Outlook-Tipp: E-Mails mit PGP signieren und verschlüsseln

Versionen: Outlook 98 bis 2003

Sie wollen vertrauliche Informationen sicher per E-Mail verschicken? Dann nutzen Sie doch moderne Verschlüsselungstechnologien, um den Nachrichtenaustausch zu schützen. Zu den etabliertesten Verfahren gehört PGP (Pretty Good Privacy). Sie können die deutschsprachige Version von PGP Freeware von folgender Internetseite herunterladen:

http://www.pgp.com/products/de/freeware.html

Im Gegensatz zur kostenpflichtigen Variante besitzt PGP Freeware kein spezielles Plug-In für Outlook. Das bedeutet, dass Sie jede sicherheitsrelevante E-Mail selbst signieren und/oder verschlüsseln müssen und dass Sie schützenswerte Dateianhänge selbst in ein sicheres Format konvertieren müssen. Ansonsten steht Ihnen aber das gesamte Spektrum der E-Mail-Sicherheit zur Verfügung.

Bevor Sie PGP sinnvoll einsetzen können, müssen Sie das Programm installieren und konfigurieren. Das heisst, Sie müssen ein eigenes Schlüsselpaar aus öffentlichem und privatem Schlüssel anlegen und fremde (öffentliche) Schlüssel in das Schlüsselverwaltungs-Tool (das Programm-Modul «PGPkeys») importieren.

Bei der Installation gibt es nur wenig zu beachten, da sie von einem leicht verständlichen Setup-Assistenten begleitet wird. Nur so viel: Auch die Freeware-Version fragt Sie nach den zu installierenden PGP-Komponenten. Da aber weder die Outlook- und Outlook Express-Plug-Ins noch PGPdisk freigeschaltet sind, sollten Sie die Komponenten gar nicht erst ankreuzen. Sie ersparen sich dadurch lästige Lizenzhinweise beim Starten von Outlook, und falls Sie doch noch die kommerzielle PGP-Version erwerben wollen, können Sie die fehlenden Programmteile später ohne grossen Aufwand nachinstallieren.

Lassen Sie sich während der Installation auch nicht dadurch irritieren, dass irgendwann die Eingabe einer Lizenznummer verlangt wird. Klicken Sie einfach auf die Schaltfläche Später, wenn Sie momentan nur die Freeware-Version nutzen möchten.

Als neuer PGP-Nutzer erhalten Sie beim Setup-Vorgang Gelegenheit, einen eigenen Schlüssel anzulegen. Erzeugt wird dabei ein Paar aus privatem Schlüssel und öffentlichem Schlüssel. Der private Schlüssel dient später zum Signieren ausgehender und zum Entschlüsseln eingehender E-Mail-Nachrichten. Den öffentlichen Schlüssel geben Sie an andere Personen weiter, damit diese die von Ihnen signierten Mails verifizieren und die an Sie gerichteten Mails verschlüsseln können.

Es spricht nichts dagegen, den «PGP-Schlüsselerstellungs-Assistenten» auch ohne «Expertenmodus» einzusetzen. Sie erstellen damit einen Schlüssel nach dem PGP-typischen «Diffie-Hellmann/DSS»-Verfahren mit einer Schlüssellänge von 2048 Bits. Dazu brauchen Sie nur Ihren Namen, Ihre E-Mail-Adresse und anschliessend eine so genannte «Passphrase» – also das persönliche, frei wählbare Kennwort für den Schlüssel - einzugeben. Merken Sie sich die Passphrase gut, da Sie sie später immer wieder benötigen!

Nach erfolgreicher Installation greifen Sie über ein Symbol am rechten Ende der Windows-Taskleiste auf die PGP-Funktionen zu (es hat die Form eines Vorhängeschlosses). Kernstück der Software ist das Programm-Modul PGPkeys, das Sie nach einem Mausklick auf dem

www.ilbasch.ch

Symbol über das aufklappende Menü erreichen. PGPkeys ist das Tool, in dem Sie Ihre eigenen Schlüssel und die anderer Personen verwalten.

Daran erkennen Sie auch das generelle Konzept von PGP: Ob ein Schlüssel echt ist und von dem stammt, der in der Benutzer-ID genannt wird, entscheiden letztendlich Sie selbst. Es gibt keine offiziellen oder gar amtlichen Zertifizierungsstellen, die die Echtheit eines Schlüssels prüfen und garantieren. Sie ganz allein haben die Verantwortung für die Sicherheit des Nachrichtenaustausches. PGP sorgt nur dafür, dass Ihre Daten so gut «verpackt» werden, dass Sie nicht von Hackern gelesen werden können.

Wenn Sie vorher noch nicht mit PGP gearbeitet haben, sehen Sie in der angezeigten Liste zunächst nur Ihren eigenen Schlüssel, den Sie während der Installation angelegt haben. Als nächstes müssen Sie öffentliche Schlüssel mit Ihren E-Mail-Partnern austauschen. Ihren eigenen Schlüssel verschicken Sie am schnellsten wie folgt:

1. Starten Sie PGPkey.
2. Markieren Sie Ihren eigenen Schlüssel in der angezeigten Liste.
3. Wählen Sie im Menü Server erst Senden an und dann Mail-Empfänger an.
4. Daraufhin öffnet sich ein neues E-Mail-Fenster mit einer vorgefertigten Betreffzeile und einem Dateianhang, hinter dem sich Ihr öffentlicher PGP-Schlüssel verbirgt. Geben Sie in die An-Zeile nur noch den oder die Empfänger ein und klicken Sie dann auf Senden, um den Schlüssel zu verteilen.

Sprechen Sie die Aktion mit Ihren E-Mail-Partnern ab, damit Sie ebenfalls öffentliche Schlüssel anderer Personen erhalten. Die entsprechenden Mails landen in Ihrem Outlook-Posteingang. Anschliessend gehen Sie folgendermassen vor:

1. Öffnen Sie die Mail, die den öffentlichen PGP-Schlüssel einer anderen Person enthält.
2. Doppelklicken Sie auf den Dateianhang - normalerweise eine Datei mit der Endung ASC.
3. Auf die Frage, ob Sie die Datei öffnen oder speichern wollen, klicken Sie auf Öffnen. Oder – in älteren Windows-Versionen – Sie aktivieren die Option Öffnen und klicken dann auf Ok.
4. Es öffnet sich automatisch ein Dialogfenster mit Informationen zum fremden PGP-Schlüssel. Klicken Sie auf die Schaltfläche Importieren.

Damit haben Sie den Schlüssel zu Ihrem PGP-Schlüsselbund hinzugefügt. Das Resultat sehen Sie, wenn Sie erneut das Programm-Modul PGPkey starten. Die Liste enthält jetzt den fremden Schlüssel.

Wenn Sie einen fremden Schlüssel erhalten und in Ihr PGP-Schlüsselbund importieren, können Sie nicht sicher sein, dass der fremde Schlüssel tatsächlich von der jeweiligen Person stammt. Unter Umständen wurde der Schlüssel zuvor manipuliert oder es wurde Ihnen ein Schlüssel unter falschem Namen untergeschoben. Um derartige Angriffe auf Ihre E-Mail-Sicherheit auszuschliessen, besitzt jeder Schlüssel einen eindeutigen «Fingerabdruck». Vor der PGP-Kommunikation sollten Sie diesen Fingerabdruck gemeinsam mit dem Urheber überprüfen.

Dazu klicken Sie das PGP-Symbol in der Windows-Taskleiste an und starten über das aufklappende Menü das Schlüsselverwaltungs-Tool PGPkeys. Nun markieren Sie den Schlüssel, den Sie abstimmen wollen. Das kann Ihr eigener oder ein fremder Schlüssel sein. An-

www.lubasch.ch

schliessend rufen Sie im Menü Schlüssel den Befehl Eigenschaften auf. Im Bereich Fingerabdruck sehen Sie jetzt eine Folge englischsprachiger Begriffe. Die erscheinen auf den ersten Blick zwar recht merkwürdig, sie sind aber bewusst so gewählt, dass sie akustisch leicht voneinander zu unterscheiden sind - und das auch bei einer möglicherweise schlechten Telefonverbindung.

Rufen Sie also Ihren E-Mail-Partner an und lesen Sie die Ausdrücke im Bereich Fingerabdruck vor. Wenn sie identisch sind, können Sie dem fremden Schlüssel vertrauen. Alternativ können Sie natürlich auch das Kontrollkästchen Hexadezimal aktivieren und die Hexadezimalzahl austauschen. Telefonisch ist das allerdings nicht empfehlenswert, sodass sich in diesem Fall eher der gute alte Postweg (per Brief) anbietet. Danach verlassen Sie das Dialogfenster mit der Schaltfläche Schliessen.

Sobald Sie die Echtheit eines Schlüssels überprüft haben, erklären Sie ihn für gültig und sprechen ihm Ihr Vertrauen aus. Das erreichen Sie mit folgenden Schritten:

1. Starten Sie PGPkeys.
2. Markieren Sie den geprüften fremden Schlüssel.
3. Wählen Sie im Menü Schlüssel den Befehl Signieren an.
4. Übernehmen Sie die Standardeinstellungen des daraufhin angezeigten Dialogfensters mit Ok.
5. Prüfen Sie, ob im Dropdown-Feld Signierschlüssel Ihr eigener PGP-Schlüssel ausgewählt ist, und geben Sie dann die «Passphrase» (das Kennwort) Ihres Schlüssels ein. Die Eingabe bestätigen Sie mit Ok.
6. Dass sich der Status des Schlüssels geändert hat, erkennen Sie anhand des inzwischen grünen Symbols in der Gültigkeitsspalte von PGPkeys. Das hat aber noch keinen Einfluss auf die Vertrauensstufe des Schlüssels. Um ihn als vertrauenswürdig einzustufen, wählen Sie im Menü Schlüssel den Befehl Eigenschaften an.
7. Im daraufhin angezeigten Dialogfeld stellen Sie den Schieberegler im Bereich Vertrauensstufe von «Nicht vertraut» auf «Vertraut» um. Danach klicken Sie auf Schliessen.

Sie haben nun drei Möglichkeiten: Entweder Sie signieren ausgehende Nachrichten, um dem Empfänger zu garantieren, dass eine Mail tatsächlich von Ihnen stammt. Oder Sie verschlüsseln die Nachrichten, damit auch der Inhalt einer Mail verborgen bleibt und nur von der beabsichtigten Zielperson gelesen werden kann. Oder Sie kombinieren beide Verfahren. Die Vorgehensweise ist in allen Fällen nahezu identisch, deshalb hier eine allgemeine Anleitung:

1. Legen Sie wie gewohnt eine neue E-Mail in Outlook an - mit Empfängerauswahl, Betreffzeile und Nachrichtentext (zum Versand von verschlüsselten Anhängen kommen wir später noch).
2. Sorgen Sie dafür, dass sich der Cursor im Bereich des Nachrichtentextes befindet, und klicken Sie dann auf das PGP-Symbol in der Windows-Taskleiste.
3. Wählen Sie im aufklappenden Menü erst Aktuelles Fenster und dann je nach gewünschter Aktion entweder Signieren, Verschlüsseln oder Verschlüsseln & Signieren an.

www.lubasch.ch

4. Wenn Sie sich entschieden haben, eine Nachricht zu signieren, wählen Sie im anschliessenden Dialogfenster, sofern Sie mehrere eigene Schlüssel besitzen, den passenden Signierschlüssel aus und geben Sie dann die «Passphrase» für diesen Schlüssel ein. Falls Sie sich für das Verschlüsseln einer Nachricht entschieden haben, zeigt PGP ein Dialogfenster an, in dem Sie den gewünschten Empfänger aus einer allgemeinen Übersicht mit der Maus in die Empfängerliste ziehen können. Sollte Ihr eigener Schlüssel nicht automatisch in der Empfängerliste erscheinen, fügen Sie ihn ebenfalls hinzu; sonst können Sie den Nachrichtentext später selbst nicht mehr entschlüsseln. Nach einem Klick auf Ok wird der Nachrichtentext verschlüsselt.

5. Nun versenden Sie die E-Mail in gewohnter Art und Weise aus Outlook.

Oft geht es aber gar nicht so sehr darum, den Text einer E-Mail abzusichern. Oft müssen vertrauliche Dateianhänge geschützt werden. Bei PGP verpacken Sie dann nicht die komplette E-Mail inklusive Anhang. Stattdessen verschlüsseln Sie die Datei(en), die mitgeschickt werden soll(en), separat. Diese Aktion führen Sie im Windows-Explorer aus:

1. Starten Sie den Windows-Explorer und wechseln Sie in das Verzeichnis mit der zu verschlüsselnden Datei.

2. Klicken Sie den Dateinamen mit der rechten Maustaste an und wählen Sie im Kontextmenü zuerst PGP und dann entweder Verschlüsseln, Signieren oder Verschlüsseln & Signieren an.

3. Gehen Sie wie beim Senden einer sicheren E-Mail vor, um die «Passphrase» Ihres Signierschlüssels einzugeben oder um den Empfänger auszuwählen, der die verschlüsselte Datei weiterbearbeiten soll. Beachten Sie, dass Ihnen beim Verschlüsseln unter anderem eine Option zum Überschreiben der Originaldatei zur Verfügung steht. Setzen Sie diese Funktion mit äusserster Vorsicht ein, damit Sie nicht später selbst Probleme bekommen, die normale Datei zu öffnen.

4. Die Signatur bzw. die verschlüsselte Datei werden im selben Ordner wie das Original gespeichert. In beiden Fällen wird der ursprüngliche Dateiname beibehalten und ihm zusätzlich die Endung .SIG (Signatur) oder .PGP (Verschlüsselung) angehängt.

5. Nun können Sie eine normale E-Mail erstellen, der Sie im Fall einer signierten Datei sowohl das Original als auch die SIG-Datei anhängen oder nur die verschlüsselte PGP-Datei beifügen.

6. Senden Sie die E-Mail wie gewohnt.

Auf Empfängerseite müssen alle Dateien, die irgendwie mit PGP behandelt worden sind, auf der Festplatte gespeichert werden. Im Windows-Explorer lässt sich dann entweder die SIG- oder die PGP-Datei per Doppelklick öffnen. Die PGP-Software überprüft daraufhin die Signatur und gibt eine entsprechende Gültigkeitsmeldung aus oder sie entschlüsselt die Datei, wofür allerdings die Eingabe der «Passphrase» des Empfängers erforderlich ist.

So bleibt Ihre E-Mail-Kommunikation immer vertraulich und Sie brauchen keine Angst zu haben, dass Ihre Informationen auf dem Weg zum Empfänger manipuliert werden.

www.lbasch.ch