IT+Technik

Gut **verpackt**!

Die Enthüllungen von Edward Snowden haben gezeigt – Verschlüsselung ist essentiell, um Daten vor unbefugtem Zugriff zu schützen.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Sie kennen das wahrscheinlich: Beim Aufruf einer Internetseite mit sensiblen Daten steht in der Adresszeile des Browsers ganz vorne ein https://..., oftmals grün hinterlegt oder durch ein Schloss ergänzt. Dies deutet daraufhin: Hier wird verschlüsselt. Aber was heißt *„verschlüsselt"* eigentlich?
Eine (sichere) Verschlüsselung erlaubt die geheime Kommunikation zwischen zwei Parteien über ein unsicheres Netzwerk – also z.B. die Eingabe Ihrer Kontodaten bei einem Versandhändler über das Internet. Das Prinzip ist, dass durch Anwendung eines (oder mehrerer) Schlüssel ein Klartext (jede Art von Datei) vor dem Versand in einen nicht ohne weiteres interpretierbaren Geheimtext – das Chiffrat – umgewandelt wird. Der Empfänger mit Kenntnis des ursprünglichen Schlüssels kann dann aus Schlüssel und Chiffrat den Klartext wieder generieren.
Aber Verschlüsselung ist nicht immer sicher – das Brechen des Codes der „Enigma" im Zweiten Weltkrieg war mit ein Grund für den Sieg der Alliierten.

Neben der sicheren Nutzung von Online-Angeboten dient Verschlüsselung auch zur vertraulichen Kommunikation über E-Mail. Da sich eine symmetrische Verschlüsselung angesichts des im Vorhinein auszutauschenden, gemeinsamen Geheimnisses der jeweiligen Kommunikationspartner in der digitalen Welt als schwer realisierbar darstellt („Welches Kennwort habe ich für den Verteiler meines Vereins gewählt? Und welches nur für den Vorstand?"), bietet sich die Verschlüsselung per öffentlichem Schlüssel an. Leider sind auch hier die Einstiegshürden durch Schlüsselerstellung und -verteilung – vor dem Hintergrund konkurrierender Standards und unzureichender Implementierung in Systemen und Plattformen – für den Otto Normalverbraucher recht hoch. Bei regelmäßiger Kommunikation kann sich der Aufwand aber durchaus lohnen.
Der Versand sensibler Informationen über das Internet oder deren Speicherung bei einem Onlinedienst kann alternativ auch durch Verschlüsselung der übermittelten bzw. gespeicherten Dateien selbst erfolgen. Hier wird in der Regel der AES-Standard eingesetzt (s. Kasten).

Grundsätzlich gilt: Ein Mehr an Sicherheit bedeutet Zusatzaufwand. Setzen Sie Verschlüsselung für sensible Daten ein!

Symmetrische vs. Asymmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird für die Ver- und Entschlüsselung immer der gleiche Schlüssel verwendet. Dieser muss auf einem anderen, gesicherten Weg (z.B. per Post oder persönlich) zwischen Kommunikationspartnern ausgetauscht werden. Derzeit gängige Methode ist der Advanced Encryption Standard (AES; optimal mit einer Schlüssellänge von 256 Bit), den man auch in gängigen Komprimierungstools auswählen kann.
Die asymmetrische Verschlüsselung hingegen basiert auf einem Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel. Mit dem öffentlichen Schlüssel des Empfängers wird der Klartext chiffriert, der Empfänger wendet dann seinen privaten Schlüssel für die Dechiffrierung an. Das hierfür gängige Verfahren nennt sich „RSA" und wird z.B. auch beim HZV-Online Key für den sicheren Transport eingesetzt. Ausführlicheres zum HZV-Online Key in einer der nächsten Ausgaben von „Der Hausarzt".