2.3 Sichere E-Mail – bessere und vertrauenswürdige Kommunikation

Die Apologeten der neuen „sozialen Medien“ wie Facebook und Twitter verkünden zwar immer wieder, das Ende der E-Mail sei gekommen. Aber ebenso wenig, wie wir in absehbarer Zukunft das „papierlose Büro“ erleben werden, werden E-Mails als gängiges Mittel zur Kommunikation über das Netz verschwinden. So kommen dann E-Mails jeden Tag an fast jedem Arbeitsplatz wie selbstverständlich zum Einsatz – so selbstverständlich, dass sich viele Anwender bisher kaum Gedanken über die Sicherheit dieses Kommunikationskanals gemacht haben.

Das gewaltige mediale Echo, das die Snowdon-Enthüllungen hervorgerufen haben, hat nicht zuletzt auch viele Nutzer dazu gebracht, sich etwas eingehender mit den Sicherheitsaspekten bei Versand, Empfang und Einsatz von E-Mails zu befassen. Wir haben in unserer FAQ-Aufstellung einige wichtige Fragen, Antworten und Lösungen rund um das Thema „E-Mail sicher nutzen“ zusammengestellt.

2.3.1 Wie sicher ist der Inhalt einer E-Mail?

Es wurde schon oft geschrieben und gesagt, aber viele Anwender scheinen es immer wieder zu vergessen: Der Inhalt einer E-Mail ist grundsätzlich nicht gesichert. Alles, was ein Nutzer in einer E-Mail-Nachricht schreibt, geht im Klartext über die Verbindung. Deshalb wird eine solche Nachricht auch immer wieder gerne mit einer Postkarte verglichen: Auch die kann jeder lesen, der sie zufällig (oder absichtlich) in die Hand bekommt. Um Daten mitzulesen, die offen über eine Netzwerkverbindung gesendet werden, bedarf es zudem keiner großartigen „Hacker-Kenntnisse“: Werkzeuge zur Netzwerküberwachung – sogenannte Sniffer – wie etwa das bekannte Wireshark (www.wireshark.org) oder auch Microsofts Network Monitor (http://blogs.technet.com/b/netmon/p/downloads.aspx) erlauben das einfache Mitlesen der Nachrichten im Klartext.

Praxis-Tipp: Überlegen Sie immer gut, was Sie in einer Mail schreiben, und überlegen Sie, ob Sie diese Informationen auch einer Postkarte anvertrauen würden. Kreditkarten- und Bankkontodaten sowie ähnlich sensible Daten haben in einer normalen Mail nichts verloren!

2.3.2 Reicht eine AV-Lösung auf dem System zum Schutz der E-Mail?

Es ist wohl selbstverständlich, dass heute kein System mehr ohne eine entsprechende Antivirenlösung betrieben werden sollte. Doch braucht sich ein Anwender keine Gedanken mehr um die Gefahren machen, die aus den E-Mail-Nachrichten drohen, wenn sein System mit einer solchen Sicherheitslösung geschützt ist? Ein

großer Teil der Schadprogramme gelangt heute mittels einer E-Mail auf die Systeme und damit häufig auch in die Netzwerke.

Antivirenprogramme tragen dieser Entwicklung Rechnung und können häufig bereits auf dieser Ebene eingreifen. Aber gerade wenn eine der ansonsten sehr guten freien AV-Lösungen zum Einsatz kommt, kann es sein, dass diese nicht dezidiert die Nachrichten und – noch viel wichtiger – die diversen Anhänge durchsucht. Einige Anbieter stellten diese Möglichkeiten erst mit den kommerziellen Versionen ihrer Antivirenlösungen zur Verfügung. Deshalb ist eine Antivirensoftware auch in Hinblick auf die Sicherheit der E-Mail nur ein Baustein in der Abwehr von Angriffen auf die Computersysteme.

Auch die Gefahren, die beispielsweise durch den Einsatz von HTML-Nachrichten entstehen – wir gehen darauf in diesem Bericht noch detaillierter ein –, können durch diese Programme nicht erkannt und bewältigt werden.

2.3.3 Wie kann ich E-Mail-Nachrichten sicherer versenden?

Die einfache Antwort auf diese Frage lautet: Verschlüsseln Sie Ihre Nachrichten! Warum aber verschlüsseln dann nicht mehr Anwender ihre Nachrichten standardmäßig? Wer zudem einmal versucht hat, einem Geschäftspartner oder gar einer Bank oder Behörde eine verschlüsselte Nachricht zu übermitteln, wird ebenfalls festgestellt haben, dass die Verbreitung dieser Sicherheitsmaßnahme eher gering ist. Das liegt unter anderem daran, dass die Anbieter von Mail-Programmen keine entsprechende Standardlösung in ihren Produkten integrieren (oder auch nur so etwas etablieren) und viele Lösungen auf dem Markt leider recht unpraktisch in der Anwendung sind.

Lösungen zum Verschlüsseln der E-Mails: Das BSI (Bundesamt für Sicherheit in der Informationstechnik) unterstützt aktiv die Lösung GPG4win (GNU Privacy for Windows). Sie steht für Windows-Systeme zum kostenlosen Download bereit (www.gpg4win.org/download-de.html). Die Software kann nicht nur die E-Mail-Nachrichten, sondern auch Dateien und Ordner auf dem PC verschlüsseln. Die Integrität der Daten lässt sich dabei ebenfalls mittels der Software durch den Einsatz digitaler Signaturen sichern. Als Standards werden dabei OpenPGP (www.openpgp.org) und S/MIME (X.509) unterstützt. Neben dem eigentlichen Verschlüsselungsprogramm GNUPG beinhaltet das Paket eine Software mit Namen „Kleopatra“, die als Zertifikatsmanager arbeitet. Die Software ist so angelegt, dass sie sich leicht unter Windows installieren lässt. Sie arbeitet mit Windows XP (das aber aus Sicherheitsgründen gerade in diesem Zusammenhang NICHT mehr zum Einsatz kommen sollte), Vista, Windows 7 und Windows 8/8.1 zusammen und unterstützt dabei sowohl 32- als auch 64-Bit-Systeme.

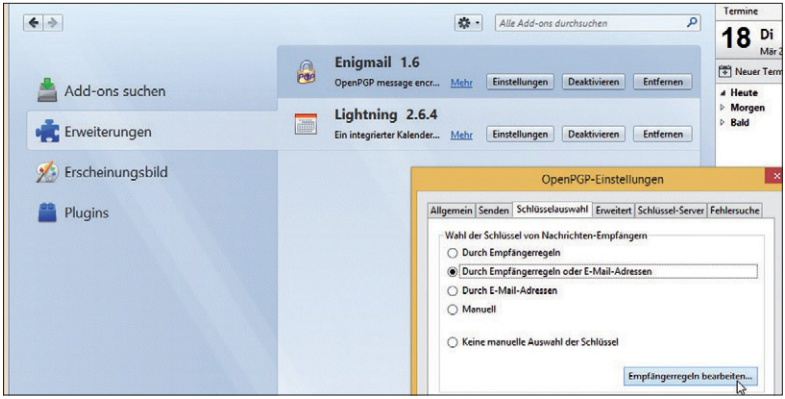
Wer Microsoft Outlook in der Version 2003 oder 2007 verwendet, findet nach der Installation einen neuen Menüpunkt in seinem Programm, der ihm das Verschlüsseln und Signieren seiner Nachrichten erlaubt. Das Programm führt schon bei der

Installation durch das Anlegen eines entsprechenden Schlüsselpaares. Auch für die Outlook-Versionen 2010 oder 2013 steht jetzt ein GpgOL-Plug-in bereit, das aber nach wie vor vom Anwender ein wenig zusätzliche „Handarbeit“ erfordert, will er seine Nachrichten verschlüsseln. Wichtiger Hinweis: In allen Fällen unterstützt die Software nur die 32-Bit-Versionen von Outlook.

Verschlüsselung bringt Sicherheit: Mit der Software GPG4win steht eine Lösung zur Verfügung, die unter anderem OpenPGP auch für Windows-Systeme bereitstellt.

2.3.4 Security auch für Thunderbird

Für Anwender von Mozillas Thunderbird bietet sich die Erweiterung EnigMail (http://enigmail.mozdev.org/) an, die ebenfalls auf OpenPGP aufsetzt und eine entsprechende Integration in das Mail-Programm bietet: Sie ist im Gegensatz zu GPG4win nicht von der Version des Mail-Programms abhängig und arbeitete in unseren Tests problemlos auch mit der Version 13 von Thunderbird zusammen.



Auch für Thunderbird existieren entsprechende Lösungen zur Verschlüsselung: Mithilfe der Erweiterung „Enigmail“ steht der Einsatz von OpenPGP direkt im Mail-Programm zur Verfügung.

Praxis-Tipp: Wer diese beiden Anwendungen testet, wird feststellen, dass es zunächst einmal eine gewisse Lernkurve zu bewältigen gilt. Das größere Problem dürfte es aber sein, sein Gegenüber vom Einsatz einer solchen Lösung zu überzeugen – hier gilt es noch Pionierarbeit zu leisten. Unser Vorschlag deshalb: Setzen Sie eine der gängigen freien Verschlüsselungslösungen wie Truecrypt (www.truecrypt.org) ein, erzeugen damit einen sicheren Container, schreiben Ihren Text in dem Textverarbeitungsprogramm ihrer Wahl und legen ihn in diesen Container.

Dieser wird an den Empfänger als E-Mail-Attachment geschickt, das benötigte Passwort zum Entschlüsseln wird dabei natürlich auf einem anderen Weg (beispielsweise per Telefon oder persönlich) übermittelt.

Wichtig: Die meisten Verschlüsselungsprogramme bieten auch die Möglichkeit, selbst-entpackende, ausführbare Dateien zu erstellen. Auch wenn dieses Vorgehen zunächst wie eine gute Idee erscheint, sollten Sie diese Methode nicht verwenden: Diese Programme erzeugen zumeist Dateien mit der Endung *.exe, und solche Anhänge werden aus Sicherheitsgründen von einem Großteil der Mail-Server und -Gateways blockiert und nicht angenommen.

2.3.5 Warum sollte man keine HTML-Nachrichten verwenden?

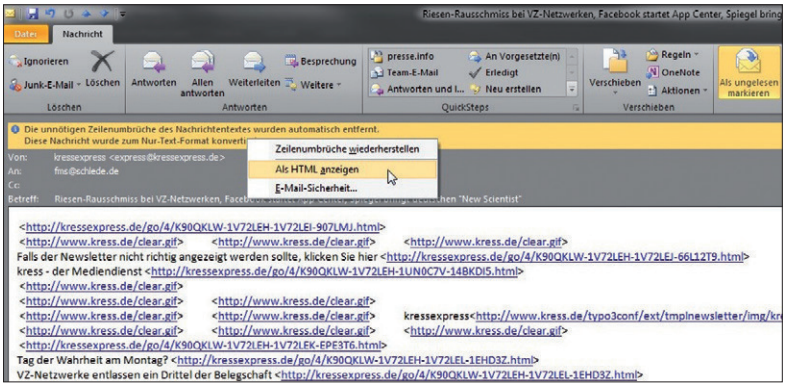
Reine Textnachrichten sind langweilig – jedenfalls scheinen das sowohl die Entwickler der meisten E-Mail-Programme als auch die Absender eines Großteils der Nachrichten zu meinen: Nachrichten im HTML-Format sind zumeist Standard. Vom Standpunkt der Sicherheit aus betrachtet stellt der Einsatz dieses Formats allerdings ein erhebliches Risiko da. Durch die Möglichkeit, in HTML auch entsprechende Skripte einzubetten, können so ungewollt potenziell gefährliche Programme auf den Rechner gelangen. Auch wenn die Nachrichten dann keine „bunten" Überschriften und eingebetteten Bildern bieten – das reine Textformat ist der sicherere Weg.

2.3.6 Welche Sicherheitseinstellungen sind bei Outlook sinnvoll?

In Zusammenhang mit der vorherigen Frage ist es zunächst einmal sehr sinnvoll, das Mail-Programm so zu konfigurieren, dass es automatisch alle Nachrichten nur noch im Textformat anzeigt. Dies gelingt in neueren Outlook-Versionen über das sogenannte Vertrauensstellungscenter (bis Outlook 2007) oder Sicherheitscenter (ab Outlook 2010).

Erreicht werden können diese Einstellungen über den Weg: Datei/Optionen/Sicherheitscenter/Einstellungen für das Sicherheitscenter/E-Mail-Sicherheit. Dort kann ein Anwender festlegen, dass Standardnachrichten (und auch signierte

Nachrichten) nur im Textformat angezeigt werden. Zeigt sich beim Lesen einer derart konvertierten E-Mail, dass sie im Textformat nur schwer oder überhaupt nicht lesbar ist, lassen sich die ursprünglichen Formatierungen wiederherstellen. Dies geschieht per Mausklick auf „als HTML anzeigen". Bitte nur anwenden, wenn die Nachricht aus einer verlässlichen Quelle stammt!



Mit einem Klick rückgängig: Ist die Nachricht im Nur-Text-Format nur noch schlecht oder überhaupt nicht mehr zu lesen und kann man sich sicher sein, dass sie von einem vertrauenswürdigen Absender stammt, so kann sie mittels eines Klicks wieder im HTML-Format angezeigt werden.

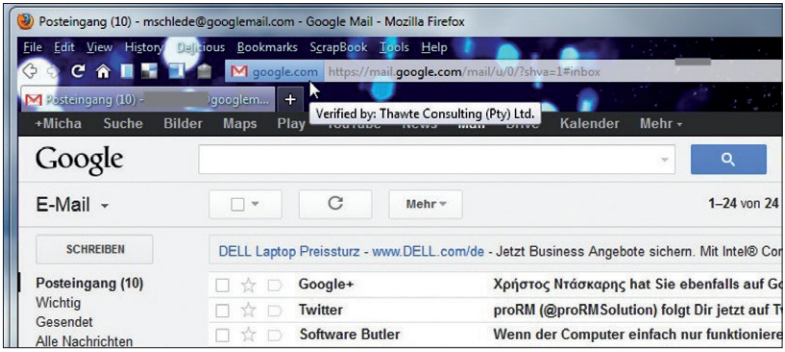
Wer nicht ganz auf HTML-Nachrichten verzichten will, dabei aber die Sicherheit verbessern möchte, kann im Sicherheits- oder Vertrauensstellungscenter auch den Eintrag „Automatischer Download" auswählen. Hier sind verschiedene Konfigurationen möglich, wie das Ausschalten des automatischen Bilder-Downloads in HTML-Nachrichten. Höchste Sicherheit bietet nur das Sperren aller angebotenen Optionen – seien Sie sich jedoch darüber im Klaren, dass die Nachrichten dann nicht mehr unbedingt „leserfreundlich" aussehen.

2.3.7 Ist vom Einsatz einer Web-Mail-Lösung grundsätzlich abzuraten?

Grundsätzlich können Web-Mail-Lösungen heute ebenso gut eingesetzt werden wie „althergebrachte" E-Mail-Lösungen auf dem Rechner. Allerdings gilt beim Einsatz von Web-Mail-Anwendungen das Gleiche wie für Cloud-Dienste ganz allgemein. Wer eine Web-Mail-Lösung verwendet, muss immer ein besonderes Augenmerk auf die Client-Server-Verbindung haben (sei es auf Notebook, Tablet oder Smartphone) und die folgenden Grundsätze beachten:

- Zugriff auf Web-Mail-Konten nur und ausschließlich über SSL-Verbindungen – nie eine offene Verbindung zulassen.

- Sicherstellen, dass die Webseite auch schon bei der Anmeldung verschlüsselt ist – mache Seiten schalten die SSL-Verbindung erst NACH dem Verbindungsaufbau ein, wodurch der Name und das Passwort des Anwenders unverschlüsselt übertragen werden.
- Kommt das Mail-Konto für geschäftliche Zwecke zum Einsatz, sollte sichergestellt sein, dass der Provider die Daten in Deutschland oder mindestens in der EU hostet.
- Wer mit seinem mobilen Client auf eine Web-Mail-Lösung oder auch auf den regulären Mail-Server zugreift, sollte dazu NIEMALS einen öffentlichen nicht verschlüsselten WLAN-Hotspot verwenden.



Ein wichtige Grundregel beim Einsatz von Web-Mail-Anwendungen: Der Übertragungsweg muss immer verschlüsselt sein – wie hier bei Google-Mail mittels einer SSL-Verbindung.

Ein Web-Mail-Konto eignet sich gut als „Zweit-Postfach“: Wer sein eigenes „echtes“ Mail-Postfach konsequent nur für die wichtige Kommunikation mit vertrauenswürdigen Absendern/Empfänger verwendet, kann ein solches (zumeist kostenloses) Zweitkonto gut dazu verwenden, beispielsweise interessante Beiträge von Firmenseiten herunterzuladen, die zumeist die Eingabe einer E-Mail-Adresse verlangen. Auch die Teilnahme an Gewinnspielen und ähnlichen Aktivitäten wird so sicherer: Werden im Rahmen dieser Kontakte Spam-Nachrichten ausgelöst (was leider immer noch der Fall ist), landen diese nur auf dem Zweitkonto und verstopfen nicht die wirklich wichtige Adresse.

2.3.8 Last but not least: sichern, sichern, sichern…

Einen Ratschlag sollte jeder Anwender immer beherzigen: Sichern Sie ihre Mail regelmäßig und häufig. Heute werden sehr viele Nachrichten und Informationen über diesen Kanal verschickt, die für den Geschäftsbetrieb wichtig sind. Geht die komplette gesammelte Mail verloren, weil beispielsweise die Festplatte im Rechner