ILLUSTRATION DANIEL BRÜHLMANN

Vertrauliche Daten und E-Mails müssen Sie verschlüsseln. Mit PGP 8.0 ist ein Gratis-Programm erhältlich, das Ihre Daten nach den aktuellen Sicherheitsstandards schützt.

von Beat Rüdt

Sobald eine Internetverbindung aufgebaut ist, drohen Ihrem Computer Angriffe aus aller Welt. Hat sich ein Hacker Zugang zu Ihrer Arbeitsstation verschafft, kann er alle Daten sehen. Und wenn Sie eine E-Mail schreiben, liest fast jeder mit: der Systemadministrator, der Provider, staatliche Stellen, Hacker. So lange Sie keine sensiblen Daten speichern oder verschicken, müssen Sie sich wenig Sorgen machen. Was ist aber mit Daten, die – aus welchen Gründen auch immer – niemand zu Gesicht bekommen sollte? Wie verhindern Sie, dass ein Angreifer Ihre Daten auswertet oder die Konkurrenz Ihre geheime Post im Internet abfängt?

Es ist grundsätzlich unvermeidbar, dass Sie Spuren im Internet hinterlassen: Die Provider sind sogar gesetzlich verpflichtet, sämtliche Verkehrsdaten (nicht aber den Inhalt von Mails) zu sichern. Darüber haben Sie nicht die geringste Kontrolle.

Mit dem Verschlüsselungsprogramm PGP haben Sie immerhin die Gewähr, dass niemand unbefugt den Inhalt Ihrer Mails anschauen kann. Im Folgenden stellen wir Ihnen PGP vor, das meist verbreitete Programm für sichere E-Mails und zum Verschlüsseln geheimer Daten. Anhand der Ende November erschienenen Version 8.0 erfahren Sie, wie PGP funktioniert.

Was ist PGP? PGP ist die Abkürzung für Pretty Good Privacy, was etwa mit «ziemlich gute Privatsphäre» übersetzt werden kann. Es wurde vom Amerikaner Phil Zimmermann entwickelt und hat von Anfang an für Wirbel gesorgt. Mehr dazu lesen Sie in der Box «Die Geschichte von PGP», Seite 41.

PGP kann Dateien verschlüsseln, verschlüsselte E-Mails versenden, Daten komplett und unwiderruflich löschen und den Absender einer E-Mail zweifelsfrei feststellen.

So funktioniert PGP: Mit PGP lassen sich Daten verschlüsseln und natürlich auch wieder entschlüsseln. Für diese beiden Vorgänge werden zwei verschiedene Schlüssel verwendet. Man spricht daher von einer asynchronen Verschlüsselung. Mehr über die asynchrone Verschlüsselung lesen Sie im PCtip 1/2003, Seite 94, im Artikel «Was ist eigentlich ein 128-Bit-Schlüssel?» oder im Internet unter **http://www.pctip.ch/archiv/2003/1.asp** .

Grundsätzlich gilt: Die Daten werden immer mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und mit dessen privatem Schlüssel entschlüsselt.

Wenn Sie also jemandem eine verschlüsselte Botschaft zukommen lassen, müssen Sie zuerst dessen öffentlichen Schlüssel besitzen. Der kann per E-Mail mitgeteilt werden oder auf einer Website zur Verfügung stehen. Die neuen Versionen von PGP bieten Server an, die öffentliche Schlüssel verwalten. Wie das genau geht, zeigen wir im nächsten Abschnitt «So installieren Sie PGP».

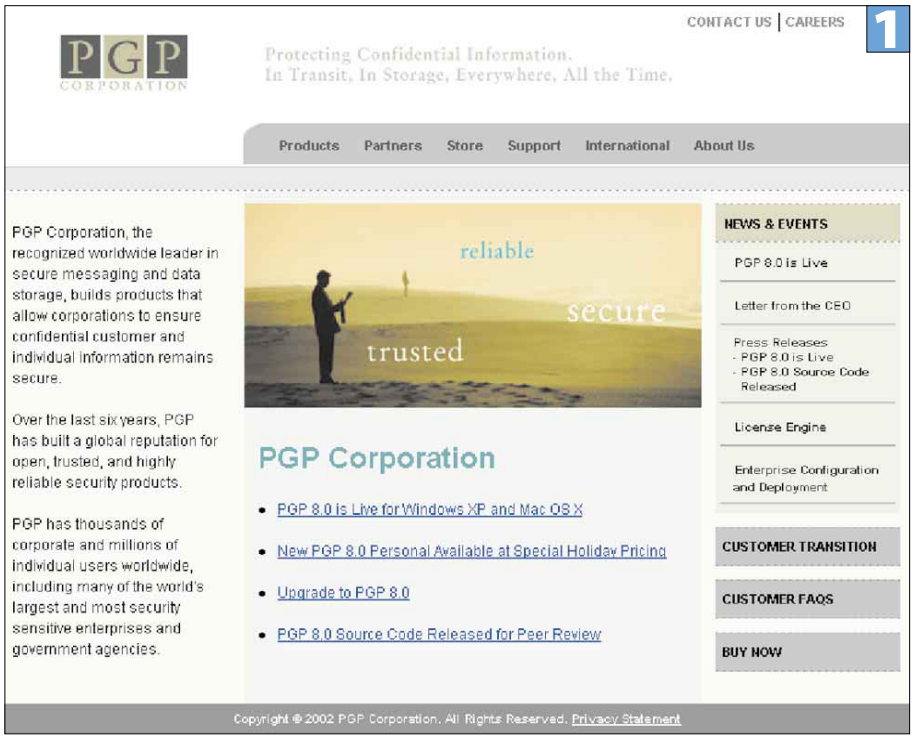
Entschlüsseln kann diese Nachricht nur der Empfänger mit seinem eigenen, privaten und somit geheimen Schlüssel. Dieser private Schlüssel darf unter keinen Umständen an Dritte weitergegeben werden!

All diese Schlüssel werden von PGP an einen virtuellen Schlüsselanhänger (Keyring) gehängt, der die Verwaltung sowie den Im- und Export der Schlüssel vereinfacht.

Das Verwenden des privaten und der öffentlichem Schlüssel auf Ihrem PC ist durch ein Passwort geschützt, das vor dem Ver- und Entschlüsseln eingegeben werden muss.

PGP kann nicht nur Nachrichten, sondern auch einzelne Dateien verschlüsseln. Die kostenpflichtige Version verschlüsselt sogar ganze Verzeichnisse und Laufwerke. Die Informationen in diesem Artikel beziehen sich aber nur auf den Funktionsumfang der Gratisversion.

Beim Einrichten von PGP erstellt das Programm nicht nur das Schlüsselpaar (privater und öffentlicher Schlüssel), sondern auch eine digitale Signatur, die an Dokumente und E-Mails angehängt wird. Dank dieser fälschungssicheren Signatur stellt der Empfänger zweifelsfrei fest, von wem die Datei stammt. Im Normalfall werden die Daten in einem Arbeitsgang verschlüsselt und mit der Signatur versehen.



Ein Klick auf PRODUCTS und anschliessend auf PGP FREEWARE bringt Sie zur Download-Seite.

So installieren Sie PGP: Nachfolgend erfahren Sie Schritt für Schritt, wie Sie PGP richtig installieren und anwenden. Diese Anleitung gilt für alle Windows-Versionen.

Auf der Website **http://www.pgp.com/** finden Sie immer die aktuellste Version, zurzeit 8.0, die Ende November erschienen ist. Klicken Sie oben im Menü auf PRODUCTS, **Screen 1**, und anschliessend links im Menü auf PGP FREEWARE. Unten auf der Seite bestätigen Sie, dass Sie die Lizenzvereinbarungen gelesen haben und akzeptieren, indem Sie das Kontrollkästchen aktivieren (neben «Please check this box to confirm you have read and understand the License Agreement terms and condition and the export rules regarding this source code.»). Dann klicken Sie auf den Schalter DOWNLOAD NOW neben Ihrem Betriebssystem (z. B. «PGP 8.0 for Windows»).

Automatisch öffnet sich das Fenster «Dateidownload». Klicken Sie auf SPEICHERN und wählen Sie im neuen Fenster «Speichern unter» einen Ordner, zum Beispiel «Eigene Dateien».

Die Datei ist fast 8,5 MB gross. Es kann je nach Verbindung also einige Minuten dauern, bis Sie weitermachen können.

Die Datei, die Sie herunterladen, ist komprimiert und hat die Endung «.zip». Um sie zu öffnen, benötigen Sie zum Beispiel das Gratis-Tool UltimateZip, das Sie auf der PCtip-Webseite unter **http://www.pctip.ch/downloads/dl/19861.asp** finden. Installieren Sie dieses oder ein anderes Programm, das fähig ist, ZIP-Dateien zu öffnen, bevor Sie mit der Installation von PGP fortfahren.

Ein Doppelklick auf die von der PGP-Homepage heruntergeladene Datei öffnet das Archiv und Sie sehen die Installationsdatei (PGP8.exe). Ein Doppelklick darauf startet die Installation von PGP 8.0.

Es folgt ein Standard-Installationsdialog, in dem Sie den Lizenzvertrag akzeptieren müssen. Sie werden auch gefragt, ob Sie bereits «Keyrings», also Schlüssel für PGP besitzen. Falls Sie PGP zum ersten Mal installieren, aktivieren Sie den Button «No, I'm a new user». In den folgenden Fenstern bestimmen Sie, wo das Programm installiert wird und mit welchen Programmen es arbeiten soll. Wir empfehlen, die Standardeinstellungen zu belassen. Danach installiert das Programm seine Dateien. Das Installationsprogramm fordert Sie nun auf, das System neu zu starten. Bestätigen Sie mit FINISH.

Nach dem Neustart fragt das Installationsprogramm, das immer noch aktiv ist, nach Ihrem Namen und der Seriennummer. Da Sie für die Gratis-Version keine Seriennummer benötigen, klicken Sie auf LATER.

Jetzt startet der «Key Generation Wizard», ein Programm, das den öffentlichen und den privaten Schlüssel generiert. Nach einem Klick auf WEITER geben Sie Ihren Namen und Ihre E-Mail-Adresse an. Nach einem erneuten Klick auf WEITER generieren Sie Ihr Passwort. (Sie geben es zwei Mal ein.) Beachten Sie dazu die Box «Sichere Passwörter», Seite 44. Ein Klick auf WEITER bestätigt das neue Passwort. Nun drücken Sie FERTIG STELLEN. ▶

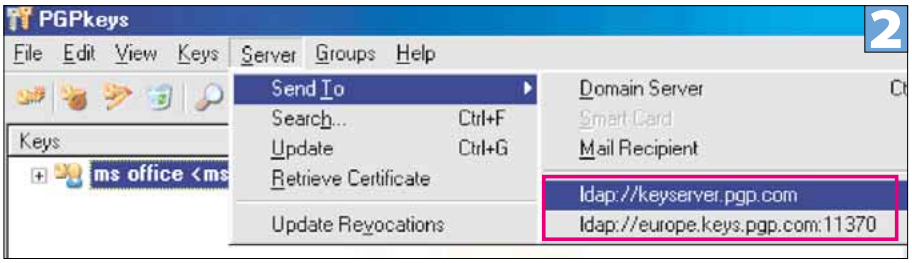
Hintergrund

Die Geschichte von PGP

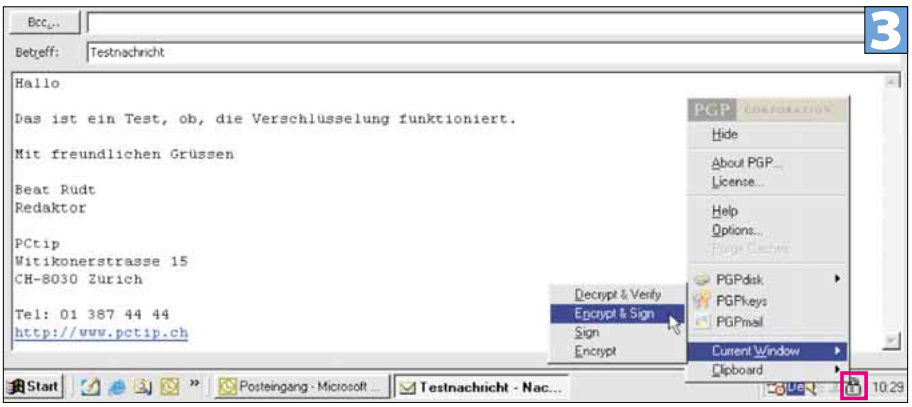
1976 und 1977 entstanden die ersten Verschlüsselungssysteme mit öffentlichen Schlüsseln. Vom ersten Moment an war dieses System der amerikanischen National Security Agency (NSA) ein Dorn im Auge. Sie versuchte, die Veröffentlichung zu verhindern. Aber noch 1977 publizierten die Erfinder einen Artikel über die neue Verschlüsselungsmöglichkeit.

Die asymmetrischen Verschlüsselungssysteme wurden in der Folge weiter erforscht. Eine brauchbare Version mit öffentlichen Schlüsseln entwickelten z. B. in den USA ausgebildete Studenten für den Irak während des Krieges gegen den Iran.

1991 kam das erste PGP 1.0 als Gratisversion auf den Markt. Drei Jahre später folgte eine ausgebaute, kostenpflichtige Version.
1997 erschien mit PGP 5.5 eine standardisierte Fassung. Ein Standard definierte die PGP-Protokolle, damit sie untereinander kompatibel wurden.
1998 kam mit der Version 6.0 noch PGP-Disk dazu, das ganze Laufwerke verschlüsseln kann. Ab 7.1 (2001) wurden die einzelnen Teile (Mail, Disk etc.) in verschiedene Programme aufgeteilt. Danach stockte die Weiterentwicklung fast eineinhalb Jahre. Es fehlten Versionen für Windows XP und Mac OS X. Erst Ende November 2002 kam endlich das neuste PGP 8.0 auf den Markt.



Machen Sie den öffentlichen Schlüssel auf einem der beiden Keyserver publik.



Der Befehl zum Verschlüsseln und Signieren versteckt sich hinter dem Schlosssymbol.

Jetzt ist PGP schon fast einsatzbereit. Sie finden das Programm im Startmenü unter PROGRAMME/PGP. Zum Senden und Empfangen verschlüsselter Mails sind noch zwei Schritte nötig, die Sie mit dem Teilprogramm PGPKEYS ausführen:

- Andere PGP-Nutzer müssen Ihren öffentlichen Schlüssel kennen, bevor sie Ihnen eine Nachricht schicken können. Wählen Sie SERVER/SEND und einen der vorgeschlagenen Keyserver. Keine Angst, es gibt nur zwei: einen für Europa und einen für den Rest der Welt, **Screen 2**. Danach wird der Schlüssel automatisch übermittelt.

Wie Sie den Schlüssel nicht aller Welt publik machen, sondern nur an einige ausgewählte Personen schicken, erfahren Sie im Abschnitt «Schlüssel weitergeben», Seite 44.

- Umgekehrt benötigen Sie die öffentlichen Schlüssel der Personen, denen Sie verschlüsselte Mailbotschaften zukommen lassen. Klicken Sie auf SERVER/SEARCH... Im Fenster «PGPkeys Search Window» geben Sie nun den Namen der gesuchten Person ein. Wenn Sie nach dem Klick auf SEARCH kein Resultat erhalten, stellen Sie unter «Search for keys on» den anderen Server ein. Haben Sie den Schlüssel der gesuchten Person gefunden, hängen Sie ihn an Ihren Schlüsselbund:

Rechtsklick auf die gewünschte Adresse und dann im Menü mit der linken Maustaste auf IMPORT TO LOCAL KEYRING klicken.

E-Mails mit PGP: Mit PGP wollen Sie wahrscheinlich vor allem Ihre E-Mails verschlüsseln. Für das folgende Beispiel verwenden wir Microsoft Outlook 2002, die gezeigten Schritte funktionieren aber mit jedem beliebigen E-Mail-Programm.

Schreiben Sie eine ganz normale E-Mail mit einem Betreff und einem kurzen Text. Nun wählen Sie mit der rechten Maustaste das Schlosssymbol in der Systemleiste am rechten unteren Bildschirmrand aus und klicken danach mit der linken Maustaste unter CURRENT WINDOW auf ENCRYPT & SIGN, **Screen 3**.

Nun öffnet sich das Fenster «PGPtray – Key Selection Dialog». Oben sehen Sie die öffentlichen Schlüssel, die Sie sich bereits beschafft haben. Wählen Sie daraus mit einem Doppelklick den Empfänger der Nachricht, **Screen 4**. Dann klicken Sie auf OK und die Nachricht wird – nach Eingabe Ihres Passwortes – verschlüsselt, **Screen 5**.

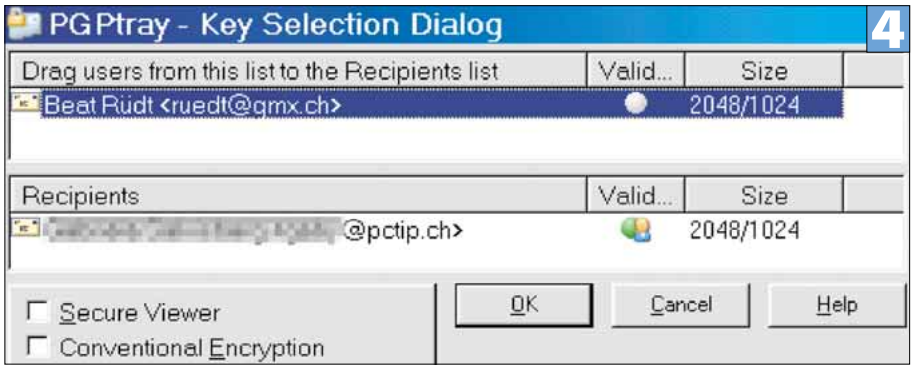
Jetzt sehen Sie nur noch einen sinnlosen Buchstabensalat. Ohne grössten Aufwand ist diese Nachricht für Schnüffler nicht mehr einsehbar.

Für das Entschlüsseln einer erhaltenen Nachricht laufen die Schritte praktisch genau gleich ab: Die Nachricht kommt codiert in Ihrer Mailbox an und ist unlesbar. Sie klicken auf das Schlosssymbol und wählen unter CURRENT WINDOW/DECRYPT & VERIFY. Dann geben Sie das Passwort ein und die entschlüsselte Nachricht wird in einem neuen Fenster («Text Viewer») angezeigt, **Screen 6**.

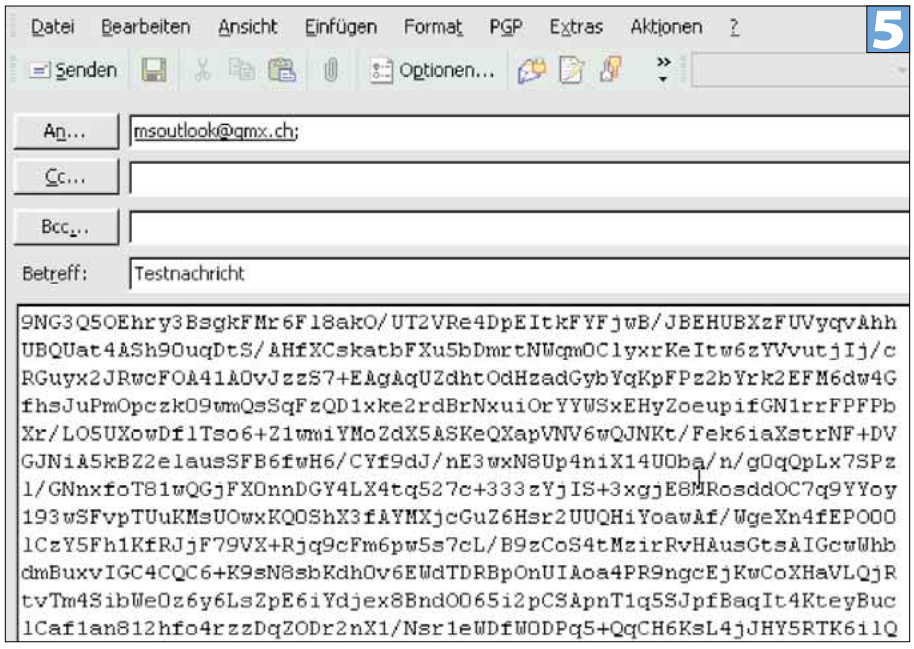
Verschlüsseln von Dateien: Auf die genau gleiche Art werden auch Textdateien (zum Beispiel in Word) mit PGP verschlüsselt und entschlüsselt. Dazu klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen im Menü PGP/ENCRYPT oder PGP/ENCRYPT & SIGN, falls Sie die Datei auch signieren möchten, wie das bei E-Mails auch möglich ist. Wie eine solche Signatur aussieht, sehen Sie im **Screen 6**, oben.

Sie können nun bestimmen, welche Benutzer die Datei entschlüsseln dürfen. Im Normalfall wählen Sie nur sich selbst als User; so dürfen Sie als Einziger die Datei wieder lesen. Vielleicht möchten Sie aber ein Word-Dokument mit geheimen Informationen für jemand anderen verschlüsseln. Dann wählen Sie aus dem Schlüsselbund den oder die Empfänger aus. Die verschlüsselte Datei kann so von allen gelesen werden, die Sie ausgewählt haben.

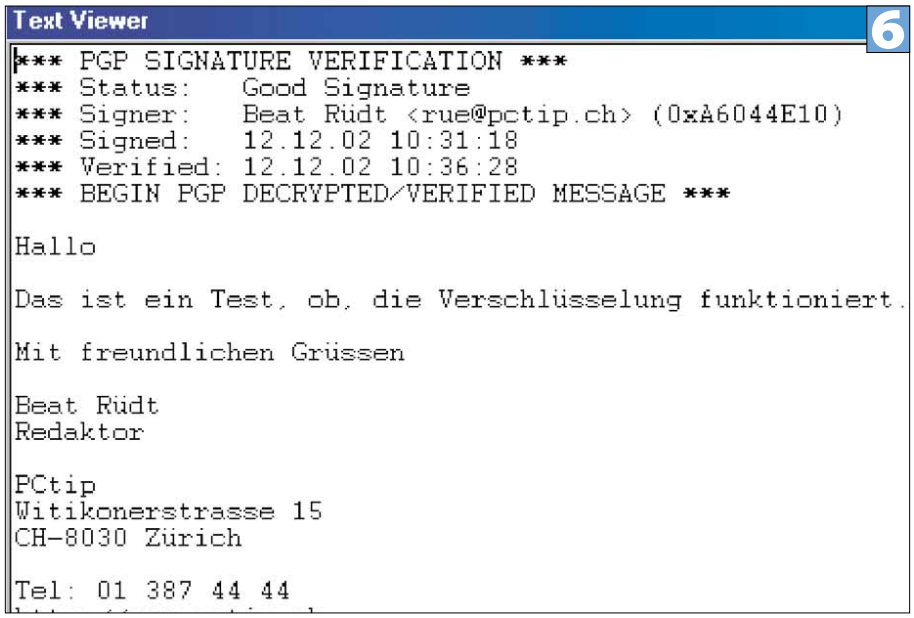
Achtung: Nach dem Verschlüsseln einer Datei bleibt das Original erhalten. Auf Ihrem Rechner befinden sich sowohl die verschlüsselte wie auch die unverschlüsselte Version. Der Dateiname der verschlüsselten Datei lautet genau gleich wie jener der unverschlüsselten, mit dem Unterschied, dass die verschlüsselte um die Endung «.pgp» erweitert wurde. ▶



In der oberen Hälfte des Fensters sind die öffentlichen Schlüssel, die Sie sich beschafft haben.



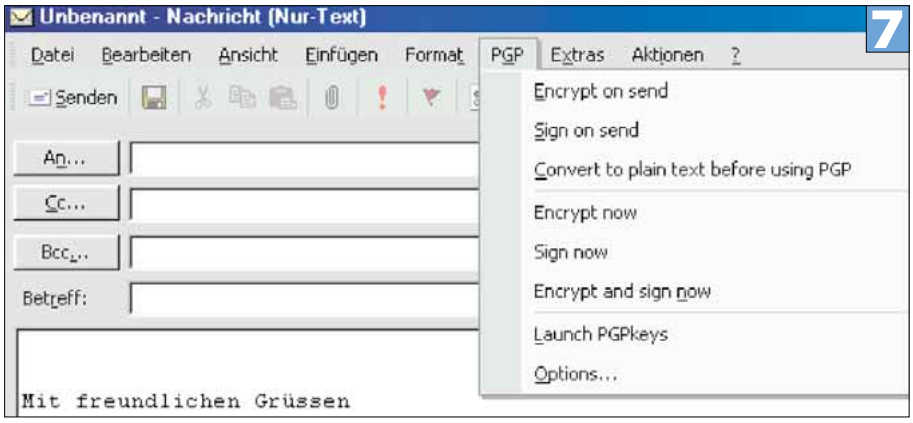
Die verschlüsselte Nachricht



Die entschlüsselte Nachricht wird im Text Viewer angezeigt, oben die Signatur.

Vollständiges Löschen von Dateien: Das Löschen einer Datei hat einen Haken: Wird sie einfach in den Papierkorb verschoben, kann sie jederzeit wiederhergestellt werden. Nicht einmal nach dem Leeren des Papierkorbs ist die Datei vollständig verschwunden. Experten würden sie problemlos wieder auf Ihrer Harddisk finden und in ihren Originalzustand zurückversetzen. Das können Sie mit PGP verhindern.

Klicken Sie mit der rechten Maustaste auf die Datei. Sie finden unter PGP die Option WIPE. Ein Fenster fragt Sie «Are you sure you want to secure delete this file?» («Sind Sie sicher, dass Sie diese Datei sicher entfernen wollen?»). Mit einem Klick auf YES bestätigen Sie die Aktion und löschen die Datei für immer.



PGP-Plug-Ins in Outlook funktionieren nur in der bezahlten Version.

Schlüssel weitergeben: Bei der Beschreibung der Installation wurde erläutert, wie Sie Ihren öffentlichen Schlüssel auf einem Server veröffentlichen. Vielleicht möchten Sie aber nicht, dass Ihnen jedermann verschlüsselte Nachrichten senden kann. In diesem Fall geben Sie Ihren öffentlichen Schlüssel nur an ausgewählte Personen weiter.

Öffnen Sie mit einem Rechtsklick auf das Schlosssymbol das Programm PGPKEYS. Wählen Sie im Menü KEYS/EXPORT, um einen öffentlichen Schlüssel zu exportieren. Sie können ihn zum Beispiel auf einer Diskette speichern und per eingeschriebener Post an den Empfänger senden. Importiert wird der so erhaltene Schlüssel im selben Programm unter KEYS/IMPORT.

Es kann auch sein, dass Sie Ihren höchst geheimen privaten Schlüssel exportieren möchten, um ihn z. B. sowohl auf Ihrem Desktop-Computer wie auch auf Ihrem Laptop zu verwenden. Das geht nicht so einfach mit einem Rechtsklick wie beim öffentlichen Schlüssel. Hier ist etwas Handarbeit angesagt: Die Schlüssel sind – wenn Sie bei der Installation keine anderen Einstellungen vorgenommen haben – im Verzeichnis «Eigene Dateien/pgp/» abgelegt. Der Schlüsselbund mit den öffentlichen Schlüsseln anderer Teilnehmer heisst pubring.pkr, der Schlüsselbund mit Ihrem privaten Schlüssel secring.skr. Diese Dateien lassen sich direkt auf eine Diskette kopieren.

Ist auf dem anderen Computer PGP installiert, öffnen Sie die Datei auf der Diskette mit einem Doppelklick. Sorgen Sie dafür, dass das Programm PGPkeys bereits geöffnet ist. Als Resultat sehen Sie beide «Schlüsselanhänger» geöffnet. Mit der Maus ziehen Sie die Schlüssel bequem von der Diskette auf die Festplatte.

Kostenpflichtige Versionen: Wie bereits angetönt, ist der Funktionsumfang der kostenpflichtigen Version von PGP grösser, wir haben die Verschlüsselung ganzer Laufwerke erwähnt. Auch die Funktionsweise ist besser. Das sehen Sie zum Beispiel im E-Mail-Programm Outlook: PGP installiert schon in der Gratis-Version die kleinen Hilfsprogramme (Plug-Ins), **Screen 7**. Das ist aber nur ein Werbegag: Jedes Mal, wenn Sie über einen dieser Menüpunkte eine Aktion vornehmen wollen, werden Sie darauf hingewiesen, dass das nur mit der gekauften Version funktioniert.

Der Hersteller unterscheidet grundsätzlich Anwendungen für Private und für Unternehmen. Für Private gibt es neben der vorgestellten Gratisversion auch die kostenpflichtige Version, bei der die Plug-Ins funktionieren und mit PGPdisk ganze Verzeichnisse und Laufwerke verschlüsselt werden.

Die Enterpriseversion, also jene für Geschäftskunden, ermöglicht ausserdem das Anlegen eines eigenen Keyservers, dem Server für die öffentlichen Schlüssel, der sich dann betriebsintern nutzen lässt.

PGP – sicher oder nicht? Seit es PGP gibt, kursieren wilde Gerüchte um das Programm. Nachdem sich die amerikanische National Security Agency (NSA) schon für die frühesten Versionen interessierte, ist immer wieder behauptet worden, es gebe einen Generalschlüssel zum Entschlüsseln aller Nachrichten. Möglich wäre dies, kann doch eine Nachricht an mehrere Empfänger weitergeleitet werden. Der zusätzliche Generalschlüssel könnte leicht mit eingebaut werden.

Die Macher von PGP betonen zwar immer wieder, dass es keine solche Hintertür gibt, beweisen lässt sich aber weder das eine noch das andere.

Auch Tüftler versuchen, Wege zu finden, PGP-Nachrichten abzufangen und zu entschlüsseln. Tatsächlich wurden Möglichkeiten entwickelt, die funktionieren könnten. Aber sie sind derart aufwändig, dass sie nur theoretisch gefährlich sind.

Die neuste Version von PGP ist einfach zu bedienen und entspricht dem heutigen Standard für die Sicherheit elektronischer Daten. Wer 100-prozentige Sicherheit will, muss alles in seinem Kopf speichern – und darf nicht im Schlaf sprechen...

Tipp

Sichere Passwörter

Der durchschnittliche Westeuropäer hat ein Passwort zum Entsperren seines Handys, für das Aufstarten seines Computers am Arbeitsplatz, für die Bankkarte und für das E-Mail-Konto. Für Internetangebote von Banken, Kaufhäusern, Auktionen, für personalisierte Services und so weiter kommen weitere Passwörter dazu.
Am sichersten ist für jede Anwendung ein eigenes Passwort. Das führt dazu, dass die Anwender möglichst einfache Passwörter wählen, die sind leicht zu merken: das Geburtsdatum, eine Kombination von Vor- und Nachnamen, das Lieblingsessen und so weiter. Solche Passwörter gelten aber als unsicher.
Wenn jemand ein Passwort knacken will, wird er zuerst die offensichtlichsten Möglichkeiten probieren, also jene, die oben beschrieben sind. Hacker benutzen zudem Tools, die mit so genannten «Brute-Force-Attacken» so lange Passwörter ausprobieren, bis das Richtige gefunden ist. Spezialisierte Programme benutzen dazu Wörterbücher, die für Benutzernamen und Passwort oft verwendete Wörter und Namen kombinieren.
Sichere Passwörter bestehen deshalb aus einer Kombination von Zahlen und Buchstaben (gross und klein) und sind mindestens acht Zeichen lang, zum Beispiel «dKFkbC25Fu70R». Während es noch zumutbar ist, sich ein solches Passwort zu merken, ist es schier unmöglich, zehn oder zwanzig solcher Kombinationen im Kopf zu behalten. Erschwerend kommt dazu, dass ein sensibles Passwort mindestens einmal pro Monat geändert werden sollte.
Das führt zum absurden Umstand, dass Anwender oft eine Passwortliste führen. Nicht selten findet man die Passwortliste einer Firma auf dem Pult des Systemadministrators. Andere sammeln alle Passwörter in einer verschlüsselten Datei. Es reicht, diese eine Datei zu knacken, um alle Passwörter zu kriegen.
Damit das Passwort gut zu merken und trotzdem sicher ist, gibt es eine ziemlich einfach Methode: Merken Sie sich einen simplen Satz, der Ihnen im Zusammenhang mit dem verwendeten Dienst jederzeit einleuchtet. Nehmen wir an, Sie benötigen ein Passwort für Online-Shopping bei Coop, könnte der Satz zum Beispiel «das Kilo Fleisch kostet bei Coop 25 Franken und 70 Rappen» heissen. Das Passwort lautet dementsprechend «dKFkbC25Fu70R».
Mehr zum Thema Passwort-Management erfahren Sie im PCtip 3/2003 nächsten Monat.