

Verschlüsseln – Ich?!

.:ToXiC:.

2. Januar 1999

Zurück in die Zukunft!

Endlich, der Schritt in die Zukunft ist getan - nun habe ich endlich meine eigene Email-Adresse. Endlich kann ich mit anderen Menschen durch die internationalen Datennetze kommunizieren! Nur leider, verschickt jeder im Datennetz nur Postkarten – jeder Postbote im unendlichen Datennetz kann diese Postkarte lesen, nach bestimmten Begriffen durchsuchen und dann auch auswerten.

1984 ist nicht weit.

Ist unverschlüsselte Email wirklich so unsicher?

Durch Internet verschickte Daten werden in den seltensten Fällen direkt von Rechner zu Rechner geschickt – meistens wird die Nachricht über viele Zwischenrechner geschickt. Auf jedem Zwischenrechner kann die Nachricht sowohl geändert, als auch mitgelesen werden.

Mit Sicherheit werden insbesondere im internationalen Datenverkehr Email automatisiert nach Schlüsselbegriffen durchsucht. Der hierbei betriebene Aufwand ist äußerst gering: Ein Rechner geschickt plaziert, guckt sich alle Emails an, und speichert sie einfach mit bestimmten Schlüsselbegriffen ab. Alle paar Tage oder Wochen kann die ganze Sache dann ausgewertet werden. Jemand der die Begriffe „radikal“, „Waffenlieferung“ und „Mossad“ verwendet, bleibt sicherlich in einem der internationalen Mailfilter „stecken“.

Warum ausgerechnet PGP?

PGP ist für die Verschlüsselung von Email sehr gut geeignet, es gilt als sehr sicher und da viele PGP einsetzen gilt es de facto als Standart für Verschlüsselung im Internet. Es ist einfach zu bedienen (wenn man´s mal kapiert hat) und ist umsonst verfügbar.

Wie funktioniert PGP?

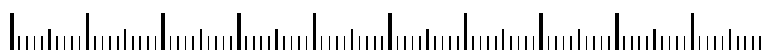
PGP verwendet ein sogenanntes asymmetrisches Verschlüsselungsverfahren – jeder Benutzer erzeugt sich mit PGP ein Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel. Email oder Dateien die mit dem einem Schlüssel verschlüsselt worden sind, können nur mit dem jeweils anderen Schlüssel wieder entschlüsselt werden – auch ist es nicht möglich aus einem Schlüssel den anderen zu berechnen.

Verschlüsseln:

Will man eine Nachricht verschlüsseln, verschlüsselt man diese mit dem öffentlichen Schlüssel des Empfängers, den dieser z.B. auf einer Internetseite zum runterladen bereitgestellt hat. Der Empfänger hat den passenden geheimen Schlüssel (den natürlich nur er selbst besitzt) und kann die Nachricht deshalb wieder „zurückrechnen“. So geht die Nachricht verschlüsselt durchs Netz.

Unterschreiben:

Angenommen ich möchte nun eine Email unterschreiben, kann ich sie einfach mit meinem geheimen Schlüssel verschlüsseln – Da nur ich diesen (geheimen) Schlüssel besitze, kann der Empfänger die Mail mit meinem



öffentlichen Schlüssel entschlüsseln und hierdurch mit Sicherheit sagen, daß die Email / die Datei von mir stammt. – Allerdings vorausgesetzt, daß er sicher ist, daß der öffentliche Schlüssel, den er hat, auch wirklich von mir ist.

Wo bekomme ich PGP?

PGP ist so weit verbreitet, daß es in vielen Mailboxen und im Internet ohne Probleme gefunden werden kann – Einfach PGP und DOWNLOAD in eine Suchmaschine eingeben und sofort werden Tausende von Seiten aufgelistet.

PGP wird auch immer wieder auf CD-ROMs die Computerzeitschriften beiliegen draufkopiert. Auch viele Provider legen es ihrer Zugangssoftware bei.

Das neueste ist gerade gut genug!?

Mittlerweile sind im Internet auch die Versionen 5.xx und 6.xx zum Download verfügbar – allerdings heißt neuer nicht unbedingt besser. Gerade bei diesen Versionen kann es Schwierigkeiten geben, wenn mit unterschiedlichen Versionen hantiert wird.

Mit Version 2.6.3i gibt es diese Probleme sicherlich nicht.

Wir empfehlen die Version 2.6.3i, die auf (fast) allen Betriebssystemen verfügbar ist. Auch sind für diese Version viele grafische Frontends verfügbar.

Das Web of Trust...

Die Idee mit öffentlichem und privatem Schlüssel hat auch so seine Probleme – wenn sich zwei Menschen noch nie begegnet sind, und sich gegenseitig ihre öffentlichen Schlüssel schicken, dann könnte jemand, über den die Kommunikation der beiden hin und her läuft (z.B. ein Systemadministrator), eine sogenannte „Man in the middle attack“ durchführen – auch dies wurde von den PGP-Machern bedacht. Schlüssel können unterschrieben und bestimmte Vertrauensparameter zugeordnet werden. – Zum Beispiel kann ich jemandem Vertrauen, der mir seinen PGP-Key auf Diskette gegeben hat. Diesen Schlüssel kann ich unterschreiben und „sicher“ sein, daß dieser Schlüssel auch wirklich von ihm ist.

So bildet sich ein sogenanntes **Web of Trust**, bei dem jeder anderen vertraut oder eben nicht. Schlüssel unterschreiben ist bei den neueren Versionen von PGP (5.xx oder 6.xx) nicht so gut möglich. Außerdem gibt es die Möglichkeit des „Key Recovery“ – also das Entschlüsseln einer Nachricht, für die ich den Schlüssel gar nicht habe. So soll z.B. ein Chef die Mail mitlesen können, oder falls der Angestellte vom Auto überfahren wird, die Mail wieder entschlüsseln. Dies sind natürlich Möglichkeiten die *nicht unbedingt gewünscht* sind.

Surfen & Telnet

Natürlich gibt es nicht nur Email im Internet – auch andere Daten gehen einfach ganz ungeniert und unverschlüsselt durchs Netz. So „surft“ z.B. niemand wirklich anonym. Meist (oder vielmehr: **fast immer**) wird die Rechneradresse gespeichert, von der eine Seite abgerufen wird. Lediglich Verbindungen mit SSL werden verschlüsselt übertragen. Leider wird dieser (auch nicht ganz sichere) Dienst fast nur für Bezahlungen mit Kreditkarten oder ähnlichem genutzt.

Auch andere Dienste sind meist nicht verschlüsselt. Der wichtige Dienst „Telnet“, über den man sich in andere Rechner einloggen kann, wird immer unverschlüsselt übertragen. Hierfür gibt es mittlerweile eine gute Alternative: SSH – die Secure Shell. Mit Terminalprogrammen wie CRT oder Tera-Term kann dieser Dienst auch unter Windoze 9x genutzt werden. Von unverschlüsselten Telnetverbindungen ist unbedingt abzuraten!

Weitere Informationen

Weitere Infos findet ihr bei [<http://pgp.squat.net>]

Mail an: toxic@squat.net

PGP Key fingerprint: EB 6E E2 AF A0 03 36 F3 31 AC 2D E8 52 10 5B 25

