Elektronisches Briefgeheimnis

[3]E-Mail Privacy FAQ
by
Andre Bacard, Author of
Computer Privacy Handbook ("The Scariest Computer Book of the Year")
[FAQ Updated September 1, 1996]

Translated by [4]Lutz Donnerhacke to spread this knowledge. This translation is GPLed.
Last changes: 20.12.1996

Die geplante [5]Kryptoregulierung der Bundesregierung kann die Benutzung dieser Software für ILLEGAL erklären!

Dieser Text enthält einen nichttechnischen Überblick über mögliche Gefahren DEINER privaten eMail. Er stellt 2 Basisverfahren zum Schutz Deiner Privatsphäre vor. Ich habe ihn speziell für humorvolle Personen geschrieben. Diese (unveränderte) FAQ kann für den nichtkommerziellen Gebrauch frei verbreitet werden.

Kann jemand (unbemerkt) Deine eMail lesen?

Mit ziemlicher Sicherheit. Der größte Teil der eMail ist notorisch öffentlich. EMail ist wenig sicher und in den vielen Belangen deutlich gefährlicher als eine perönliche oder geschäftliche Nachricht per Postkarte zu versenden.

Wer kann unbemerkt Deine eMail lesen?

In einer _MacWorld_ Umfrage gaben etwa 25% aller befragten Geschäftleute zu, die Computerdateien, die eMail und die Voicemail ihrer Angestellten zu lesen. Diese 25% umfassen nicht die ungenehmigte eMailüberwachung. Als ich einen Geschäftführer einer Firma im Silicon Valley fragte, ob er eMail benutze, sagte er: "Um Gottes willen, Andre. Die Hälfte der Dummköpfe in meiner Firma können eMail ansehen. EMail ist wie eine Konferenzschaltung!"

Internet eMail -mit der sich diese FAQ befaßt- abzufangen, ist ein Kinderspiel. Eine typische eMail wandert durch viele Computer. Auf jedem dieser Computer hat man Zugriff auf Deine persönliche und geschäftliche Korrespondenz.

Es ist sicher, daß die Admins (von Hackern ganz zu schweigen) von Mailboxen, Instituten, kommerziellen Informationsdienstleistern und Internetprovidern Deine eMail lesen können. Natürlich werden die meisten Schnüffler abstreiten, derartiges zu tun, weil sie so weitermachen wollen. (... und weil es meistens strafbar ist. -LD)

Schützt mich mein Passwort nicht?

In seinem hervorragenden Artikel "Bosses With X-Ray Eyes" (Chefs mit Röntgenaugen) stellt Charles Piller eine _MacWorld_ Studie über Macintosh Software vor. Hier ist ein Auschnitt aus Pillers Zusammenfassung:

> "All the major electronic-mail and groupware products that combine messaging, file management, and scheduling (such as WordPerfect

Office) allow the network administrator to change passwords at any time, then read, delete, or alter any messages on the server. With few exceptions, network-monitor programs such as AG Group's LocalPeek, Farallon Computing's Traffic Watch II, and Neon Software's NetMinder, allow astute managers to read files transmitted over the net. In short, these tools are only slightly less invasive than others specifically designed for surveillance and used primarily on mainframe systems."

Alle großen eMail und Groupware Produkte, die den Nachrichtenversand, Dateiverwaltung und Terminplaner (wie bspw. WordPerfect Office) verbinden, gestatten es dem Netzwerkadmin, die Passworte jederzeit zu wechseln und danach beliebige Nachrichten auf dem Server zu lesen, löschen und zu verändern. Mit einigen wenigen Ausnahmen gestatten Netzwerküberwachungsprogramme wie LocalPeek (AG Group), Traffic Watch II (Farallon Computing) und NetMinder (Neon Software) den Admins, Dateien während der Übertragung über das Netz zu lesen. Kurz gesagt sind diese Programme beinahe ebensogut zur Überwachung geeignet, wie speziell entwickelte Überwachungssoftware in Mainframe Umgebungen.

Unix, Dos und andere Netzwerksoftware sind genauso leicht durch die Admins zu manipulieren. Wer hält Deinen Internetprovider oder jeden anderen Netzwerkadmin davon ab, Dein Passwort zu benutzen oder weiterzugeben?

Verschwindet meine eMail nicht, nachdem ich sie gelesen und "gelöscht" habe?

In vielen Fällen: NEIN! Viele Internetprovider und Netzwerkadministratoren "archivieren" (speichern) Deine ein- und ausgehende Mail auf Festplatten für sechs Monate oder mehr, obwohl Du glaubst, Deine Mail gelöscht zu haben. Wenn Dich jemand verklagt (bspw. in einer Scheidungsklage), könnte er oder sie Dich vorladen lassen und Deine alte Korrespondenz GELESEN haben. Natürlich können nichtberechtigte Schnüffler Dein Archiv auch aus anderen Gründen lesen.

Was motiviert einen Schnüffler?

Möglicherweise ist er ein Dieb, der die Firmenpläne oder Kundenlisten verkauft. Vielleicht ist es die Tratschtante aus dem Büro, die versucht Kollegen gegen Dich aufzubringen. Es kann auch ein verrückter Fan sein, wie der, der die Schauspielerin Rebecca Schaffer erschoß. Denkbar ist auch ein Erpresser. Ein altmodischer Voyeur ist auch nicht ausgeschlossen.

Information ist Macht. Schüffler wollen Macht.

Was soll's? Ich habe nichts zu verheimlichen. Wozu brauche ich geheime eMail?

Zeige mir Einen, der keine finanziellen, sexuellen, gesellschaftlichen, politischen oder geschäftlichen Geheimnisse vor seiner Familie, seinen Nachbarn oder seinen Kollegen versteckt und ich zeige Dir jemanden der ein außerordentlicher Exhibitionist oder ein unglaublicher Dummkopf ist.

Zeige mir eine Firma, die keine Firmengeheimnisse hat und ich zeige Dir ein Geschäft, das nicht läuft.

Robert Ellis Smith, der Herausgeber des _Privacy Journal_, witzelte: "Ein Angestellter, der nichts zu verheimlichen hat, hat nichts zu bieten."

Geheimhaltung, Diskretion, Vertraulichkeit und Besonnenheit sind die Markenzeichen dieser Zivilisation.

Einverstanden, ich will eMail geheimhalten. Was kann ich tun?

Es gibt zwei große, praktische Schritte, die Du tun kannst. Zuerst installiere PGP (Pretty Good Privacy), um Deine eMail und Deine Dateien zu verschlüsseln, so daß ein Schnüffler diese nicht lesen kann. PGP ist der de facto Weltstandard für eMail Geheimhaltung. Danach benutze anonyme Remailer, um in Newsgruppen zu posten oder Deinen eMailverkehr abzuhalten und um den Empfängern und Schnüfflern Deine wahre Identität und eMailadresse zu verheimlichen.

Wo kann ich mehr über diese Geheimhaltungssoftware erfahren?

Zwei wundervolle Startpunkte sind die Usenet Newsgruppen alt.security.pgp und alt.privacy.anon-server.

Noch etwas, was ich wissen sollte?

DEINE Privatsphäre und Sicherheit können gefährdert sein! Umfangreiche Banken-, Kreditkarten- und medizinische Datenbanken, eMail Überwachung und Computerschnüffelprogramme sind nur einige wenige Faktoren, die jeden gesetzestreuen Bürger treffen. Kurz gesagt, unsere in Privatsachen schnüffelnde Gesellschaft dient den Kriminellen und serviert Deine Daten auf einem Silbertablett.

Zurück zu [6]Bacard's Home Page

This page maintained by abacard@well.com
Übersetzungsfehler bitte an lutz@iks-jena.de