

(Elektronischer) Brief und (digitales) Siegel

Christoph Becker, KIM, Security Manager

Wissen Sie genau, von wem die E-Mails in Ihrem Posteingang tatsächlich stammen? Ganz sicher kann man sich ja nie sein, oder? Das zeigt uns unsere Erfahrung mit dem E-Mail-System, denn die meisten haben schon einmal E-Mails bekommen, die angeblich von unserer Bank, einem Inkassounternehmen oder einem alten Schulfreund sein sollen. In den meisten Fällen können wir einen Täuschungsversuch von einer authentischen E-Mail unterscheiden, denn bewusst oder unbewusst prüfen wir die Absenderkennung, den Betreff und den Inhalt, einschließlich deren Links und Anhänge. Aber vielleicht mussten Sie auch schon einmal feststellen, dass die Bewertung der Echtheit einer E-Mail nicht immer so leicht fällt.

Jetzt versetzen Sie sich in die Lage Ihrer Kommunikationspartner. Glauben Sie, dass Ihr Gegenüber immer genau wissen kann, dass E-Mails in Ihrem Namen tatsächlich auch von Ihnen stammen? Eigentlich ebenso wenig, denn E-Mails können in fremden Namen gesendet werden - und das passiert täglich milliardenfach im Internet und ist die Grundlage von Spam und Phishing-Mails.

Mit einer digitalen Signatur Ihrer E-Mail könnte Ihr Kommunikationspartner erkennen, dass diese mit an Sicherheit grenzender Wahrscheinlichkeit tatsächlich von Ihnen stammt und unverändert ist.

In nur drei einfachen Schritten werden zukünftig alle Ihre ausgehenden E-Mails automatisch von Ihrem E-Mail-Client elektronisch signiert.

Die Grundlage dafür ist ein persönliches Zertifikat, welches Sie beim Deutschen Forschungsnetz (DFN) im ersten Schritt beantragen. Nach dem Erhalt des Zertifikats im zweiten Schritt installieren Sie es im dritten Schritt in Ihrem E-Mail-Programm (z.B. Thunderbird, Outlook oder AppleMail) und konfigurieren Ihren E-Mail-Account zur Verwendung des Zertifikats. Senden Sie nun eine E-Mail, erzeugt Ihr E-Mail-Programm von sich aus eine elektronische Signatur und fügt diese an. Die meisten E-Mail-Programme können die Signatur auch automatisch verifizieren. Dann weiß Ihr Kommunikationspartner, dass tatsächlich auch nur Sie diese E-Mail abgesendet haben konnten und das Problem, nie genau zu wissen, von wem die E-Mails in unserem Posteingang tatsächlich stammen, ist gelöst. Ganz nebenbei kann Ihnen danach Ihr Kommunikationspartner verschlüsselt antworten und somit sensible Inhalte übermitteln, die ausschließlich auch nur Sie lesen können sollen. Denn in einer signierten E-Mail senden Sie Ihr Zertifikat mit, welches Ihr Kommunikationspartner für eine digitalen Verschlüsselung benötigt. Einfache Anleitungen zu den drei Schritten finden Sie auf unserer Homepage¹.

Fußnote

¹ <http://www.kim.uni-konstanz.de/email-und-internet/it-sicherheit-und-privatsphaere/e-mail-sicherheit/>