Programme im Praxistest

Entschlüsselung von E-Mails

Aus der Erfahrung im privaten Bereich haben sich viele Mitarbeiter an die einfach zu bedienenden Web-Mail-Oberflächen der Free-Mail-Anbieter wie Hotmail, GMX oder Yahoo gewöhnt. Auch im Unternehmen geschieht der Zugriff auf verschlüsselte geschäftliche E-Mails immer häufiger per Web-Mail-Oberfläche – zumal der Zugriff so von überall möglich ist. Wir zeigen, mit welchen Tools das Lesen von verschlüsselten E-Mails möglich ist und wo sie an ihre Grenzen stoßen.

Alle gängigen E-Mail-Clients – von Outlook bis Thunderbird – unterstützen eine Verschlüsslung von E-Mails.

In der Regel wird S/Mime nativ und OpenPGP über Plugins oder Addons unterstützt. Darüber hinaus nutzen etliche Unternehmen und Behörden die E-Mail-Verschlüsselung über Proxies wie PGP Universal oder Utimaco SafeGuard MailGateway.

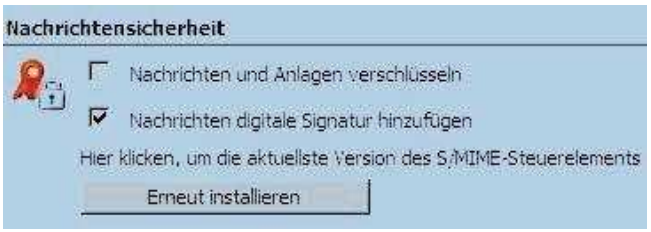
Unabhängig von der konkreten Realisierung der E-Mail-Verschlüsselung im Betrieb stellt sich die Frage, welche Möglichkeiten es gibt, damit die Mitarbeiter über ihre Web-Mail-Oberfläche die verschlüsselten Unternehmens-E-Mails ohne Sicherheitsrisiko lesen können.

Möglichkeit 1: Zugriff mit Outlook Web Access – funktionell, …

Eine sehr funktionelle Oberfläche bietet Outlook Web Access (OWA). Damit können Mitarbeiter unter Verwendung des Internet Explorers auf die Mails auf dem Exchange-Server zugreifen.

Der Benutzer sieht im OWA allerdings zunächst nur die verschlüsselte – und damit unlesbare – E-Mail. Um dieses Problem zu lösen, schuf Microsoft das OWA S/Mime Control. Es lässt sich einfach über den Menüpunkt „*Optionen*“ und dann unter „*Nachrichtensicherheit*“ direkt aus der Web-Oberfläche installieren.

Zur Installation sind Administrator-Rechte nötig. Voraussetzung zur Installation sind ein Microsoft Windows 2000/XP/Vista und der Internet Explorer 6 oder 7. Aufgrund der ActiveX-Technologie ist der Einsatz mit anderen Browsern und unter anderen Betriebssystemen nicht möglich.



Konfiguration des S/Mime-Steuerelements im Outlook Web Access (OWA)

… aber nicht auf fremder Hardware möglich

Das OWA S/Mime Control funktioniert einwandfrei und erlaubt das Lesen verschlüsselter E-Mails. Es bleibt jedoch ein grundlegendes konzeptionelles Problem: Zur Entschlüsselung ist der private Schlüssel nötig. Damit muss das ActiveX Control den privaten Schlüssel im Zugriff haben.

Die Verwendung auf fremder Hardware – z.B. im Internet-Café – ist somit nicht zulässig.

Bei OWA den Schlüssel sorgfältig speichern und nicht auf fremder Hardware verwenden!

Der private Schlüssel muss entweder im lokalen Zertifikat-Speicher – de facto die Registry – oder auf einer Hardware (Chipkarte oder USB-Dongle)

gespeichert sein. Eine Installation des eigenen privaten Schlüssels auf einem fremden, nicht vertrauenswürdigen Rechner ist unverantwortlich.

Die Verwendung des Hardwarespeichers scheitert in der Regel an den fehlenden Treibern, die man nicht installieren kann oder darf.

Damit lässt sich das OWA S/Mime Control nur auf eigener Hardware einsetzen. Dass der Anwender einen fremden Rechner nutzt, um die E-Mail zu checken, ist konzeptionsbedingt nicht möglich.

Möglichkeit 2: Freenigma arbeitet mit Schlüsselhandling auf dem Server

Einen völlig neuen Weg geht die Firma Freiheit.com mit Freenigma, einem OpenPGP-kompatiblen Produkt. Das Firefox-Plug-in trennt den Umgang mit den Schlüsseln von den Ver- und Entschlüsselungsroutinen. Das gesamte Schlüsselhandling findet auf einem Server statt.

Freenigma ist als „Software as a Service“ konzipiert, die man immer über das Internet nutzt. Während der jetzigen Testphase steht der Server bei der Firma freiheit.com, auf Dauer steht der Server im eigenen Unternehmen.

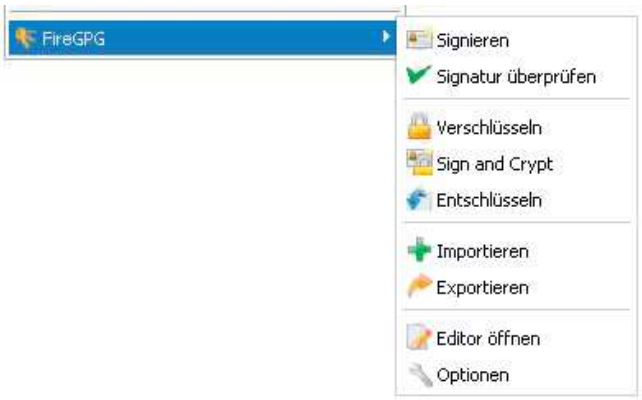
In der derzeitigen öffentlichen Testphase fehlen noch Möglichkeiten, Schlüssel zu importieren oder zu exportieren.

Die Schlüsselgenerierung findet – ähnlich einem Verschlüsselungs-Gateway – auf dem Server statt. Die Verschlüsselung findet im Browser/Plug-in statt. Es wird dabei kein Klartext an den Server übertragen.

Links:

FireGPG:
http://firegpg.tuxfamily.org

Freenigma:
http://www.freenigma.com



Das Kontext-Menü des FireGPG erlaubt den Zugriff auf die Funktionalitäten.

Die Verschlüsselung über Freenigma benötigt kein lokales Verschlüsselungsprogramm

Freenigma unterstützt derzeit die Freemailer Google-Mail, Yahoo! Mail, Hotmail und GMX. In die Webseite lässt sich ein Button, über den die Bedienung erfolgt, einbinden. Ein lokal installiertes Verschlüsselungsprogramm (GnuPG oder PGP) ist nicht erforderlich.

Mit Freenigma lassen sich verschlüsselte Mails gefahrlos auch auf fremder Hardware lesen

Auch wenn Freenigma noch kein fertiges Produkt ist, zeigt es doch völlig neue Ansätze. Man kann damit auf fremder Hardware verschlüsselte E-Mails lesen, ohne seinen privaten Schlüssel zu kompromittieren.

Voraussetzung ist lediglich die Installation des Firefox-Plug-ins.

Möglichkeit 3: FireGPG lässt sich nur nach Installation von GnuPG nutzen

FireGPG ist ein Firefox-Plug-in, das ein installiertes GnuPG auf dem lokalen Rechner voraussetzt. Damit ist die Nutzung auf fremder Hardware schwierig.

Die Schlüssel müssen im lokalen Schlüsselring vorhanden sein.

Damit gelten die gleichen Restriktionen bei der Speicherung von privaten Schlüsseln wie für das OWA S/Mime Control.

Die Bedienung erfolgt über ein Kontext-Menü. Der Bedienungskomfort entspricht in etwa den üblichen Werkzeugen zur Verschlüsselung einer Datei über eine Explorer-Erweiterung.

Nur Freenigma schützt auf fremder Hardware den privaten Schlüssel

Ein grundlegendes Problem beim Lesen verschlüsselter E-Mails auf fremder Hardware ist bei den meisten Programmen ungelöst: der sichere Schutz des privaten Schlüssels vor Kompromittierung.

Das Plugin Freenigma zeigt in der Homepage des Freemailers einen Button an, über den Sie das Ver- und Entschlüsseln steuern können.

Einzig Freenigma hat einen vielversprechenden innovativen Ansatz.

Was wo am besten einsetzen?

Will der Mitarbeiter von seinem vertrauenswürdigen privaten Rechner auf verschlüsselte Firmen-E-Mails zugreifen, eignen sich ActiveX Control oder FireGPG am besten.

Freenigma ist einsetzbar, sobald das Schlüsselhandling auf einem Unternehmensserver stattfindet.

Prof. Dr. Rainer W. Gerling