Internet Corner

Sprechen Sie Kryptisch?

E. Gysling

Nein: eine Sprache ist die Kryptographie nicht wirklich. Das Verschlüsseln ist jedoch gerade für Angehörige der medizinischen Berufe von allerhöchster Bedeutung, wenn man nicht auf die elektronische Übermittlung (und Aufbewahrung) von vertraulichen Daten ganz verzichten will. Deshalb komme ich auch schon wieder – nachdem wir erst im letzten September über «Pretty Good Privacy» (PGP) berichtet haben – auf dieses Thema zurück.

Die Erfahrung zeigt nämlich, dass PGP erst dann gut und schnell anwendbar ist, wenn unsere Korrespondenzpartnerinnen und -partner wirklich alle auf dieses System eingespielt sind und auch mitmachen. Diese Voraussetzung ist zum heutigen Zeitpunkt in der Schweiz noch nicht gegeben. Zudem handelt es sich bei PGP um ein Programm, mit dem man sich doch mit einem gewissen Aufwand vertraut machen muss. Wir haben uns verlagsintern nochmals damit befasst und können grundsätzlich bestätigen, dass PGP zuverlässig und – mit einiger Übung – ohne Mühe angewandt werden kann.

Dennoch stellt sich die Frage, ob allenfalls «einfachere» Alternativen zur Verfügung stehen. Vielen ist die Verschlüsselungstechnik bekannt, die vom *Health-Info-Net* (HIN; http://www.hin.ch) verwendet wird. Hier liegt das hauptsächlichste Problem darin, dass die Verschlüsselung nur innerhalb des HIN funktioniert. Wenn ich daher aus diesem System heraus mit Personen oder Institutionen korrespondiere, die nicht am HIN teilnehmen, so geht die Verschlüsselung verloren, sobald der geschlossene Kreis des HIN verlassen wird.

Von einer wirklich einfachen Lösung kann nur gesprochen werden, wenn es mir möglich ist, auch dann eine verschlüsselte Meldung zu übermitteln, wenn ich lediglich die (beliebige) E-mail-Adresse einer Person kenne. Eine solche Lösung existiert, allerdings nicht gratis. ZixMail (http://www.zixmail.com) erlaubt mir, Mails oder Attachments zuverlässig auf meinem Computer zu verschlüsseln und zu versenden. Selbstverständlich kann man die Mail (wie in PGP) auch mit einer Signatur versehen, die als garantierte Absenderadresse dient. Geht die Mail an eine Adresse, von der ich weiss, dass sie auch dem ZixMail-System angeschlossen ist, funktioniert alles besonders einfach. Andernfalls geht es aber auch, ich wähle dann die Zustellart «SecureDelivery», die der Empfängerin oder dem Empfänger ermöglicht, die verschlüsselte Nachricht via Web abzuholen. Im Ganzen habe ich den Eindruck gewonnen, es handle sich um ein vergleichsweise einfaches und gutes Verfahren, das den Preis von $ 24 pro Jahr wert ist.

Ähnlich funktioniert Certifiedmail (http://www.certifiedmail.com); diese Software ist für den persönlichen Gebrauch gratis. Ein kleiner Nachteil: die Mail muss auf alle Fälle via Web abgeholt werden.

Es gibt noch verschiedene andere Systeme für «sichere» Mails. Ein Artikel, der zu diesem Thema weitere Informationen vermittelt, findet sich in einer kürzlich veröffentlichten Nummer des PC Magazine: http://www.zdnet.com/products/stories/reviews/0,4161,2669357,00.html.

Die Schlussfolgerung lautet jedenfalls: es gibt heute keine Entschuldigung mehr – vertrauliche Daten können und sollen verschlüsselt übermittelt werden.

Korrespondenz:
Infomed-Verlags-AG
Blumenaustrasse 7
CH-9500 Wil

infomed@infomed.org

Aus: infomed-screen 2001;3(5):24.