nämlich mit jeder signierten E-Mail zusammen mit dem zugehörigen Zertifikat automatisch mitgeschickt. Ein frei zugängliches Verzeichnis aller öffentlichen Schlüssel, wie es in der PGP-Community geführt wird, gibt es jedoch nicht. Fehlt Ihnen der Schlüssel eines Empfängers, müssen Sie ihn also zunächst bitten, Ihnen eine signierte Nachricht zu schicken.

Umgekehrt sollten Sie selbst Ihren öffentlichen Schlüssel und Ihr Zertifikat breit streuen. Schon deshalb ist es sinnvoll, jede Mail mit einer S/MIME-Signatur zu versehen. Wenn Sie viele Mail-Partner haben und Ihr Programm schon lange in Betrieb ist, schauen Sie doch einmal nach, wie viele persönliche Zertifikate Ihr Mailer ohne Ihr Zutun bereits gesammelt hat. In Thunderbird etwa finden Sie die abgespeicherten Schlüssel von Mail-Partnern unter dem Reiter „Personen" in der Zertifikatsverwaltung.

ES KANN LOSGEHEN

Die meisten Mail-Programme verwalten die Zertifikate nicht selbst, sondern greifen auf das Betriebssystem zurück, so zum Beispiel Outlook in allen Varianten seit 2003. Im aktuellen Outlook 2013 finden Sie die S/MIME-Optionen unter „E-Mail-Sicherheit" in den Truat-Center-Einstellungen. Unter Windows nutzt Outlook den dortigen Zertifikatspool, unter Mac OS greift es auf den Schlüsselbund zu.

Auch der Mac-Bordmailer Apple Mail bedient sich der Schlüsselbundverwaltung des Betriebssystems. Gestatten Sie dem Mail-Programm am besten den Zugriff auf Ihren privaten Schlüssel ohne vorherige Nachfrage. Das geschieht entweder beim ersten Versenden einer signierten Mail oder zuvor in der Schlüsselbundverwaltung von OS X: Klicken Sie in der Liste Ihrer Zertifikate auf das kleine Dreieck neben dem Mail-Zertifikat, damit der zugehörige private Schlüssel sichtbar wird. Anschließend klicken Sie doppelt auf den Schlüs-



Öffnet man in der Android-App Kaiten Mail eine mit S/MIME verschlüsselte Mail, muss das Programm auf einen externen Viewer verweisen.

sel (nicht das Zertifikat) und fügen dann unter „Zugriff" das Programm „Mail" hinzu.

Der populäre Open-Source-Mailer Thunderbird verwaltet die Zertifikate selbst, unabhängig vom Betriebssystem. Darum macht es auch von der Bedienung her keinen Unterschied, ob Sie Windows, Linux oder Mac OS X benutzen. Wählen Sie im „Extra"-Menü den Punkt „Konto-Einstellungen...". Für jedes Ihrer Mail-Konten gibt es einen Konfigurationseintrag „S/MIME-Sicherheit"; dort findet sich eine Schaltfläche „Zertifikate verwalten...", hinter der sich der Zertifikat-Manager verbirgt.

Der Zertifikat-Manager von Thunderbird entspricht dem von Firefox. Via „Importieren..." können Sie eine p12-Datei mit Schlüssel und Zertifikat öffnen. Wenn Sie den Zertifikat-Manager schließen, können Sie das neu importierte Zertifikat unter „Digitale Unterschrift" und „Verschlüsselung" auswählen. Die dortige Checkbox ermöglicht es, alle ausgehenden Mails automatisch signieren zu lassen.

Jedes Mail-Programm weist anders darauf hin, dass eine eingegangene Nachricht signiert und/oder verschlüsselt ist. Bei Thunderbird etwa gibt es zwei Icons, die rechts oben eingeblendet werden: Der Briefumschlag mit Siegel steht für die digitale Unterschrift und das Vorhängeschloss für eine verschlüsselte E-Mail.

SICHERHEIT MOBIL

Der einfachste Weg, ein Zertifikat und zugehörigen Schlüssel auf ein Smartphone oder Tablet zu bekommen, ist, sich selbst eine E-Mail zu schicken, der die exportierte p12-Datei anhängt. Dieser Weg wird oft empfohlen und beschritten, entspricht aber nicht dem Grundsatz, Aufbewahrung und Transport der schützenswerten Datei möglichst sicher zu halten. Mail-Server oder Postfächer können kompromittiert sein, auf dem Weg der Mail lauert Gefahr durch Langfinger, die man meiden sollte.

Falls die Übertragung unbedingt per Mail geschehen muss, dann sollte der Mail-Server wenigstens unter eigener Kontrolle und per SSL zugänglich sein. Alternativ können Sie die Datei auf einen eigenen Webserver daheim kopieren und von dort aus vom mobilen Gerät herunterladen. Dieser Server sollte nach außen abgeschottet sein.

Die sicherste Variante ist aber, Schlüssel und Zertifikate über die USB-Schnittstelle vom Rechner ins Smartphone oder Tablet zu übertragen. Für iOS eignet sich zu diesem Zweck Apples kostenloses „iPhone-Konfigurationsprogramm". Dieses Tool ist primär für Administratoren zur raschen Voreinstellung vieler iPhones gedacht. Mit dem Konfigurationsprogramm lassen sich Profile erstellen und zum angeschlossenen iOS-Gerät schicken.

Das iOS-Konfigurationsprogramm für Windows pflegt Apple bedauerlicherweise seit Anfang 2013 nicht mehr. Mit iOS 7 kann nur die Mac OS-Version des Werkzeugs umgehen. Deshalb sind iOS-7-Nutzer dazu verdonnert, sich entweder einen Apple-Rechner zu suchen oder das Zertifikat als Mail-Anhang zu importieren.

Nach dem Start des Tools schließen Sie das iPhone oder iPad via USB an den Rechner an, das Gerät sollte dann in der Liste des Konfigurationsprogramms auftauchen. Anschließend erstellen Sie ein neues Konfigurationsprofil, dem Sie einen Namen und eine beliebige Kennung geben müssen. In den Optionen wählen Sie den Punkt „Zertifikate" und importieren hier Ihr Zertifikat inklusive Schlüsselpaar. Vorsicht: Unter Windows klappt das nur, wenn das Zertifikat bereits im Pool des Betriebssystems liegt. Die Mac-Variante des Tools erlaubt auch den Import einer Zertifikatsdatei, zum Beispiel aus dem Download-Ordner.

Nachdem dieses Profil eingerichtet ist, übertragen Sie es zum angeschlossenen iOS-Gerät. Dort können Sie das Profil in den allgemeinen Einstellungen einsehen. Mit einem Fingertip auf „Installieren" wandert das mit dem Profil importierte Zertifikat in den Spei-

cher des iPhones oder iPads. An derselben Stelle können Sie es später bei Bedarf auch entfernen.

Jetzt müssen Sie die Mail-App von iOS nur noch dazu bringen, das Zertifikat auch zu verwenden: Starten Sie die Einstellungen und navigieren Sie zu „Mail, Kontakte, Kalender". Wählen Sie dort den Mail-Account – zweimal hintereinander –, in der dann erscheinenden Liste ganz unten unter „Erweitert" befindet sich der Punkt „S/MIME". Dort können Sie für das Signieren und das Verschlüsseln jeweils ein Zertifikat auswählen. Das müssen Sie für jeden Ihrer Mail-Accounts wiederholen.

Sobald die Mail-App einen zum Empfänger passenden Schlüssel findet, aktiviert sie automatisch die Verschlüsselung. Im Entwurfsfenster der E-Mail tauchen deshalb zwei neue Knöpfe unter der Betreffzeile auf: ein Schloss, über das Sie die Verschlüsselung auf Wunsch deaktivieren können, und ein Haken, der die digitale Signatur ein- oder ausschaltet.

Eigentlich macht die Mail-App von iOS nun das sichere Mailen mit S/MIME zum Kinderspiel. Fast alles funktioniert automatisch, aber leider eben nur fast alles: Die empfangenen Zertifikate müssen manuell abgespeichert werden. Eine signierte E-Mail erkennen Sie an einem Haken neben dem Namen des Absenders.

Tippen Sie auf den Absendernamen, erscheint ein Informationsfenster mit dem Namen des Absenders und einer Schaltfläche, die das Zertifikat anzeigt. In dieser Detailansicht können Sie erkennen, ob Mail die Zertifizierungsstelle als vertrauenswürdig einstuft, und auf Knopfdruck das Zertifikat installieren. Erst wenn Sie diesen Schritt ausgeführt haben oder das Zertifikat des Empfängers auf anderem Weg importiert haben, können Sie dem Absender verschlüsselt antworten.

S/MIME MIT ANDROID

Was den Import des Zertifikats angeht, haben es Android-Nutzer einfacher als Apple-Nutzer: Schließen Sie das Smartphone oder Tablet via USB an den Rechner an und kopieren Sie die Zertifikatsdatei ins Hauptverzeichnis des „USB-Speichers". In den Einstellungen unter „Sicherheit" finden Sie den Menüpunkt „Zertifikate von Speicher installieren". Android sucht sich die Datei und installiert Zertifikat und Schlüssel.

Leider ist es mit einer gelungenen Unterstützung von S/MIME in den gängigen Mail-Apps für Android nicht weit her. Weder der vorinstallierte Google-Mailer noch die populären Clients K9 und Kaiten können von sich aus mit den im Betriebssystem installierten Zertifikaten umgehen. Sie benötigen externe Unterstützung.

Die beiden kostenlosen Android-Apps Djigzo und X509Tools übernehmen diesen Job und fungieren jeweils als S/MIME-Proxy für Mail-Anwendungen. Beide Werkzeuge bedienen sich des Zertifikatpools von Android. Djigzo ist außerdem in der Lage, selbst X.509-Zertifikat-Schlüssel-Sets auf dem Gerät zu erstellen. Diese Zertifikate sind aber wenig hilfreich, weil sie die Empfänger keiner Vertrauenskette zuordnen können. Unter Freunden und Bekannten mag das noch gehen, für Geschäftliches taugt es nicht.

Nach der Installation eines der beiden Tools sind Sie in der Lage, Signaturen auszuwerten und Mails zu lesen, die mit Ihrem öffentlichen Schlüssel chiffriert wurden. Allerdings ist das umständlicher als beispielsweise im iPhone: Den verschlüsselten Teil zeigt das Mail-Programm als „p7m-Anhang" an, den Sie antippen müssen. Erst dann schalten sich Djigzo oder die X509Tools dazwischen, dekodieren den Teil mit Ihrem privaten Schlüssel und zeigen den Inhalt. Möchten Sie selbst verschlüsseln, müssen Sie Ihre Mails mit den Tools verfassen.

Die österreichische Sicherheitsfirma rundquadrat, die die X509Tools als „Proof of concept" entwickelt hat, geht deshalb mittlerweile einen anderen Weg: Sie hat einen kompletten Mail-Client namens R2Mail2 entwickelt, der sowohl POP und IMAP als auch S/MIME beherrscht. Diese kostenlose App funktionierte in unserem Test problemlos, allerdings bietet sie naturgemäß längst noch nicht den Komfort und die Übersichtlichkeit wie K9 oder Kaiten.

Ganz schlechte Karten bezüglich E-Mail-Verschlüsselung haben übrigens Nutzer des Microsoft-Betriebssystems Windows Phone. Weder PGP noch S/MIME werden in der aktuellen Version 8 unterstützt. Dies sorgt in Foren insbesondere für Unmut bei Geschäftskunden, die an eine auf S/MIME setzende Exchange-Infrastruktur angedockt sind. (hob)

Gratis-Zertifikate mit 12 Monaten Laufzeit

Anbieter	Produktname	gewerbliche Nutzung erlaubt	Webadresse
Comodo CA Ltd.	Free Secure Email Certificate	nein	https://www.comodo.com/home/email- ecurity/free-email-certificate.php
StartCom Ltd.	StartSSL© Free	ja	https://www.startssl.com/?app=1

Recht auf Verschlüsselung

Polizei, Staatsanwaltschaften und andere Vertreter der Obrigkeit verlangen gern per E-Mail Auskünfte von Unternehmen. Der Bequemlichkeit halber erwarten sie dabei eine unverschlüsselte Preisgabe sogar von personenbezogenen Daten. Aber auch für Vater Staat gilt das Datenschutzrecht. IT-Verantwortliche und betriebliche Datenschutzbeauftragte, die eine unverschlüsselte Übermittlung ablehnen, bekommen Rückenwind vom Bundesgerichtshof (BGH).

Von **Prof. Dr. Noogie C. Kaufmann**

Für die Aufklärung von Straftaten oder Ordnungswidrigkeiten, aber auch bei vielen anderen Gelegenheiten machen Behörden sich Informationen zunutze, die Unternehmen auf ihren Servern gespeichert haben. In E-Mail-Eingangsordnern von Firmen trudeln auf diese Weise allerlei Wünsche nach Auskünften ein. Auch wenn derartige Anfragen mit ordnungsgemäßen Absenderangaben und gescanntem Behördenwappen versehen sind, fehlt in den allermeisten Fällen die Möglichkeit, verschlüsselt zu antworten. Solche Anfragemails, gerichtet an die Geschäftsführung, landen dann zur Bearbeitung beim System-Admin oder auch beim Datenschutzbeauftragten des Unternehmens.

Wenn der gewissenhaft damit umgeht, muss er eigentlich die unverschlüsselte Übermittlung verweigern. Geht es etwa um Namen und Adressen von Kunden oder Mitarbeitern, liegen personenbezogene Daten vor. In Deutschland ist dann das Bundesdatenschutzgesetz (BDSG) einzuhalten. Dieses Hauptgesetz zum Schutz der Privatsphäre untersagt die unberechtigte Übermittlung personenbezogener Daten. Dazu gehört aber auch, dass ein Unternehmen bei einer berechtigten Übermittlung dieser Daten übers Internet sicherstellen muss, dass unbefugte Dritte nichts davon abgreifen können.

Ein anderer Aspekt ist die Pflicht des für die Datenübermittlung Verantwortlichen gegenüber dem eigenen Unternehmen: Er muss vermeiden, dass Betriebs- und Geschäftsgeheimnisse im Netz umhervagabundieren. Eine Klartext-E-Mail würde aus der gewünschten Auskunft gewissermaßen eine öffentlich einsehbare elektronische Postkarte machen. Der Versand eines (auch unchiffrierten) Datenträgers im verschlossenen Umschlag hingegen würde bereits als hinreichend sicher gelten. Per E-Mail transportiert man die gewünschten Daten sinnvollerweise verschlüsselt. Eine praktikable Lösung hierfür ist der Einsatz von

S/MIME (siehe Seite 92): Eine Alternative zu diesem System, das mit gewerblichen Zertifizierungsstellen arbeitet, ist PGP (siehe Seite 82).

BEHÖRDLICHE DROHKULISSE

In einer Zwickmühle können IT-Verantwortliche sich dann sehen, wenn die anfragende Behörde Druck macht und trotz aller Bedenken eine unverschlüsselte Datenübermittlung per Mail verlangt. Es ist schon vorgekommen, dass den betreffenden Mitarbeitern mit bösen Mitteilungen an deren Vorgesetzte gedroht wurde.

Hartnäckige Vertreter von Polizei oder Staatsanwaltschaften gehen noch einen Schritt weiter und bringen das böse Wort „Strafvereitlung" ins Spiel, wenn ihr Ansprechpartner in einem Unternehmen die gewünschte E-Mail-Auskunft verweigert. Mancher IT-ler lässt sich davon einschüchtern und schiebt die verlangten Informationen trotz aller Bedenken ungesichert durchs Netz. Klärende Worte zu diesem Dilemma hat im Frühjahr dieses Jahres der Bundesgerichtshof (BGH) gesprochen. Die obersten deutschen Zivilrichter entschieden, dass es keinen Zwang gibt, „unternehmensinterne Daten über eine ungesicherte E-Mail-Verbindung an (eine) Behörde zu übermitteln" [1].

In dem Fall, den es zu entscheiden galt, wollte ein öffentlich-rechtlicher Wasserversorger der anfragenden Kartellbehörde partout keine unternehmenssensiblen Daten „in elektronischer Form per E-Mail als Excel-Datei" herausgeben.

Der Zwist landete vor dem Brandenburgischen Oberlandesgericht (OLG). Die dortigen Richter verurteilten den Versorger zwar dazu, Auskunft zu erteilen, stärkten ihm aber dahin gehend den Rücken, dass eine ungeschützte Übermittlung nicht in Betracht komme [2]. So sah es dann auch der BGH, der von der Kartellbehörde anschließend bemüht wurde. Anders als noch das OLG ließ er offen, ob es sich bei den verlangten Informationen tatsächlich um Betriebs- und Geschäftsgeheimnisse handelte oder nicht. Nach Auffassung der Karlsruher Richter reicht es sogar aus, dass es „nur" um unternehmensinterne Daten geht. Ganz pragmatisch haben die Bundesrichter der Behörde dann noch ins Stammbuch geschrieben, dass die Datenübermittlung ja auch „auf einem Datenträger oder auf einem gesicherten elektronischen Übermittlungsweg" erfolgen kann.

VERSCHLÜSSELUNGSPFLICHT?

Aufgrund dieser BGH-Entscheidung kam es in Foren und Blogs wieder einmal zu hitzigen Diskussionen darüber, ob bei der Übermittlung personenbezogener Daten nicht eine generelle Pflicht zur Verschlüsselung bestehen müsse. Eine solche Pflicht ist im Gesetz nicht ausdrücklich festgeschrieben.

Zu dem Streitthema hat bis dato vornehmlich das Verwaltungsgericht (VG) Berlin Stellung bezogen: Ihm zufolge kann jedenfalls dann ohne Schutz kommuniziert werden, wenn der Empfänger ausdrücklich darin eingewilligt hat [3]. Aber auch für den Fall, dass keine Zustimmung vorliegt, gehen namhafte Juristen davon aus, dass keine ausdrückliche Pflicht zur Verschlüsselung besteht [4].

KONSEQUENZEN

Die Entscheidung des BGH betraf einen Wasserversorger, der in der Form eines öffentlich-rechtlichen Verbands organisiert ist. Allerdings muss das Urteil auch für alle Privatunternehmen gelten. Deren Rechtsform kann schließlich nicht dafür verantwortlich sein, dass sie ein geringeres Geheimhaltungsbedürfnis hätten. Interessant ist auch, dass der BGH bereits bloße unternehmensinterne Daten unter den Schutz der Verschlüsselung stellt. Daraus lässt sich ableiten, dass personenbezogene Daten von Kunden oder Mitarbeitern erst recht nicht ohne Chiffrierung an Behörden gemailt werden müssen. Schließlich gilt für derartige Daten ausdrücklich das BDSG.

Für die tägliche Praxis von IT-Verantwortlichen, die mit derartigen Anfragen konfrontiert werden, hat die Entscheidung des BGH eine handfeste Auswirkung: Wünsche nach der Herausgabe von Daten in ungesicherter Form müssen nicht erfüllt werden. Wenn Behördenvertreter dennoch darauf bestehen, sollte man standhaft bleiben: Ein Verweis auf das BGH-Urteil kann dabei Wunder bewirken. (psz)

Der Autor ist Honorarprofessor an der Fachhochschule Münster und Rechtsanwalt in Hamburg (info@kanzlei-kaufmann.de).

LITERATUR

[1] Offene E-Mail-Übermittlung unternehmensinterner Daten an eine Behörde darf man verweigern: BGH, Beschluss vom 26. 2. 2013, Az. KVZ 57/12; Online-Fundstellen siehe c't-Link

[2] Brandenburgisches OLG, Beschluss vom 11. 9. 2012, Az. Kart W 2/12

[3] Zum Streit um eine Verschlüsselungspflicht: Noogie C. Kaufmann, Personal im Datenformat, Rechtliche Fallstricke bei Online-Bewerbungen, c't 12/12, S. 140

[4] Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, § 9, Randnummer 83

Alle Links zum Artikel
www.ct.de/hb1401098

Verschlüsseln mit selbst signierten Zertifikaten

Wer eine zuverlässige Mail-Verschlüsselung für den Privateinsatz braucht, muss sich nicht auf SSL-Zertifikate von kommerziellen Anbietern verlassen. Wir zeigen, wie man selbst signierte S/MIME-Zertifikate auf OS X und Windows 8.1 mit Bordmitteln erzeugt und in gängigen Mail-Clients einsetzt.

Von **Dušan Živadinović**

Will man den Mail-Verkehr verschlüsseln, hat man heute die Wahl zwischen Regen und Traufe: Das selbstorganisierte PGP gilt als umständlich. Und das von kommerziellen Dienstleistern gestützte S/MIME ist zwar in vielen Betriebssystemen und Mail-Clients bereits integriert und im Prinzip leicht zu handhaben, wie wir ab S. 92 gezeigt haben. Aber mit den Einbrüchen bei Comodo und Diginotar hat es einen herben Vertrauensverlust erlitten. Nun kann man trotz Zertifikat einer übergeordneten Stelle auch bei S/MIME nicht wirklich sicher sein, wer eine Mail abgeschickt hat (siehe dazu den Kasten „Kleines Krypto-Einmaleins“ auf Seite 105).

Wer den kommerziellen Anbietern misstraut, kann auch selbst signierte Zertifikate einsetzen. Die Betriebssysteme und Mail-Programme können diese zwar nicht anhand der üblichen Einordnung in die vorinstallierte SSL-Vertrauenskette als vertrauenswürdig einstufen, aber wenn sich Freunde, Familienmitglieder oder Mitarbeiter kleiner Unternehmen ihre selbsterstellten S/MIME-Elemente persönlich überreichen, dann sind diese im Prinzip sogar vertrauenswürdiger als die kommerzieller Anbieter.

Der Unterschied liegt darin, dass solche öffentlichen Schlüssel mit den privaten CA-Zertifikaten der Herausgeber signiert sind, zum Beispiel von Klein-Fritzchen und

Klein-Erna. Im OS und den Mail-Clients sind deren Zertifikate zunächst nicht aufgeführt, sondern nur Zertifikate von geprüften Zertifizierungsstellen. Um diese privaten Zertifikate benutzen zu können, muss man sie also per Ausnahmeregel als vertrauenswürdig einstufen.

Es ist jedoch kaum bekannt, wie man selbst signierte S/MIME-Zertifikate auf Macs und Windows-PCs erzeugt - lediglich für Linux und OpenSSL kursieren entsprechende Anleitungen im Internet. Zudem hören die meisten spätestens dort auf, wo es um die Einbindung in Mac- und Windows-Mail-Clients geht. Wir beschreiben die Schritte detailliert für Apple Mail, Windows Live Mail und Thunderbird. Dabei werden in einem Rutsch Zertifikate und Schlüssel erzeugt, die ausschließlich für die Mail-Verschlüsselung ausgelegt sind.

Grundsätzlich gilt: Bevor Sie irgendeinem selbst signierten Zertifikat den Persilschein erteilen, öffnen Sie es in der Schlüsselverwaltung und prüfen Sie anhand der Zertifikateinträge, von wem es stammt und für welche Zwecke es ausgelegt ist: Gegen Mail-Kryptografie mit vertrauenswürdigen Personen spricht nichts. Sollten dort noch weitere Zwecke aufgeführt sein, löschen Sie es besser, es könnte ein Angriff auf Ihren Rechner sein, mit der Absicht, ihn auf präparierte Server zu leiten.

VORSICHTSMASSNAHMEN

Im Grunde sollte diese Anleitung beim Erzeugen der Zertifikate beginnen. Wenn Sie jedoch S/MIME bereits eingesetzt haben, zunächst eine dringende Warnung:

Bevor man irgendein selbst signiertes Zertifikat importiert, sollte man dessen Vertrauenswürdigkeit sicherstellen und prüfen, für welche Zwecke es ausgestellt ist.

Vermeiden Sie etwaige Aufräumaktionen in Ihrer Zertifikatssammlung, ob in den Mail-Programmen oder im Betriebssystem. Selbst wenn Sie alte Zertifikate und Schlüssel nicht mehr für den Mail-Versand verwenden wollen: Sie brauchen sie, um die damit verschlüsselten alten Mails lesen zu können - ohne die zugehörigen Zertifikate und Schlüssel lassen sich die Nachrichten nicht mehr dechiffrieren.

Im Weiteren zeigen wir der Reihe nach, wie man die Zertifikate auf Mac OS X erzeugt und für Apple Mail und Thunderbird einrichtet. Anschließend folgen dieselben Schritte für Windows 8.1 und Windows Live Mail. Die Thunderbird-Konfiguration ist in diesem Punkt auf OS X und Windows gleich (durchgespielt mit diversen Thunderbird-Versionen ab 2.0.0.24). Die auf OS X und Windows 8.1 erzeugten Zertifikate ließen sich über Kreuz mit allen genannten Mail-Clients auf OS X und Windows 8.1 nutzen.

OS X: ZERTIFIKAT ERZEUGEN

Mit dem Mac erzeugten wir korrekte selbst signierte Zertifikate und Schlüssel mit dem Certificate Assistant; wir haben das mit Mac OS X 10.7.4, 10.8.x und 10.9.1 ausprobiert. Das geht von jedem Account aus, dazu muss man kein Admin sein. Als kleine Vorarbeit empfiehlt es sich, die eigene Visitenkarte mitsamt der Mail-Adresse in den Kontakten anzulegen; diese Daten nutzt der Zertifikatsassistent dann für Voreinstellungen beim Zertifikatsbau.

Der Assistent bietet zwar schon in der Grundeinstellung die Option, ein selbst signiertes S/MIME-Zertifikat zu erzeugen, aber wenn man ihn einfach so machen lässt, kommt ein Zertifikat dabei heraus, anhand dessen Apple Mail nur signieren will. Die Verschlüsselung scheitert dann trotz korrektem öffentlichen Schlüssel des Empfängers.

Bei näherer Betrachtung muss man annehmen, dass diese Option bei Apple niemand geprüft hat, denn gängige Mail-Clients setzen Zertifikate voraus, die einige spezielle Einträge in den Bereichen „Schlüsselverwendung" und „Erweiterte Schlüsselverwendung" enthalten. Apples Assistent trägt jedoch nicht alle ein, obwohl er das durchaus könnte. Eingeschaltet sein müssen die Optionen „Signing" (signieren), „Non-repudiation" (Rechtsgültigkeit), „Key Encipherment" (Schlüsselverschlüsselung) und „Data Encipherment" (Datenverschlüsselung).

Starten Sie den Vorgang, indem Sie die Schlüsselbundverwaltung öffnen. Wählen Sie das Menü „Schlüsselbundverwaltung", darin das Menü „Zertifikatsassistent" und dann den Befehl „Zertifikat erstellen".

Übernehmen Sie die ersten drei Voreinstellungen, also den Namen des Zertifikatnutzers sowie „Root, selbst-signiert" und „Zertifikatstyp S/MIME (E-Mail)". Klicken Sie dann darunter „Standardwerte überschreiben" an und „Fortfahren". Legen Sie im nächsten Dialog die Gültigkeit fest: Der Assistent akzeptiert maximal 7300 Tage (rund 20 Jahre). Fahren Sie fort.

Wenn Sie mehr als eine Mail-Adresse in Ihrer Visitenkarte haben, können Sie im nächsten Dialog per Menü jene auswählen, für die das Zertifikat erstellt werden soll. Alternativ kann man hier auch eine neue Mail-Adresse eintragen, falls diese nicht in der Visitenkarte steht. Der Rest kann leer bleiben. Fahren Sie zu den „Informationen zum Schlüsselpaar" fort und übernehmen Sie die Voreinstellungen (2048 Bit, RSA).

In der „Erweiterung Schlüsselverwendung" müssen diese vier Optionen angeklickt sein: Signatur, Unleugbarkeit (Rechtsgültigkeit), Verschlüsseln von Schlüsseln und Datenverschlüsselung.

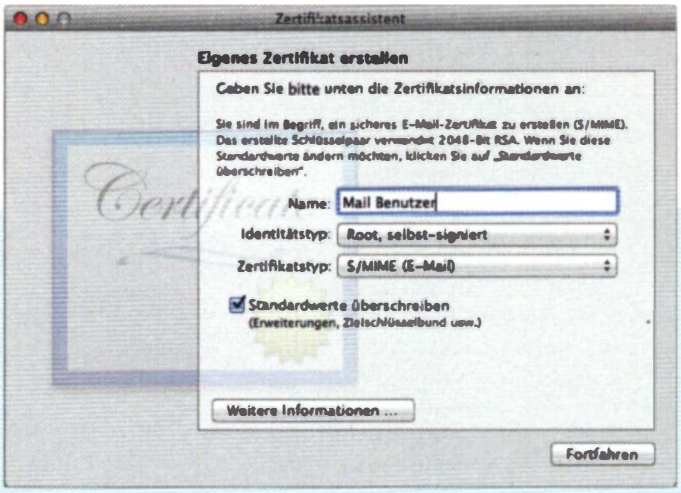
Auf der nächsten Seite „Erweiterung erweiterte Schlüsselverwendung" übernehmen Sie die Voreinstellungen, also: „Erweiterung erweiterte Schlüsselverwendung einschließen", „Erweiterung ist kritisch" und „E-Mail-Schutz".

Klicken Sie zweimal auf Fortfahren („Grundlegende Einschränkungen" nicht benutzen) und übernehmen Sie die Optionen auf der Seite „Alternativer Name des Inhabers". Klicken Sie auf „Fortfahren" und lassen Sie zu, dass das Zertifikat in den Schlüsselbund „Anmeldung" übernommen wird – klicken Sie auf „Erstellen".

Nun blendet das Programm die Zertifikatszusammenfassung mit gelbem Warndreieck ein: „Dieses Zertifikat wurde nicht von einem Drittanbieter verifiziert." Das Zertifikat und die Schlüssel sind zwar fertig, aber damit kann man zunächst nur Mails signieren, weil sie mangels Zertifizierung durch eine übergeordnete Instanz kein Betriebssystem und kein Mail-Client für vertrauenswürdig hält. Damit sie dennoch akzeptiert werden, muss man für jeden Client, der sie verwenden soll, Ausnahmeregeln anlegen.

APPLE MAIL EINRICHTEN

Apple Mail überlässt die Schlüsselverwaltung dem Betriebssystem. Öffnen Sie im Schlüsselbund den Abschnitt „Zertifikate" und doppelklicken Sie das neue Zertifikat, sodass sich dessen Einstellungen öffnen. Öffnen Sie den Bereich „Vertrauen" (schwarzes Dreieck klicken) und schalten Sie dort für die drei Optionen „S/MIME", „Code-Signierung" und „X.509-Standardrichtlinien" die Auswahlmenüs auf „Immer vertrauen" um. Schließen Sie das Fenster und geben Sie Ihr Login-Passwort ein, um die Einstellungen zu übernehmen.



Wenn man den Assistenten einfach machen lässt, liefert er unbrauchbare S/MIME-Zertifikate.

Starten Sie Apple Mail neu, damit es die Einstellung übernimmt – jetzt ist das Programm für S/MIME-Verkehr eingerichtet, sodass es in der Voreinstellung zumindest signierte Mails verschickt. Das erkennt man daran, dass unterhalb der Betreffzeile auf der rechten Seite ein schwarzes Getrieberädchen mit einem Häkchen eingeblendet ist.

Wenn Sie jemand anschreiben, dessen Public Key bereits im Schlüsselbund aufgenommen und als vertrauenswürdig markiert ist, verschlüsselt Apple Mail die Nachricht – und zwar automatisch. Das sieht man daran, dass neben dem Signiersymbol das schwarze Schloss geschlossen wird. Public Keys von vertrauenswürdigen signierten Mails sammelt Apple Mail automatisch und legt sie im Schlüsselbund ab. Um die Verschlüsselung und die Signatur fallweise abzuschalten, genügt es, auf die Symbole zu klicken, sodass dann das Schloss geöffnet und das Häkchen entfernt ist.

APPLE MAIL: EMPFANG

Apple Mail zeigt in der Grundeinstellung nicht an, ob eingegangene Mails signiert und verschlüsselt sind. Öffnen Sie dafür eine Mail und klicken Sie auf „Details".

Nun wird bei signierten Mails die neue Zeile „Sicherheit" mitsamt dem Getrieberädchen und dem

Damit ein selbst signiertes Zertifikat genutzt wird, muss man für jeden Client, der es verwenden soll, Ausnahmeregeln anlegen. Hier ein Beispiel für OS X und Apple Mail.

Häkchen eingeblendet. Wenn Sie auf das Getrieberad klicken, erscheinen die Zertifikatsangaben. Bei Zertifikaten, die eine dem System bekannte CA ausgestellt hat, steht da ein weißes Häkchen auf grünem Kreis und „Dieses Zertifikat ist gültig" und das System hat es bereits in den Schlüsselbund aufgenommen – man braucht also nichts weiter zu tun.

Bei Mails mit selbst signierten Zertifikaten blendet das Programm eine gelbe Zeile mit der Warnung „Die Nachrichtensignatur konnte nicht überprüft werden" ein. Um das Zertifikat zu sehen, klicken Sie auf „Details einblenden" und „Zertifikat einblenden". Wenn Sie dieser Signatur fortan grundsätzlich vertrauen wollen, setzen Sie das Häkchen bei „E-Mails von xy sind gültig, wenn sie von xy signiert sind". Geben Sie Ihr Login-Passwort ein, um die Änderung zu speichern. Erst mit dieser Einstellung können Sie dem Absender auch verschlüsselt antworten.

THUNDERBIRD

Der Thunderbird-Mailer hat eine eigene Zertifikatsverwaltung, in die das selbst generierte Zertifikat und die Schlüssel importiert werden müssen, bevor man sie einem Mail-Konto zuordnen kann.

Dafür braucht Thunderbird zwei Auszüge aus der Schlüsselverwaltung: eine cer-Datei, die nur das Zertifikat mit dem Public Key enthält, und eine p12-Datei, die auch den privaten Schlüssel enthält. Beide kann man aus Apples Schlüsselbund exportieren und zwar so: Klicken Sie auf das Zertifikat, öffnen Sie das Kontextmenü, wählen Sie „Exportieren" und das Format p12 und sichern Sie die Datei (zum Beispiel auf den Desktop). Tragen Sie auf Nachfrage ein Kennwort zum Schutz des Zertifikats ein.

Das ist wichtig, weil sonst jeder, der in dessen Besitz gelangt, den privaten Schlüssel nutzen kann, um Mails unter Ihrem Namen zu versenden. Geben Sie dann Ihr Login-Passwort als Einverständnis ein, dass die Datei exportiert werden darf. Wiederholen Sie den Export für die cer-Datei. Dabei ist keine Passworteingabe erforderlich – es wird ja kein privater Schlüssel exportiert, der geschützt werden müsste.

Starten Sie Thunderbird, öffnen Sie die „Einstellungen", klicken Sie auf „Zertifikate" und nochmals „Zertifikate". Von offiziellen Stellen signierte Zertifikate würde man nun über den Bereich „Ihre Zertifikate" importieren. Das klappt jedoch mit selbst signierten Zertifikaten nur scheinbar: Thunderbird gibt beim Import noch keine Fehlermeldung, kann in der Folge aber Mails weder signieren, noch verschlüsseln.

Das liegt daran, dass für das selbst signierte Zertifikat keine Ausnahmeregel angelegt wurde – es gibt ja an dieser Stelle gar kein Interface, um diese Regel einzutragen. So verwundert es kaum, dass selbst signierte Zertifikate mit Thunderbird nicht gebräuchlich sind – es ist schlichtweg kaum bekannt, wie man das Programm dafür einrichtet. Mit beherztem Experimentieren haben wir aber einen Weg gefunden.

Weil es sich beim selbst signierten Zertifikat um ein Root-Zertifikat handelt, könnten Sie auf den Gedanken kommen, es über den Bereich „Zertifizierungsstellen" hinzuzufügen; dort lassen sich nämlich Ausnahmeregeln eintragen. Aber das verweigert Thunderbird (this is not a certificate authority certificate, so it can't be imported into the certificate authority list). Nehmen Sie stattdessen den Umweg über die Rubrik „Server". Dafür brauchen Sie die cer-Datei.

Sobald diese eingelesen ist, klicken Sie darauf und dann auf „Vertrauen bearbeiten". Stellen Sie dort ein „Der Echtheit dieses Zertifikats vertrauen". Klicken Sie auf „CA-Vertrauen bearbeiten" und setzen Sie im nächsten Menü bei der Option „Dieses Zertifikat kann Mail-Benutzer identifizieren" ein Häkchen. Schließen Sie die Fenster über OK und starten Sie Thunderbird neu.

NACHTWANDERUNG

Öffnen Sie über die „Einstellungen" wieder die „Zertifikate". Das über „Server" importierte Zertifikat ist nach den neuen Vertrauenseinstellungen in die Rubrik „Zertifizierungsstellen" gewandert. Das trifft auf die Mac-

Der Import von selbst signierten Zertifikaten klappt bei Thunderbird auf dem üblichen Weg nicht – aber es gibt Tricks.

Version des Programms zu; bei Thunderbird für Windows gibt es den Eintrag nun sowohl im Bereich „Server" als auch im Bereich „Zertifizierungsstellen".

Klicken Sie auf „Vertrauen bearbeiten" und stellen Sie sicher, dass die Option „Dieses Zertifikat kann Mail-Benutzer identifizieren" angekreuzt ist. Klicken Sie auf OK. Wenn Sie den Eintrag nicht unter den Zertifizierungsstellen finden, liegt das Zertifikat noch immer im Server-Bereich – löschen Sie es dann und wiederholen Sie den Vorgang. Andernfalls liefert Thunderbird bei den nächsten Schritten zwar keine Fehlermeldung, wird Mails aber nur signieren und nicht verschlüsseln.

Fahren Sie also nur dann fort, wenn Ihr selbst signiertes Zertifikat im Bereich „Zertifizierungsstellen" liegt. Öffnen Sie dann „Ihre Zertifikate" und importieren Sie die p12-Datei (wenn Sie sie wie unten beschrieben aus Windows 8.1 exportiert haben, hat sie die Endung .pfx). Geben Sie auf Aufforderung das Passwort ein, das Sie beim Export vergeben haben.

Wenn das korrekt war, erscheint der Dialog „Warnung – Ihre Sicherheitszertifikate und privaten Schlüssel wurden erfolgreich wiederhergestellt". Thunderbird setzt diesen Dialog normalerweise für die Wiederherstellung von Zertifikaten aus Backups ein, deshalb die unpassende Mitteilung. Klicken Sie zweimal auf OK und schließen Sie die „Einstellungen".

Ordnen Sie jetzt das Zertifikat dem zugedachten Mail-Konto zu. Öffnen Sie dafür das Menü „Extras" und „Konten-Einstellungen". Klicken Sie im entsprechenden Mail-Konto auf „S/MIME-Sicherheit" und wählen Sie für die „Digitale Unterschrift" und die „Verschlüsselung" das neu importierte Zertifikat aus. Setzen Sie zum Schluss bei „Nachrichten digital unterschreiben (als Standard)" das Häkchen, wenn jede ausgehende Nachricht dieses Mail-Kontos signiert werden soll (empfehlenswert). Starten Sie Thunderbird neu, damit es die neuen Einstellungen übernimmt.

Wundern Sie sich nicht: Wenn Sie jetzt wieder die Zertifikatsverwaltung öffnen, dann finden Sie unter „Ihre Zertifikate" wie erwartet Ihr neues Zertifikat. Aber den Eintrag aus dem Bereich „Zertifizierungsstellen" hat Thunderbird stillschweigend entfernt … dennoch: Im Endeffekt hat es die manuellen Einstellungen zur Vertrauenswürdigkeit übernommen, sodass Sie jetzt signierte Mails versenden können.

Eine Signatur erkennen Sie im Mail-Entwurfsfenster am kleinen Briefumschlag mit dem roten Punkt rechts unten in der Ecke (Siegel). Soll die Mail verschlüsselt werden, muss Thunderbird den Public Key des Empfängers bereits erhalten haben. Ob das der Fall ist, sehen Sie in der Zertifikatsverwaltung im Bereich „Personen". Wenn ja, dann können Sie die Verschlüsselung im Entwurfsfenster einschalten: Klicken Sie auf das schwarze Dreieck neben dem S/MIME-Icon, um das Untermenü zu öffnen und wählen Sie „Nachricht verschlüsseln" aus.

THUNDERBIRD: EMPFANG

Thunderbird importiert selbst signierte Zertifikate und zugehörige Schlüssel nicht selbstständig in seine Verwaltung und weigert sich auch, wenn man sie aus Thunderbird als pem-Datei exportiert und per Hand in die Rubrik „Personen" importieren will.

Aber mit einem ähnlichen Trick, mit dem man ein eigenes selbst signiertes Zertifikat schmackhaft macht, geht es auch mit Zertifikaten und Schlüsseln, die man von anderen Mail-Teilnehmern erhalten hat: Exportieren Sie sie zunächst als pem-Datei und importieren Sie sie im Bereich „Server". Klicken Sie den neuen Eintrag an und dann die Option „Vertrauen bearbeiten".

Stellen Sie „Der Echtheit dieses Zertifikats vertrauen" ein und klicken Sie auf „CA-Vertrauen bearbeiten". Setzen Sie im nächsten Menü bei der Option

KLEINES KRYPTO-EINMALEINS

Klein-Erna möchte Klein-Fritzchen geheime E-Mails schicken. Das geht nicht ohne Weiteres, beginnt aber damit, dass sie in ihrem Mail-Client auf „Signieren" und auf „Senden" klickt. Nun berechnet ihr Rechner eine Prüfsumme der Mail (Hash), verschlüsselt sie mit ihrem privaten Key und hängt sie mit ihrem öffentlichen Key an die Mail an. Beide Elemente bilden Klein-Ernas individuelle Signatur.

Fritzchens Rechner entschlüsselt den Hash mittels Ernas öffentlichem Key und berechnet ebenfalls den Hash der empfangenen Mail. Stimmt sein Ergebnis mit dem mitgeschickten überein, gilt die Mail als unverfälscht. Ob die Signatur tatsächlich von Erna stammt, prüft er zum Beispiel, indem er per Telefon den Fingerprint des Schlüssels abfragt. Wenn Erna ihren privaten Key nicht aus den Händen gibt, kann niemand anderes Mails mit dieser Signatur verfassen. Fritzchen kann also annehmen, dass sie zweifelsfrei von ihr stammen.

Fritzchen kann nun mit Ernas öffentlichem Schlüssel Mails verschlüsseln, die nur Erna lesen kann – weil sie als einzige den privaten Schlüssel hat, mit dem sich die Nachricht dechiffrieren lässt. Dass die Mail tatsächlich von Fritzchen stammt und unverfälscht ist, erkennt sie anhand seiner Signatur. Diese enthält auch seinen öffentlichen Schlüssel, sodass nun beide einander verschlüsselte Mails senden können. Diese Methode entspricht weitgehend dem heutigen PGP und den beiden reicht das Verfahren zunächst komplett aus.

Vergebliches Vorkosten

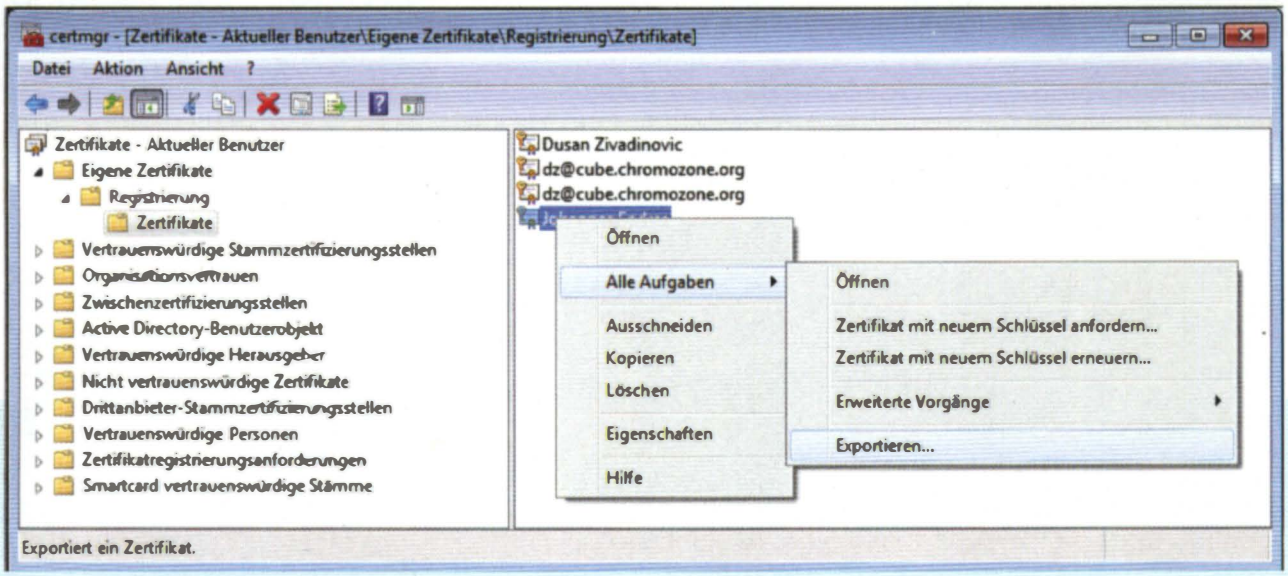
Wenn sie nun Mails von Fremden erhalten, zum Beispiel von gerhard.schroeder@gefaerbte-haare.de, können sie jedoch nicht mit vertretbarem Aufwand prüfen, von wem diese tatsächlich stammen. Das kann eine öffentliche Stelle übernehmen: Sie stellt die Identität des Schlüsseleigners anhand seines Ausweises fest und signiert seinen Schlüssel mit ihrem eigenen Schlüssel. Nun müssen Fritzchen und Erna nicht jeden öffentlichen Schlüssel überprüfen, sondern nur noch die öffentliche Stelle, die die Schlüssel zertifiziert hat. Das geht bei PGP zum Beispiel, indem man die Signatur einer Zertifizierungsstelle mit öffentlich hinterlegten Daten vergleicht (Key IDs, Fingerprints …). Längst nicht alle PGP-Schlüssel sind aber zertifiziert, sodass die Überprüfung unbekannter Keys bei PGP nicht immer klappt.

Bei S/MIME hat der Hersteller des Betriebssystems (oder der Hersteller des Mail-Clients, z. B. Mozilla bei Thunderbird) bereits viele Zertifizierungsstellen (Certification Authority, CA) selbst überprüft und deren Stammzertifikate in der Schlüsselverwaltung hinterlegt. Wenn also das Zertifikat eines öffentlichen S/MIME-Schlüssels kryptografisch an ein übergeordnetes, bereits vorgeprüftes Stammzertifikat gebunden ist, gibt das Betriebssystem grünes Licht für die jeweilige Signatur.

Auf diese Weise arbeiten fast alle Mail-Clients, die S/MIME nutzen. Fritzchen und Erna könnten also den CAs vertrauen, die öffentliche Schlüssel unbekannter Mail-Absender signieren.

Freilich tun sie es nicht mehr, denn bereits zwei CAs, Comodo und Diginotar, sind ungenügend gesichert gewesen und Einbrüchen zum Opfer gefallen, sodass Angreifer deren Signiermaschinerie missbrauchen konnten.

Damit ist das Vertrauen in CAs geschwächt und deren Zertifikate bei kritischer Betrachtung hinfällig. Mail-Clients setzen aber grundsätzlich zertifizierte Schlüssel voraus, sodass es nicht genügt, ein Schlüsselpaar zu erzeugen (etwa mit OpenSSL). Fritzchen und Erna können sich aber behelfen, indem sie eigene private CA-Zertifikate erzeugen und damit ihre eigenen Schlüssel selbst signieren. Damit diese Schlüssel die Betriebssysteme und Mailer akzeptieren, müssen sie nur noch per Ausnahmeregel in die Liste der vertrauenswürdigen Zertifikate aufgenommen werden …



Selbst signierte Mail-Zertifikate lassen sich leicht mit Windows-Bordmitteln erzeugen. Sie landen stillschweigend im Systemschlüsselbund, von wo aus man sie auch exportieren kann.

„Dieses Zertifikat kann Mail-Benutzer identifizieren" ein Häkchen, klicken Sie zweimal auf OK und schließen Sie die Zertifikatsverwaltung.

Jetzt können Sie dem Sender verschlüsselt antworten. Diese Option kann man grundsätzlich in der Kontoverwaltung einschalten oder separat für jede neue Mail über das Menü neben dem S/MIME-Knopf.

WINDOWS 8.1 PRO

Windows 8.1 verfügt zwar in Gestalt des certmgr.msc wie OS X über ein grafisches Frontend, mit dem sich selbst signierte Zertifikate und Schlüssel erzeugen lassen, aber der Weg ist umständlich. Unter anderem erwartet certmgr einen Richtlinien-Server nebst Directory Server, die man nur in Enterprise-Umgebungen aufsetzen möchte. Etwas einfacher geht es mit Kommandozeilenprogrammen wie makecert.exe (Bestandteil des Microsoft-SDK). Damit erzeugte Zertifikate akzeptieren aber nicht alle Mail-Clients, sodass wir anders als manche Anleitung im Internet davon abraten.

Statt dessen empfiehlt sich certreq.exe, das Microsoft mit Windows XP eingeführt hat. Zu beachten ist, dass die mit Windows 2000 ausgelieferte Version im Funktionsumfang limitiert und daher für die im Weiteren beschriebenen Schritte nicht geeignet ist. Wir beziehen uns auf die Windows-8.1-Version.

Selbst signierte Zertifikate und zugehörige Schlüssel erstellt certreq.exe unter anderem anhand von inf-Dateien. Es gibt auch ausführliche Dokumentationen dazu, beispielsweise bei Microsoft Technet (siehe c't-Link am Ende des Artikels). Die Crux an certreq ist, dass praktisch alle Anleitungen nur selbstsignierte Zertifikate für Web-Server zum Ziel haben. Wir haben dennoch einen Weg gefunden, auch S/MIME-Zertifikate zu erzeugen. Hat man eine inf-Datei erzeugt, ist der Vorgang in kurzer Zeit erledigt. Ein Muster, in dem Sie lediglich den Namen des Benutzers und dessen Mail-Adresse ändern müssen, haben wir zum kostenlosen Download bereitgestellt (siehe c't-Link).

Besonders wichtige Einträge der inf-Datei sind „Exportable" (damit der private Schlüssel auch außerhalb der Windows-Schlüsselbundverwaltung eingesetzt werden kann), KeySpec und KeyUsage (darüber legt man den Anwendungsbereich zum Signieren und Verschlüsseln fest), ProviderName und -Typ (daraus bezieht die Software die Verschlüsselungsmethoden), RequestType (damit veranlasst man die Selbstsignatur) sowie die OID-Typen (das sind erweiterte Schlüsselanwendungen). Die meisten der Optionen hat

Die Vertrauenswürdigkeit der S/Mime-Zertifikate lässt sich ohne Umwege zur Schlüsselverwaltung direkt über Windows Live Mail einstellen.

Microsoft umfassend dokumentiert, aber in unterschiedlichen, teils ausufernd langen Dokumenten. Einige Optionen haben wir nur durch mühsames Experimentieren ermitteln können.

Wenn Sie das inf-File (im Beispiel dz-SMIME.inf genannt) an Ihre Bedürfnisse angepasst haben, erzeugen Sie das Zertifikat mit diesem simplen Kommando:

```
certreq -new dz-SMIME.inf dz-SMIME.crt
```

Das self-signed Zertifikat dz-SMIME.crt liegt dann im selben Ordner wie das inf-File. Es enthält jedoch keinen privaten Key – den hat das Kommando stillschweigend zwar ebenfalls erzeugt, aber im Systemschlüsselbund hinterlegt.

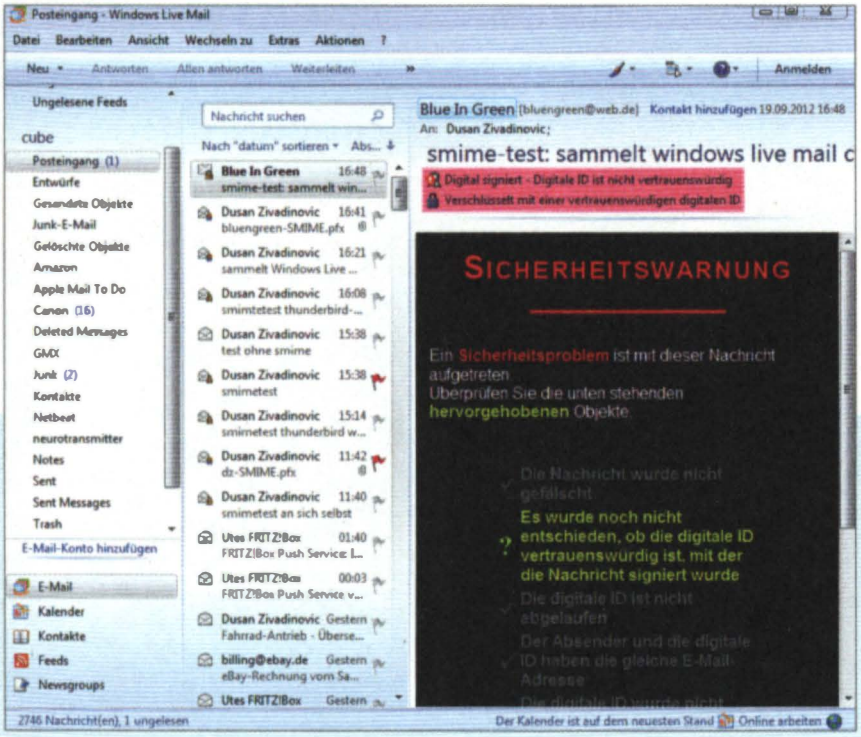
WINDOWS LIVE MAIL

Damit Sie das Zertifikat und den privaten Schlüssel mit Windows Live Mail nutzen können, öffnen Sie certmgr.msc (geben Sie den Programmnamen im Startmenü ein und schließen Sie die Eingabe mit „Enter" ab), steuern Sie den Bereich „Eigene Zertifikate" und „Zertifikate" an und klicken Sie das neue Zertifikat an. Kopieren Sie es per Ctrl-C. Öffnen Sie dann „Vertrauenswürdige Stammzertifizierungsstellen" und „Zertifikate", fügen Sie das Zertifikat aus der Zwischenablage dort ein (Ctrl-V) und nicken Sie die Sicherheitsabfrage ab.

Starten Sie nun Windows Live Mail, klicken Sie auf das Menü „Datei", „Optionen", dann auf „Sicherheitsoptionen" und dort auf „Sicherheit", „Digitale IDs" und schließlich „Eigene Zertifikate". Klicken Sie auf das neue Zertifikat und dann unten auf den Knopf „Anzeigen". Dort sollte stehen: „Dieses Zertifikat ist für folgende Zwecke beabsichtigt: 'Schützt E-Mail-Nachrichten, alle ausgegebenen Richtlinien'."

Wenn das nicht der Fall ist und stattdessen „Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig ..." dort steht, dann haben Sie entweder noch keine Kopie in den „Vertrauenswürdigen Stammzertifizierungsstellen" angelegt oder das Zertifikat nur dorthin verschoben. Es muss aber in beiden Ordnern vorhanden sein.

Schließen Sie die beiden letzten Anzeige-Fenster. Wenn Sie Ihre Nachrichten grundsätzlich signieren und verschlüsseln wollen (empfehlenswert), schalten Sie unten die zwei Häkchen ein für die Optionen „Alle ausgehenden Nachrichten und Anlagen verschlüsseln" und „Alle ausgehenden Nachrichten digital signieren". Schließen Sie die „Sicherheitsoptionen" über „OK". Schließen Sie alle Programme, melden Sie Ihre



Vor selbst signierten Zertifikaten warnt Windows Live Mail – mit wenigen Mausklicks lässt sich das bei Bedarf aber abschalten.

aktuelle Windows-Sitzung ab, melden Sie sich neu an und starten Sie Windows Live Mail.

Legen Sie eine neue Mail an (Ctrl-N) und tragen Sie für einen ersten Test als Empfänger ihre eigene Adresse ein, von der aus Sie verschlüsselte Mails senden wollen. Windows Live Mail ist nämlich so voreingestellt, dass es an sich selbst adressierte Mails wenn möglich ebenfalls verschlüsselt. Tragen Sie also einen Betreff und eine Mitteilung ein und schicken Sie sich die Nachricht selbst. Kurz darauf sollte sie im Eingangsordner zu sehen sein. Windows Live Mail sollte dabei diesen Text anzeigen: „Digital signiert und überprüft, verschlüsselt mit einer vertrauenswürdigen ID".

LIVE MAIL: EMPFANG

Nun sendet das Programm signierte Mails. Um diese auch noch zu verschlüsseln, braucht man für jeden Empfänger dessen öffentlichen S/MIME-Schlüssel. Windows Live Mail sammelt diese zwar selbst ein und nutzt sie auch automatisch zum Verschlüsseln, aber nur, wenn es sie für vertrauenswürdig hält. Das ist in der Voreinstellung nur bei kommerziellen Zertifikaten der Fall.

Wenn es Mails mit selbst signierten Zertifikaten empfängt, warnt Windows Live Mail mit der Meldung „digitale ID ist nicht vertrauenswürdig". Wenn Sie sicherstellen können, dass die Signatur und damit der öffentliche Schlüssel von einem vertrauenswürdigen Absender stammt, können Sie die Einstufung ändern, indem Sie neben der Sicherheitswarnung auf das weiße Ausrufezeichen im roten Kreis klicken und im Bereich „Sicherheit" die „Zertifikate anzeigen".

Klicken Sie dann auf den dritten Button von oben namens „Zertifikat des Absenders" und darin auf „Vertrauensstellung". Vergewissern Sie sich, dass das Zertifikat vertrauenswürdig ist (falls nicht: schließen Sie den Dialog über das weiße „X" im roten Rechteck rechts oben). Falls ja: Schalten Sie die Option „Dieses Zertifikat als vertrauenswürdig einstufen" ein, beenden Sie den Dialog über OK und klicken Sie auf den vierten Button von oben: „Zu Kontakten hinzufügen".

Nicken Sie die Übernahme des Zertifikats ab und schließen Sie die übrigen Sicherheitsdialoge über OK. Wenn Sie nun die ursprüngliche Mail mit dem zunächst nicht vertrauenswürdigen Zertifikat erneut in Live Mail öffnen, sollte der Warnhinweis nicht mehr auftauchen. Jetzt sollten Sie dem Absender verschlüsselt antworten können.

Beide S/MIME-Optionen, das Signieren und das Verschlüsseln, lassen sich in Windows Live Mail bei Bedarf für jede neue Mail per Hand auch abschalten. Wenn Sie

eine neue Mail ohne Verschlüsselung oder Signatur verfassen wollen, klicken Sie im Entwurfsfenster auf „Optionen". Nun sollte das Entwurfsfenster die Menübefehle „verschlüsseln" und „digital signieren" anzeigen.

WINDOWS: ANDERE CLIENTS

Um ein mit Windows 8.1 erzeugtes Zertifikat außerhalb von Windows Live Mail nutzen zu können, muss es exportiert werden. Klicken Sie dafür auf das Startmenü, tippen Sie „certmgr.msc" und starten Sie es (drücken Sie die Enter-Taste). Steuern Sie den Bereich „Eigene Zertifikate" und „Zertifikate" an. Dort liegt Ihr neues Zertifikat mitsamt dem privaten Schlüssel.

Klicken Sie es an, öffnen Sie über die rechte Maustaste das Kontextmenü und darin das Untermenü „Alle Aufgaben". Starten Sie den Schlüssel-Export über den Befehl „Exportieren".

Klicken Sie im Export-Assistenten auf „Weiter", „Ja, privaten Schlüssel exportieren" und nochmals „Weiter". Schalten Sie unter dem Bereich „Privater Informationsaustausch" die beiden Optionen „Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen" und „Alle erweiterten Eigenschaften exportieren" ein.

Alle Links zum Artikel
www.ct.de/hb1401100

Klicken Sie dann „Weiter" und geben Sie ein Passwort für den privaten Schlüssel ein, das möglichst nicht leicht zu erraten ist – andernfalls lässt sich der private Schlüssel leicht missbrauchen, wenn er Dritten in die Hände fällt. Nutznießer können dann verschlüsselte Mails lesen, die an Sie gerichtet sind und Mails in Ihrem Namen signieren.

Legen Sie im nächsten Dialog den Exportpfad (z. B. Ihren Desktop) und den Dateinamen fest (z. B. dz-SMIME). Übernehmen Sie die pfx-Dateiendung, die der Export-Dialog vorschlägt und klicken Sie auf „Speichern", „Weiter" und „Fertig stellen".

Das pfx-Format ist der Vorgänger des heute für den Export von privaten Schlüsseln verwendeten p12-Formats und wird von gängigen Mail-Clients anstandslos akzeptiert.

Um das Zertifikat in Thunderbird zu nutzen, brauchen Sie noch das Zertifikat ohne den privaten Key. Wiederholen Sie den Export aus certmgr heraus, stellen Sie dabei aber die Optionen „Nein, privaten Schlüssel nicht exportieren" sowie „Base-64-codiert X.509 (.cer)" ein. Wenn beide Dateien vorliegen, importieren Sie sie wie für Thunderbird Mac beschrieben. **(dz)** c't

SSL-Verbindungen besser sichern

Die SSL-Verschlüsselung kann man verblüffend leicht austricksen – wegen gravierender Konzeptschwächen. Prinzipiell lassen sich daher HTTPS-Zugriffe auf Online-Banking, Webmail und andere vertrauliche Dienste attackieren, der Aufwand ist nicht einmal hoch. Abhilfe versprechen Pinning-Techniken, mit denen Entwickler Programme besser vor Lauschern schützen können.

Von **Reiko Kaps**

Das besser unter seinem alten Namen Secure Socket Layer (SSL) bekannte Transport Layer Security (TLS) gilt landläufig als Garant für vertrauliche, weil verschlüsselte Online-Kommunikation. Doch das SSL-System lässt sich austricksen:

Bevor eine verschlüsselte SSL-Verbindung aufgebaut wird, muss sich üblicherweise der Server gegenüber dem Client ausweisen. Andernfalls wäre für den Client unklar, ob er mit dem richtigen Server kommuniziert, und Angreifer könnten so leicht Fallen stellen. Als Ausweis wird bei SSL ein digitales Zertifikat eingesetzt. Darin beglaubigt der Aussteller dem Nutzer dessen Identität. Als Aussteller arbeiten Zertifizierungsstellen, die im Grundsatz als vertrauenswürdig gelten (Certificate Authorities).

Das Zertifikat erzeugt eine CA aus einem über Common Name und dem öffentlichen Server-Schlüssel ermittelten Hash, den sie mit ihrem privaten Schlüssel verschlüsselt. Anschließend fügt sie den verschlüsselten Hash (digitale Unterschrift) an den öffentlichen SSL-Schlüssel des Servers an, der dieses Zertifikat an seine Clients ausliefert.

Auf den Clients sind üblicherweise übergeordnete CA-Zertifikate installiert, mittels derer sich die Echtheit der Serverzertifikate prüfen lässt (Chain of Trust, Vertrauenskette). Der Client greift sich die Unterschrift aus dem Serverzertifikat und sucht in seinem lokalem Speicher nach dem Zertifikat der unterzeichnenden CA. Findet er es, extrahiert er daraus den öffentlichen CA-Schlüssel, entschlüsselt damit die Unterschrift und vergleicht sein Ergebnis mit dem Hash-Wert des öffentlichen Serverschlüssels und dessen Common Name. Stimmen beide Hash-Werte überein, handelt es sich um eine gültige Unterschrift. Der Client setzt daraufhin den weiteren SSL-Verbindungsaufbau fort, handelt also die Verschlüsselung mit einem separaten kryptografischen Schlüssel aus. Scheitert die Prüfung des Serverzertifikats, scheitert auch die SSL-Verbindung, weil ja unklar ist, ob der Client dem Server vertrauen kann.

LÜCKEN

Bei diesem Verfahren hängt die Sicherheit maßgeblich an der Vertrauenswürdigkeit der CAs. Daraus ergeben sich zwei prinzipielle Angriffsszenarien auf den Client: Kapern einer CA und das Unterschieben eines CA-Zertifikats. Zunächst zum Kaperungsfall:

Kommen Kriminelle – etwa durch den Einbruch in eine CA – in den Besitz eines gültigen, privaten CA-Schlüssels, können sie jederzeit SSL-Schlüssel für beliebige Domains unterzeichnen. Da es sich um von einer CA signierten Schlüssel handelt, bemerken die Clients davon nichts und der Nutzer wähnt sich in einer Verbindung mit einem vertrauenswürdigen Server. Im Falle des Mitte 2011 aufgeflogenen Einbruchs bei der niederländischen CA Diginotar stellten sich die Einbrecher gültige Zertifikate für Google-Dienste aus. Damit wäre etwa die iranische Regierung in der Lage, alle Google-Mail-Nutzer im eigenen Land zu überwachen (siehe c't-Link am Ende des Artikels). Dabei muss der Client nicht einmal auf das öffentliche Zertifikat dieser missbrauchten CA zugreifen: Eine Validierung des Server-Zertifikats klappt schon, wenn der Client das Zertifikat einer Root-CA an Bord hat, die ihrerseits der gekaperten CA vertraut.

Beim zweiten Szenario wird dem Client ein Zertifikat untergejubelt, das nur scheinbar von einer CA stammt. Bekommt der Client bei Anfragen von dieser vorgeblichen CA unterschriebene Server-Zertifikate präsentiert, akzeptiert er sie ohne Weiteres. Dieses Verhalten nutzen die oft in Firmennetzen installierten SSL-Gateways, um aus- und eingehenden SSL-Verkehr zu prüfen – also zu entschlüsseln. Denkbar wäre aber auch, dass eine Schadsoftware ein CA-Zertifikat auf dem Client installiert. Wie auch das SSL-Gateway muss sie dem Client dann nur noch vortäuschen, dass er mit dem richtigen Server spricht.

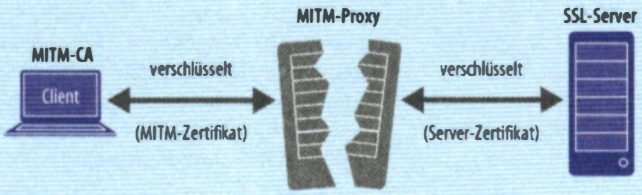
Ein mit diesem CA-Schlüssel ausgestattetes SSL-Gateway übergibt beim Verbindungsaufbau dem Client ein von genau dieser CA unterschriebenes und von ihr selbst erzeugtes Serverzertifikat. Das sorgt für den unterbrechungsfreien SSL-Verbindungsaufbau beim Client, weil er ja das Zertifikat der vermeintlich vertrauenswürdigen CA an Bord hat.

Lieferte das SSL-Gateway stattdessen ein Serverzertifikat aus, das nicht von einer CA, sondern vom Inhaber des SSL-Schlüssels selbst unterzeichnet wurde (Selfsigned Certificate), warnen alle aktuellen Browser den Nutzer vor dieser Verbindung. Ihnen fehlt ja die CA, die die Identität des Server bestätigt. Der Nutzer

Browser warnen immer vor Serverzertifikaten, die der SSL-Schlüsselinhaber selbst unterschrieben hat. Anders als ein untergeschobenes CA-Zertifikat betrifft ein vom Nutzer akzeptiertes Serverzertifikat nur den jeweiligen Hostnamen.

Man-in-the-Middle bei SSL

Vertraut der Client einmal einer CA, lässt sich über ein Gateway SSL-verschlüsselter Netzwerkverkehr leicht belauschen.



muss nun selbst entscheiden, ob er dem Server vertraut – und in der Regel eine Ausnahmeregel im Browser für diesen SSL-Server einrichten. Das nötige Vertrauen lässt sich etwa über den Abgleich des Zertifikatsfingerabdrucks herstellen.

Dank des untergeschobenen CA-Zertifikats können sich SSL-Gateways aber unbemerkt zwischen Nutzer und Server klemmen und nach dem Aushandeln der weiteren SSL-Parameter den gesamten, vom Client ausgehenden SSL-Traffic entschlüsseln. Die Client-Anfragen kann das SSL-Gateway nun entweder einfach zum Zielserver weiterleiten oder auch ändern (siehe Grafik oben).

Wer diese SSL-Schwäche nutzt, umgeht die Verschlüsselung wirkungsvoll. Diese ist zwar weiterhin zuverlässig, aber dennoch ausgehebelt. Auf dem CCC-Kongress 29C3 Ende 2012 in Hamburg konstatierte daher der Niederländer Axel Arnbak: „Das SSL-System ist grundlegend defekt – und jemand muss es reparieren."

WAS TUN?

Um es vorwegzunehmen: Bislang gibt es noch kein komfortables und umfassendes Verfahren, das diese Reparatur erledigen könnte. Die derzeit nutzbaren SSL-Absicherungen sind von Betriebssystem zu Betriebssystem und von Anwendung zu Anwendung unterschiedlich implementiert. Sie gründen darauf, dass Clients Listen (Whitelists) konsultieren, auf denen feste Zuordnungen von Servern und Zertifikaten niedergelegt sind (Pinning): Dabei ordnen diese Listen einem Hostnamen entweder ausdrücklich ein oder mehrere öffentliche SSL-Schlüssel (Public Key Pinning), SSL-Zertifikate (Certificate Pinning) oder CAs zu, die sein SSL-Zertifikat unterzeichnen dürfen.

Während Apps unter Android 4.2 und neuer auf eine systemweite Pinning-Liste zurückgreifen können, lernt der Internet Explorer unter Windows solche Regeln über ein zusätzliches Tool. Bei anderen Betriebssystemen liegt es an den Anwendungsentwicklern, Pinning in ihre Programme einzubauen. Dazu stehen zahlreiche How-tos im Internet bereit. Ganz ähnlich funktionieren die Pinning-Verfahren für iOS- oder Android-Apps. Wie man seine Anwendungen mit Pinning-Regeln nachrüstet, beschreiben Moxie Marlinspike für Android-Apps sowie Graham Lee für Mac OS X/iOS. Viele weitere Beiträge im Internet beleuchten das Thema auch für andere Plattformen (siehe c't-Link auf Seite 114).

Google setzt die Pinning-Technik in seinem Chrome-Browser bereits seit 2011 ein und konnte damit einige Missbrauchsfälle des SSL-Systems ans Tageslicht bringen. Das Unternehmen packt seinem Browser eine Liste von öffentlichen CA-Schlüsseln bei und nur diese CA-Schlüssel sind zur Beglaubigung der Zertifikate von Google und einigen anderen Anbietern berechtigt. Erhält der Browser ein SSL-Zertifikat für www.google.de, das eine nicht aufgeführte CA unterschrieben hat, blockiert das Programm den weiteren Verbindungsaufbau. Dadurch können Chrome-Nutzer beim Zugriff auf Google-Dienste sicher sein, dass Lauscher zumindest nicht über untergeschobene Zertifikate mithören können.

Ein Nachteil dieses Verfahrens ist, dass andere Anwendungen auf dem Rechner nicht in den Genuss von Googles CA-Festlegung kommen. Auch wird die fest eingebaute Liste nur beim Browser-Update auf den aktuellen Stand gebracht. Die Chrome-Liste nutzen inzwischen auch andere Anbieter wie Twitter (siehe c't-Link).

INTERNET EXPLORER

Unter Windows und auf geknackten Android-Geräten (Root-Zugang aktiviert) lässt sich CA-Pinning ohne Programmierarbeit einrichten. Das kostenlose Tool EMET 4.0 (Enhanced Mitigation Experience Toolkit) legt auf Windows nicht nur Ausführungsrichtlinien für Anwendungen und Dienste fest, sondern kettet die SSL-Zertifikate von Host- und Domainnamen an CAs respektive deren Zertifikate. Diese Regeln kombiniert das Tool mit einem Verfallsdatum, einer minimalen Schlüssellänge, erlaubten Länder-Kennungen und dem öffentlichen Schlüssel. Außerdem blockiert es als zu schwach erwiesene Hash-Algorithmen.

EMET läuft zwar auch auf allen Windows-Versionen, die Pinning-Regeln kann es aber nur dem auf dem klassischen Windows-Desktop laufenden Internet Explorer vorgeben – der gekachelte IE in Windows 8.x nutzt sie laut der beigefügten Hilfe nicht.

Wenn Sie CA-Pinning im IE einschalten wollen, müssen Sie zuerst den Prozess iexplore.exe über EMETs etwas irreführenden Menü-Punkt „Apps" in die Liste der überwachten Anwendungen aufnehmen (Add Application). Dann schließen Sie dieses Fenster und rufen den Menü-Punkt „Trust" auf. Im nächsten Fenster fügen Sie zuerst über „Add Website" einen Domain- oder Hostnamen hinzu und wechseln dann zum zweiten Reiter „Pinning Rules".

Dort legen Sie eine Regel für den Zugriff auf diese Domain an: Die benötigt einen Namen, ein oder mehrere aus dem Windows-Zertifikatsordner auszuwählende CA-Zertifikate sowie ein Verfallsdatum. Optional setzen Sie mit „Minimum Key Size" eine Untergrenze für die Länge des öffentlichen CA-Schlüssels, die Vorgabe, aus welchem Land die unterschreibende CA kommt (Allowed Country) und welche Hash-Algorithmen die unterschreibende CA nicht verwenden darf (Blocked Hashes). Wenn Sie „PublicKey Match" aktivieren, überprüft EMET nur den öffentlichen CA-Schlüssel, was man laut Hilfe nur in Ausnahmefällen tun sollte. Wechseln Sie danach wieder zum Reiter „Protected Websites" und verknüpfen Sie die Regel mit der Ziel-Domain.

Für den EMET-Funktionstest empfiehlt es sich, in der neuen Regel als CA eine vom SSL-Zertifikat abweichende auszuwählen – also eine, die das SSL-Zertifikat der Domain nicht unterschrieben hat. Ruft man nun die Webseite auf, warnt EMET vor der Regelverletzung. Meldungen im Windows-Systemlog lassen sich übers EMET-Hauptmenü hinzuschalten und über die Ereignisanzeige auswerten, sodass man sie auch zentral abfragen kann – etwa in Firmennetzen.

Passt ein SSL-Zertifikat nicht auf die EMET-Vorgaben, meldet das Programm den Regelverstoß.

FIREFOX

Für Mozillas Firefox gibt es das Add-on Certificate Patrol, das sowohl zum Nachladen angebotene SSL-Zertifikate samt einiger Details meldet als auch Änderungen in bereits installierten Zertifikaten anzeigt. Es lässt sich einstellen, ob es auch harmlose Änderungen meldet, wie es mit Wildcard-Zertifikaten umgeht und ob es Zertifikate mit unkritischen Änderungen automatisch annehmen darf. In einer Ausnahmeliste lassen sich zudem Domainnamen aufnehmen, die das Add-on nicht überprüft.

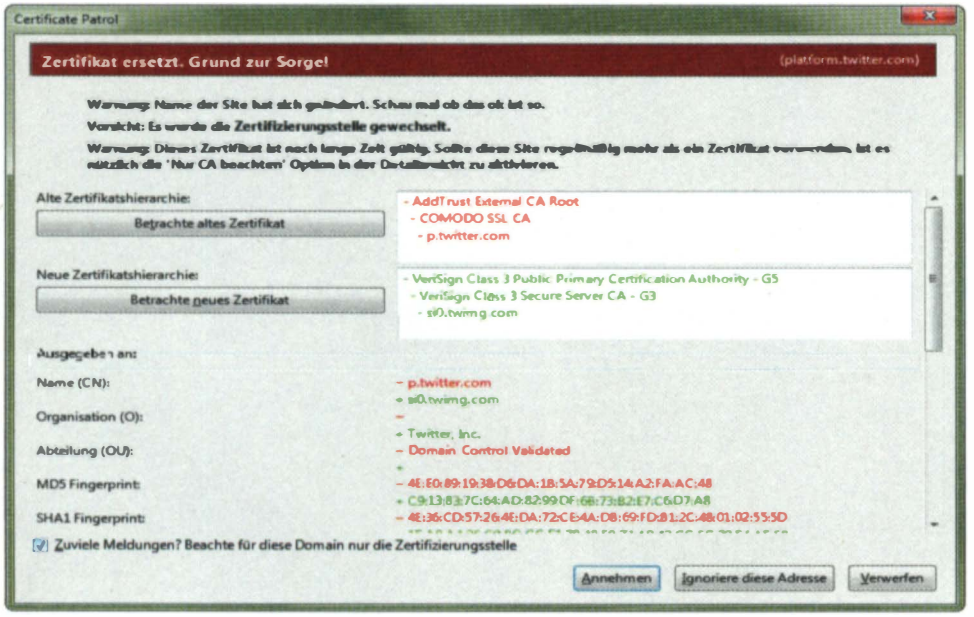
ANDROID

Googles Mobilbetriebssystem bringt seit Version 4.2 einen einfachen, systemweit nutzbaren Pinning-Mechanismus mit. Doch lässt sich dieser derzeit nur auf Geräten einschalten, bei denen ein Root-Zugang eingerichtet ist [1].

Die Pinning-Regeln liest Android 4.2 aus der Datei /data/misc/keychain/pin, falls sie vorhanden ist. Pro Zeile lässt sich dort ein Host- oder Domainname mit einer oder mehreren CAs verknüpfen:

```
heise.de=true|SPKI SHA512-Hash,SPKI SHA512-Hash
```

Mit „heise.de=true" schaltet man die CA-Pinning-Regel für heise.de ein. Hinter dem Schlüsselwort SPKI listet man die Hash-Werte der zeichnungsberechtigten CAs. Ablaufdaten oder andere einschränkende Optionen kennt dieses Verfahren nicht. Außerdem befolgen Apps diese Regeln nur dann, wenn sie Webzugriffe über die Standard-HTTP-Bibliothek abwickeln. Alternativ können Apps die Pin-Regeln über die Android-Funktion TrustManagerImpl abfragen. Die in einigen Apps eingesetzte ältere Methode checkServerTrusted() igno-



Änderungen an Zertifikaten erkennt Certificate Patrol zuverlässig. Dabei zeigt es die Unterschiede der Versionen, überlässt das weitere Vorgehen aber dem Nutzer.

riert die in der Datei festgelegten Vorgaben, erklärt Nikolay Elenkov in einem Blog-Beitrag von Ende 2012 (siehe c't-Link).

Nikolay Elenkov hat für diesen Mechanismus die Beispiel-App Cert Pinner geschrieben, über die man die Pin-Datei mit eigenen Vorgaben erweitern und testen kann (siehe c't-Link). Die Software muss man aber vor Gebrauch selbst übersetzen, die Quellen sind auf Github veröffentlicht.

VERTEILTE ZERTIFIKATSVERGLEICHE

Ein Man-in-the-Middle-Angriff auf eine SSL-Verbindung lässt sich auch anders aufdecken: Die recht junge Open-Source-Software DetecTor.io versucht es über Vergleiche. Will ein Client eine SSL-verschlüsselte Verbindung zu heise.de aufbauen, holt sich DetecTor.io über fünf verschiedene Tor-Routen das SSL-Zertifikat des Heise-Servers und vergleicht es mit dem über die direkte Verbindung ermittelten. Weicht dieses von den anderen ab, blockiert DetecTor.io den weiteren Verbindungsaufbau.

DetecTor.io klinkt sich sehr tief ins Betriebssystem ein: Derzeit nutzt es den Name Service Switch (NSS) von Unix-Betriebssystemen. Mittels NSS entscheidet das Betriebssystem, welche Quellen es für die Namensauflösung, Benutzerinformationen oder Ähnliches einsetzt. Indem es sich in die NSS-Entscheidungsvorgänge einklinkt, greift das Verfahren bei fast allen Anwendungen, die diesen Mechanismus einsetzen. Der Entwickler Kai Engert nennt in seinem Whitepaper als Beispielanwendungen Mozillas Firefox und Thunderbird, die quelloffene Variante des Google-Browsers Chromium, den Gnome-Mailclient Evolution sowie das Instant-Messaging-Tool Pidgin.

LITERATUR

[1] Hannes A. Czerulla, Martin Holland, **Entfesselt**, Smartphones mit Android rooten, Teil 2, c't 14/12, S. 168

Alle Links zum Artikel
www.ct.de/hb1401110

AUSBLICK

CA-Pinning mag für einzelne App- und Diensteanbieter ein brauchbarer Weg sein, das Risiko für Man-in-the-Middle-Angriffe bei SSL zu senken. Doch es erfordert Tabellen und lässt sich nicht einfach auf alle Web-Clients übertragen. Google schlägt daher eine HTTP-Erweiterung vor: Mit der „Public Key Pinning Extension for HTTP" sollen Webdiensteanbieter einen anfragenden Client (User Agent) anweisen, sich die kryptografische Identität ihres Servers für einen bestimmten Zeitraum zu merken. Innerhalb dieser Zeit darf der Server nur Zertifikate an den Client ausliefern, die von CAs unterzeichnet wurden, die der Webseitenbetreiber vorher festgelegt hat (siehe c't-Link).

Keine der Techniken löst das Problem von Man-in-the-Middle-Angriffen bei SSL vollständig. Denn eigentlich müsste dafür ein komplett anderes SSL-System her. (rek) c't