„Sie haben **Post**!“

Einige deutsche Provider haben die Initiative **„E-Mail Made in Germany“** ins Leben gerufen. Experten fordern eine Ende-zu-Ende Verschlüsselung. Was steckt hinter all dem?

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Die sichere Nutzung von E-Mails hat mehrere Dimensionen. Zum einen ist in diesem Zusammenhang die Art der Übertragung zu nennen, aber auch die Nutzung durch den Anwender.

Spam haben Sie bestimmt schon mal erhalten. Zumeist ist er harmlos und wird immer effizienter ausgefiltert. Wenn Sie sogenannte **„Phishing Mails“** bekommen, müssen Sie allerdings aufmerksamer sein. Das sind oft gut gemachte Fälschungen echter Firmenkommunikation, um an geheime Informationen wie Zugangsdaten oder Kreditkarteninformationen zu kommen. Sie können diese oftmals an leicht abgewandelten Absender-Domänen erkennen, einer unpersönlichen Ansprache sowie an grammatikalischen Fehlern. Enthaltene Hyperlinks sollten Sie nicht anklicken, beigefügte Dateianhänge nicht öffnen. Diese Vorsichtsmaßnahmen schützen im Zweifel Ihre Daten.

Die von Ihnen geschriebenen E-Mails sind im Prinzip aber immer noch durch Dritte lesbar.

„Verschlüsselung“: Das Siegel „E-Mail Made in Germany“ drückt aus, dass eine E-Mail, die Sie von Ihrem E-Mail Account an einen Empfänger senden, dessen elektronisches Postfach ebenfalls bei einem die Initiative unterstützenden Anbieter liegt, beim Transport von Anbieter A zu Anbieter B verschlüsselt wird. Im Ergebnis ist die E-Mail während der Übertragung geschützt, der Inhalt weiterhin im Klartext auf dem Server des Anbieters vorhanden. Liegt das Postfach eines Adressaten aber bei einem anderen Anbieter, ist die E-Mail auch während der Übertragung nicht gegen Zugriff oder sogar Manipulation durch Dritte geschützt.

Zusätzlich zu betrachten ist, wie die E-Mails vom und zum Anbieter gelangen. Nutzen Sie ein E-Mail Verwaltungsprogramm (z. B. Microsoft Outlook oder Mozilla Thunderbird), können Sie hier ebenfalls eine Absicherung während der Übertragung für Versand und Empfang konfigurieren – sofern vom Anbieter unterstützt. Anleitungen, oft in Verbindung mit dem Begriff „TLS“/„Transport Layer Security“ (deutsch etwa: Transportschichtsicherheit), finden Sie auf den Internet-Seiten der Anbieter.

Stichwort Internet-Seite: Oftmals haben große E-Mail-Anbieter auch sogenannte Web-Frontends, mittels derer Sie auf Ihre E-Mails zugreifen und neue versenden können. Hier bieten mittlerweile eigentlich alle Anbieter nur noch gesicherten Zugriff an, was Ihnen ein in der Adressleiste des Browsers voran gestelltes „https“ signalisiert. Wirklich sicher wird die Kommunikation erst, wenn Sie E-Mails vor dem Versand verschlüsseln – mit einem Schlüssel, den nur Sie und der Empfänger kennen. Hier kommt die asymmetrische Verschlüsselung nach dem Vorbild von PGP (Pretty Good Privacy) zum Tragen, alternativ und kostenfrei implementiert mit der GPG-Lösung. Hier ist Eigeninitiative gefragt, denn Sie benötigen ein eigenes Schlüsselpaar und müssen vor Versand die öffentlichen Schlüssel der Empfänger besitzen. Derzeit gibt es zumindest Tendenzen in der Politik, hier langfristig für eine Vereinfachung zu sorgen. Wünschenswert ist es allemal.

Foto: Coloures-pic - Fotolia