DER OPTIMALE SCHUTZ

DATENVERSCHLÜSSELUNG IN DER PRAXIS

von Andreas Wisler

Der Wunsch nach Vertraulichkeit ist so alt wie die Menschheit selbst. Schon früh hat sich der Mensch darüber Gedanken gemacht, wie Informationen sicher zwischen zwei Stellen ausgetauscht werden können. Heutzutage werden moderne Algorithmen eingesetzt, um die Sicherheit und die Vertraulichkeit der Nachrichten zu gewährleisten.

Es kommt auch in der IT-Welt auf den Schlüssel an.

Weit in die Vergangenheit zurück waren etwa Sprachen, die nur eine eingeschränkte Anzahl an Menschen spricht und verstehen konnte, eine Möglichkeit zum Austausch. Oder Lederbänder, die um einen Stock gewickelt und die Nachricht darauf aufgeschrieben wurde. Nur wer den genau gleich dicken Stock hatte, konnte die Nachricht wieder entschlüsseln. Cäsar nutzte eine Rotation des Alphabets um einige Zeichen. So wurde das A -> D, B -> E. Die Gegenstelle musste nur die Anzahl Zeichen wissen, um die Nachricht lesen zu können. Auch Sklaven wurden für den Transport sensibler Nachrichten verwendet. Dazu wurde die Nachricht auf den rasierten Schädel geschrieben, die Haare wieder wachsen lassen und dann den Sklaven losgeschickt. Damals waren die Nachrichten noch nicht so zeitkritisch wie heutzutage, und solche Methoden sind zweifellos nicht mehr zeitgemäss.

«E-Mails sind wie Postkarten zu sehen. Alle, die sie in die Finger bekommen, können sie lesen.» Diese Aussage – und zugleich dieser Fakt – ist allgegenwärtig, und hier hilft nur die Verschlüsselung: Sie schützt E-Mails, Webseiten-Aufrufe, aber auch

Daten in der Cloud effektiv vor fremden Zugriffen. Zwei Verfahren haben sich hier etabliert: PGP und S/MIME.

PGP MIT SCHLÜSSELPAAR

PGP wurde von dem Atomgegner Phil Zimmermann entwickelt. Bei seinen organisierten Demonstrationen war jedoch meist immer die Polizei vor ihm vor Ort. Das hat ihn ziemlich verärgert, und so hat er sich dazu entschlossen, das Programm PGP zu entwickeln, um in diesem Fall die Polizei auszuspielen. Der Vorteil an PGP ist, dass weder ein Staat noch eine Institution dahintersteht. Inzwischen gehört PGP der Firma Symantec, und deshalb verwenden viele die freie Version GPG (Gnu PG), welche nicht von einer Firma kontrolliert wird. Wenngleich PGP und GPG miteinander kompatibel sind. Bei PGP erstellt der Benutzer selbst ein Schlüsselpaar, auch Zertifikat genannt: einen öffentlichen und einen privaten Schlüssel.

DER ÖFFENTLICHE SCHLÜSSEL

Der öffentliche Schlüssel, wie es der Name bereits sagt, kann (und muss) frei ausgetauscht werden. Alle, die miteinander kommunizieren möchten, müssen diesen besitzen. Ein wichtiger Schritt geht dabei oft vergessen. Es muss zwingend überprüft werden, ob der öffentliche Schlüssel tatsächlich zum Empfänger gehört. Leider gibt es «Schlaumeier», die Namen fälschen und die öffentlichen Schlüssel verteilen. Die Verifikation ist aber sehr einfach. Beim Erzeugen des Schlüsselpaars wird ein Fingerabdruck erzeugt, der auf einem zweiten Weg via Telefon, SMS, Anruf oder Ähnliches, verifiziert werden kann.

Zum Verschlüsseln einer Nachricht benötigt man nun diesen öffentlichen Schlüssel des Empfängers. Bei der Installation der Software wird für viele E-Mail-Programme bereits ein Plugin installiert. So muss in Outlook nur noch der Button «verschlüsseln» gedrückt werden, das Programm findet automatisch den zur E-Mail passenden öffentlichen Schlüssel und verschlüsselt die Nachricht. Beim Empfänger angekommen wird die Nachricht mit dem privaten Schlüssel des Empfängers wieder entschlüsselt und normal angezeigt. Dank des integrierten Plugins muss der Empfänger überhaupt nichts machen, denn die E-Mail wird wie gewohnt geöffnet. Je nach Einstellung kann es aber sein, dass das Passwort zum Entschlüsseln noch abgefragt wird.

DER PRIVATE SCHLÜSSEL

Der private Schlüssel kann hingegen für einen zweiten Effekt verwendet werden, und zwar zum Signieren einer E-Mail. Mit der Signatur bestätigt der Absender, dass das E-Mail tatsächlich von ihm kommt. Über die gesamte Nachricht wird ein Hash berechnet (eine Art Quersumme). Dieser Hash-Wert wird mit dem privaten Schlüssel, verschlüsselt und an die Nachricht angehängt wie eine Art Unterschrift unter den Brief. Der Empfänger der Nachricht kann diese Signatur mit dem öffentlichen Schlüssel wieder entschlüsseln und mit dem selber berechneten Hash-Wert der Nachricht vergleichen. Sind die Hash-Werte identisch, kam die Nachricht unverändert an.

S/MIME MIT CERTIFICATE AUTHORITY

Nun gibt es ein zweites Verfahren: S/MIME (Der genaue Standard heisst X.509). Hier werden die Schlüssel nicht mehr selber verifiziert, sondern es steht eine CA (Certificate Authority) im Hintergrund zur Verfügung. Bei kommerziellen CA's kann gegen eine Gebühr ein Zertifikat gekauft werden. Die CA hat die Pflicht zu überprüfen, wer das Zertifikat beantragt. Je nach Sicherheitsstufe genügt die Verifikation per E-Mail, das heisst, der Nutzer muss – wie bei Newslettern bekannt – auf einen zugestellten Link zur Bestätigung klicken. In sensitiven Bereichen wird aber empfohlen, ein teureres Zertifikat auszuwählen. Hier muss die Identität mit einem Ausweis beglaubigt werden. In der Schweiz sind dies beispielsweise die Gemeinden, die Post oder SBB-Schalter, die dies (gegen ein Entgelt) übernehmen. Inzwischen gibt es auch kostenlose CA's, die diesen Prozess übernehmen. Meistens kommt hier aber nur die Verifikation der E-Mail-Adresse zum Einsatz. Daher lohnt es sich abzuwägen, welche Zertifikate benötigt werden und was gegenüber der externen Stelle kommuniziert werden soll. Sobald dies erledigt ist, stellt die CA ein Zertifikat aus, und dieses wird auf dem eigenen Computer installiert.

GÜLTIGE ZERTIFIKATE FÜR DATENÜBERTRAGUNG

Die Funktionsweise zum Ver- und Entschlüsseln ist identisch zu PGP. S/MIME hat sich hier aber durchgesetzt und ist in allen bekannten Systemen bereits integriert. So muss weder auf dem Handy noch auf dem Mac oder PC eine Software installiert werden.

Die erwähnten CA's können aber nicht nur Zertifikate für die E-Mail-Sicherheit herausgeben. Die zweite Anwendung ist der Schutz von über das Internet übertragenen Daten. Ersichtlich ist dies am HTTPS in der Internet-Adresse (URL). Beim Aufruf einer sicheren Webseite wird vom eigenen Browser der öffentliche Schlüssel übermittelt. Der Browser überprüft nun, ob der Name des Zertifikates mit der aufgerufenen Seite übereinstimmt und ob das Zertifikat gültig ist. Nun gilt es zu kontrollieren, ob die CA bereits bekannt ist. Die Browser- und Betriebssystemanbieter führen dazu eine regelmässig aktualisierte Liste von vertrauenswürdigen CA's. Falls die CA bekannt ist, überprüft der Browser, ob der übermittelte öffentliche Schlüssel wirklich von dieser CA ausgestellt wurde (entspricht dem Fingerprint, welcher bei PGP manuell überprüft wird). Wenn ja, wird optional noch bei der CA nachgefragt, ob nicht doch noch ein Problem mit dem Zertifikat vorliegt. Wurden alle Prüfungen erfolgreich bestanden, wird die sichere Verbindung zur Webseite aufgebaut. Somit kann der Nutzer sicher sein, dass es die richtige Seite ist und dass die Daten vor fremden Blicken geschützt sind. Wichtig: Wenn eine Fehlermeldung angezeigt wird, dass etwas mit dem Zertifikat nicht stimmt, sollte man auf keinen Fall auf «Weiter» klicken. Hier handelt es sich vermutlich um einen Angreifer, der sich in die Verbindung einschleichen möchte.

Der Aufwand für eine sichere Kommunikation ist daher entsprechend gering. Mit zwei Schlüsseln können sicher E-Mails ausgetauscht werden, wie auch sicher im Internet gesurft werden kann. Daher sollte man diese Möglichkeit nutzen, um sensitive Informationen zu schützen. ■

ANDREAS WISLER

ist dipl. Ing. FH CSMO und Chairman of the Board der goSecurity GmbH.

www.gosecurity.ch