E-Mail

E-Mail ist in der heutigen Zeit nicht mehr wegdenkbar. Es ist zu einem unverzichtbaren Hilfsmittel geworden. Schnell noch letzte geschäftliche Informationen austauschen, einen Termin abmachen, einen Tisch im Restaurant reservieren, mit Kollegen, Bekannten und Verwandten kommunizieren, usw.

Dass dabei die Nachricht wie eine Postkarte versandt wird, ist oft nicht bekannt. Somit kann die E-Mail von allen Stationen zwischen Sender und Empfänger gelesen oder gar manipuliert werden! Dieser Beitrag soll aufzeigen, wie E-Mails sicher übermittelt werden können.

Versand von E-Mails

Der Versand von E-Mails erfolgt über das Protokoll SMTP (Simple Mail Transfer Protokoll). Es regelt die Sprache der Server. So wird zuerst die Verbindung zum Zielserver aufgebaut, und danach Sender und Empfänger mitgeteilt. Im dritten Schritt folgen die Informationen (der Inhalt der E-Mail). Ist alles übertragen, erfolgt die Abmeldung.

Ein Versand kann auch sehr einfach mit dem Tool «Telnet», welches sich auf jedem Computer befindet, von Hand bewerkstelligt werden (Ausnahme Windows Vista, hier muss es von Hand nachinstalliert werden). Im nebenstehendem Kasten ein Beispiel dazu.

Sicherheit

Die Übertragung von E-Mails hat einen grossen Nachteil: die E-Mails beziehungsweise der Inhalt wird unverschlüsselt übertragen. Sitzt ein potenzieller Angreifer dazwischen, kann er problemlos alles Lesen (eine sogenannten Man-in-the-Middle-Attacke). Daher wird bei E-Mails oft auch von Postkarte gesprochen, auch diese kann von jeder Person zwischen Sender und Empfänger gelesen werden (Im Internet sind es die zwischen Empfänger und Sender weiterleitenden Server). Vertrauliche E-Mails sollten daher NIE unverschlüsselt übertragen werden. Als Lösung bieten sich zwei Möglichkeiten an: der Verschlüsselung des E-Mails oder die sichere Übertragung im Internet.

ZUM AUTOR

Andreas Wisler –
IT-Redaktion Maschinenbau

Verschlüsselung des E-Mail-Inhaltes

Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text (Klartext) mit Hilfe eines Verschlüsselungsverfahrens in eine «unleserliche», das heisst nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird. Als entscheidend wichtiger Parameter der Verschlüsselung werden hierbei ein oder auch mehrere Schlüssel verwendet.

Diese Arbeit übernehmen Programme, der Anwender muss sich nur am Rande mit der Verschlüsselung auseinander setzen. Auf dem Markt buhlen sich momentan zwei Verfahren um die Gunst der Anwender: PGP und X.509.

PGP

PGP steht von Pretty Good Privacy und wurde 1991 von Phil Zimmermann entwickelt. Die Grundidee war es, Daten von der Regierung ungesehen von einem Ort an den anderen zu transportieren. Seit Ende der 90er-Jahre ist das Programm (fast) auf der ganzen Welt verfügbar.

PGP basiert auf einer sehr cleveren und schnellen Art der Verschlüsselung. Für den Inhalt der Nachrichten wird ein symmetrisches Verfahren verwendet (Empfänger und Sender verwenden den gleichen Schlüssel). Dies aus dem einfachen Grund, dass symmetrische Verfahren weniger Rechenintensiv und damit schneller sind. Damit jedoch die Benutzer dieses geheime Passwort nicht jedes Mal auf einem sicheren Weg übermitteln müssen, wird für die Verschlüsselung des Passwortes das asymmetrische Verfahren verwendet (oft auch als Public-Key bezeichnet). Dabei besitzt jede Person ein Schlüsselpaar, einen öffentlichen (Public Key) und einen geheimen (Private Key) Schlüssel. Diese beiden Schlüssel sind mathematisch voneinander abhängig, es ist jedoch nicht möglich (beziehungsweise nur mit einem exorbitanten Aufwand) vom öffentlichen auf den privaten Teil zu gelangen.

Zur Verschlüsselung wird jeweils der öffentliche Schlüssel verwendet, entschlüsselt werden kann die Nachricht nur mit dem privaten Schlüssel. PGP verwendet als Technik unteranderem den DH/DSS-Algorithmus (welcher aber hier nicht genauer vorgestellt wird).

PGP basiert auf dem Web-of-Trust verfahren. Die Idee hinter dieser «Technik» ist, dass sich die Benutzer gegenseitig die Echtheit des öffentlichen Schlüssels bestätigen. Dies soll verhindern, dass sich ein fremder Benutzter als eine bekannte Person ausgeben kann. Als Motto gilt: Ich vertraue jedem, dem jemand vertraut, dem ich vertraue. Und umgekehrt: Jeder, der jemandem vertraut, der mir vertraut, vertraut auch mir.

X.509

Einen anderen Weg schlägt X.509 ein. X.509 wurde erstmals 1988 veröffentlicht und setzt ein striktes hierarchisches System von vertrauenswürdigen Zertifizierungsstellen (engl. certificate authority, kurz CA) voraus, die Zertifikate erteilen können. Dieses Prinzip steht im Gegensatz zum vorher beschriebenen Web of Trust-Modell. X.509 kommt übrigens auch immer dann zum Einsatz, wenn Sie eine verschlüsselte Internetseite besuchen (erkennbar am https). Die gleiche Technik wird auch für die Verschlüsselung von E-Mails verwendet.

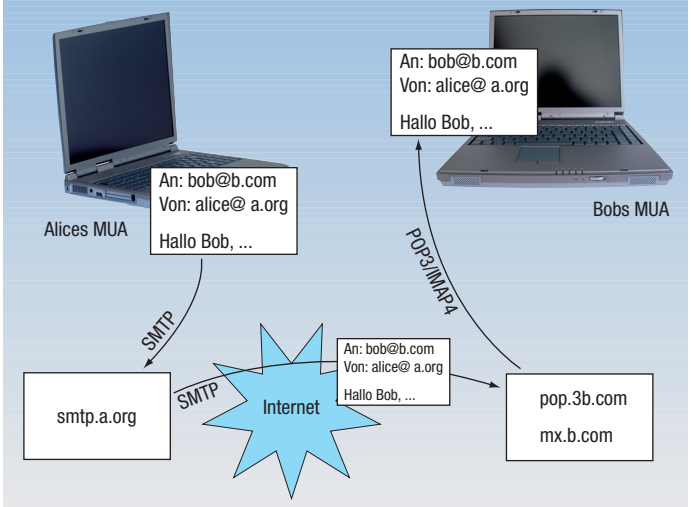
Im Internet finden sich zahlreiche Zertifizierungsstellen, die solche Zertifikate ausstellen. Die eigene Identität muss dabei mit einem Ausweis bestätigt werden.

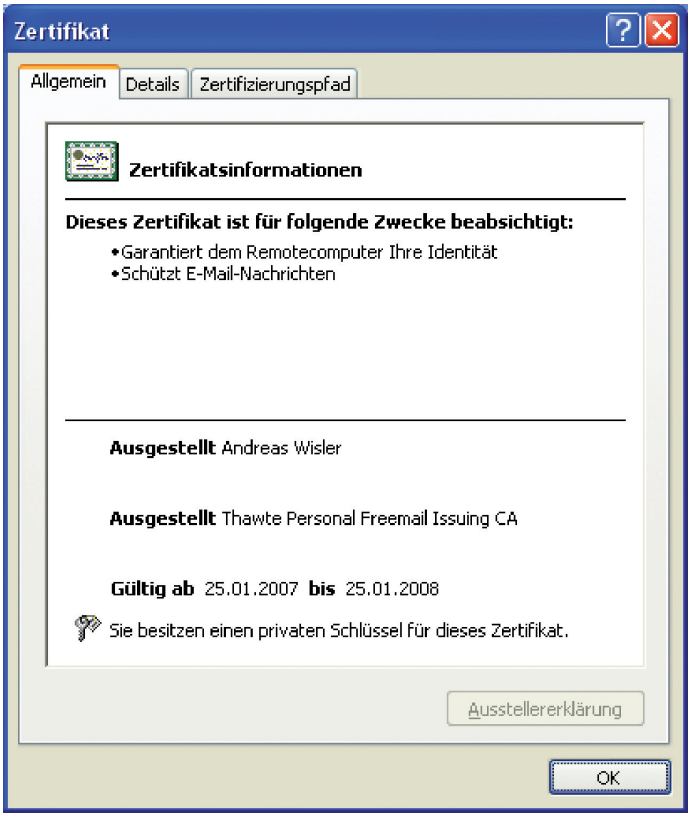
helo mailserver	Guten Tag, ich heisse Mailserver
mail from:name@domain.ch	Die E-Mail kommt von name@domain.ch
rcpto to:empfaenger@domain.ch	Ich schicke eine E-Mail an empfaenger@domain.ch
data	Ab jetzt folgen Daten
Freundliche Gruesse	Inhalt der E-Mail
.	Meistens ist ein alleine stehender Punkt das Endzeichen
quit	Besten Dank, ich bin fertig

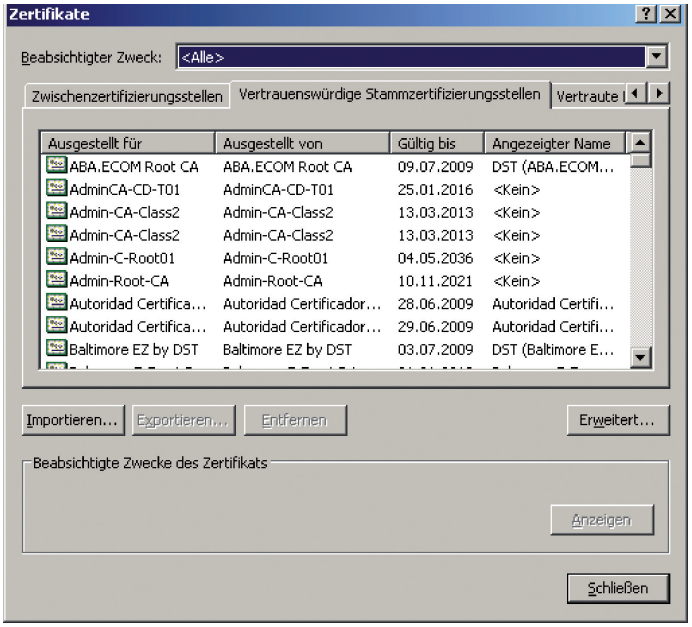
Kasten Ende

> Der Empfänger E-Mailserver quittiert dies mit einer Vollzugs- oder Fehlermeldung.

> Das E-Mail liegt nun beim Empfänger zum Abholen bereit.







Sobald dies geschehen ist, übernimmt die ausstellende Stelle die Garantie, dass die Person wirklich die Person ist, auf welche das Zertifikat lautet. Für diesen Service wird ein jährlicher Betrag verlangt. Die Zertifikate sind dementsprechend auch nur ein Jahr gültig und müssen dann erneuert werden (im Gegensatz zu PGP, wo Zertifikate «unendlich» lange gültig sind). Der grosse Vorteil liegt aber darin, dass Sie sich nicht um die Kontrolle der Person kümmern müssen, sondern können sich «blind» auf diese Unternehmen verlassen. Nun stellt sich die Frage, wieso ich diversen Zertifizierungsstellen blind vertraue? Die Antwort liegt im eigenen Computer. Als Grundvoreinstellung sind diverse Stellen bereits als Vertrauenswürdig eingestuft. Sie gelangen im Internet Explorer via Extras – Internetoptionen – Inhalte – Zertifikate – Vertauenswürdige Stammzertifizierungsstellen zur Antwort. Allen diesen Stellen wird vertraut. Das heisst, ein Zertifikat, welches von einem dieser Zertifizierungsstellen ausgestellt wurde, wird als Vertrauenswürdig angesehen. Möchten Sie einer Stelle nicht mehr trauen, dann können Sie diese mit einem Klick auf «Entfernen» aus der Liste verbannen.

Sichere Übertragung der E-Mails

Wie erwähnt, kann nicht nur der Inhalt von E-Mails vor neugierigen Augen geschützt werden, sondern auch der Transport zum Ziel. Zum Einsatz gelangen die sicheren Protokolle SSMTP (zum Versenden von E-Mails) sowie POP3S und IMAP4S. Allen gemeinsam ist die Verschlüsselung auf Basis von SSL. Dies funktioniert analog von HTTPS.

In Outlook genügt unter den Konteneinstellungen ein einfacher Klick auf «Server erfordert eine verschlüsselte Verbindung (SSL)» und Ihre E-Mails werden vor fremden Augen sicher an den Provider übertragen. In der Schweiz, wie auch auf dem Rest der Welt, unterstützen leider nur wenige Provider diese Art der sicheren Kommunikation. Dies verhindert eine geschützte Verbindung vom Start bis ins Ziel. Daher bleibt vorerst nur der Weg über die Verschlüsselung des Inhaltes.