

Big Brother is Reading Your E-Mail



Nehmen wir einmal an, Sie arbeiten in einer liechtensteinischen Bank und möchten einem Treuhänder in der Schweiz eine E-Mail zustellen. Diese Nachricht braucht dank der Datenautobahn nur wenige Sekunden bis zum Treuhänder, passiert währenddessen jedoch Server und Leitungen von vier bis sechs oder mehr Firmen.

Wussten Sie, dass jede dieser Firmen diese Nachricht lesen kann?

Wäre der Treuhänder in Florida oder Singapur, würde Ihre E-Mail wahrscheinlich zehn oder mehr Firmen durchqueren, von denen alle die Nachricht mitlesen könnten. Dank der einfachen Belauschbarkeit stehen heute in Amerika bei vielen Providern und Datenknoten «Carnivores» – Fleischfresser – der Regierung, welche alle Daten automatisch nach beliebigen Mustern durchsuchen. Ob es sich hier nur um «Terrorbekämpfung» oder eher um Wirtschaftsspionage handelt, dürfen Sie selbst spekulieren.

Auch wenn diese Kommunikation selten belauscht wird, ist allein die Tatsache, dass es möglich wäre, sehr bedenklich.

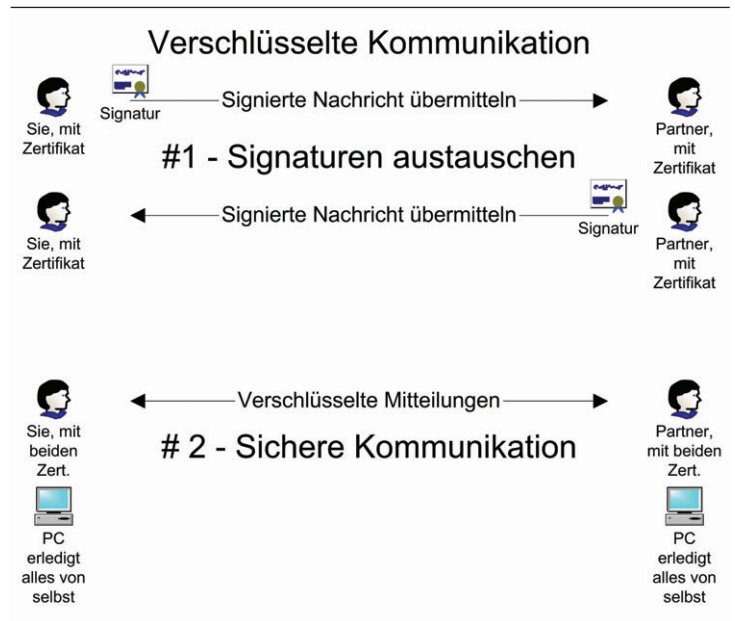
Wie übermittelt man denn vertrauliche Daten im Internetzeitalter? Zurück zur Diskette? Natürlich nicht! Denn dieses Problem

wurde schon vor langer Zeit gelöst und standardisiert. Fast alles, was Sie dazu brauchen, liegt schon lange brach auf Ihrem PC. Die von uns empfohlene Lösung basiert auf einer Verschlüsselung und Signierung mit Hilfe von digitalen Zertifikaten und einer Public Key Infrastructure. Was hier imposant klingt und mathematisch extrem kompliziert berechnet wird, ermöglicht (nach korrekter Einrichtung) absolute Sicherheit mit wenigen Mausklicks.

Wie kann es eingesetzt werden?

Die Vorgaben sind einfach: Beide Parteien brauchen ein digitales Zertifikat, welches im Outlook oder einem anderen Mailprogramm installiert wurde.

Zuerst senden sich beide Parteien gegenseitig ein signiertes E-Mail. Dieses E-Mail ist nicht verschlüsselt, sondern enthält eine elektro-



From	Subject
Zert2 2Sic	Dies ist eine verschlüsselte Nachricht
Zert2 2Sic	Dies ist eine signierte Nachricht

nische Unterschrift, die den Absender identifiziert. Dadurch werden im Hintergrund automatisch verschiedene Datenschlüssel ausgetauscht. Ein signiertes E-Mail erkennt man im Outlook anhand der roten Schleife neben dem E-Mail. Aufwand: ein bis zwei Minuten.

Danach kann jedes E-Mail zwischen diesen beiden Parteien ver-

schlüsselt werden. Sobald der Absender das Mail zur Verschlüsselung kennzeichnet, wird es automatisch so codiert, dass es Tausende von PC-Jahren brauchen würde, um den Code zu entziffern. Eine verschlüsselte E-Mail erkennen Sie an der blauen Schleife im Outlook. Mehraufwand: Zehn Sekunden (fünf Mausklicks).



>> www.2sic.com

Wie sicher ist es?

A: Sehr sicher. In einem Experiment (mit über 300'000 PCs) brauchte das Decodieren einer kurzen Nachricht umgerechnet 85'145 PC-Jahre.

Mit welchen E-Mail Programmen funktioniert diese Verschlüsselung?

A: Auf praktisch allen aktuellen Programmen wie Outlook, Outlook Express, Netscape, Lotus Notes usw.

Werden auch Anhänge verschlüsselt?

A: Ja.



Churerstrasse 35
CH-9470 Buchs
Telefon: +41 81 740 52 99
Mail: info@2sic.com

Daniel Mettler
ist Geschäftsleiter
der 2sic Internet
Solutions GmbH
info@2sic.com