zertificon®
Einfach. Sicher. Verschlüsseln.

WHITE PAPER

Ende-zu-Ende-Verschlüsselung für Unternehmen

Wie Ende-zu-Ende-Verschlüsselung für E-Mails in Unternehmensumgebungen definiert ist und leicht umgesetzt werden kann

Ende-zu-Ende-Verschlüsselung für Unternehmen

Wie Ende-zu-Ende-Verschlüsselung für E-Mails in Unternehmens-umgebungen definiert ist und leicht umgesetzt werden kann

E-Mail-Verschlüsselung ist 2014 durch Edward Snowdens Enthüllungen um die NSA in den Fokus der Öffentlichkeit gerückt. Seit 2018 erhält das Thema durch die EU Datenschutz-Grundverordnung (EU DS-GVO) und eine steigende Digitalisierungsrate stetige Aufmerksamkeit. Von 2014 bis heute wurde in unzähligen Artikeln die Ende-zu-Ende-Verschlüsselung für den E-Mail-Austausch als One-Size-fits-All-Lösung für Unternehmen und Privatuser propagiert – allerdings fast immer ohne die Sicherheits- und Compliance-Anforderungen im Businessumfeld zu bedenken.

Wir möchten Ihnen mit diesem White Paper helfen, einen Überblick zu gewinnen und Medienberichte sowie Marktaussagen richtig einzuordnen. Dazu stellen wir Ihnen die unterschiedlichen Möglichkeiten, Standards und Abhängigkeiten für Ende-zu-Ende-Verschlüsselung im Unternehmenskontext in Abgrenzung zum Privatbereich vor. So können Sie eine informierte Entscheidung für Ihr Unternehmen treffen.

Ende-zu-Ende-Verschlüsselung, eine Definitionssache

Bei E-Mails wird unter Ende-zu-Ende-Verschlüsselung üblicherweise die lückenlose Verschlüsselung vom Sendegerät bis zum Empfangsgerät verstanden. Es wird dabei vorausgesetzt, dass einzig der Empfänger über die Möglichkeit verfügt, die für ihn bestimmten Daten zu entschlüsseln.

In der geschäftlichen Kommunikation kann jedoch auch das Unternehmen an sich als ein Ende der Ende-zu-Ende-Kommunikation angesehen werden und nicht der einzelne Mitarbeiter mit seinem PC oder Smartphone. Viele Firmen und Behörden setzen zentrale Secure Mail Gateways für die Verschlüsselung von E-Mails ein. Das Gateway steht am Übergang des Unternehmensnetzwerkes zum Internet und ver- und entschlüsselt E-Mails für den Transport über das Internet nach festgelegten Regeln.

Es gibt Szenarien, in denen die Sicherung der E-Mails mit einem Gateway gegen Angriffe über das Internet nicht ausreicht, da E-Mail-Inhalte auch auf internen Servern oder in der Cloud geschützt werden müssen.

Zwei wichtige Erkenntnisse zu Beginn:

1. Ende-zu-Ende-Verschlüsselung für E-Mails muss zwingend die beteiligten Parteien sowie die spezifischen Anwendungsfälle berücksichtigen.

2. Je höher die Sicherheitsstufe, desto mehr Fachwissen ist bei den Anwendern, den eigenen Mitarbeitern, erforderlich und desto höher wird die Mitarbeiterverantwortung, weil weniger automatisiert werden kann.

Warum Privatanwenderlösungen für Unternehmen nicht funktionieren

Wie in vielen anderen Bereichen auch ist bei der E-Mail-Verschlüsselung eine Lösung, die für Privatleute gut geeignet ist, für Unternehmen nicht sinnvoll einsetzbar.

Aus Gründen der Compliance und zur Umsetzung zentraler IT-Sicherheitsaufgaben benötigen Unternehmen Zugriff auf den E-Mail-Verkehr. Anforderungen wie Dokumentationspflichten, Archivierung oder die Einhaltung der EU DS-GVO brauchen Privatanwender nicht zu kümmern. Für Unternehmen sind sie entscheidend, genau wie die Themen Data Loss Prevention sowie zentral ausgeführte Spam- und Virenscans.

In der privaten E-Mail-Kommunikation ist die Verschlüsselung mit kostenfreien selbst ausgestellten OpenPGP-Schlüssel verbreitet. Im Unternehmensbereich wird überwiegend der S/MIME-Standard genutzt. Dabei werden kostenpflichtige durch Trustcenter ausgestellte X.509-Zertifikate als öffentliche Schlüssel verwendet.

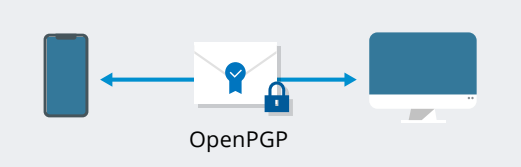

Abb. 1: E-Mail-Verschlüsselung im Privatbereich ist immer Ende-zu-Ende-Verschlüsselung

S/MIME und OpenPGP – und damit die private sowie die geschäftliche sichere Kommunikation – sind nicht miteinander kompatibel. Um sicher und dennoch effizient E-Mails auszutauschen, benötigen Unternehmen eine Lösung, die verschiedene Verschlüsselungsarten parallel unterstützt. Mit allen Kontakten – egal, ob diese OpenPGP, S/MIME oder auch keine eigene Verschlüsselungslösung nutzen – muss der sichere Austausch gelingen.

Privatanwender können mit einigem Aufwand den eigenen Schlüssel und die Schlüssel der Kommunikationspartner auf ihren Geräten verwalten. In Unternehmen dagegen kann die Verwaltung von Schlüsseln und Zertifikaten nicht dem einzelnen Mitarbeiter überlassen werden. Automatisierung ist der einzige Weg, um effzient zu skalieren und menschliche Fehler – beispielsweise bei der Gültigkeitsprüfung von E-Mail-Zertifikaten – zu vermeiden. Compliance-Vorgaben erfordern auditierbare Lösungen. Dies ist kaum umsetzbar, wenn die Mitarbeiter selbst für die Schlüsselverwaltung und Verschlüsselung auf den Geräten verantwortlich sind.

Ein Secure Mail Gateway als „Ende“ der Kommunikation

Im Gegensatz zu Privatpersonen verwenden Unternehmen im Allgemeinen keine E-Mail-Verschlüsselung vom Sendergerät zum Empfängergerät. In der sicheren Unternehmenskommunikation haben sich sogenannte Secure Mail Gateways etabliert. Diese bilden das Ende des Unternehmens in der Kommunikationskette. Ein Gateway übernimmt die Ver- und Entschlüsselung von ein- und ausgehenden Nachrichten für die gesamte Belegschaft sowie für automatisierte Geschäftssysteme.

Gateways können sowohl mit S/MIME als auch mit OpenPGP verschlüsseln. Sollte der Kommunikationspartner weder ein X.509-Zertifikat noch einen PGP-Schlüssel besitzen, bieten viele Gateways alternative Verschlüsselungsverfahren mit Passwort an. Diese Art der sicheren Ad-hoc-Kommunikation ist sehr gefragt für den datenschutzkonformen Austausch mit Privatpersonen. Durch eine weitgehende Automatisierung wird eine höhere Sicherheit als durch einfachen Passwortschutz gewährleistet.

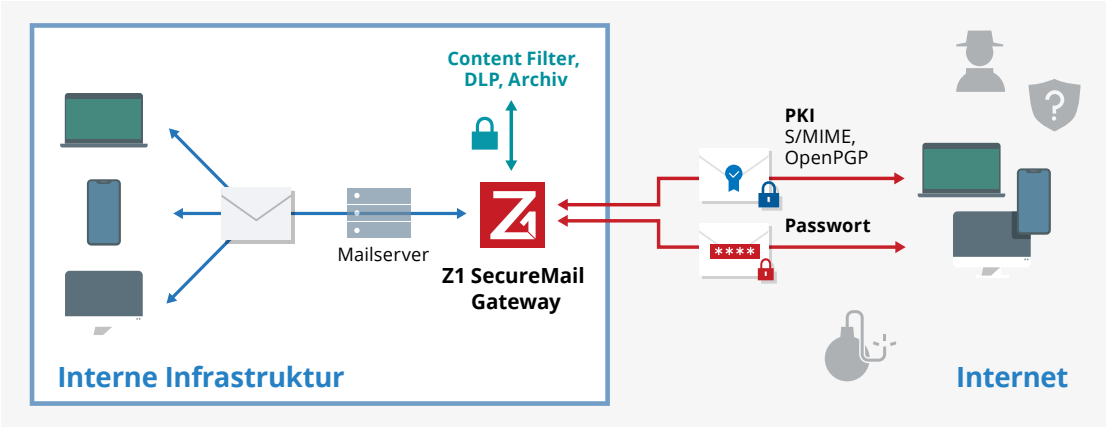

Abb. 2: E-Mail-Verschlüsselung mit Secure E-Mail Gateway. Alle E-Mails sind beim Versand über das Internet gegen Angriffe geschützt.

Innerhalb des Firmennetzwerkes werden E-Mails jedoch unverschlüsselt transportiert. Mit Firewalls verhindern Unternehmen den unbefugten Zugriff auf die E-Mails im eigenen Unternehmensnetz. Für den Schutz gegen Wirtschafts- und Industriespionage sowie Cyberangriffe über das Internet ist das eine sichere und bewährte Methode (siehe Abb. 2). Auch die Compliance ist vollumfänglich erfüllt. Sollten dies Ihre Beweggründe für E-Mail-Verschlüsselung sein, haben Sie eine Lösung gefunden!

Wenn Sie sich für Zertificons Z1 SecureMail Gateway entscheiden, erhalten Sie nicht nur die Durchsetzung der E-Mail-Compliance durch zentral konfigurierbare Sicherheitsrichtlinien, sondern auch einen unerreichten Grad an Automatisierung in der sehr komplexen, fehleranfälligen und herausfordernden Welt des E-Mail-Zertifikatsmanagements. Mit einem Z1 SecureMail Gateway sichern Sie Ihr Ende der Kommunikation zuverlässig ab!

Der hohe Sicherheitsstandard der Verschlüsselung und Signatur mit einem Gateway ist in vielen Branchen bereits weit verbreitet. Damit sind Sie sofort anschlussfähig, wenn Kooperationspartner oder Auftraggeber Sie zur verschlüsselten Kommunikation auffordern.

Lesen Sie weiter, wenn Sie für Ihr Unternehmen die Notwendigkeit einer Ende-zu-Ende-Verschlüsselung für E-Mails auch auf internen Strecken bis zum Endgerät sehen.

E-Mail-Verschlüsselung bis zum Endgerät: Motivation und Hürden für Unternehmen

Unternehmen sollten sich mit Ende-zu-Ende-Verschlüsselung für E-Mails bis zum Endgerät der Mitarbeiter beschäftigen, wenn Smartphones und Notebooks für geschäftliche E-Mails genutzt werden. Denn auch die unternehmensinterne E-Mail-Kommunikation wird 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 Strecken verschlüsseln.

Bei der Umsetzung von Ende-zu-Ende-Verschlüsselung bis zum Endgerät müssen Unternehmen verschiedene Fragestellungen bedenken:

- Mit welchem Verschlüsselungsstandard soll verschlüsselt werden, wenn die Standards nicht miteinander kompatibel sind?

- Wie funktioniert die Verschlüsselung 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 Management der internen Schlüssel und der Schlüssel externer Kommunikationspartner umgesetzt werden?
- Was passiert bei Mitarbeiterwechseln oder Krankheit, wenn nur der Mitarbeiter Zugriff auf seine E-Mails besitzt?

Bei Zertificon sind diese Herausforderungen bekannt. Wir haben dafür „Organizational End2End"-Verschlüsselung entwickelt.

„Organizational End2End"-Verschlüsselung mit Gateway-Touch

Um den Unternehmensanforderungen für Ende-zu-Ende-Verschlüsselung ab dem Mitarbeiter-PC oder -Smartphone gerecht zu werden, kann das bewährte Z1 SecureMail Gateway um die Komponente Z1 SecureMail End2End erweitert werden. Damit werden E-Mails nicht nur über das Internet, sondern auch innerhalb der firmeninternen Netze verschlüsselt. Das Gateway arbeitet Hand in Hand mit Z1 SecureMail End2End als Schnittstelle zwischen interner und externer Verschlüsselung (siehe Abb. 4).

Während über das Internet weiterhin alle Verschlüsselungsmethoden unterstützt werden, arbeitet die interne Verschlüsselung ausschließlich in einer eigenen S/MIME-Welt. Die dazu notwendigen S/MIME-Schlüsselpaare werden exklusiv im eigenen Unternehmensnetz genutzt. Sie verlassen das Unternehmen niemals. E-Mail-Programme unterstützen S/MIME als Standard; für Mobilgeräte stehen Apps zur Verfügung.

Z1 SecureMail End2End übernimmt das Schlüssel- und Zertifikatsmanagement auf den Endgeräten der Mitarbeiter.

So funktioniert Organizational End2End

Ausgehende E-Mails werden auf dem Endgerät mit dem S/MIME-Zertifikat des Gateways verschlüsselt. Das Z1 SecureMail Gateway entschlüsselt die E-Mail und sucht nach dem Zertifikat des Empfängers. Je nach Verfügbarkeit von Zertifikaten der externen Kommunikationspartner wird neu verschlüsselt nach S/MIME oder OpenPGP. Sollte kein Zertifikat gefunden werden, wird passwortbasiert verschlüsselt.

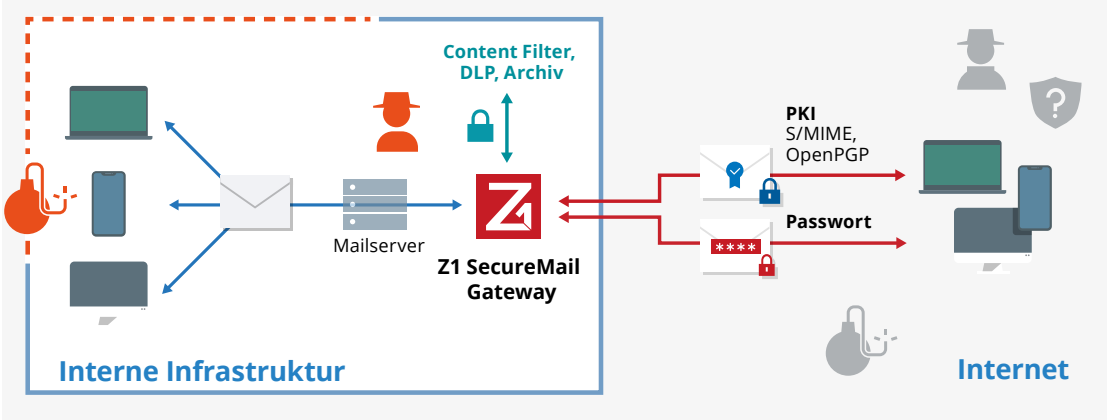

Abb. 3: Bei der Nutzung von mobilen Endgeräten oder wenn Admins am Mailserver keinen Zugriff auf die E-Mails haben sollen, braucht es bei der E-Mail-Verschlüsselung auch den Schutz der internen Strecke.

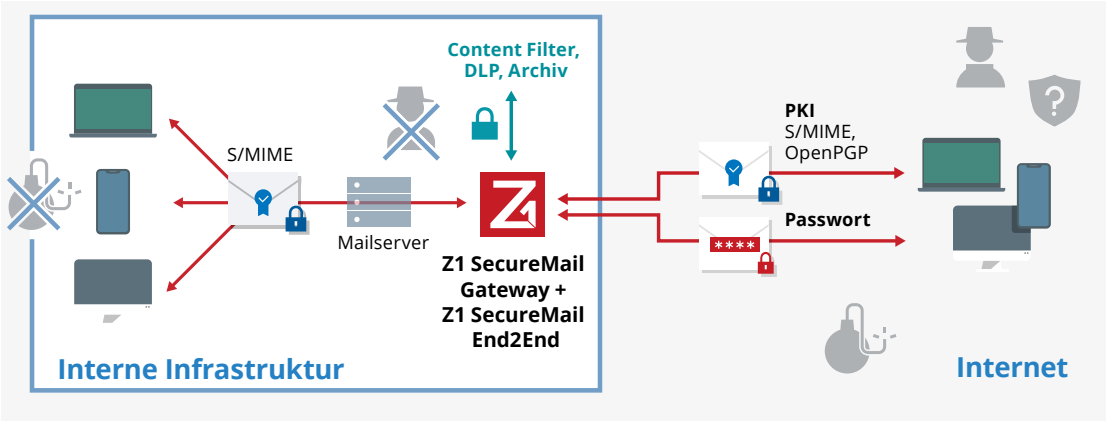

Abb. 4: ***Organizational End2End*** *State-of-the-Art der E-Mail-Verschlüsselung*
– Intern S/MIME, extern je nach Technologie des Kommunikationspartners ver- und entschlüsseln –

Eingehende E-Mails werden auf dem Gateway entschlüsselt und wieder verschlüsselt. Unabhängig von der Originalverschlüsselung wird vom Gateway zur internen Zustellung – ob an Mitarbeiter oder automatisierte Systeme – S/MIME verwendet.

Im Moment der Umverschlüsselung auf dem Gateway greifen die Schnittstellen für Antivirus, Antispam, DLP, Archivierung etc. sowohl bei eingehenden als auch bei ausgehenden E-Mails.

Personal End2End Encryption

Z1 SecureMail End2End ermöglicht auch Personal Ende-zu-Ende-Verschlüsselung wie aus dem Privatnutzerbereich bekannt – von Endgerät zu Endgerät ohne Umverschlüsselung auf dem Gateway. Dabei unterstützt Z1 SecureMail End2End das Schlüssel- und Zertifikatsmanagement auf dem Endgerät sowohl beim Verschlüsseln als auch beim Entschlüsseln und erhöht so die Anwenderfreundlichkeit der Ende-zu-Ende-Verschlüsselung.

Der zentrale Zugriff von Drittsystemen ist nicht möglich. Wir empfehlen, Personal End2End nur in ausgewählten Kommunikationsszenarien einzusetzen, beispielsweise im Austausch zwischen Vorstandsmitgliedern.

Die nächsten Schritte

Sie haben gelernt, dass Zertificon alle Ihre Anforderungen an Ende-zu-Ende-Verschlüsselung für E-Mails erfüllt. Mit Z1 Lösungen können E-Mails auf allen Strecken im Internet, im eigenen Netz, auf Servern und Endgeräten verschlüsselt werden. Mit Zertificon gestalten Sie Digitalisierung sicher und setzen firmenweite Compliance einfach und sehr effizient um.

Z1 SecureMail Gateway ist auch für Sie in jedem Fall die richtige Investition für Sicherheit und Compliance. Weitere Ausbaustufen für Organizational oder Personal End2End können Sie jederzeit hinzubuchen.

Was sind Ihre Herausforderungen in der sicheren geschäftlichen Kommunikation? Wir erfüllen sie ganz bestimmt.

Weitere Informationen:

Z1 SecureMail Gateway

Z1 SecureMail End2End

Oder kommen Sie gern direkt auf uns zu: sales@zertificon.com.

Um als erster von neuen White Papers, Webinaren etc. zu erfahren, registrieren Sie sich für unseren Zertificon-Newsletter

Über Zertificon Solutions GmbH

Zertificon ist führender Software-Hersteller im Bereich IT-Sicherheit mit Sitz in Berlin. Als unabhängiges, vom Gründer geführtes Unternehmen mit eigenen Abteilungen für Entwicklung, Vertrieb und Support beschäftigt Zertificon knapp 120 Mitarbeiter.

Mit dem preisgekrönten **Z1 SecureMail Gateway** leistete das Zertificon-Team vor über 15 Jahren Pionierarbeit im Markt der serverbasierten E-Mail-Verschlüsselung. Heute zählt das Unternehmen mit neuen, zukunftsweisenden Entwicklungen zu den treibenden Kräften bei IT-Sicherheit und Datenschutz in der geschäftlichen elektronischen Kommunikation.

Bei Zertificon liegt der Fokus auf der Entwicklung anwenderfreundlicher und wirtschaftlicher Gesamtkonzepte für den vertraulichen E-Mail- und Datenaustausch. Neben dem **Z1 SecureMail Gateway,** der bewährten Lösung zur E-Mail-Verschlüsselung und E-Mail-Signatur, sowie dem **Z1 CertServer** zur zentralen Zertifikatsverwaltung und -validierung gehört der **Z1 SecureHub** zum Portfolio: eine webbasierte Portallösung zum sicheren Transfer von Dateien aller Formate und Größen. Mit **Z1 MyCrypt BigAttach** wird Z1 SecureHub direkt aus dem Mailprogramm bedient.

Nicht zuletzt bietet die jüngste Innovation **Z1 SecureMail End2End** als Erweiterung des Z1 SecureMail Gateways unternehmenstaugliche Ende-zu-Ende-Verschlüsselung und definiert den State-of-the-Art als Organizational oder Personal End2End. Für die Nutzung auf Endgeräten steht **Z1 MyCrypt Mail** als Add-in für MS Outlook und Lotus Notes oder als App für iOS und Android bereit.

Für die einfache Integration sowie den effizienten und reibungslosen Betrieb der Z1 Lösungen hat Zertificon virtuelle **Z1 Appliances** entwickelt. Als Betriebssystem setzt Zertificon seit Jahren Linux auf Basis der in der IT Security Community hoch angesehenen Debian-Distribution ein.

In Betriebsfragen bietet der viel gelobte **Zertificon-Herstellersupport** mit direkten Ansprechpartnern schnelle und kompetente Hilfe.

Zertificon ermöglicht auch Ihrem Unternehmen die einfache Erfüllung höchster Sicherheits- und Compliance-Anforderungen in der sicheren geschäftlichen Kommunikation. Melden Sie sich noch heute, wir haben auch für Sie das passende Angebot.