Sicherheit von E-Mail

Beim gegenwärtigen Entwicklungsstand von Programmen und Technik ist E-Mail ein nicht unter allen Umständen sicheres Medium. Eine E-Mail muss eher mit einer Postkarte als mit einem herkömmlichen Brief (im Umschlag) verglichen werden. Das ist um so bedeutsamer, als im Gegensatz zum „klassischen“ Postverkehr die Sicherheitsrisiken bei E-Mail allgemein wenig bekannt sind.

Auf ihrem Weg vom Sender zum Empfänger kann eine Mail eine Vielzahl von Rechnern als Zwischenstation passieren. Überall wird sie dabei im Klartext, d. h. ohne jede Verschlüsselung, übertragen und gespeichert. Jeder, der Administrator-Rechte für einen der beteiligten Rechner hat, kann daher die Mail lesen. Dabei spielt es – technisch gesehen – keine Rolle, ob diese Rechte legal oder illegal („Hacker“!) erworben wurden. Das Lesen fremder Mails ist zwar nicht ganz einfach und außerdem verboten, mit den entsprechenden Systemkenntnissen jedoch durchaus möglich. Darüber hinaus können technische Störungen auftreten, die u. U. dazu führen, dass eine Mail den Empfänger nur unvollständig oder gar nicht erreicht. Glücklicherweise passiert dies relativ selten, ist aber doch nie ganz auszuschließen.

Ein weiteres Risiko ist mit dem Lesen von Mails in öffentlichen PC-Pools über POP-Mailprogramme verbunden: Sie sollten vor dem Verlassen des PCs Ihre auf die Festplatte kopierten Mails löschen (vergessen Sie auch den „Trash“ nicht) sowie Ihre persönlichen Angaben (vor allem Ihr Passwort!) aus den Programmeinstellungen wieder entfernen. Tun Sie dies nicht, könnte der nächste Benutzer dieses PCs

- Ihre auf der Festplatte gespeicherten Mails lesen und
- neue für Sie eingehende Mails abrufen, die Sie dann (das dürfte für Sie noch schlimmer sein) eventuell gar nicht mehr zu sehen bekommen, da die Mails bei entsprechenden Programmeinstellungen im Unix gelöscht werden.

Nun könnten Sie einwenden, dass Ihre Post ja gar nicht so geheim und so wichtig sei, und wer sich unbedingt die Mühe machen will, sie zu lesen, der soll das doch ruhig tun. Aber die Missbrauchsmöglichkeiten gehen noch weiter. So lassen sich abgeschickte Mails unterdrücken oder auch verfälschen. Es ist sogar möglich, Mails mit falschen Absenderangaben zu versenden! Die Ursachen dafür liegen in den recht alten Protokollen, die im Internet verwendet werden, aber auch in der erst vor relativ kurzer Zeit eingetretenen Sensibilität der Anwender für diese Problematik, weshalb Entwicklungen auf diesem Gebiet lange vernachlässigt wurden.

Eine Möglichkeit, E-Mails „in einen Briefumschlag zu legen“, bietet die Anwendung kryptografischer Verfahren, d. h. die Nachrichtentexte werden verschlüsselt. Wie das geht, erfahren Sie im Artikel *E-Mails: Verschlüsselt und unterschrieben*.

Wir wollen hier keine Panik verbreiten. Doch spätestens dann, wenn Sie eine Mail erhalten, die anscheinend von einem Freund oder Bekannten stammt und in der Sie zu ungewöhnlichen Handlungen aufgefordert werden, sollten Sie misstrauisch werden. Darüber hinaus sollten Sie ständig folgende Punkte im Hinterkopf behalten:

- Vertrauen Sie nicht darauf, dass Ihre Mails in jedem Fall ankommen. Vergewissern Sie sich, dass wichtige Mails den Empfänger auch tatsächlich erreicht haben.
- Denken Sie an den „Postkartencharakter“ von E-Mail.
- Vergessen Sie nicht das „Aufräumen“ der Festplatte, wenn Sie Mail über POP an einem PC gelesen haben, der nicht Ihr eigener ist.
- Ziehen Sie das Verschlüsseln vertraulicher Nachrichten in Erwägung.
- Teilen Sie in Mails an die Benutzerberatung niemals Ihr Passwort mit (auch dann nicht, wenn Sie dazu aufgefordert werden!).

Bert Wendland
bert.wendland@rz.hu-berlin.de