Internet

Ein gewisser Schutz muss sein

Intimsphäre auf dem Web – na denkste! ... oder gibt es sie doch?

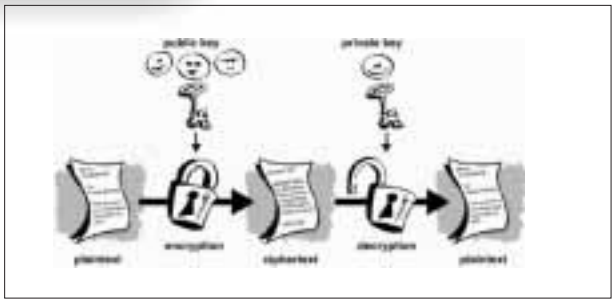
Es geht nicht darum, Paranoia zu schüren, und sicher auch nicht darum, Kinderpornographen in obskuren Chatrooms das Leben zu erleichtern. Doch wer denkt: «Verschlüsselung, brauche ich nicht, was ich schreibe, kann jeder lesen!», der ist nicht nur blauäugig, sondern schreibt vermutlich auch nur Postkarten und keine Briefe. Wer hingegen zu jenen Internet-Benutzern zählt, die E-Mail nicht nur für unverfängliche Korrespondenz nutzen, sondern auch, um z.B. mit seinem Treuhänder in Vaduz neue Anlagestrategien auszutauschen oder mit seiner Mätresse ein Schäferstündchen zu vereinbaren, der wünscht sich sicher etwas mehr Schutz vor indiskreten Augen ... Doch Spass beiseite: Man darf nicht vergessen, dass der Weg einer E-Mail viel weiter ist, als man sich vorstellt. An jedem Knotenrechner, an dem sie vorbeikommt, ist der Text wenigstens dem Systemadministrator zugänglich (und auch ohne Spuren zu hinterlassen veränderbar!), von anderen Hackern ganz zu schweigen. Beim Übermitteln von Patientendaten muss zudem die ärztliche Schweigepflicht in jedem Fall gewahrt bleiben. Die Frage ist bloss: Wie? Das Thema tauchte kürzlich in verschiedenen Diskussionsforen wieder vermehrt auf. Anlass genug, sich mit der Funktionsweise des «Klassikers» in Sachen Wahrung der Intimsphäre zu befassen.

Thomas Vauthier
Th.vauthier@bluewin.ch

PGP steht für Pretty Good Privacy

Pretty Good Privacy («ziemlich gute Privatsphäre») oder PGP ist ein höchst effizientes Programm zum Verschlüsseln und Entschlüsseln von Daten. Es bietet ausserdem die Möglichkeit, Mails mit digitalen Unterschriften zu zertifizieren. Ursprünglich wurde das Programm von Philip R. Zimmermann, einem Computerprogrammierer aus Colorado, entwickelt. Bei herkömmlichen (symmetrischen) Verschlüsselungsverfahren wird ein einziger Schlüssel benutzt; sowohl zum Ver- als auch zum Entschlüsseln der Daten. Beim so genannten «Public-Key»-Verfahren wird dagegen ein erster Schlüssel zum Verschlüsseln und ein anderer Schlüssel zum Entschlüsseln benötigt. Der Schlüssel, mit dem verschlüsselt wurde, hilft nicht bei der Entschlüsselung und umgekehrt. Einer der beiden Schlüssel kann öffentlich bekannt gemacht werden. Damit haben andere die Möglichkeit, gezielt einer Person eine verschlüsselte Nachricht zu senden, die nur diese Person entschlüsseln kann. Ausserdem lässt sich so die digitale Unterschrift einer Person anfertigen und verifizieren. Damit wird jede E-Mail dank PGP quasi zu einem «eingeschriebenen Brief», den niemand indiskret öffnen oder gar manipulieren kann.

Bis vor kurzem durfte die amerikanische PGP-Version nicht exportiert werden (also auch nicht von einer amerikanischen Website geholt werden!). Es gibt jedoch ein Reihe von internationalen Versionen, die legal ausgeführt wurden, die zwar keine «offiziellen» Versionen sind, aber die volle Funktionalität und



Kompatibilität von PGP bieten. Entgegen anders lautenden Gerüchten ist die Verwendung von PGP in den meisten Ländern Europas absolut legal.

Und wie funktioniert es?

PGP ist ein «öffentliches Schlüsselsystem» (public key cryptography). PGP generiert zwei «Schlüssel», die nur dem Benutzer gehören. Einer der PGP-Schlüssel ist der GEHEIME Schlüssel und bleibt auf dem Rechner des Absenders. Der andere Schlüssel ist ÖFFENTLICH. Dieser öffentliche Schlüssel kann allen Empfängern per E-Mail zugestellt werden. Diese können den öffentlichen Schlüssel in ihrer PGP-Software speichern. Einer der Vorteile von PGP ist, dass man diesen Schlüssel weitergeben kann, wie seine Telefonnummer. Wer die Telefonummer seines Korrespondenten hat, kann ihn zwar anrufen; aber sein Telefon nicht abheben. Dafür ist der geheime Schlüssel zuständig ...

Es gibt Versionen für DOS und Windows, ebenso für Macintosh, Unix etc. Diese Versionen von PGP sind untereinander kompatibel, und somit ist ein mit PGP unter DOS verschlüsseltes Dokument von jemanden lesbar, der PGP auf seinem Mac oder unter Unix einsetzt.

Wie sicher? Wie teuer?

Hervorragende Kryptoanalytiker und Computerexperten haben vergeblich versucht, PGP zu knacken. Wer auch immer nachweist, dass er PGP enträtselt hat, wird schnell zu Ruhm unter den Kryptographen kommen. Er wird viel Beifall ernten und eine Menge Geld angeboten bekommen. Und weil das Internet absolut transparent ist, würden es die PGP-Programmierer sofort bekannt geben.

Die PGP-Versionen, die man auf verschiedenen Web-Servern findet, sind «Freeware». Das bedeutet, sie sind absolut gratis!

Downloads und ausführliche Erklärungen zu PGP-gibt es unter anderem unter:
www.pgi.org/ oder
http://www.helmbold.de/pgp/ oder
www.uni-mannheim.de/studorg/gahg/PGP/HANDBUCH/

Fortsetzung folgt...