Sichere Kommunikation

Die Verschlüsselung von Daten wird immer wichtiger. Damit können die geforderte Vertraulichkeit, Authentizität und Integrität garantiert werden. Doch das Thema Kryptografie ist schwer zu verstehen. Dieser Beitrag soll etwas Licht ins Dunkel bringen.

Andreas Wisler

Der Wunsch, dass Informationen vertraulich und nur eingeschränkt verfügbar sind, ist so alt wie die Menschheit. Viele verschiedene Arten von Verschlüsselungstechnologien wurden entwickelt, wie spezielle Dialekte, Rotation des Alphabets, Lederbänder auf einen Stab umwickelt und viele weitere. Heutige Technologien nutzen mathematische Verfahren und die Macht grosser Zahlen (was aber auch gefährlich sein kann, wenn sich die Rechenleistung immer weiter verbessert).

Was sagt die Richtlinie?

Die ISO 27001 verlangt im Kapitel A.10 eine Richtlinie zum Gebrauch von kryptografischen Massnahmen. Darin soll geregelt sein, wie und wofür Kryptografie genutzt wird. Dazu gehört eine entsprechende Risikoanalyse. Darin muss geklärt werden, welche Verfahren eingesetzt werden können und wo der Schutz allenfalls nicht genügt. Dazu gehört auch die Verantwortlichkeit bei die Erstellung, Verwaltung und Schutz der entsprechenden Schlüssel zu regeln.

Mit der Kryptografie sollen die klassischen Schutzziele CIA erreicht werden (siehe Abb. 1):

Verfügbarkeit (Availability): Die Verfügbarkeit eines Systems wird umschrieben mit der Eigenschaft, sämtliche Daten und Funktionen zu einem bestimmten Zeitpunkt zur Verfügung stellen zu können.

Integrität (Integrity, Unversehrtheit): Lässt ein System unbefugte oder unbeabsichtigte Veränderungen an Daten oder an der Software zu, so ist deren Integrität verletzt. Es kann somit nicht mehr garantiert werden, dass alle sicherheitsrelevanten Objekte vollständig, unverfälscht und korrekt sind.

Vertraulichkeit (Confidentiality): Darunter wird verstanden, dass nur bestimmte Personen oder Prozesse auf Daten oder Systeme zugreifen können oder dürfen. Soll die Vertraulichkeit gewahrt werden, müssen die Daten so gesichert sein, dass ein Zugriff nur denjenigen Nutzern möglich ist, welche durch Zugriffsrechte die Erlaubnis erhalten.

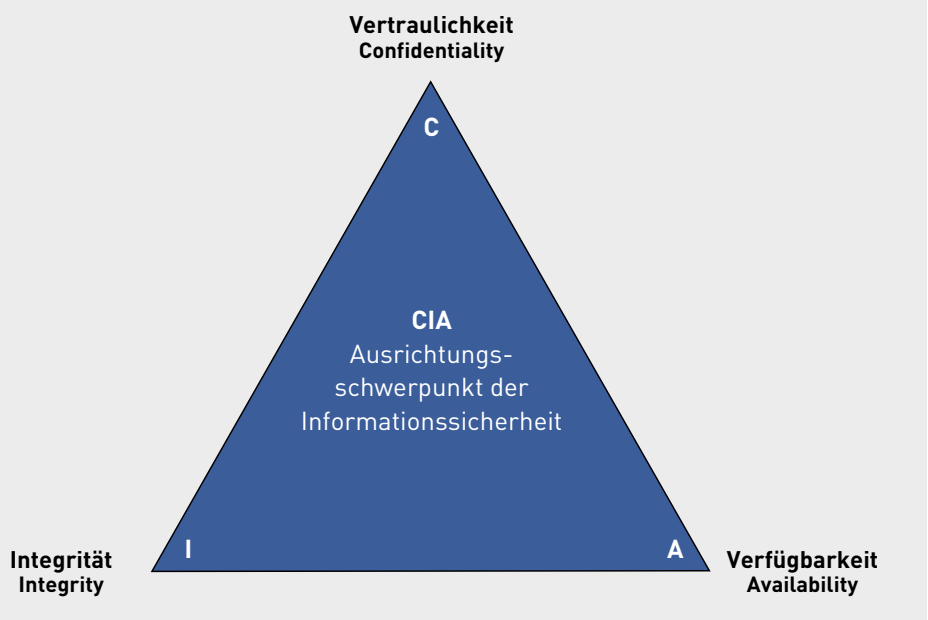

Abb. 1: Mit der Kryptografie sollen die klassischen Schutzziele CIA erreicht werden.

Immer wichtiger wird auch die Unabstreitbarkeit. Es soll klar sein, wenn jemand etwas gemacht hat. Bei einer Kommunikation sind dies beispielsweise der Versand und der Empfang. Beides soll revisionssicher geloggt werden.

Zwei Verschlüsselungsarten

Mit der Kryptografie wird auch eine sichere Authentifizierung möglich. Es werden klassisch zwei Arten unterschieden: symmetrische und asymmetrische Verschlüsselung.

Bei der symmetrischen Verschlüsselung wird zum Ver- und Entschlüsseln das gleiche Passwort verwendet. Tools wie 7-Zip, aber auch alle Festplattenverschlüsselungen (z. B. BitLocker unter Windows, VeraCrypt) und die meisten Passwortspeicher (z. B. KeePass) nutzen dies. Nur wer dieses Passwort kennt, kommt auch wieder an die Daten. Die Herausforderung bei der verschlüsselten Kommunikation zwischen zwei Stellen ist der Austausch dieses Passworts. Es darf unter keinen Umständen auf dem gleichen Weg wie die Nachricht übermittelt werden!

Das zweite Verfahren ist die asymmetrische Verschlüsselung. In diesem Fall wird ein Schlüsselpaar erzeugt (auch Zertifikat genannt). Diese sind mathematisch miteinander fest verknüpft. Man spricht von einem öffentlichen Schlüssel und einem privaten Schlüssel. Der Name sagt es schon, den öffentlichen Schlüssel kann ich frei verteilen, gar auf meine Homepage oder auf Facebook stellen. Der private Schlüssel gehört nur mir und darf unter keinen Umständen weitergegeben und muss gut geschützt aufbewahrt werden.

Die verschlüsselte Kommunikation per E-Mail funktioniert gemäss Abbildung 2.

Mit dem öffentlichen Schlüssel des Empfängers wird das E-Mail verschlüs-

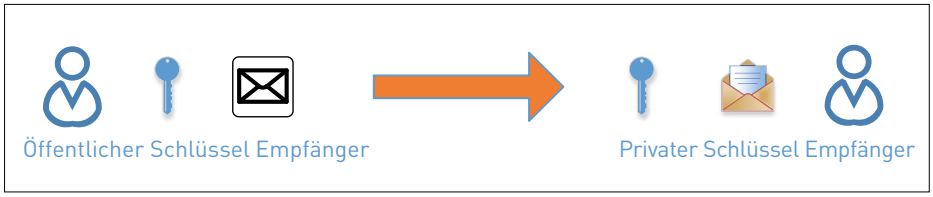

Abb. 2 zeigt, wie die verschlüsselte Kommunikation per E-Mail funktioniert.

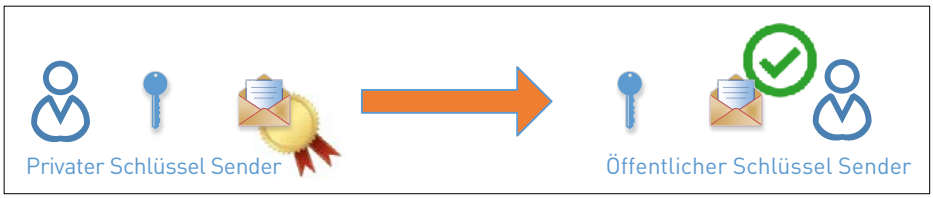

Abb. 3: E-Mails können auch digital signiert werden.

selt. Der Empfänger kann es mit dem eigenen privaten Schlüssel wieder auspacken.

Es gibt auch die Möglichkeit, E-Mails zu signieren. Dies entspricht in etwa einer Unterschrift in einem Brief. Damit kann die Unabstreitbarkeit des Sendens gewährleistet werden. Die Funktionsweise ist in Abbildung 3 dargestellt.

Mit dem eigenen privaten Schlüssel wird das E-Mail digital signiert. Das E-Mail wird im Klartext übermittelt. Der Empfänger kann die Echtheit mit dem öffentlichen Schlüssel des Senders überprüfen.

«Mit der Kryptografie wird auch eine sichere Authentifizierung möglich.»

Schlüsselverwaltung

Ein wichtiger Faktor ist auch der Umgang mit den Schlüsseln. Die nachfolgenden Punkte gilt es zu beachten.

Erzeugung: Wie werden Schlüssel erzeugt? Wird eine eigene CA (Certificate Authority) genutzt oder werden Zertifikate von einer öffentlichen Stelle bezogen? Zum Beispiel in der Schweiz bei SwissSign oder QuoVadis.

Wenn eine eigene CA betrieben wird, ist der Schutz dieses Servers extrem wichtig. Es darf nicht sein, dass fremde Personen diesen missbrauchen können. Ansonsten könnten sie sich zum Beispiel als Mitarbeitende ausgeben und durch die Signatur eine hohe Glaubwürdigkeit nachweisen. In einem Firmennetzwerk ist dies eine günstige Lösung (gerade bei vielen Mitarbeitenden). Der Nachteil ist, dass alle ausserhalb des Unternehmens diesen Zertifikaten nicht vertrauen und es kommt beispielsweise in E-Mail-Programmen zu einer Fehlermeldung. Wird mit externen Stellen kommuniziert, muss daher eine externe CA benutzt werden. Der Anbieter der CA hat dafür gesorgt, dass die meisten Programme diesen Zertifikaten vertrauen.

Ausstellung: Die Zertifikate sollten nicht ohne Prüfung ausgestellt, sondern durch eine verantwortliche Person freigegeben werden. So ist eine zusätzliche Kontrolle möglich. Bei externen CAs wird dies durch eine beglaubigte Ausweiskopie (kann bei der Post oder der Einwohnergemeinde gemacht werden) sichergestellt. Erst wenn diese bei der CA eingetroffen ist, wird das Zertifikat ausgestellt.

Verteilung: Zertifikate können in einem Windows-Netzwerk automatisch verteilt werden. Dies erleichtert die Verwaltung enorm. Bei externen CAs muss ein entsprechender Prozess initiiert werden. Viele CAs bieten die Möglichkeit an, dass eine zu definierende Person für das Unternehmen Zertifikate bestellen und verteilen darf. Das erleichtert den Bestellprozess massiv, muss doch nicht jeder Mitarbeitende selbst die beglaubigte Ausweiskopie einschicken.

Speicherung: Die sichere Speicherung der Schlüssel ist wichtig. Die Schlüssel dürfen unter keinen Umständen in falsche Hände gelangen. Der mögliche Schaden kann enorm sein, kann ich mich damit doch als jemand anderes ausgeben (fast wie der Diebstahl einer Identitätskarte). Daher sollten Schlüssel mindestens mit einem Passwort gesichert sein. Einige Systeme bieten auch die zentrale Verwaltung dieser Schlüssel an.

Änderung/Sperren von Schlüsseln: Zertifikate müssen angepasst werden (z. B. bei einem Namenswechsel) oder können abhandenkommen. Daher gilt es entsprechende Prozesse zu etablieren. Solche Zertifikate werden gesperrt. Die interne wie auch die externe CA erstellen dann eine Liste mit gesperrten Zertifikaten. Bei der Nutzung von Zertifikaten muss das entsprechende Programm jeweils prüfen, ob es gesperrte Zertifikate gibt. Dazu erstellen die CAs eine CRL (Certificate Revocation List). Darin sind alle diese gesperrten Zertifikate enthalten. Wird das Zertifikat trotzdem noch benutzt, kommt es beim Empfänger zu einer Fehlermeldung.

Archivierung: Verschlüsselte Nachrichten können nur mit dem dazu passenden privaten Schlüssel geöffnet werden. Daher müssen auch abgelaufene Schlüssel archiviert werden. Ohne diese ist es nicht mehr möglich, an die Daten zu gelangen. Wird beispielsweise eine verschlüsselte Datei aus dem Back-up geholt, kann diese ohne den passenden Schlüssel nicht mehr angeschaut werden.

Protokollierung: Jede Verwendung eines Schlüssels sowie jede Aktion einer CA müssen protokolliert werden. Damit ist eine saubere Nachvollziehbarkeit möglich.

Das Thema Kryptografie ist spannend, aber auch komplex. Dieser Artikel ging absichtlich nicht auf technische Elemente ein (verschiedene Verfahren, notwendige Schlüssellänge, Aufbau einer verschlüsselten Verbindung etc.). Mit einer Verschlüsselung ist eine sichere Kommunikation und ein Nachweis möglich. ■

ANDREAS WISLER
CSMO, Dipl. Ing. FH, CISSP, CISA, ISO 27001 und 22301 Lead Auditor, goSecurity GmbH, Wiesendangen