Verschlüsselung mit Secure E-Mail-Gateways

Geschlossene Gesellschaft

Wer verhindern will, dass sein E-Mail-Verkehr mitgelesen werden kann, muss die Nachrichten verschlüsseln. Unternehmen können dazu heute auf Secure E-Mail-Gateways zurückgreifen. Unser Beitrag beschreibt den Lösungsansatz.

Von Peggy Hüpenbecker, Zertificon Solutions GmbH

Es ist mittlerweile bekannt, dass Angreifer unverschlüsselte E-Mails mit wenig Aufwand mitlesen und manipulieren können. Dagegen können sich Unternehmen sehr leicht schützen: Eine funktionierende E-Mail-Verschlüsselung erschwert die Arbeit der Wirtschaftsspione ungemein. Sie bietet einen wirksamen Schutz vor Abhörprogrammen und Manipulationen und schafft Vertraulichkeit, Integrität und Authentizität. Auch fordern verschiedene Vorschriften und Gesetze auf nationaler und internationaler Ebene abhängig von der Sensibilität des E-Mail-Inhalts eine Verschlüsselung nach dem Stand der Technik. In vielen Fällen haftet die Geschäftsführung sogar persönlich für unzureichende IT-Sicherheitsmaßnahmen.

Ein einfacher und schneller Weg, eine E-Mail-Verschlüsselung im Unternehmen zu realisieren, ist, sogenannte Secure E-Mail-Gateways einzusetzen. Diese werden zentral im Unternehmen aufgestellt und gewährleisten die Durchsetzung der Sicherheitspolicies. Alle E-Mails, die das Unternehmen erreichen oder verlassen, werden über das Gateway geleitet und dort zentral wie in einer virtuellen Poststelle den Einstellungen entsprechend bearbeitet. Die meisten Gateway-Lösungen arbeiten mit Contentfiltern, Antiviruslösungen oder Data-Loss-Prevention-(DLP)-Tools zusammen. Ein weiterer Vorteil ist, dass sie Benutzer nicht in ihrer täglichen Arbeit beeinträchtigen. So stellt sich auch die Frage nach der Akzeptanz nicht.

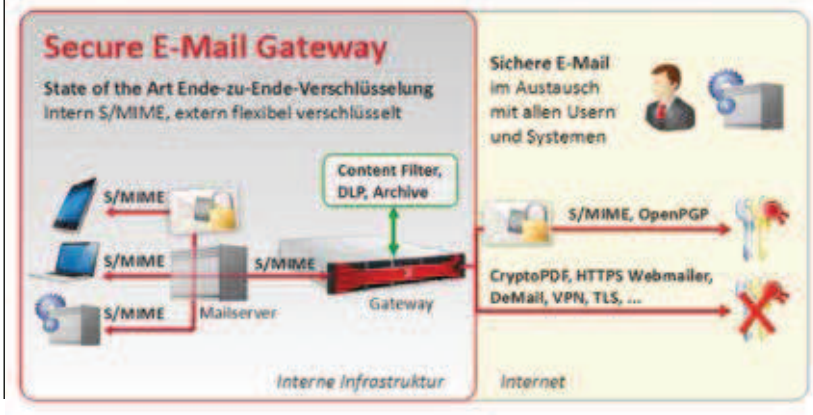
Alternative Zustellmethoden

Die heutigen Standards für verschlüsselte und signierte Daten sind S/MIME und OpenPGP. Hier besitzen die Kommunikationspartner je zwei Schlüssel, einen privaten und einen zertifizierten öffentlichen Schlüssel – das Zertifikat. Wie in einem Telefonverzeichnis werden öffentliche Schlüssel (Zertifikate) einer Person oder einem System zugeordnet.

Mit der Anzahl der Teilnehmer wächst die Komplexität einer Public-Key-Infrastruktur (PKI). Da Zertifikate für einen bestimmten Zeitraum ausgestellt werden, können diese ablaufen und auch widerrufen werden. Wirklich sicher wird das System aber nur, wenn man sich im Moment der verschlüsselten Kommunikation darauf verlassen kann, dass die Zertifikate echt und gültig sind. Dafür wurden Zertifikatsserver entwickelt, die das Management der Zertifikate und öffentlichen Schlüssel einschließlich der Verifizierung und Validierung automatisiert übernehmen.

Zertifikatsserver sind über verschiedene Schnittstellen mit den Trustcentern und den Zertifizierungsstellen (CAs) größerer Firmen verbunden. Sie rufen Gültigkeitsinformationen über Rückruflisten (Certificate Revocation Lists) ab und führen Echtzeitabfragen durch. So werden Daten eingeholt, Prüfsummen verglichen und der lokale Zertifikatsbestand permanent aktualisiert. Optimalerweise greifen Secure E-Mail-Gateways zur PKI-basierten Verschlüsselung auf Dienste der Zertifikatsserver zu.

Kann für einen Kommunikationspartner kein Zertifikat gefunden werden, stehen alternative Zustellmethoden zur Verfügung, bei denen ein Passwort den privaten Schlüssel



Die Grafik zeigt die Arbeitsweise des Z1 SecureMail Gateways von Zertificon.

ersetzt. Secure E-Mail-Gateways können dadurch neben S/MIME- und OpenPGP-verschlüsselten E-Mails auch passwortverschlüsselte PDF-, HTML- oder ZIP-Container ausliefern. Auch die ad-hoc-Erstellung sicherer Webmailer-Accounts ist eine beliebte Alternative. De-Mail-Anbindungen, VPN- und TLS-Unterstützung sind ebenfalls auf einigen Gateways verfügbar. Mit einem gut ausgewählten Secure E-Mail-Gateway, ist so die komplette Sicherung des E-Mail-Verkehrs von und nach außen sichergestellt, unabhängig von der IT-Umgebung der Empfänger.

Mobile Kommunikation

Eine besondere Herausforderung stellt der mobile E-Mail-Versand über Smartphones oder Notebooks dar. Zur Verschlüsselung der mobilen Kommunikation benötigen die Geräte eine Client-Anbindung an die PKI, sodass eine Ende-zu-Ende-Verschlüsselung umsetzbar ist. Diese wird jedoch von den Herstellern recht unterschiedlich interpretiert und birgt als „echte“ Ende-zu-Ende-Verschlüsselung große unternehmerische Risiken. Da die E-Mail direkt auf dem Client verschlüsselt und erst wieder beim Empfänger entschlüsselt wird, können auch keine IT-Sicherheitssysteme wie Contentfilter, Antivirus, Antispam, DLP und Archivierung auf die Daten zugreifen. Das Fehlen dieser Standards widerspricht jedoch den Compliance-Anforderungen und birgt hohe Risiken für den Geschäftsbetrieb. Auch ist die echte Ende-zu-Ende-Verschlüsselung für den normalen Geschäftsbetrieb kaum geeignet, da Sender und Empfänger genau den gleichen Standard nutzen müssen: S/MIME oder OpenPGP.

Um den mobilen E-Mail-Versand abzusichern, ermöglichen einige Secure E-Mail-Gateways eine Verknüpfung zwischen interner und externer E-Mail-Verschlüsselung, sodass Nachrichten nicht nur über das Internet, sondern auch innerhalb der firmeninternen Netze in verschlüsseltem Zustand übertragen werden. Dazu wird eine interne gekapselte PKI aufgesetzt, die eine S/MIME-Verschlüsselung direkt auf dem Client umsetzt. Die eigens dafür ausgestellten X.509 Zertifikate verlassen das Unternehmen nie.

Ausgehende E-Mails werden dann per S/MIME auf dem mobilen Client mit dem Zertifikat des Gateways verschlüsselt. Die E-Mail-Clients unterstützen S/MIME von Haus aus, für Mobilgeräte gibt es leicht zu installierende Apps. Das Secure E-Mail-Gateway entschlüsselt die E-Mail und sucht nach dem Zertifikat des Empfängers. Je nach Verfügbarkeit von Zertifikaten der externen Kommunikationspartner wird flexibel neu verschlüsselt, zum Beispiel nach S/MIME, OpenPGP, CryptoPDF, De-Mail oder TLS. Umgekehrt erreichen alle eingehenden in jedweder Art verschlüsselten Nachrichten den internen Empfänger als S/MIME-verschlüsselte E-Mail. Im Moment der Umverschlüsselung liegen die Daten im Klartext vor und können von den anderen Sicherheitslösungen, wie Antispam oder DLP, geprüft beziehungsweise verarbeitet werden. Für Daten mit einem sehr hohen Schutzbedarf kann man Secure E-Mail-Gateways auch mit einer echten Ende-zu-Ende-Verschlüsselung kombinieren. Das eignet sich beispielsweise für einen sehr kleinen und exklusiven Empfängerkreis. ■