Was ist starke Verschlüsselung?

Starke Verschlüsselung schützt die Daten von Privatleuten und Unternehmen – doch was ist darunter zu verstehen? Ein knapper Überblick erklärt Grundlagen der Datenverschlüsselung.

Eine starke Verschlüsselung ist notwendig, um zu verhindern, dass Cyberkriminelle oder Geheimdienste Daten auslesen.

Nur starke Verschlüsselung kann verhindern, dass Cyberkriminelle oder Geheimdienste Daten abfangen können. Dieser Satz sagt und schreibt sich leicht, doch ganz so einfach ist die Sache nicht. Um beurteilen zu können, ob eine Verschlüsselung tatsächlich ausreichend stark ist, sind einige Dinge zu beachten.

Zunächst einmal ein Blick auf die Grundlagen: Datenverschlüsselung ist eine Technik, mit der sinntragende Datenpakete (zum Beispiel Textdateien) in sinnlose Abfolgen von Bytes verwandelt werden. Das Prinzip ist sehr einfach: Zwei Kommunikationspartner vereinbaren eine Regel, Informationen so zu verändern, dass niemand ihren Sinn erschließen kann.

Die Verschlüsselungsregel wird Schlüssel genannt, die unverschlüsselte Information Klartext und die verschlüsselte Schlüsseltext. Zum Schlüssel und dem Schlüsseltext gehören zwei zusätzliche Informationen: Verschlüsselungs- und Entschlüsselungsfunktion. Schlüssel, Verschlüsselungs- und Entschlüsselungsfunktion zusammen bilden ein so genanntes Kryptosystem.

Asymmetrische Verschlüsselung

Ein Beispiel: Ein einfaches Kryptosystem basiert auf der Verschiebung von Buchstaben im Alphabet, zum Beispiel um drei Stellen. Dadurch wird A zu D wird, B zu E und so weiter. Dieses Verfahren ist jedoch unsicher. Der Schlüssel kann bei einem umfangreichen Schlüsseltext durch Auswertung der Regelmäßigkeiten im Schlüsseltext erkannt werden.

Moderne Kryptosysteme nutzen weitaus kompliziertere Funktionen. Bei der asymmetrischen Verschlüsselung werden zweiteilige Schlüssel eingesetzt: Ein öffentlicher und ein privater Schlüssel. Sie heißt auch Public-Key-Verschlüsselung, da lediglich der private Schlüssel geheim bleiben muss. Der öffentliche Schlüssel dagegen kann jedem mitgeteilt werden.

Der Trick bei der asymmetrischen Verschlüsselung: Sie benutzen den öffentlichen Schlüssel einer anderen Person, um eine Nachricht an sie zu verschlüsseln. Nur der Besitzer des dazu passenden privaten Schlüssels (also ihr Kommunikationspartner) kann die Information entschlüsseln und damit lesen.
In vielen Fällen ist dieses Vorgehen jedoch zu umständlich. Zahlreiche Verfahren zur Absicherung von Festplatten, aber auch zur Verschlüsselung von Kommunikationswegen setzen einzelne Schlüssel ein. Dies nennt sich symmetrische Verschlüsselung, da dort ein- und derselbe Schlüssel zum Ver- und Entschlüsselung eingesetzt wird.

Gefährdet sind Daten auch während der Übertragung über das Internet und bei der Speicherung auf „fremden“ Servern, zum Beispiel bei Cloudservices. Hierbei ist es ein Unterschied, ob Sie die Daten selbst verschlüsseln oder ob Sie einen verschlüsselten Übertragungsweg nutzen.

Im ersten Fall sind die Daten für Dritte nicht lesbar und können problemlos auch über unsichere Kanäle verbreitet werden: Selbst wenn sie abgefangen werden, sind sie für die Cyberkriminellen nicht zu entziffern.)

Im zweiten Fall werden die Daten vor der Übertragung verschlüsselt, dann übertragen und schließlich am Zielort wieder entschlüsselt. An den beiden Endpunkten gibt es jeweils unverschlüsselte Daten. Das letzte Verfahren entspricht der Transportverschlüsselung von Daten mit TLS/SSL im Internet.

Ende-zu-Ende-Verschlüsselung

Ein wichtiges und immer wieder vorkommendes Stichwort hierbei ist Ende-zu-Ende-Verschlüsselung. Damit ist grundsätzlich gemeint, dass Daten während der Übertragung über alle Übertragungsstationen hinweg verschlüsselt werden. Die normale Transportverschlüsselung im Internet ist zwar eine Ende-zu-Ende-Verschlüsselung, bietet aber nur eine recht eingeschränkte Sicherheit. Ein Beispiel: Ein Mail-Dienstleister überträgt alle E-Mails mit TLL/SSL. Die eigentlichen Mails liegen jedoch auf den Servern des Anbieters als Klartext vor.

Ein zweites Beispiel: Dienstleister für Online-Festplatten bieten eine abgesicherte Übertragung an, nutzen jedoch keine Verschlüsselung für den eigentlichen Speicherbereich. Wer Probleme mit der Datensicherheit in solchen Fällen umgehen will, muss eigene Verschlüsselungsverfahren einsetzen.

So ist es deutlich sicherer, Dateien vor dem Speichern auf eine Online-Festplatte auf dem eigenen Computern zu verschlüsseln und nur die verschlüsselten Dateien dort zu speichern. In diesem Fall kennt nur der Besitzer der ursprünglichen Daten den Schlüssel.

Im Grunde handelt es sich nur in einem Fall um eine echte Ende-zu-Ende-Verschlüsselung: Wer die Daten verschlüsselt, kennt auch den Schlüssel und kann sie wieder entschlüsseln. Eventuell beteiligte Dritte wie Internet-Provider für die Übertragung oder Cloud-Dienstleister für die Speicherung dürfen den Schlüssel nicht kennen.

Doch nicht nur die „Durchgängigkeit“ der Verschlüsselung ist entscheidend für die Sicherheit von Daten. Ebenso wichtig ist die Schlüssellänge. Grundsätzlich gilt: Je länger ein Schlüssel, desto sicherer die Information.

Schlüssel sollten übrigens möglichst lang gewählt werden, denn kurze Schlüssel sind inzwischen durchaus zu berechnen. Das Minimum bei Public Key-Kryptografie sind Schlüssel mit 2048 Bit Länge. Bei symmetrischer Verschlüsselung gelten heute die Verfahren AES (Advanced Encryption Standard, normiert) und Twofish (Public Domain) mit jeweils 256 Bit Schlüssellänge als besonders sicher.

Der Vorteil der symmetrischen Verschlüsselung: Sie ist um den Faktor 1000 schneller als die asymmetrische. In der Praxis gehen Anwendungen für Public-Key-Kryptosysteme deshalb anders vor: Der öffentliche Schlüssel chiffriert den zufällig erzeugten Schlüssel eines

symmetrischen Verfahrens. Der eigentliche Schlüsseltext wird dann mit diesem symmetrischen Schlüssel erzeugt. Damit sind die Vorteile beider Typen von Kryptosystemen vereint: Einfacher Schlüsselaustausch und rasche Ver-/Entschlüsselung.