E-MAIL

Verschlüsselung im Organisationsalltag

VON ALEXANDER KULBARTSCH
UND THOMAS ALTHAMMER

Alexander Kulbartsch ist IT-Sicherheitsspezialist und als Senior Security Consultant für die Althammer & Kill GmbH & Co. KG tätig. Er verfügt über langjährige Erfahrung im Aufbau sicherer Software-Architekturen und ist zertifizierter Datenschutzbeauftragter.
www.althammer-kill.de

Thomas Althammer ist Geschäftsführer der Althammer & Kill GmbH & Co. KG und begleitet bundesweit Einrichtungen und Träger in IT-Strategiefragen, als externer Datenschutzbeauftragter und bei Fragen zur IT-Sicherheit. Beim Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e. V. (FinSoz) leitet er die Arbeitsgruppe IT-Compliance.
www.althammer-kill.de

Datenschutz und Schweigepflicht erfordern in sozialen Organisationen einen sorgsamen Umgang mit den persönlichen Daten der Nutzer. Dazu gehört die standardmäßige Verschlüsselung des E-Mail-Verkehrs, für die es mittlerweile durchaus praktikable Methoden gibt.

Es reicht einfachste Technik, um E-Mail-Nachrichten auf ihrem Weg mitlesen zu können. Jeder Computer und jedes Netzwerkgerät durch das die Nachricht läuft ist in der Lage diese mitzuschneiden und eine Kopie abzuzweigen. Dabei wandert unsere E-Mail durch viele Zwischenstationen. Vor Verlassen einer kleinen Einrichtung sind schon rund fünf IT-Geräte am Versand beteiligt. Bis die Nachricht auf dem Bildschirm unseres Empfängers zu sehen ist, wurde diese durch eine dreistellige Zahl von Computersystemen verarbeitet. Unsere E-Mails werden dabei protokolliert, gescannt und oft auch einfach Kopien vorgehalten, die wir nicht wünschen. Solche Daten können wir nicht mehr vor dem Zugriff Dritter schützen.

Wenn Informationen über Personen in Klartext auf fremden Geräten liegen, verstößt dies für sich schon gegen das Bundesdatenschutzgesetz und die Datenschutz-Verordnungen der Katholischen und Evangelischen Kirche. Die einschlägigen Gesetze definieren den vertrauensvollen und gesicherten Umgang mit personenbezogenen Daten.

Eine weitere rechtliche Falle ergibt sich aus der Verletzung der Schweigepflicht. Gerade in der Gesundheits- und Sozialwirtschaft unterliegen viele der per E-Mail ausgetauschten Informationen dem § 203 Strafgesetzbuch oder dem Sozialdatenschutz.

Die Konsequenzen bei Datenschutzverstößen sind nicht unerheblich. Bei einem unzulässigen Umgang mit den anvertrauten personenbezogenen Daten können durch die Aufsichtsbehörden Bußgelder festgesetzt werden. Das Bundesdatenschutzgesetz sieht Strafen bis zu 300.000 Euro vor, wobei das Strafmaß im Einzelfall festgelegt wird. Weitaus gravierender sind heutzutage jedoch die Folgen von bekannt gewordenen Datenschutzpannen und der damit einher gehende Imageschaden. Kritische Vorfälle werden heute gern von der Presse aufgegriffen und verbreitet (vgl. www.projekt-datenschutz.de).

Die Herausforderungen

Auf akademischer Ebene ist das Thema E-Mail-Verschlüsselung längst gelöst. Bislang hapert es an der praxistauglichen Umsetzung. Dazu müssen die folgenden Herausforderungen gemeistert werden:

- Komplexität: E-Mail-Verschlüsselung geht nicht »einfach so«. Es ist komplizierte Software und viel Wissen über Verschlüsselungsalgorithmen erforderlich.
- Kommunikationspartner: Die Gegenstellen müssen mitmachen. Es muss eine Sensibilisierung in allen Bereichen geschaffen werden, damit vertraulich mit Daten umgegangen wird.
- Verbreitung: Es werden Lösungen benötigt, die für alle Kommunikationspartner verfügbar sind und bei denen jeder bereit ist, diese auch zu nutzen.

Hier sind offene Standards gefragt, die von allen technischen Plattformen unterstützt werden.

- Gemeinsames Geheimnis: Wann immer zwei Parteien eine geheime Botschaft austauschen wollen, müssen sie einmalig eine Information – das »gemeinsame Geheimnis« – austauschen. Sie müssen sich sicher sein, dass diese unverändert von dem Kommunikationspartner stammt. Dies ist die Basis für jede weitere Kommunikation.
- Kosten: Eine Verschlüsselungssoftware an sich, aber auch administrativen Kosten und der Schulungsaufwand für die Mitarbeiter, wollen bezahlt werden. Nicht zu vergessen sind Folgekosten durch eine Verlangsamung der Prozesse, beispielsweise wenn der Kommunikationspartner eine Nachricht nicht entschlüsseln kann.

Technische Möglichkeiten

Inzwischen sind Lösungen auf dem Markt, die die Herausforderungen angegangen sind und praktikable, gesetzeskonforme Lösungen bieten. Als grundlegende Verschlüsselungsverfahren haben sich S/MIME und PGP etabliert.

- S/MIME ist in vielen Mail-Programmen umgesetzt, beispielsweise in Microsoft Outlook und auf allen gängigen Smartphones. Allerdings verstecken sich die Funktionen in schwierigen Konfigurationsdialogen. S/MIME nutzt zentrale Notare die – mit unterschiedlichen Qualitätsklassen – Anwender-Zertifikate unterschreiben. Die Notare sind die durch SSL (HTTPS) schon bekannten Stellen wie Comodo und D-Trust. Die öffentlichen Schlüssel von einer Reihe von Notaren sind in den E-Mail-Programmen und Betriebssystemen hinterlegt.
- PGP steht für Pretty Good Privacy, was ebenso wie S/MIME militärischen Standards im Bereich der Verschlüsselung entspricht. PGP wird auch als Oberbegriff für die kompatiblen und freien Versionen GPG bzw. GnuPG und OpenPG verwendet. Gerade die freie Verfügbarkeit hat PGP zu großer Beliebtheit verholfen. Im Gegensatz zu S/MIME basiert PGP auf einem Vertrauensnetzwerk, dem sogenannten »Web of Trust«. Hier werden öffentliche Schlüssel eines geprüften Kommunikationspartners digital signiert. Weiterhin kann ich wiederum dem Schlüssel eines Dritten trauen, wenn dieser auch von einem mir bekannten Kommunikationspartner signiert wurde. So wird ein Vertrauensnetzwerk nach dem Motto »Der Freund meines Freundes ist auch mein Freund« aufgespannt.

In den letzten Monaten sind einige Produkte auf den Markt gekommen, die eine eigene, neue Herangehensweise an die Thematik versuchen. Diese »Nicht-Standard-Produkte« verwenden zwar meist mathematisch erprobte Algorithmen für die Verschlüsselung, allerdings ohne dabei die etablierten Verfahren S/MIME oder PGP in kompatibler Weise zu verwenden. Dadurch entsteht eine Produktabhängigkeit (Vendor Lock-In) für beide Kommunikationspartner.

Eine praktische und elegante Lösung für Unternehmen ist die Nutzung eines E-Mail-Gateways. Der Gateway wird zwischen dem E-Mail-Server und dem Internet eingerichtet. Sobald eine Nachricht das interne, sichere Netzwerk verlässt, wird diese verschlüsselt und so auf sicherem Wege dem Empfänger zugestellt. Bei eingehenden E-Mails entschlüsselt der Gateway die Nachrichten, bevor sie an den internen E-Mail-Server weitergereicht werden.

Es gibt erste E-Mail-Gateways auf dem Markt, die automatisch je nach Gegenstelle die verschiedenen Verschlüsselungsverfahren (S/MIME oder PGP) anwenden. Eine dezentrale Verwaltung von Zertifikaten auf einzelnen PCs im Netzwerk entfällt, da die Schlüssel zentral im Gateway abgelegt sind. Sollte der Kommunikationspartner keinen der beiden Standards einsetzen, werden sensible Nachrichten als verschlüsselte PDF-Datei versendet. Dabei werden auch Anhänge verschlüsselt und in das PDF eingebettet.

Das Verschlüsselungskennwort wird dem Empfänger einmalig über einen sicheren Weg mitgeteilt (z. B. als SMS oder telefonisch). Das PDF-Dokument enthält zusätzlich eine Verknüpfung zu einer gesicherten Web-Seite, über die der Empfänger wiederum verschlüsselt antworten kann. Die Webseite steht dem externen Kommunikationspartner jederzeit für das Schreiben sicherer Nachrichten zur Verfügung.

Da PDF-Dateien praktisch von jedermann und auf jedem Gerät geöffnet werden können, kann über diesen Umweg eine pauschale Verschlüsslung aller E-Mail-Nachrichten realisiert werden. Aus Sicht des Unternehmens kann so ein Rechtsbruch verhindert werden. Selbstverständlich müssen bei dieser Lösung die Kommunikation zwischen Gateway und internem E-Mail Server sowie zu den E-Mail-Programmen wie Outlook, Mail oder auch Mobilgeräten verschlüsselt werden. Dies ist inzwischen aber allgemeinhin üblich und stellt keine Herausforderung dar.

Die Lösung erweist sich als elegant, da im internen Netzwerk keine weiteren Anpassungen notwendig sind. Eine Einführung im Unternehmen kann mit geringem Informationsaufwand erfolgen und sukzessive umgesetzt werden. ■

Spielarten der E-Mail-Verschlüsselung

1. Bei der Private-Key- bzw. symmetrischen Verschlüsselung gibt es genau einen Schlüssel (= ein Kennwort), das zum Verschlüsseln und Entschlüsseln genutzt wird. Dieser Schlüssel muss mit dem Kommunikationspartner ausgetauscht werden, darf dabei aber nicht in die Hände eines Dritten fallen. Dies Verfahren ist beispielsweise bekannt durch die Vergabe eines Kennwortes für ein Word-Dokument.

2. Bei der Public-Key-Verschlüsselung hat man zwei Schlüssel. Den privaten Schlüssel behält man immer für sich. Der öffentliche Schlüssel kann beliebig publiziert werden. Der öffentliche Schlüssel wird verwendet, um Nachrichten zu verschlüsseln. Man kann sich ein Schloss vorstellen, dass mit dem öffentlichen Schlüssel nur verschlossen werden kann. Allein der private Schlüssel erlaubt es die Daten zu entschlüsseln oder – dem Bildnis entsprechend – das Schloss zu öffnen. Essentiell ist bei diesem Verfahren, dass der verwendete öffentliche Schlüssel tatsächlich zu dem gewünschten Empfänger gehört und einem kein anderer Schlüssel untergeschoben wurde. Dieses kann durch eine dritte, möglichst vertrauensvolle Stelle – einem Notar – realisiert werden.

Alexander Kulbartsch und Thomas Althammer