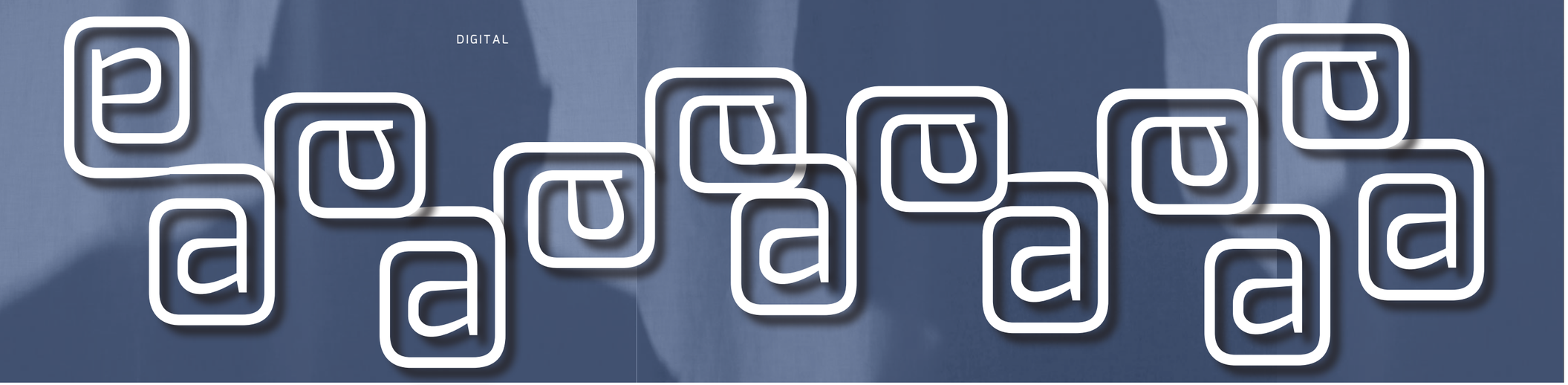

Fotoquelle: BilderBox.com

Sichere Kommunikation

WIE VERSCHLÜSSLE ICH MEINE E-MAILS? E-Mails reisen heute durchs Internet wie früher Postkarten durch die Ämter: Jede Stelle zwischen Sender und Empfänger kann den Inhalt lesen. Die Verschlüsselung verhindert dies.

TEXT ANDREAS WISLER

E-Mail ist eine der wichtigsten Funktionen, die das Internet mit sich gebracht hat. Jeden Tag werden viele Tausende E-Mails verschickt und empfangen. Gerade im geschäftlichen Umfeld ist E-Mail nicht mehr wegzudenken. Oft werden auch vertrauliche Mitteilungen verschickt. Dabei ist vielen nicht bewusst, wie einfach E-Mails abgefangen und gelesen werden können. Daher gilt es, den E-Mail-Inhalt entsprechend zu schützen. Zwei verschiedene Standards ermöglichen den sicheren Transport des vertraulichen E-Mail-Inhalts: X.509 (SMIME) und PGP.

Werden E-Mails mit X.509 verschickt, wird dafür ein öffentlich ausgestelltes Zertifikat benötigt. Technisch handelt es sich um das gleiche Zertifikat, welches beim Aufruf einer Webseite mit HTTPS genutzt wird (zum Beispiel beim Online-Banking oder beim Online-Shopping). Jedoch ist die Verwendung auf E-Mails beschränkt.

Verschiedene Anbieter rund um den Globus bieten solche Zertifikate an. Auch in der Schweiz buhlen diverse so genannte Zertifizierungsstellen um Kunden. Für etwa 30 Franken pro Jahr kann ein Zertifikat gekauft werden. Mit dem eigenen Computer wird die Seite der Zertifizierungsstelle aufgerufen und nach Eingabe einiger Angaben das Zertifikat erstellt. Bevor es jedoch genutzt werden kann, muss sich der Besteller identifizieren. Dafür wird in der Regel eine ID oder ein Pass benötigt. Diese(r) kann, je nach gewählter Lösung, bei der Post, bei der Gemeinde oder an einem SBB-Schalter gezeigt werden. Bei ausländischen Zertifizierungsstellen wird oft nur überprüft, ob die angegebene E-Mailadresse wirklich der bestellenden Person gehört. Einige Tage später erhält man per E-Mail eine Bestätigung, dass alles in Ordnung ist und das Zertifikat abgeholt werden kann.

PRIVATER UND ÖFFENTLICHER SCHLÜSSEL

Nun wird die bereits bekannte Webseite erneut aufgerufen und der Installationsprozess abgeschlossen. Das nun von der Zertifizierungsstelle unterschriebene Zertifikat besteht aus zwei Teilen: einem privaten und einem öffentlichen Schlüssel. Wie der Name bereits andeutet, ist der öffentliche Schlüssel öffentlich, das heisst, er kann frei im Internet verteilt werden. Er darf sogar auf der eigenen Website platziert oder in jeder E-Mail verschickt werden. Der private Schlüssel hingegen ist privat und darf unter keinen Umständen weitergegeben werden. Für die sichere Kommunikation per E-Mail werden zwei Anwendungsszenarien unterschieden: E-Mails signieren oder verschlüsseln. Beim Signieren wird die E-Mail digital mit dem privaten Schlüssel unterzeichnet. Wie eine handschriftliche Unterschrift gilt diese Unterschrift als rechtsgültig. Der E-Mail-Inhalt ist immer noch für Dritte lesbar, er kann aber nicht verändert werden, ohne dass die Unterschrift zerstört und beim Empfänger eine entsprechende Fehlermeldung angezeigt wird. Der Empfänger kann die Echtheit mit dem öffentlichen Schlüssel des Senders verifizieren. Probleme machen hin und wieder öffentliche E-Mail-Dienste wie «zur Verfügung gestellt von Anbieter XY» oder Anti-Spam/Anti-Viren-Programme, die den Hinweis «Diese E-Mail ist virenfrei, da mit XY geprüft wurde» an die E-Mail hängen. Damit wird leider die Signatur zerstört. Daher sollten diese Funktionen unbedingt ausgeschaltet werden.

FUSSABDRUCK: VERTRAUENSWÜRDIG!

Zur Verschlüsselung wird der öffentliche Schlüssel des Empfängers benötigt. Das heisst, dieser muss im Vorfeld zugestellt werden. Dies kann problemlos auch per E-Mail geschehen. Damit wird die E-Mail so verschlüsselt, dass niemand sie mehr lesen kann. Nur der Empfänger kann mit seinem privaten Schlüssel aus den Hieroglyphen wieder lesbaren Text machen. Beide Vorgänge sind mit den klassischen E-Mail-Programmen sehr einfach. Es reicht, den entsprechenden Button zu drücken und schon wird die E-Mail signiert und verschlüsselt. Während beim Standard X.509 eine öffentliche Zertifizierungsstelle prüft, ob die Person wirklich diejenige ist, die sie behauptet zu sein, nutzt PGP das Web-of-Trust. Das bedeutet, dass die Benutzer sich gegenseitig das Vertrauen bescheinigen. Dazu wird der öffentliche Teil des Schlüssels, wie bereits erwähnt, ausgetauscht und anschliessend über einen anderen Weg (Telefon, Fax und so weiter) verifiziert. Stimmt der «Fussabdruck» des Schlüssels, kann er als vertrauenswürdig markiert werden. Die Funktionsweise ist analog zu jener von X.509. Es genügt, nach der Installation der entsprechenden Software den entsprechenden Button zu drücken. Der Vorteil von PGP ist sicherlich, dass das Programm kostenlos ist. Leider sind X.509 und PGP nicht kompatibel.

VERSCHLÜSSELUNG IM UNTERNEHMENSKONTEXT

Für Unternehmen stellen sich einige Herausforderungen mehr als für Privatpersonen. Die Zertifikate sind in der Regel für eine Person ausgestellt. Verlässt diese das Unternehmen, wird der entsprechende Schlüssel gelöscht. Damit sind aber alle verschlüsselt empfangenen E-Mails nicht mehr lesbar. Auch wenn die E-Mail in einem CRM-System abgelegt wurde, kann nur der Besitzer des privaten Schlüssels sie lesen. Dies gilt auch für das Back-up der E-Mails. Ein Zugriff darauf ist ohne das passende Zertifikat nicht möglich. Diesen Umstand gilt es bereits bei der Planung der Verschlüsselung zu berücksichtigen. Inzwischen gibt es einige Anbieter mit geeigneten Lösungen. Das Zertifikat wird nicht mehr einer Person zugeordnet, sondern dem Unternehmen. Die Verschlüsselung übernimmt nicht mehr der einzelne Mitarbeiter, sondern der zentrale E-Mail-Server. Ist der öffentliche Schlüssel des Empfängers bekannt, wird die E-Mail automatisch verschlüsselt. Werden verschlüsselte E-Mails empfangen, entschlüsselt der E-Mail-Server die Nachrichten und leitet sie unverschlüsselt an den entsprechenden Benutzer weiter. Somit sind die Ablage im CRM-System und das Back-up wieder möglich, sodass auch später auf Nachrichten zurückgegriffen werden kann.

Die E-Mail-Kommunikation kann mit wenigen Vorkehrungen sicher ausgeführt werden. Dazu müssen aber beide Seiten ein entsprechendes Zertifikat nutzen. Danach ist es problemlos möglich, vertrauliche Inhalte sicher über das unsichere Internet zu verschicken.

DER AUTOR

Andreas Wisler ist CISA, CISSP sowie ISO 27001 und 22301 Lead Auditor. Er ist Inhaber der GO OUT Production GmbH, die sich seit 2001 durch IT-Security Audits, Penetration Tests und Beratungen mit der ganzheitlichen Betrachtung der IT-Sicherheit auseinandersetzt. Er publiziert regelmässig Fachberichte in KMU- und technischen Zeitschriften und ist Dozent im CAS Information Security & Risk Management an der Hochschule für Wirtschaft FHNW.