Kryptografie

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.

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).

Richtlinie

Die ISO 27001 verlangt im Kapitel A.10 eine Richtlinie zum Gebrauch von kryptografischen Massnahmen. Darin soll geregelt sein, wie und für was Kryptografie genutzt wird.

Dazu gehört eine entsprechende Risiko-Analyse. Darin muss geklärt werden, welche Verfahren eingesetzt werden können und wo der Schutz allenfalls nicht genügt.

Dazu gehört auch die Verantwortlichkeit für die Erstellung, Verwaltung und Schutz der entsprechenden Schlüssel zu regeln.

Arten der Verschlüsselung

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 (zum Beispiel Bitlocker unter Windows, VeraCrypt) und die meisten Passwortspeicher (zum Beispiel KeePass) nutzen dies. Nur wenn ich dieses Passwort kenne, komme ich auch wieder an die Daten. Die Herausforderung bei der verschlüsselten Kommunikation zwischen zwei Stellen ist der Austausch dieses Passwortes. Es darf unter keinen Umständen auf dem gleichen Weg wie die Nachricht übermittelt werden. Ich muss immer schmunzeln, wenn ich eine E-Mail mit einer verschlüsselten ZIP-Datei bekomme und das Passwort steht in der gleichen oder nachfolgenden E-Mail. Das darf nicht sein.

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 werden und muss gut geschützt aufbewahrt werden. Bild 1 zeigt, wie die verschlüsselte Kommunikation per E-Mail funktioniert.

Mit dem öffentlichen Schlüssel des Empfängers wird die E-Mail verschlüsselt. Das heisst, bevor dies funktioniert, benötige ich etwas von der Gegenstelle. Dies stellt für mich eine der grössten Herausforderungen dar. Hat die Gegenstelle keinen entsprechenden Schlüssel, kann ich nicht sicher kommunizieren. Ist der öffentliche Teil des Zertifikats bei mir eingelesen, genügt es in Outlook (und anderen Mail-Programmen) den entsprechenden Button zu drücken und das E-Mail wird vor dem Versenden verschlüsselt. Zum Öffnen und Anzeigen benötigt die Gegenstelle den eigenen privaten Schlüssel. Damit wird das E-Mail wieder ausgepackt und lesbar dargestellt. Dies geschieht ohne dazutun des Anwenders (Bild 2).

Mit den Schlüsseln kann aber noch mehr gemacht werden. Der private Schlüssel kann dazu genutzt werden, das E-Mail zu signieren. Das entspricht der Unterschrift unter einem Brief. Die Gegenstelle kann mit dem öffentlichen Schlüssel diese Unterschrift überprüfen. Ist alles in Ordnung, wird dies in der E-Mail so angezeigt. Wichtig: die E-Mail ist dabei unverschlüsselt. Die beiden Funktionen lassen sich aber gleichzeitig verwenden. Damit die Gegenstelle nicht noch das öffentliche Zertifikat suchen muss, schickt es beispielsweise Outlook bei jeder signierten E-Mail mit.

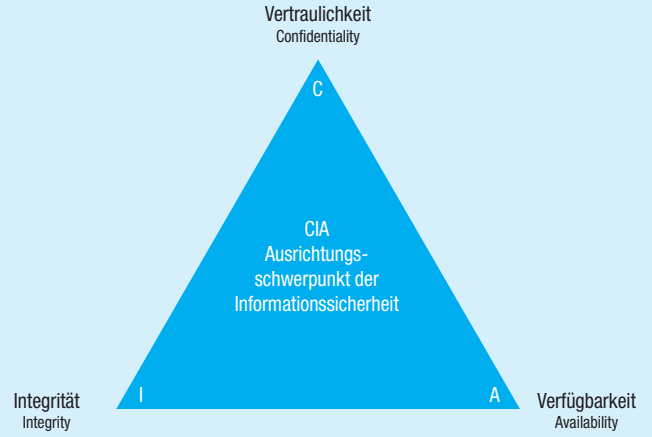
Anwendungen

Momentan sind zwei Verfahren gebräuchlich: PGP und X.509.

PGP wurde von Phil Zimmerman entwickelt. Als aktiver Atomkraft-Gegner hat er mehrere Demos organisiert. Doch die Polizei war aber oft vor ihm dort. Da hat er sich entschlossen, eine Verschlüsselungssoftware zu entwickeln. PGP war geboren. Die Installation ist sehr einfach. In den Linux-Systemen ist dies seit Jahren Bestandteil. Bei Windows

Schutzziele

Mit der Kryptografie sollen die klassischen Schutzziele CIA erreicht werden:



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.

Nichtabstreitbarkeit (Non Repudiation)
Immer wichtiger wird auch die Nichtabstreitbarkeit. 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.

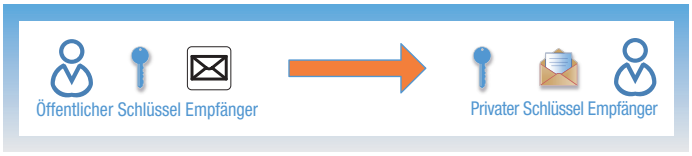


Bild 1.

kann unter www.gpg4win.de/ die kostenlose Software heruntergeladen werden. Diese Version wird aktiv vom BSI (dem Deutschen Bundesamt für Sicherheit in der Informationstechnik) gefördert. Die Installation ist mit wenigen Klicks durchgeführt. Die Integration in Outlook wird während der Installation ebenfalls erledigt.

Die Funktionsweise von X.509 gegenüber PGP unterscheidet sich nur wenig. Dieser Artikel geht bewusst nicht auf die verwendeten mathematischen Funktionen ein. Auch hier wird ein Schlüsselpaar erstellt. Anders als bei PGP wird dieses jedoch immer von einer CA (Zertifikatsstelle) verifiziert. Ein Unternehmen kann dabei die CA selber betreiben. Dies hat den Nachteil, dass die Gegenstelle eine hässliche Fehlermeldung bekommt, da der CA zuerst vertraut werden muss. Daher sollten Sie eine vertrauenswürdige CA nutzen. In der Schweiz sind dies beispielsweise SwissSign (Lösung der Schweizer Post) oder Quo Vadis aus St.Gallen bekannt. Gegen eine Gebühr erhalten Sie ein entsprechendes Zertifikat. Der Vorteil von X.509-Zertifikaten ist die Integration in die Betriebssysteme: weder bei Windows, Mac, iPhone/iPad noch Android müssen Sie etwas installieren – alle sind entsprechend vorbereitet.

Schlüsselverwaltung

Das zweite Unterkapitel des ISO-Kapitels A.10 definiert Anforderungen an die Schlüsselverwaltung. Dazu gehören:

Erzeugung

Wie werden Schlüssel erzeugt? Wird eine eigene CA (Certificate Authority) genutzt oder Zertifikate von einer öffentlichen Stelle bezogen. Wird eine eigene CA betrieben, muss der Schutz dieses Servers im Fokus stehen. 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 Firmen-Netzwerk ist dies zwar eine günstige Lösung (gerade bei vielen Mitarbeitenden), der Nachteil ist, dass alle ausserhalb des Unternehmens diesen Zertifikaten nicht vertrauen und es kommt beim Empfänger 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.

Bild: Archiv

Verschlüsselte Nachrichten können nur mit dem dazu passenden privaten Schlüssel geöffnet werden.

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 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 Bestell-Prozess 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 (zum Beispiel 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 Revokation 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 diesen ist es nicht mehr möglich, an die Daten zu gelangen. Wird beispielsweise eine verschlüsselte Datei aus dem Backup geholt, kann diese 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 usw.). Mit einer Verschlüsselung sind aber eine sichere Kommunikation und ein Nachweis möglich. Ich hoffe, dass in Zukunft vermehrt Unternehmen auf Kryptografie setzen. Nur wenn viele mitmachen, kann der Austausch von sensitiven Nachrichten sicherer gemacht werden.

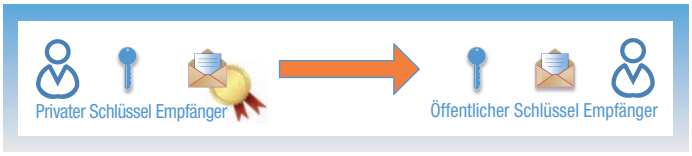


Bild 2: E-Mails signieren.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch