SECURITY
FACHARTIKEL

Freiwilliger Verzicht auf Privatsphäre

Wer unverschlüsselt E-Mails versendet, handelt fahrlässig. Das Mitlesen der elektronischen Post ist heute einfacher denn je. Abhilfe verschaffen einzig ausgereifte Verschlüsselungsprogramme und umsichtiges Handeln.

von Muris Bajrica

Über öffentliche Web-Konten wie GMX oder Hotmail wird fast ausschliesslich im Klartext gemailt. Warum sollte man verschlüsselte E-Mails versenden, fragen sich private User und Unternehmen weltweit. Darauf gibt es eine einfache Antwort: Weil somit die Privatsphäre und das Geschäftsgeheimnis am besten geschützt werden.

Die Wahrscheinlichkeit, dass ein Dritter die elektronische Post anderer mitliest, ist gross. Aufsehen erregende Fälle ausgeklügelter Wirtschaftsspionage beweisen: wer nicht chiffriert, wird ausgetrickst. Doch das Einlegen der E-Mail in ein Kuvert scheitert oft schon im Ansatz. Will man codieren, muss entsprechende Software heruntergeladen und installiert werden. Aber damit ist es nicht getan. Der User muss zusätzlich die Codes, sprich Schlüssel, in deren Besitz er sich fortan befindet, an seine Kontaktpersonen weitergeben. Und das machen die wenigsten Nutzer.

Die Verschlüsselung ist nach Expertenmeinung ein zukunftsträchtiges Betätigungsfeld. Während sich die Anwender auf der einen Seite der Gefahren und mangelnden Sicherheit des «Simple Mail Transfer Protocol» (SMTP) immer bewusster werden, stehen auf der anderen Seite die Händler und Service-Anbieter in den Startlöchern: Sie entwickeln derzeit wirksame, aber dennoch einfach zu nutzende Lösungen mit geeigneten Verschlüsselungsverfahren und Signatur-Lösungen. Die Trendforscher der Radicati

Group gehen davon aus, dass in der gesamten IT-Sicherheitsindustrie das Marktsegment Verschlüsselung in den kommenden vier Jahren am schnellsten wachsen wird.
Auf dem Softwaremarkt gibt es eine Vielzahl von Programme, die ein Kuvertieren, also Verschlüsseln, des elektronischen Briefes ermöglichen. Sie sind mehrheitlich ausgereift und bei optimaler Verwendung machen sie E-Mails für Bösewichte des Webs beinahe unknackbar. Sie versperren den Geheimdiensten, die sich nun – da der Kalte Krieg zu Ende ist – grossteils der Ausspionierung der Unternehmen widmen, die Sicht auf den Inhalt des Briefes. Und eines sollten alle Anwender wissen: bei E-Mail besteht kein Postgeheimnis. Es darf also mitgelesen werden. Somit ist die Strafbarkeit nicht gegeben.

PGP oder GNUPG?

Die meisten privaten Internet-Nutzer aber auch Unternehmen versenden ihre E-Mails im Klartextformat. Auf dem Weg zum Empfänger passiert die elektronische Post endlos viele Schaltstellen, so genannte Router. An solchen Schaltstellen können bestimmte Programme der Geheimdienste und Hacker in die Leitung eingreifen und den Inhalt des gesamten Mailverkehrs nach ganz bestimmten Kriterien durchsuchen.
Auch Netzwerkadministratoren haben ohne weiteres die Möglichkeit, den gesamten elektronischen Briefverkehr abzufangen und zu analysieren. «Der technische Aufwand, der eine Überwachung des E-Mailverkehrs ermöglicht, ist gar nicht so gross», sagt der Consult für den Bereich IT-Security der Frankfurter Börse, Rudolf Hartmann (siehe Interview).
Neuerdings werben auch kommerzielle Anbieter mit professioneller E-Mail-Spionagesoftware. Mit solchen Programmen wird nicht nur der E-Mail-Verkehr, sondern auch die gesamte Computerarbeit aufgezeichnet. «Da ist es fahrlässig, nicht zu verschlüsseln», warnt der Security-Beauftragte der Börsianer aus Frankfurt.
Doch wie schützt man sich vor bösen Blicken und Angriffen aus dem Netz? Um die digitale Post zu verschlüsseln, braucht der Absender ein Zertifikat des Empfängers. Dieses Zertifikat enthält alle öffentlichen Schlüssel, die in der Umgangssprache der versierten Computer-Anwender «Public Keys» heissen. Mit diesem Key wird die Nachricht verschlüsselt. Der Empfänger entschlüsselt die Nachricht mit seinem eigenen privaten Schlüssel, «Private Key», den niemand anderer sehen sollte.
Die bekanntesten Verschlüsselungsprogramme heissen PGP («Pretty Good Privacy») und GnuPG Privacy Guard. Beide Programme können kostenlos benutzt werden, wobei angemerkt werden muss, dass nur noch GnuPG-Software aus Deutschland als Open Source-Software gilt. Nachdem PGP übernommen worden ist, wird der Quellcode der Software nicht mehr bekannt gegeben.
Findige Programmierer des Sicherheitsanbieters Onaras aus Wettingen, die die User-Gewohnheiten kennen und auch um das wenig vorhandene Bemühen um Verschlüsselung wissen, haben ein Tool entwickelt, das eine Chiffrierung möglich macht, ohne dass der Empfänger aktiv werden muss. Mit Sepp, der Secure E-Mail Appliance, geschieht die Verschlüsselung der Nachrichten automatisch. Damit wird nach Angaben der Entwickler ein sicherer Versand von E-Mails gewährleistet.

Verschlüsseln bei Free-Mail.de und my-mail.ch

Jeder Anwender kennt sie: GMX, Hotmail und Co, die beliebtesten – aber nicht die besten – E-Mail-Dienste im Internet. Das Chiffrieren der eigenen Post ist den meisten webbasierten E-Mailanbietern ein Fremdwort. Mit zwei Ausnahmen: Free-Mail.de und my-mail.ch offerieren ihren Kunden den besonderen Schutz der Privatsphäre durch eine eigene Verschlüsselungstechnik.
Aber auch da gibt es viel zu beachten. Will man bei Free-Mail.de verschlüsseln, muss der Anbieter das Zertifikat des Empfängers kennen. Ist das nicht der Fall, muss der Empfänger eine signierte E-Mail an den Sender schicken. Deren Public Key wird gespeichert und steht fortan allen Free-Mail-Anwendern zur Verfügung.
Im Auswahl-Menü kann die Verschlüsselungsstärke ausgewählt werden. Innerhalb der Free-Mail-Oberfläche spielt die Verschlüsselungsstärke allerdings eine unbedeutende Rolle. Hat der E-Mail-Partner keine Free-Mail-Adresse oder kein E-Mail-Zertifikat, kann er im Trustcenter von web.de eine Signatur für seine E-Mail-Adresse beantragen.
Doch auch wenn den Anweisungen des Providers gefolgt wird, ist der Erfolg noch längst nicht garantiert. Bei unserem Testversuch, über Free-Mail.de codierte Post zu verschicken, scheiterten sämtliche Anfangsversuche. Die Post kam entweder unverschlüsselt an oder ein Hinweis wurde eingeblendet, dass das Chiffrieren gerade nicht möglich ist. Gerade auch aus diesem Grund sollte man vermeiden zu erleben, was einem Unternehmensanwalt passierte: «Ich wollte keine Geheimnisse des Unternehmens preisgeben, ich hatte nur meine E-Mail nicht verschlüsselt.» ■

Rudolf Hartmann

«Vorsicht bei Klartext – jeder kann mitlesen»

Rudolf Hartmann, Computerspezialist und Consult für den Bereich IT-Security der Frankfurter Börse im Gespräch mit ICT kommunikation.

ICT kommunikation

Herr Hartmann, worin besteht die grundlegende Gefahr beim E-Mail-Verkehr?

Rudolf Hartmann: Die grösste Gefahr besteht im viel zu sorglosen Umgang mit den Medien Internet und elektronische Post. E-Mails werden tatsächlich in überwiegender Zahl im Klartext gesendet. Dabei werden Meetings besprochen, Bestellungen aufgegeben und so weiter. Eine andere Gefahr besteht darin, dass nur noch wenige Staaten die Benutzung starker Verschlüsselung beschränken. Die meisten Länder haben auf verlangen der USA starke Chiffrierung freigegeben; auch die US-Regierung selber hat den Export starker Verschlüsselungsprogramme weitgehend liberalisiert. Das ist die so genannte kontrollierte Liberalisierung, die an

das Wassenaar-Abkommen von Dezember 1998 anlehnt, das keine Exportkontrollen mehr vorsieht für 64 Bit-Produkte, 56 Bit-Verschlüsselungskomponenten sowie 512 Bit-Schlüsselmanagement-Produkte.

Wer spioniert und warum?
Um den Verlust der Überwachungsmöglichkeiten durch den Gebrauch starker Verschlüsselung zu kompensieren, rüsten viele Staaten die Geheimdienste mit viel Geld und weitreichenden Rechten aus. Angemerkt sei hier die geplante Gesetzgebung Enfopol, «EU-Abhörstandards für die Telekommunikationsnetze», die das Belauschen europaweit erleichtern würde, da die Hersteller und die Betreiber von Kommunikationsanlagen technische Vorkehrungen zum Abhören einbauen müssten. Als Beispiele dienen der transatlantische Streit um das Lauschsystem Echelon und die möglicherweise betriebene Wirtschaftsspionage. Oder das Sorm-System des russischen Geheimdienstes, das einen direkten Zugriff auf die Server der Internetprovider zulässt.

Wem nutzen solche Infos?
Jedes Unternehmen sollte sich selbst die Frage stellen, warum es verschlüsseln sollte. Was nutzt es der Konkurrenz zu wissen, wie die Auftragslage aussieht oder die Bestellscheine ansehen zu können?

Wie gross ist der Aufwand, E-Mail abfangen zu können?
Die meisten Privatpersonen und Unternehmen versenden ihre E-Mail im Klartextformat. Diese Übertragung von E-Mail gleicht dem Versenden von Postkarten. Eine Mail erreicht ihr Empfänger-System nicht auf direktem Weg, sondern oft über eine Vielzahl anderer beteiligter Systeme. Bei jedem der beteiligten Server besteht prinzipiell eine Mitlesmöglichkeit. Bei der heute meist üblichen Netzwerkstruktur werden Datenpakete an alle angeschlossenen Rechner übermittelt. Normalerweise filtert der Rechner nur die Datenpakete, die an ihn adressiert sind. Wird der Rechner im so genannten Promiscous-Mode betrieben, ändert sich das: Nun werden alle Datenpakete empfangen. Jeder im gleichen Netzwerk-Segment kann an diese Informationen kommen. Und an solchen Stellen können bestimmte Sniffer-Programme angesetzt werden. Bei E-Mail könnten «Generelle Angriffe», also Grossangriffe gestartet werden, bei denen alle E-Mails abgefangen und die Briefköpfe (Header) nach bestimmten Empfängern und Domains analysiert werden.

Macht man sich strafbar, wenn man E-Mails abfängt und mitliest?
Ich glaube, das Gleichnis «Vor meinem Fenster schreit jemand seine EC-Pin heraus, und wenn ich das Fenster öffne, kann ich ihn verstehen» trifft es am ehesten. Die Kenntnisnahme solcher Daten ist nicht verboten, das Verwenden der Information allerdings schon.

Wie sollte man der E-Mail-Spionage vorbeugen?
Der Quasi-Standard gegen Mail-Spionage heisst Pretty Good Privacy (PGP) und ist so sicher, dass der Krypto-Rebell Philip Zimmermann, der geistige Vater von PGP, in einigen Ländern hinter Gittern muss. Zwei Jahre nach der Einführung des Sicherheitstools leitete das FBI ein formelles Ermittlungsverfahren gegen ihn ein, weil er sich bis heute weigert, eine Hintertür in das Programm einzubauen, mit der der Staat auch PGP-geschützte E-Mails entschlüsseln kann.
Auch mit GnuPG kann man sich schützen. Das Programm ist ein vollwertiger PGP-Ersatz und entspricht weitestgehend dem OpenPGP-Standard RFC 2440. GnuPG bringt in Bezug zu PGP einige Verbesserungen, Erweiterungen und zusätzliche Sicherungsmechanismen mit sich. Es ist ein vollständiger und freier Ersatz für PGP. Es benutzt den patentierten IDEA-Algorithmus nicht und kann deswegen ohne Einschränkungen benutzt werden. GnuPG ist eine RFC-2440-(OpenPGP) kompatible Anwendung

Wie funktioniert das Prinzip von GnuPG?
Bei GnuPG-Public-Key-Verfahren (auch: asymmetrischen Verfahren) besteht der Verschlüsselungscode aus zwei Teilen: einem öffentlichen Schlüssel (Public Key) und einem geheimen Schlüssel (Private Key). Der geheime Schlüssel bleibt im Besitz des Senders, er darf nicht übermittelt werden. Der Public Key wird mit Hilfe von frei zugänglichen Keyservern veröffentlicht und damit allen Kommunikationspartnern zugänglich gemacht. Der Sender verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Empfängers. Entschlüsselt wird die Nachricht dann mit dem privaten Schlüssel des Empfängers. Nur mit beiden Schlüsseln, dem öffentlichen und dem geheimen, und einem Passwort kann der berechtigte Empfänger die Mail wieder entschlüsseln.

Wieso sollte mich jemand angreifen?
Auch auf einem Heim-PC lagern häufig sensible Daten. Das sind etwa Anmeldename und Passwort des Internetproviders, mit denen ein Angreifer unter Umständen kostenlos surfen könnte. Noch interessanter sind Daten für das Online-Banking. Einige Anwender speichern in ihren Programmen nicht nur die Kontonummer, sondern auch PIN (Personal Identification Number) und TAN (Transaktionsnummer), also alles, was für eine Überweisung nötig ist. Besonders begehrt sind auch die Visa- oder Eurocard-Nummern. Mit Namen des Inhabers und dieser Nummer können Hacker im Internet auf dessen Kosten einkaufen. Zum anderen interessieren sich Hacker für den Heim-PC, um diesen als Ausgangsbasis für neue Angriffe auf andere Rechner zu benutzen. Einige wollen aber auch «nur» fremde Mails lesen und versenden oder einfach nur herumspionieren. ■