zertificon®
Einfach. Sicher. Verschlüsseln.

White Paper

Ende-zu-Ende E-Mail-Verschlüsselung für alle?

Warum Privatleute und Unternehmen verschiedene Lösungen benötigen

White Paper

Ende-zu-Ende E-Mail-Verschlüsselung für alle?

Warum Privatleute und Unternehmen verschiedene Lösungen benötigen

E-Mail-Verschlüsselung ist besonders seit Edward Snowdens Enthüllungen um die NSA inklusive PRISM und Tempora ein brennendes Thema. Vielfach wurde in den Medien Ende-zu-Ende-Verschlüsselung für den E-Mail-Austausch als Lösung allen Übels propagiert.

Doch die Ende-zu-Ende-Verschlüsselung für E-Mails sollte abhängig vom Anwendungsfall sehr differenziert betrachtet werden. Ende-zu-Ende-Verschlüsselung bedeutet die lückenlose Verschlüsselung vom Sendegerät bis zum Empfangsgerät. Die Nachrichten liegen nirgendwo sonst im Klartext vor, nicht mal für Sekundenbruchteile beim Provider. Nur Sender und Empfänger verfügen über die notwendigen Schlüssel zum Ver- und Entschlüsseln der E-Mail.

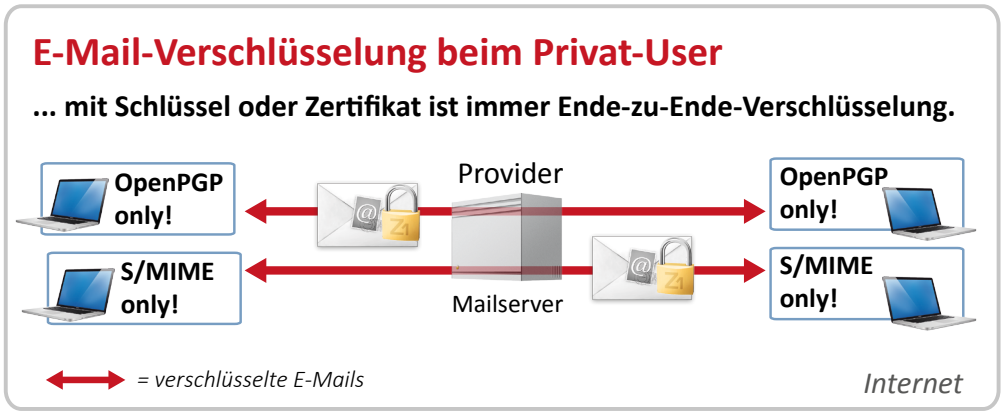
Vorschriften beim E-Mail-Einsatz

Wie in vielen anderen Bereichen ist bei der E-Mail-Verschlüsselung eine Lösung, die für Privatleute sinnvoll ist, für Unternehmen nur eingeschränkt nutzbar. Die Motivationslage sowie die rechtlichen Vorschriften zur Dokumentation und zum Datenschutz unterscheiden sich im privaten und im geschäftlichen Bereich deutlich. Das Thema Data Loss Prevention sowie zentrale Spam- und Virenscans spielen für den Privat-User in der Regel keine Rolle, da im Heimbereich die Spam- und Virusfilter vor der Verschlüsselung bzw. nach der Entschlüsselung lokal auf dem Rechner arbeiten. Nicht zuletzt ist die Skalierbarkeit des Schlüsselmanagements für den Privat-User zu vernachlässigen, für Unternehmen jedoch entscheidend. Ein manuelles Schlüsselmanagement ist bei steigender Anzahl der Mitarbeiter und Kommunikationspartner nicht mehr wirtschaftlich umsetzbar.

Verschlüsselungsstandards

In der privaten E-Mail-Kommunikation ist die kostenfreie Verschlüsselung mit OpenPGP verbreitet. Im Unternehmensbereich hat sich S/MIME mit durch TrustCenter ausgestellten X.509-Zertifikaten als öffentliche Schlüssel vor der PGP-Verschlüsslung etabliert.

Beide Verschlüsselungsstandards sind nicht miteinander kompatibel. Privatleute entscheiden sich also für einen Standard und sind in der Kommunikation davon abhängig, dass der Kommunikationspartner genau denselben Standard nutzt. Wer direkt im Mailprogramm seine Mails verschlüsselt und keinen proprietären Anbieter nutzt, setzt Ende-zu-Ende-Verschlüsselung um und braucht sich um die Vertraulichkeit seiner Nachrichten nicht mehr zu sorgen.



SecureMail Gateway kompatibel mit allen Standards

Firmen nutzen oftmals sogenannte SecureMail Gateways, die sowohl mit X.509-Zertifikaten als auch mit OpenPGP Keys verschlüsseln können und teilweise zusätzlich Alternativen wie Passwortverschlüsselung bieten. Dies ist besonders praktisch, wenn der Kommunikationspartner weder ein X.509-Zertifikat noch einen PGP-Schlüssel besitzt und trotzdem ad hoc vertrauliche Nachrichten ausgetauscht werden sollen. Bei der Passwortverschlüsselung werden die Nachrichten beispielsweise als verschlüsselte PDFs oder HTML-Container im E-Mail-Anhang zugestellt oder über einen HTTPS-gesicherten Webmailer abgerufen. De-Mail-Anbindungen, VPN- und TLS-Unterstützung sind ebenfalls auf einigen Gateways verfügbar. So können Unternehmen ohne Verzögerung mit jedermann verschlüsselt kommunizieren.

Die Unternehmen nutzen dabei in der Regel keine Ende-zu-Ende-Verschlüsselung. Das SecureMail Gateway bildet eine zentrale Schnittstelle zum Internet und ent- bzw. verschlüsselt von und nach außen. Innerhalb des Firmennetzwerkes werden E-Mails jedoch unverschlüsselt transportiert. Für den Schutz gegen Geheimdienstprogramme und Wirtschaftsspionage im Internet ist das eine sichere und bewährte Methode. Die Notwendigkeit für Ende-zu-Ende-Verschlüsselung in Unternehmen ist grundsätzlich anders begründet als die des Privatmenschen, der sowieso nur Ende-zu-Ende verschlüsseln kann.

Ende-zu-Ende Motivation und Hürden für Unternehmen

Für Unternehmen wird Ende-zu-Ende E-Mail-Verschlüsselung spannend, wenn Smartphones und Notebooks für geschäftliche E-Mails genutzt werden. Denn auch in der unternehmensinternen Kommunikation werden E-Mails auf den Mobilfunkstrecken und im öffentlichen WLAN im Klartext übertragen. Ein weiterer Sicherheitsaspekt ist die unverschlüsselte Ablage der firmeninternen E-Mails auf dem E-Mail-Server. Wer nicht möchte, dass Administratoren die dort gespeicherten E-Mails mitlesen können, muss auch auf internen Teilstrecken verschlüsseln. Bei der Umsetzung einer Ende-zu-Ende-Verschlüsselung in einem Unternehmen müssen verschiedene Problemstellungen bedacht werden:

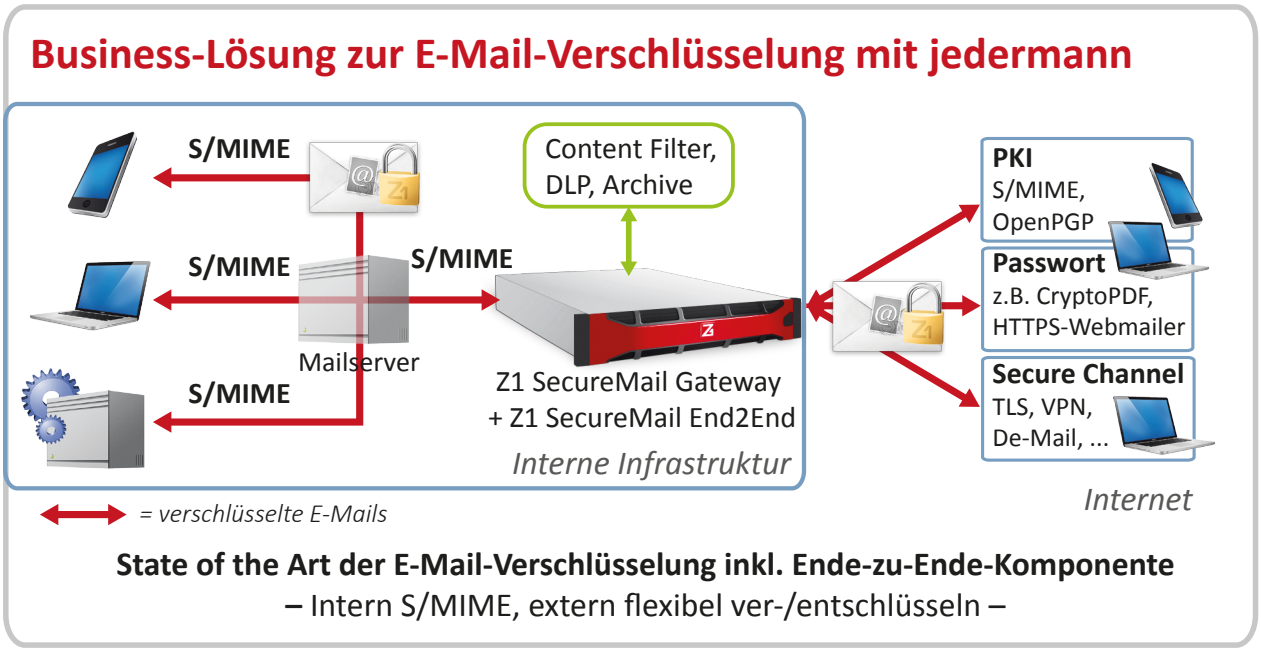
- Mit welchem Verschlüsselungsstandard soll verschlüsselt werden, wenn die Standards nicht miteinander kompatibel sind, das Ziel aber die sofortige vertrauliche Kommunikation mit jedermann ist?
- Wie verschlüsselt man mit Empfängern, die kein Zertifikat besitzen?
- Wie können eingehende verschlüsselte E-Mails lokal auf allen Endgeräten im Unternehmen entschlüsselt werden?
- Wie greifen Data Loss Prevention Systeme auf die E-Mails zu? Wie läuft der Antivirusscan, wenn die E-Mail verschlüsselt ist?
- Wie kann ein zentrales Schlüsselmanagement der internen Schlüssel und der Schlüssel externer Kommunikationspartner umgesetzt werden?
- Was passiert bei Mitarbeiterwechseln oder Krankheit, wenn wirklich nur der Mitarbeiter Zugriff auf seine E-Mails besitzt?

Hier braucht es einen cleveren Ansatz, den

State of the Art der Ende-zu-Ende E-Mail-Verschlüsselung mit flexibler Umverschlüsselung auf dem Gateway

Moderne SecureMail Gateways mit Erweiterungen ermöglichen eine Verknüpfung zwischen interner und externer E-Mail-Verschlüsselung. E-Mails werden dabei nicht nur über das Internet, sondern auch innerhalb der firmeninternen Netze in verschlüsseltem Zustand übertragen. 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 niemals.

Ausgehende E-Mails werden per S/MIME auf dem Client mit dem Zertifikat des Gateways verschlüsselt – die Mail-Clients



unterstützen S/MIME von Hause aus, für Mobilgeräte gibt es leicht zu installierende Apps. Das SecureMail Gateway entschlüsselt die E-Mail und sucht nach dem Zertifikat des Empfängers. Je nach Verfügbarkeit von Zertifikaten der externen Kommunikationspartner wird flexibel neu verschlüsselt nach S/MIME, OpenPGP, verschlüsseltem PDF oder HTML-Container, sicherem HTTPS-Webmailer, De-Mail, TLS, …

Umgekehrt erreichen alle eingehenden in jedweder Art verschlüsselten E-Mails den internen User als S/MIME verschlüsselte E-Mail. Im Moment der Umverschlüsselung auf dem Gateway greifen die Schnittstellen für Antivirus, Antispam, DLP, Archivierung etc.

SecureMail Gateways können mit echter Ende-zu-Ende-Verschlüsselung kombiniert werden, die vielleicht in einem kleinen Empfängerkreis mit ihren Vor- und Nachteilen durchaus gewünscht ist.

Bei Zertificon unterscheidet man bei Z1 SecureMail End2End in Kombination mit Z1 SecureMail Gateway zwischen **Organizational End2End** mit den genannten Vorteilen der flexiblen Umverschlüsselung auf dem Gateway und **Personal End2End**, was der Ende-zu-Ende-Verschlüsselung bei E-Mails im Privatbereich entspricht.

Die in der Post-Snowden-Zeit vielfach propagierte Ende-zu-Ende-Verschlüsselung ist demnach für Privatleute und Firmen gänzlich unterschiedlich zu betrachten. Für beide gibt es Lösungen und natürlich können Firmen auch mit Privatleuten verschlüsselt kommunizieren.

Der Dreh- und Angelpunkt für alle, die E-Mail-Verschlüsselung mit X.509-Zertifkaten oder OpenPGP-Schlüsseln durchführen, ist Z1 Global TrustPoint (www.globaltrustpoint.com). Hier können von jedermann eigene Schlüssel publiziert werden. Fremde Schlüssel können nicht nur gesucht und gefunden, sondern auch auf ihre Gültigkeit hin validiert werden. Denn auch der sicherste Verschlüsselungsalgorithmus ist nutzlos, wenn niemand prüft, ob die verwendeten Schlüssel echt und gültig sind.