Sichere Post

E-Mail-Verschlüsselung
Eine digitale Unterschrift und die Verschlüsselung machen E-Mails sicher. Zumindest am Computer schaffen das auch interessierte Laien.

PGP heißt die Sicherheitssoftware, der Edward Snowden vertraut. Die Abkürzung steht für Pretty Good Privacy, übersetzt etwa „ziemlich gute Privatsphäre". Wie Edward Snowden kann auch jeder andere Nutzer diese Sicherheitssoftware aus dem Internet herunterladen.

Snowden war Systemadministrator im amerikanischen Geheimdienst NSA. Er weiß, wie die Software einzurichten ist, und er hat Freunde, die sie ebenfalls anwenden. Normalnutzern dürfte der Start schwerer fallen als Snowden. Und die Adressaten der verschlüsselten Mails können sie nur öffnen, wenn sie die PGP-Software ebenfalls installiert haben. Wie das funktioniert, haben wir geprüft. Uns interessierte, ob die vor mehr als 20 Jahren für Personalcomputer entwickelten Verfahren auch auf Smart-

Unsicher. **E-Mails sind offen für Dritte und Absender können gefälscht sein.**

FOTOS: THINKSTOCK

phones und Tablets laufen. Zur Wahl stehen PGP und das in Mailprogramme wie Outlook und Thunderbird integrierte Verfahren S/MIME (sprich S-Meim). Die Abkürzung steht für Secure Multipurpose Internet Mail Extensions, etwa „sichere universelle Erweiterungen für E-Mail".

Erster Schritt einer sicheren Kommunikation ist die Authentizität: Wer hat die Mail geschrieben? Bei PGP kennen Nutzer einander. Sie erklären sich gegenseitig mit ihrer digitalen Unterschrift das Vertrauen. Bei S/MIME stehen Dienstleister mit einem Zertifikat für die Identität des Absenders ein. Der zweite Schritt, die Verschlüsselung der Botschaft, funktioniert wie bei PGP.

Fälschungen erkennen

Nicht nur Snowden muss sich absichern. Gefährdet sind alle. Kurz vor Weihnachten zum Beispiel wollten Kriminelle wieder einmal durch gefälschte Mails an Zugangsdaten von Kunden des Bezahldienstes Paypal kommen. Fachleute nennen das Phishing – ein Angriff so lukrativ wie ein Bankraub, nur einfacher. Auf Nummer sicher gehen Sie nur mit PGP oder S/MIME. Die zeigen per Mausklick, ob der Absender authentisch, ob ihm zu trauen ist. Prüfen Sie: Ein Buchstabe trennt Freund von Feind, zum Beispiel bei payapal.de und paypal.de.
Tipp: Geben Sie nie Zugangsdaten preis. Ignorieren Sie Mails, die Angst etwa vor Sicherheitslücken und Mahnverfahren verbreiten oder mit Gewinnen locken.

Sichere Wege

Ganz ohne PGP oder S/MIME wähnen sich bestimmt viele Nutzer deutscher Maildienste sicher. Anweisungen wie die der Telekom „Stellen Sie jetzt Ihr E-Mail-Programm auf Verschlüsselung um! Ab 31.03.2014 nur noch verschlüsselter E-Mail-Empfang und -Versand möglich!" sugge- ▶

Unser Rat

Wer in eingehenden E-Mails jeden Dateianhang ohne Nachdenken öffnet und auf Weblinks klickt, lädt schnell Schadprogramme herunter. Vorsicht und die technischen Verfahren **S/MIME** und **PGP** machen Mails sicherer. Laien können die beiden Programme problemlos nutzen. Auch das Einrichten am Computer dürfte gelingen, bei Smartphone und Tablet sollten Experten helfen.

Sicherheit mit S/MIME

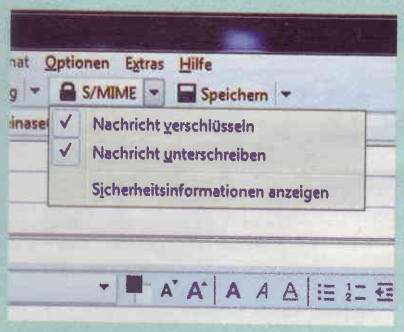
Mit Zertifikat

In Mailprogrammen wie Microsoft Outlook und Mozilla Thunderbird ist S/MIME integriert. Die Abkürzung steht für Secure Multipurpose Internet Mail Extensions und bedeutet etwa „sichere universelle Erweiterungen für E-Mail". Um es zum Laufen zu bringen, beantragt der Nutzer bei einem Dienstleister ein Zertifikat. Dem müssen alle vertrauen.

Die Identitätsprüfung. Sie erfolgt über die Zertifikatstelle. Im einfachsten Fall (Class-1-Zertifikat) bestätigt sie nicht die Identität, sondern nur die E-Mail-Adresse – niemand muss dafür persönlich einen Ausweis vorlegen. Das Zertifikat gibt es auf eine einfache Anfrage per Mail.

Die Verschlüsselung. Der eigene Internetbrowser erzeugt mit dem erworbenen Zertifikat zwei Schlüssel: einen öffentlichen und einen privaten. Wer seine Mails digital unterschreibt (signiert), verteilt damit automatisch den öffentlichen Schlüssel. Die Empfänger verschlüsseln damit ihre Antwortmails an den Zertifikatinhaber. Der öffnet die Mails mit seinem Privatschlüssel.

Die Schwachpunkte. Kostengünstige Zertifikate für Privatkunden fehlen in Deutschland noch. Die Anbieter wenden sich vorrangig an gewerbliche Nutzer. Speziell US-, aber auch andere außereuropäische Dienstleister handeln nicht gemäß unserem Datenschutzverständnis.



Vorhanden. Die Funktion steckt in jedem besseren Mailprogramm.

Sicherheit mit PGP

Mit Vertrauen

Die Sicherheitssoftware (wir nutzten das kostenlose „Open PGP") erweitert den Funktionsumfang des E-Mail-Programms um die gleichen Funktionen wie S/MIME: Es beglaubigt mit einer digitalen Unterschrift die Identität des Absenders und verschlüsselt die Botschaft. PGP steht für Pretty Good Privacy, sinngemäß : „ziemlich gute Privatsphäre".

Die Identitätsprüfung. PGP-Nutzer bestätigen sich ihre Identität gegenseitig. Sie bilden ein Vertrauensnetzwerk, das „Web of Trust". Sie kommen ohne Dienstleister aus.

Die Verschlüsselung. Die PGP-Software erzeugt zwei Schlüssel: einen privaten und einen öffentlichen. Der öffentliche Schlüssel hängt fortan an jeder versandten E-Mail oder wird auf Schlüsselservern (Key-Server) hinterlegt. Die Kontaktpartner können damit ihre Mails an den Schlüsselinhaber chiffrieren. Mit seinem Privatschlüssel kann er die Mails im Klartext lesen.

Die Schwachpunkte. Absender und Empfänger müssen beide PGP nutzen, um es entschlüsseln zu können. Für die Installation setzt das Programm viel Fachwissen oder Lernbereitschaft voraus. Einmal eingerichtet, kommen auch Laien damit zurecht. Wir hatten allerdings erhebliche Probleme mit dem Entschlüsseln von Mail-Anhängen (Dokumente, Bilder) beim Empfänger.

Nachzurüsten. Zusatzsoftware wie PGP ertüchtigt Mailprogramme.

rieren optimalen Schutz. Falsch. Der Tipp hilft zwar in einem offenen Netzwerk wie der Sony-Plaza in Berlin vor Mitlesern in der Nachbarschaft. Verschlüsselt sind die Mails aber nur auf dem Weg vom Absender zum Maildienst. Diese Transport-Sicherung verbirgt sich hinter der Funktion TLS/SSL. Die gängigen Mailprogramme beherrschen sie. Nutzer müssen die Funktion nur per Mausklick aktivieren. Die Anleitung lieferten die Mailbetreiber gleich mit ihren Hinweismails aus. Das einzuführen war längst überfällig. Aber lieber spät als nie.

Unsichere Zwischenstationen

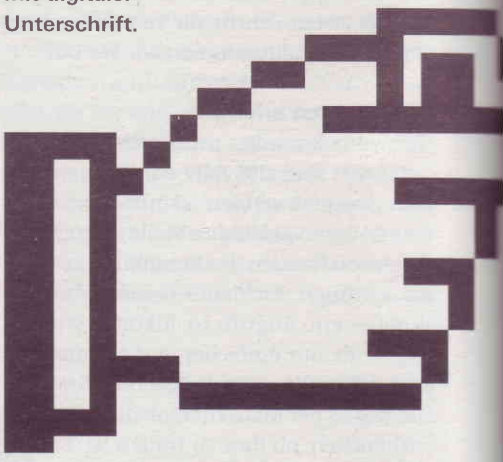
Unbehagen bleibt. Auf dem Weg vom Sender zum Empfänger passiert die Mail Zwischenstationen, Server genannt. Dort können Dritte angreifen. Und natürlich scannt der E-Maildienst die Nachrichten im Kundeninteresse gegen Viren. Google gibt sogar zu, aus den mitgelesenen Inhalten der Mails persönlich zugeschnittene Werbung für seine Gmail-Kunden zu schalten.

Lückenlos absichern

Wer das nicht will, verschlüsselt den Inhalt der Nachricht lückenlos – so, dass sie auch auf den Servern inkognito bleibt. Gleichzeitig kann der Nutzer die Herkunft der Mail mit einem Zertifikat garantieren, einer beglaubigten digitalen Unterschrift. Die kann jeder Mail-Empfänger öffnen und mit dem vom Mailprogramm gezeigten Absendernamen vergleichen. Angriffe wie der auf Paypal-Kunden scheitern daran.

Das größte Hindernis für Interessenten besteht in der Einsamkeit. Kaum einer verschlüsselt seine Mails. Dabei ist das Prinzip einfach. Verschlüsseln kombiniert zwei große Zufallszahlen. Im Fachjargon heißen sie privater und öffentlicher Schlüssel (Key), Insider nennen das Verfahren asynchrone Verschlüsselung. Es gilt als sicher, obwohl es bereits in den frühen 90er Jahren des vorigen Jahrhunderts erdacht wurde. Ausgedruckt füllt so ein Schlüssel eine Druckseite oder mehr mit einer sinnlosen Abfolge von Zahlen und Buchstaben.

Der Nutzer, sagen wir Anna, erzeugt beide Schlüssel entweder mit ihrer PGP-Software oder mit dem S/MIME-Zertifikat. Der private Schlüssel verbleibt auf Annas Rechner. Den öffentlichen Schlüssel schickt sie entweder als Mail-Anhang an alle Kontaktpartner oder hinterlegt ihn im Internet auf einem sogenannten Key-Server. Damit, sowie mit der von Anna genutzten Software verschlüsseln die Kontaktpartner ihre Mails an Anna. Sie entschlüsselt diese mit ihrem privaten Schlüssel. Das Verfahren ist bei PGP und S/MIME gleich. In die Welt der greifbaren Dinge übersetzt: Der öffentliche Schlüssel entspricht leeren Schatullen. Sie werden verteilt und kommen gefüllt mit sicherer Mail zurück. Sicher ist die Mail, weil der öffentliche Schlüssel die Schatullen beim Schließen zusperrt. Nur der private Schlüssel des Empfängers öffnet sie.



Sicher. Verschlüsselt und mit digitaler Unterschrift.

Am Rechner klappt es

Am eigenen Rechner oder Notebook klappt das Verschlüsseln. Mit Ausnahme der Standard-Mail-App von Android-Telefonen beherrscht jedes ordentliche Mailprogramm S/MIME. Die Nutzer müssen keine Extra-Software installieren, brauchen aber ein Zertifikat von Dienstleistern. Das bestätigt die Identität des Absenders und generiert beide Schlüssel. Kostenlose Zertifikate fanden wir nur außerhalb Europas, beispielsweise in Israel oder in den USA. Sie sind auf ein Jahr begrenzt. Dann durchlaufen Nutzer die Startprozedur erneut. Deutsche Anbieter verkaufen ihre Zertifikate. Der Deutsche Sparkassenverlag etwa verlangt 34,49 Euro für ein Zwei-Jahres-Zertifikat.

FOTOS: THINKSTOCK

Wege zur Verschlüsselung

Die Kosten und die Anbieter

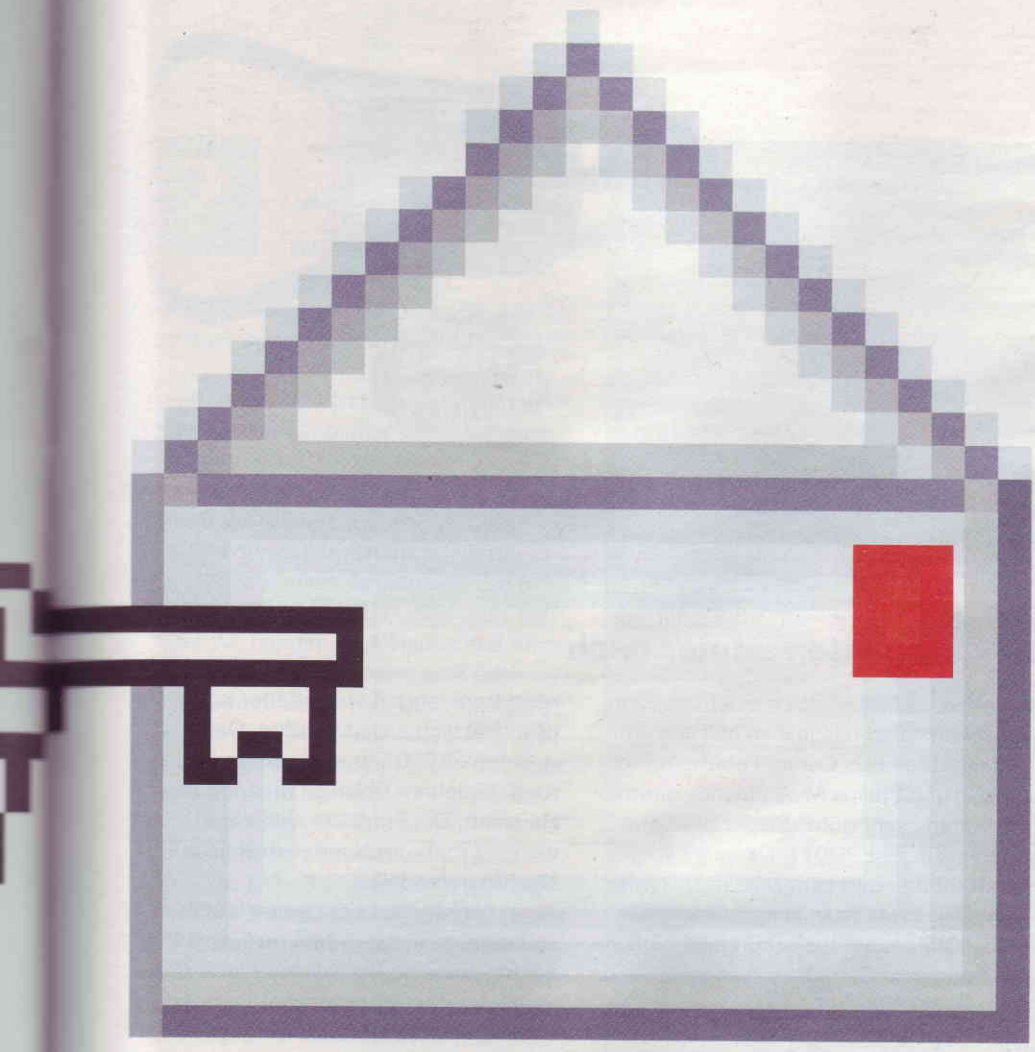
S/MIME. Kostenlose Zertifikate entsprechen dem niedrigsten Sicherheitsstandard (Class-1-Zertifikate) und sind meist auf ein Jahr begrenzt. Firmen wie Comodo aus den USA oder StartSSL aus Israel bieten sie an. Zertifikate mit zwei Jahren Laufzeit und mehr Sicherheit gibt es auch von deutschen Anbietern. Beispielsweise beim Sparkassenverlag ab knapp 35 Euro.

PGP. In der von uns eingesetzten Form (Open PGP) ist es für Computer kostenlos verfügbar. Für Windows wurden wir bei gpg4win.de fündig, für Mac bei gpgtools.org – in englischer Sprache. Für mobile Geräte wie Tablets und Smartphones mit Android- und Apple-Betriebssystem gibt es kostenlose wie auch kostenpflichtige Apps. Wir fanden aber nur englischsprachige.

Zertifikat. Zu haben unter anderem bei www.s-trust.de (kostenpflichtig).

Gpg4win - eine sichere Lösung...

Software. Zu haben unter anderem bei www.gpg4win.org (kostenlos).



Wir wünschen uns deutsche Anbieter, die es für Privatnutzer günstiger machen.

Tipp: Heben Sie abgelaufene Zertifikate auf. Das aktuelle kann frühere Mails nicht entschlüsseln.

Nix für Smartphone und Internetcafé

Zu unserem Erschrecken fanden wir keine empfehlenswerte Lösung für Smartphones. Sicherheitstechnisch sind PGP und S/MIME auf dem Stand der Technik, in der Handhabung stecken sie aber noch in der digitalen Steinzeit. Die Krux: Wie kommt der private Schlüssel vom Rechner auf das Smartphone? Vom Versand per Mail raten wir ab, denn der Schlüssel muss im Klartext gesendet werden. Mitleser freuen sich. Sicherer, aber umständlicher klappt der Import zum Beispiel über iTunes, eine Speicherkarte oder das heimische W-Lan.

Komfortabel ist das nicht. Das gilt auch für den Alltag. Wir mussten Mails zwischen zwei Apps hin- und herkopieren, scheiterten häufig beim Entschlüsseln von Anhängen und erlebten App-Abstürze. Auch die Web-Mailer, also der Zugriff beispielsweise auf GMX vom Internetbrowser aus, enttäuschten. Der Zugriff über den Internetbrowser ist auf Reisen wichtig, im Internetcafé. Die Rechner dort kennen nicht den eigenen privaten Schlüssel. Den oft gehörten Tipp, ihn zusammen mit einem Mailprogramm wie Thunderbird Portable auf einem USB-Stick mitzunehmen, geben wir nicht. Da könnten Sie auch gleich einem Dieb den Wohnungsschlüssel aushändigen: Fremde Rechner könnten ihn auslesen. Dieser USB-Stick hat immerhin Zugriff auf das Postfach, er enthält die digitale Unterschrift und den privaten Schlüssel.

PGP auf Partys lernen

Laien richten die Verschlüsselung eher auf ihrem Computer oder einem Notebook ein. Dafür wurden diese Verfahren entwickelt. Wissenshungrige finden unter www.gpg4win.org ein Kompendium. Es lässt keine Frage offen. Das Studium lohnt. Für sichere Mails mit mobilen Endgeräten brauchen aber fast alle Hilfe von Experten.

Kein Wunder, dass Nachtschwärmer nicht mehr nur Techno-, sondern auch Crypto-Partys besuchen. Da helfen Überzeugungstäter im guten Sinne des Wortes. Sie richten die Geräte ihrer Gäste fix und fertig ein. Ein Vorbild haben sie: Edward Snowden soll den Enthüllungsjournalisten auch erst PGP beigebracht haben. ■

De-Mail

Mit Behörden

So einfach wie E-Mail, so sicher wie Papierpost – mit diesem Slogan wirbt die Bundesregierung für den gesetzlich geregelten E-Mail-Kontakt der Bürger mit Behörden.

Die Kosten. De-Mail gibt es bei Maildiensten wie GMX und Web.de oder zum Beispiel bei der Deutschen Telekom. Bei GMX sind zehn Mails monatlich frei, jede weitere kostet 39 Cent. Leistungen wie Einschreiben, also Versand- und Empfangsbestätigung, kosten generell extra (GMX: 78 Cent pro Mail).

Die Identitätsprüfung. Sie erfolgt persönlich, mit Vorlage eines Personaldokuments wie Reisepass oder Personalausweis. Anbieter wie GMX kommen auf Wunsch zum Antragsteller nachhause oder zur Arbeit.

Die Verschlüsselung. Privatpersonen können praktisch nicht verschlüsseln, weil De-Mail nur direkt über die Web-Mailer läuft. Problem: Der Maildienst kennt nicht den privaten Schlüssel des Anwenders.

Die Schwachpunkte. De-Mail kann nur an Inhaber einer De-Mail-Adresse verschickt werden. Sie gilt als rechtssicher, aber technisch als unsicher: Die Maildienste entschlüsseln Nachrichten und untersuchen sie auf Schadsoftware. Dritte könnten hierbei mitlesen.

Insellösung. De-Mail klappt nur national und ist nicht sehr sicher.