Sichere Mailverschlüsselung ohne Umtriebe

Das Ciphire-Verfahren ist alltagstauglich und funktioniert mit jeder E-Mail-Software / Ein erfolgversprechender Alleingang

Eigene Nachrichtenverschlüsselung über das Internet ist stets mit Umtrieben verbunden. Die Sendung muß man eigens chiffrieren und signieren, bevor man sie wegschickt. Umgekehrt kommt zunächst Unlesbares herein. Da fühlt sich das E-Mail-Chiffrierverfahren von Ciphire einfach an wie eine Tür, die beim Zumachen von selbst ins Schloß fällt. Dabei ist es sicher und gar nicht so unkompliziert. Dreißig Leute haben drei Jahre lang in München daran gebaut, sagt uns der Gründer und Chef Erikkos Pitsos. Herausgekommen ist ein kleiner Knüller, den es für Private zudem kostenlos gibt.

Ciphires Software richtet sich in Windows 2000 und XP, Linux oder auf dem Apple-Betriebssystem Mac OS X in den gängigen E-Mail-Systemen ein, von Outlook über T-Online bis Pegasus. Es arbeitet mit den Mailprotokollen Pop3, SMTP und Imap und verschlüsselt jede ausgehende Nachricht an einen anderen Ciphire-Nutzer. Die restlichen Mails bleiben unangetastet. Sie werden nur zusätzlich digital signiert, ohne daß man Schlüssel oder Schlüsseltext zu sehen bekäme. Hereinkommende Post landet wie gehabt im Eingangskorb, fix und fertig entschlüsselt, falls sie von einem „Ciphireisten" kam. Unterwegs im Internet sind die verschlüsselten Nachrichten, was auch immer sie enthalten, reiner Buchstabensalat. Für den Nutzer ändert sich bei der Handhabung seines E-Mail-Programms nichts. Ciphire läuft im Hintergrund. Verzögerungen beim E-Mail-Versand bemerkten wir keine. Einzige sichtbare Auswirkung für den Nutzer sind kleine Zusätze in der Betreffzeile: In einer sicher empfangenen Nachricht findet sich ein „CIPHIRED" für „chiffriert gewesen", selten ein „SIGNED" für „signiert", meist noch das „U" für „unchiffriert".

Moderne digitale Verschlüsselungsverfahren arbeiten mit asymmetrischen, paarigen Schlüsseln: Den einen gibt man zum Beispiel auf seiner Website bekannt, damit er von jedermann zum Verschlüsseln genutzt werden kann; entschlüsseln läßt sich die Nachricht dann nur mit dem anderen, vom Empfänger bestens gehüteten Schlüssel. Aus dem öffentlichen Schlüssel ist der private nicht zu errechnen. Im Unterschied zu gängigen Chiffrierverfahren erzeugt und verwaltet die Ciphire-Software alle benötigten Schlüssel selbsttätig: den privaten auf dem eigenen Rechner, den öffentlichen auf dem Ciphire-Server im Internet. Ausgefeilte und schnelle Algorithmen sichern, daß auch ganz gewiß der richtige und gültige Schlüssel des Empfängers verwendet wird und keiner so tut, als sei er von Ciphire autorisiert.

Bei älteren Verfahren, etwa dem verbreiteten Pretty Good Privacy (PGP), müßten eigentlich vor jedem Mailversand über eine getrennte, sichere Verbindung zumindest die digitalen Fingerabdrücke der Schlüssel verglichen werden, was keiner tut. Vor allem macht PGP oder die vom Bundeswirtschaftsministerium geförderte Variante Gnupp immer extra Aufwand bei Sender und Empfänger, etwa Auswahl des Dokuments, Paßworteingabe und Schlüsselwahl bei jedem Ver- oder Entschlüsseln. Gewöhnliches, kostenloses PGP verschlüsselt im Gegensatz zu „Ciphire" keine Bilder, und formatierte Word-Dateien kommen unformatiert an. Allerdings können mit PGP Nachrichten und Texte mitbenutzersicher chiffriert auf dem Rechner liegenbleiben. Denn bei diesem Verfahren bleibt die E-Mail so lange verschlüsselt, bis der Nutzer die E-Mail lesen will. Dazu kann er auch offline sein. Ciphire hingegen ver- und entschlüsselt nur online und legt die E-Mails sofort unchiffriert in den Posteingang.

Wir haben die Ciphire-Software, etwas mehr als sieben Megabyte, von Ciphire.com geladen und installiert. Man muß angeben, für welche E-Mail-Adresse man die Verschlüsselung einrichten will. Das Konto wird von Ciphire online automatisch überprüft, um sicherzugehen, daß auch der Besitzer der E-Mail-Adresse am anderen Ende der Leitung sitzt. Erst dann kann mit der Installation weitergemacht werden.

Das Mailprogramm kann nach einem Rechnerstart nur mehr mit dem selbst gewählten Ciphire-Kennwort betreten werden. Das gibt persönlich Sicherheit, verhindert aber andererseits, daß der Rechner morgens ganz selbsttätig hochläuft. Deinstallieren sollte man Ciphire auch nicht, ohne sich vorher ordentlich abzumelden, läuft man sonst doch Gefahr, von seinen „sicheren" Korrespondenten weiterhin verschlüsselte Nachrichten zu bekommen, die dann niemand mehr lesen kann. Nutzt man weitere Rechner, einen Laptop unterwegs, so wird zuvor das eigene Zertifikat auch dorthin übertragen. Sicherheitsfanatiker, was willst du mehr? Gelegentlich unsicher die eigene Mail lesen, das geht bei Ciphire nicht – aber auch nicht bei PGP. So bekommen Online-Mailprogramme im Netz, sogenannte Webmailer, die man schnell einmal in einem Internet-Café aufsucht, nur Unlesbares anzuzeigen – klar, die Nachricht ist ja verschlüsselt. Blackberrys, an die verschlüsselte Mail weitergeleitet wird, bedauern, überhaupt keinen Inhalt deuten zu können. Dann muß man entweder den (erkennbaren) Absender bitten, ausnahmsweise noch einmal unverschlüsselt zu senden, oder bis zu Hause auf den Nachrichteninhalt warten. Wir haben uns einfach eine extra E-Mail-Adresse gemacht, die allein verschlüsselt wird. Wer will, kann uns da dann über „Nummer Sicher" erreichen.

Das vom Ciphire-Team entwickelte neue und dabei noch schnelle Fingerabdruck-System zur Schlüsselüberprüfung – für den Nutzer unsichtbar – läßt nicht einmal Ciphire-Mitarbeiter selbst auf deren zentralem Rechner Kundenschlüssel manipulieren, ein Novum für öffentliche Schlüsseldienste und Zertifikatsaussteller.

Für Unternehmen will Ciphire zentrale Verschlüssler (Gateways) an der Grenze in die offene Internetwelt bauen. Webmail-Programme werden, wenn die Ciphire-Idee einschlägt, und das wird sie, dafür einen Schlüsselzusatz brauchen. Der Durchbruch ist geschafft, wenn sich Ciphire-verschlüsselte E-Mails problemlos auf Web.de, GMX oder Gmail lesen lassen. FRITZ JÖRN