zertificon®
Einfach. Sicher. Verschlüsseln.

White Paper

Sichere E-Mail im Zeitalter hoher Mobility

Angewandte Kryptologie: Zertifikate, Gateways und Ende-zu-Ende-Verschlüsselung

White Paper

Sichere E-Mail im Zeitalter hoher Mobility

Angewandte Kryptologie: Zertifikate, Gateways und Ende-zu-Ende-Verschlüsselung

Im Wesentlichen sind es zwei Triebkräfte, die Entscheider dazu bringen, sich mit dem Thema Verschlüsselung zu beschäftigen. Zum einen besitzen Unternehmer ein ureigenstes Interesse, bestimmte Daten wirklich geheim zu halten. Kunden- und Finanzdaten, Konzepte und neue Entwicklungen sollen zum Schutz vor Industriespionage und Manipulation verschlüsselt werden. Zum anderen gilt es, die Compliance zu erfüllen. Der Gesetzgeber macht beispielsweise im Bundesdatenschutzgesetz (BSDG) Vorgaben zum Umgang mit personenbezogenen Daten und nimmt die Geschäftsführung persönlich in die Haftung. Hinzu kommt eine Vielzahl nationaler und internationaler, teils branchenspezifischer Vorgaben, die unter anderem die Kreditwürdigkeit mit dem Stand der eingesetzten IT-Sicherheit verknüpfen. Alle Verordnungen fordern mindestens: Verschlüsselung nach dem Stand der Technik. Verschlüsselung nach dem Stand der Technik bezieht sich auf marktübliche Angebote, Industrienormen und die Wirtschaftlichkeit der Lösungen. Um die verfügbaren Lösungen besser verstehen zu können, starten wir mit einem kleinen Exkurs in die Kryptologie.

Die moderne Kryptologie entstand in der Mitte des letzten Jahrhunderts und basiert durchweg auf Mathematik. Sie löste das Sicherheitsprinzip „Security through Obscurity“ (Sicherheit durch Unklarheit) ab, bei dem die Sicherheit durch die Geheimhaltung der Funktionsweise gewährleistet war – ein risikoreicher, durchweg proprietärer Ansatz mit hohen Abhängigkeiten.

Marktübliche Verschlüsselungsprodukte der Gegenwart setzen auf bekannte Algorithmen. Um den Klartext in einen Geheimtext umzuwandeln, wird als Parameter ein Schlüssel benötigt und dieser ist das Geheimnis. Algorithmen wie AES (Advanced Encryption Standard) gelten als sehr sicher. Der Aufwand einer Brute Force Attack, bei der alle möglichen Kombinationen durchgerechnet und ausprobiert werden, steigt mit der Schlüssellänge exponentiell. Die NSA hat nicht die Ressourcen, AES in großem Stil zu brechen. Der Angriff benötigt neben enormer Rechenzeit auch mehr Energie, als in den USA pro Jahr verbraucht wird. Spezialisten haben errechnet, dass die Größe der Geheimanlagen der NSA bei Weitem nicht ausreiche, um dort die benötigte Energie zu produzieren.[1]

Die Symmetrie der Schlüssel

Grundsätzlich wird zwischen symmetrischer und asymmetrischer Verschlüsselung unterschieden (siehe Abb. 1).

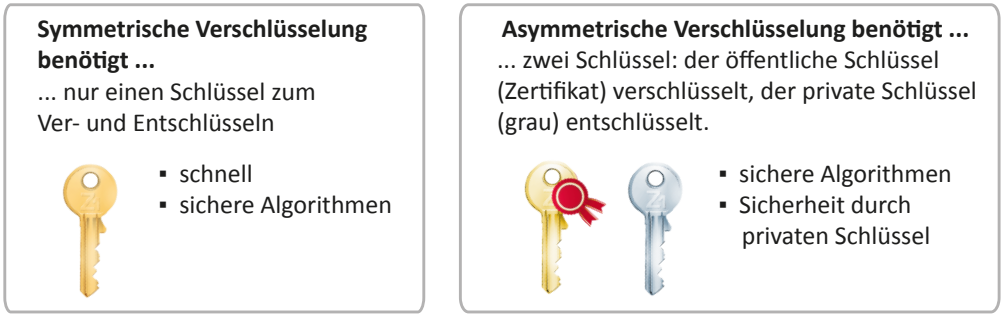

Abb. 1: Symmetrische und asymmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung, zum Beispiel nach dem AES-Standard, wird derselbe Schlüssel zum Verschlüsseln und Entschlüsseln der Daten genutzt. Die Sicherheit ist an die Geheimhaltung des Schlüssels gebunden. In der direkten Nutzung zur Kommunikation gibt es das Problem, dass mindestens zwei Parteien diesen Schlüssel zuerst initial miteinander teilen und ihn anschließend sicher verwahren müssen.

Bei der asymmetrischen Verschlüsselung werden zwei Schlüssel als Parameter genutzt: Ein öffentlicher Schlüssel dient der Verschlüsselung, ein privater Schlüssel ermöglicht die Entschlüsselung der Daten. Beide Schlüssel stehen in einer bestimmten mathematischen Abhängigkeit. Der private Schlüssel lässt sich jedoch durch die Kenntnis des öffentlichen Schlüssels nicht errechnen. RSA, benannt nach den Herren Ron Rivest, Adi Shamir und Leonard Adleman, ist ein weit verbreiteter Standard in der asymmetrischen Verschlüsselung.

Private und öffentliche Schlüssel mit Identitäten

Das initiale Problem der Schlüsselverteilung und Geheimhaltung ist mit der Aufteilung in öffentliche und private Schlüssel gelöst. Nur der private Schlüssel bleibt geheim. Der öffentliche Schlüssel zum Verschlüsseln ist kein Geheimnis und kann wie eine Telefonnummer von jedermann gefunden und gewählt werden. Es ist eben nur der Inhaber des privaten Schlüssels unter dieser Nummer erreichbar.

Asymmetrische Schlüsselpaare werden Identitäten zugeordnet. Hierin begründet sich das Modell der Public Key Infrastructure (PKI), die Basis der Public Key Kryptografie, welche die sichere Kommunikation innerhalb unsicherer Netzwerke gewährleistet. Die öffentlichen Schlüssel werden als Zertifikate auf bestimmte Identitäten ausgestellt und breit gestreut. Mit der Echtheits- und Gültigkeitsprüfung der Zertifikate können Identitäten zu einem bestimmten Zeitpunkt zweifelsfrei festgestellt werden.

PKIs werden im Bereich der E-Mail-Verschlüsselung genutzt, indem Nachrichten mit Zertifikaten verschlüsselt werden. Nur der Inhaber des privaten Schlüssels zum jeweiligen Zertifikat kann die Nachrichten entschlüsseln. Zusätzlich lassen sich durch das PKI-Modell auch digitale Signaturen erstellen, welche ebenfalls im Bereich der E-Mail-Sicherheit Anwendung finden.

Öffentliche Schlüssel werden PKI-Zertifikate

Zur PKI-basierten E-Mail-Verschlüsselung haben sich zwei Standards etabliert: S/MIME und OpenPGP. Beide nutzen im Grunde die gleichen kryptografischen Verfahren. Sie unterscheiden sich jedoch in der Zertifizierung der öffentlichen Schlüssel und damit in den Vertrauensmodellen (siehe Abb. 2).

Abb. 2: S/MIME und OpenPGP basieren auf unterschiedlichen Vertrauensmodellen

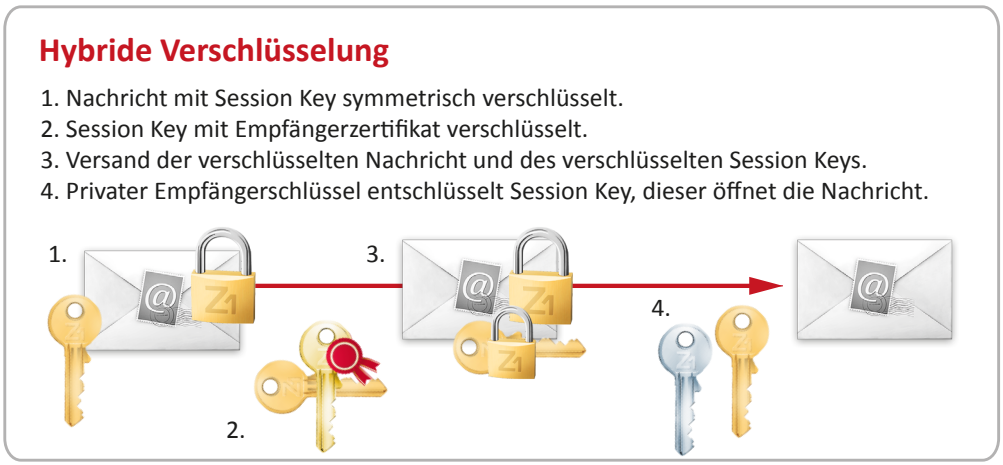

Abb. 3: Funktionsweise hybrider Verschlüsselung

S/MIME steht für Secure/Multipurpose Internet Mail Extensions und bezeichnet einen Standard, der X.509-Zertifikate nutzt. Die Zertifizierung der öffentlichen Schlüssel wird als kostenpflichtige Dienstleistung durch öffentliche Trustcenter als Certification Authoritys (CAs) angeboten. Das Vertrauensmodell ist hierarchisch. Die Identitäten werden über eine Zertfikatskette vom Nutzerzertifikat über eventuelle Sub-CAs bis hin zum WurzelCA-Zertifikat der ausgebenden Stelle verifiziert.

Beim Enrollmentprozess werden zunächst die Schlüsselpaare generiert. Der private Schlüssel verbleibt beim Nutzer, der öffentliche Schlüssel wird damit signiert und der CA zur Zertifizierung übergeben. Die CA fügt dem öffentlichen Schlüssel ihre eigene Signatur hinzu und sendet den signierten öffentlichen Schlüssel zurück. Ab diesem Moment wird ein öffentlicher Schlüssel zum Zertifikat.

X.509-Zertifikate sind zeitlich begrenzt gültig und werden in Klassen unterteilt. Diese sind jedoch nicht genormt. Mit einem Class 1 Zertifikat wird üblicherweise bescheinigt, dass die E-Mail-Adresse und der öffentliche Schlüssel zusammengehören. Höhere Klassen reichen bis zum notariellen beglaubigten Authentifizierungsprozess.
S/MIME ist als Kommunikationsstandard bereits in den gängigen Mailprogrammen implementiert und die CA- und Sub-CA-Zertifikate der bekannten Trustcenter sind zur Prüfung der Nutzerzertifikate ebenfalls installiert.

OpenPGP (Pretty Good Privacy) sieht vor, dass sich die Teilnehmer untereinander ihre öffentlichen Schlüssel signieren und damit zertifizieren. Dadurch entsteht ein „Web of trust“, ein Netzwerk des Vertrauens, das ohne Hierarchien auskommt. Schlüsselpaare werden selbst erstellt und öffentliche PGP-Schlüssel von Teilnehmern beispielsweise auf Key Signing Partys gegenseitig zertifiziert.

OpenPGP ist in den gängigen Mail-Programmen nicht vorinstalliert, sodass der Nutzung immer eine Client-Installation wie beispielsweise Enigmail für Thunderbird vorausgeht. Die Nutzung von PGP in Webmailern ist, wie bei S/MIME, noch nicht befriedigend gelöst.

In Sicherheitsaspekten rangiert OpenPGP vor S/MIME, da auch Trustcenter bereits kompromittiert wurden und von Geheimdiensten zur Ausstellung gefälschter Zertifikate verpflichtet wurden.

Die Verschlüsselung einer Nachricht

Vor dem komplexen Hintergrund der Public Key Infrastructure erscheint die eigentliche Verschlüsselung beinahe trivial, wie nachfolgendes Beispiel verdeutlicht (siehe auch Abb. 3).

Alice möchte Bob eine mit S/MIME verschlüsselte Nachricht zukommen lassen. Die Verschlüsselungssoftware generiert zunächst einen symmetrischen Session Key. Mit diesem werden die im Klartext vorliegenden Daten verschlüsselt. Der Session Key wird anschließend mit dem Zertifikat von Bob verschlüsselt und an die Nachricht angehängt.

Die verschlüsselte Nachricht enthält nun die Information, mit welchem Zertifikat die Nachricht verschlüsselt wurde, damit Bobs Software den zum Zertifikat gehörigen privaten Schlüssel zur Entschlüsselung nutzen kann.

Bob erhält die Nachricht. Mit seinem privaten Schlüssel kann er zunächst den symmetrischen Session Key entschlüsseln, den Alices Kryptoprogramm für diese Nachricht erstellt hat. Mit diesem Session Key entschlüsselt Bobs Software die Originalnachricht.

Diese hybride Verschlüsselung genannte Mischform aus symmetrischer und asymmetrischer Verschlüsselung ist gängige Praxis und wird vor allem aus Performance-Gründen angewendet. Die asymmetrischen Verschlüsselung der Originaldatei wäre wegen eines hohen Rechenaufwands nicht mehr effizient. Die asymmetrische Verschlüsselung des Session Keys dagegen ist schnell und reicht zur Gewährleistung der Sicherheit aus. Auch wenn E-Mails an mehrere Empfänger verschlüsselt werden, wird die Originaldatei nur einmal mit dem Session Key verschlüsselt und nur dieser für jeden Empfänger mit dessen eigenem Zertifikat verschlüsselt.

Sicherheit beim Zertifikats- und Schlüsselmanagement

Dass die vertrauliche Kommunikation bei Alice und Bob so einfach wie oben beschrieben funktioniert, ist der Idealfall. Vorab sind bei jeder einzelnen Verschlüsselung folgende Fragen zu klären: Woher bekommt Alice Bobs Zertifikat? Ist das Zertifikat echt? Ist das Zertifikat gültig?

Es ist unabdingbar, dass Alice Bobs Zertifikat findet. Die Verifizierung des aufgefundenen Zertifikats schützt gegen die „Man-in-the-Middle-Attack“. Bei einem solchen Angriff gibt jemand mit einem falschen Zertifikat vor, Bob zu sein. Er fängt die Nachricht ab und leitet sie anschließend mit Bobs echtem Zertifikat verschlüsselt an Bob weiter. Das könnte über Wochen und Monate geschehen, ohne dass Bob und Alice davon erfahren. Auch ein zurückgerufenes (revoked) Zertifikat könnte ohne Validierung von Angreifern weiter benutzt werden.

Die Komplexität einer PKI mit der Fülle an Informationen zur Echtheits- und Gültigkeitsprüfung macht ein manuelles

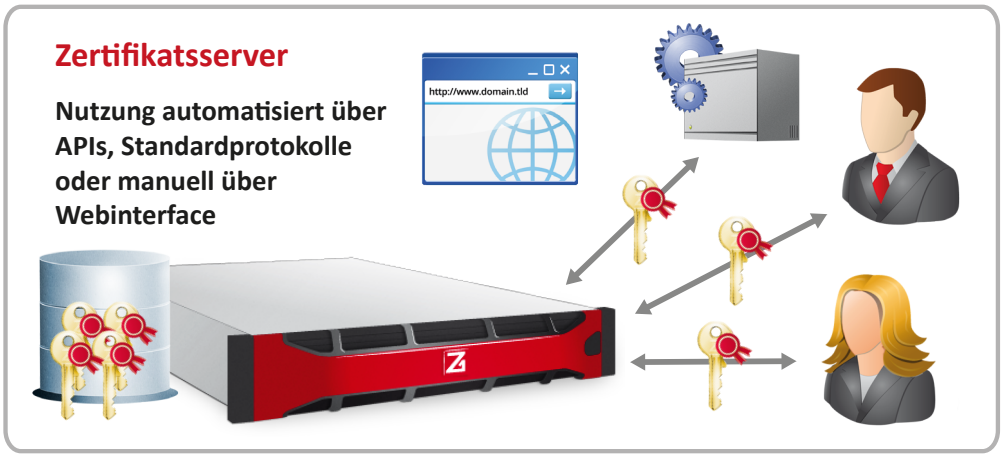

Abb. 4: Zertifikatsserver übernehmen das automatisierte Management der Zertifikate und Schlüssel

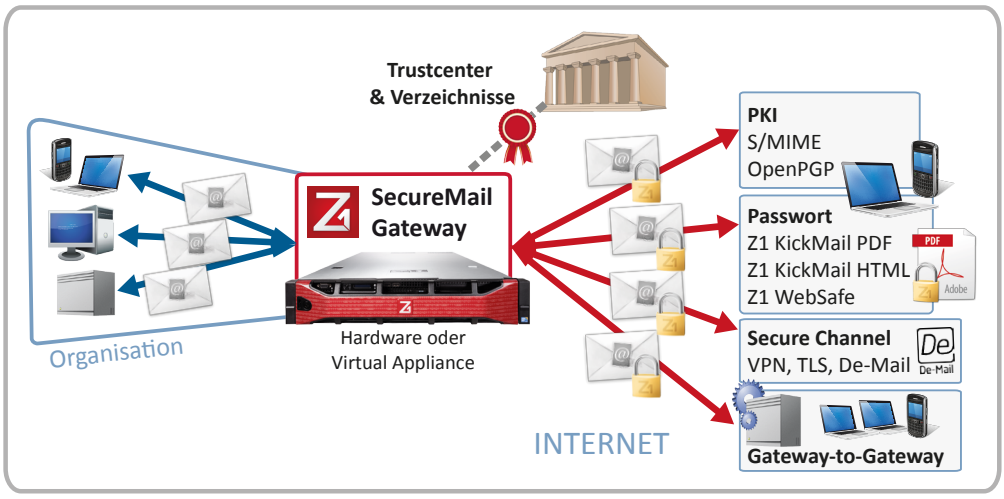

Abb. 5: E-Mail-Kommunikation mittels Gateway

Schlüssel- und Zertifikatsmanagement praktisch unmöglich. Dafür sind Zertifikatsserver entwickelt worden, die das Management der Zertifikate und öffentlichen Schlüssel einschließlich der Verifizierung und Validierung automatisiert übernehmen (siehe Abb. 4).

Zertifikatsserver sind über verschiedene Schnittstellen mit Trustcentern und CAs größerer Firmen verbunden. Sie rufen Gültigkeitsinformationen über Rückruflisten (CRLs – Certificate Revocation Lists) ab und führen Echtzeitabfragen via Online Certificate Service Protocols (OCSP) durch. So werden Daten eingeholt, Prüfsummen verglichen und der lokale Zertifikatsbestand permanent aktualisiert.

Ein öffentliches Verzeichnis mit dieser Funktionalität und zum Veröffentlichen von Zertifikaten ist Z1 GlobalTrustPoint[2], der online von jedermann kostenfrei genutzt werden kann.

Die Zertifikatsserver stehen neben der E-Mail-Verschlüsselung auch anderen PKI-basierten Anwendungen zur Verfügung. Als Identität eines Zertifikats kann statt einer Person auch ein System – beispielsweise mit Hostnamen oder IP-Adresse – eingetragen werden.

Secure E-Mail Gateways – serverbasierte E-Mail-Verschlüsselung

Im Bereich der E-Mail-Verschlüsselung sind sogenannte Secure E-Mail Gateways weit verbreitet (siehe Abb. 5). Diese sichern serverbasiert und damit zentral und transparent für die Nutzer den gesamten durchlaufenden E-Mail-Verkehr gemäß den eingestellten Regelwerken (Policies). Compliance Enforcement, hohe User-Akzeptanz sowie der Verzicht auf Client-Installationen machen den Gateway-Einsatz effizient und wirtschaftlich. Secure E-Mail Gateways greifen zur PKI-basierten Verschlüsselung auf die Dienste der Zertifikatsserver zu.

Für Kommunikationspartner ohne PKI wurden in SecureMail Gateways alternative Zustellmethoden entwickelt, bei denen ein Passwort den privaten Schlüssel ersetzt. Die Sicherheit der passwortbasierten Verschlüsselung muss der einer PKI-basierten Verschlüsselung nicht nachstehen und ist eine allgemein akzeptierte und bewährte Lösung für die adhoc Verschlüsselung, wenn kein PKI-Zertifikat zur Verfügung steht. Das Passwort wird dabei nicht als Klartext im System abgespeichert, sondern als verschlüsselter Hashwert. Die einzige Sicherheitsherausforderung ist die initiale Passwortzustellung.

Hierzu wurden verschiedene sichere und praxistaugliche Methoden entwickelt, beispielsweise die Zustellung per SMS.

Ein SecureMail Gateway kann somit neben mit S/MIME und OpenPGP verschlüsselten E-Mails auch passwortverschlüsselte PDF-, HTML- oder ZIP-Container ausliefern. Auch die adhoc Erstellung sicherer Webmailer-Accounts ist eine beliebte Alternative. De-Mail-Anbindungen, VPN- und TLS-Unterstützung sind ebenfalls auf einigen Gateways verfügbar.

Mobile Kommunikation verlangt nach Ende-zu-Ende-Verschlüsselung

Mit dem Secure E-Mail Gateway Konzept könnte man sich entspannt im Vertrauen auf die Sicherheit nach dem Stand der Technik zurücklehnen. Die Secure E-Mail Gateways wurden jedoch ursprünglich so konzipiert, dass die Verschlüsselung von und nach außen gewährleistet war. Bis vor einigen Jahren gab es kaum eine Notwendigkeit, innerhalb des firmeneigenen Netzwerks zu verschlüsseln. Der Angreifer kam von außen. Dagegen hat man sich mit Firewalls gewappnet.

Neben den noch recht jungen Erkenntnissen über Geheimdienstprogramme wie PRISM und Tempora ergeben sich vor allem durch die in den letzten Jahren zunehmende mobile E-Mail-Nutzung neue Herausforderungen. Per Smartphone und Notebook ausgetauschte E-Mails werden auch in der eigentlich unternehmensinternen Kommunikation auf Mobilfunkstrecken und im öffentlichen WLAN im Klartext übertragen. Die Lösung scheint in der Ende-zu-Ende-Verschlüsselung zu liegen. Diese wird von den Herstellern recht unterschiedlich interpretiert und birgt in der Reinform als „echte“ Ende-zu-Ende-Verschlüsselung unternehmerische Risiken. Die Reinform und zwei Interpretationen stellen wir hier vor.

„Echte“ Ende-zu-Ende-Verschlüsselung

Bei der echten Ende-zu-Ende-Verschlüsselung wird die E-Mail auf dem Client verschlüsselt und kann erst auf dem Empfänger-Client entschlüsselt werden (siehe Abb. 6). Auch in der Mailbox liegt die E-Mail in verschlüsseltem Zustand ab. Kein System kann auf dem Übertragungsweg auf die Inhalte der E-Mail zugreifen. Dies bedeutet den kompletten Verzicht auf zentrale Contentfilter. Antivirus, Antispam, Data Loss Prevention und Archivierung bleiben außen vor, was hohe Risiken für den Geschäftsbetrieb bedeuten kann.

Die Praxistauglichkeit der Lösung für den spontanen sicheren E-Mail-Verkehr ist trotz Nutzung eines Zertifikatsservers sehr gering, denn Sender und Empfänger müssen gezwungenermaßen den genau gleichen Standard nutzen: S/MIME oder OpenPGP.

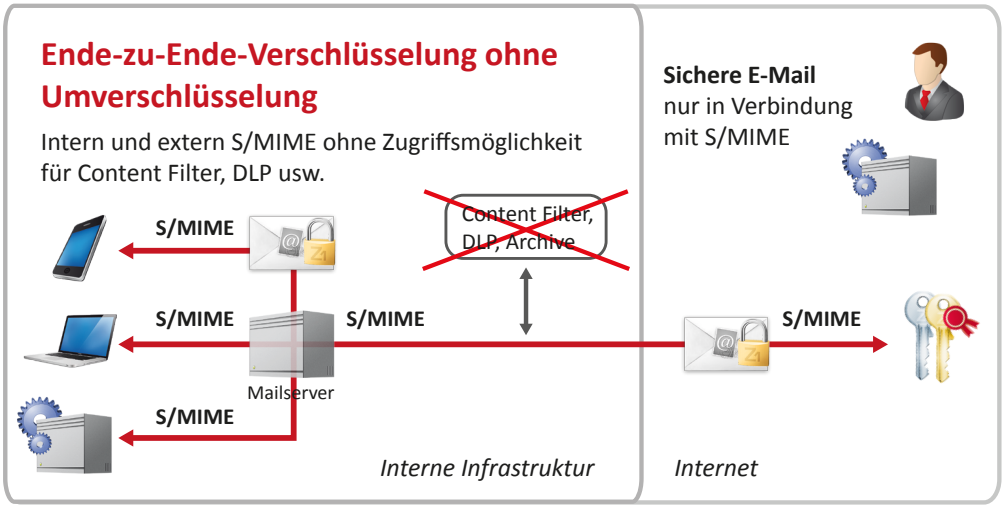

Abb. 6: „Echte“ Ende-zu-Ende-Verschlüsselung

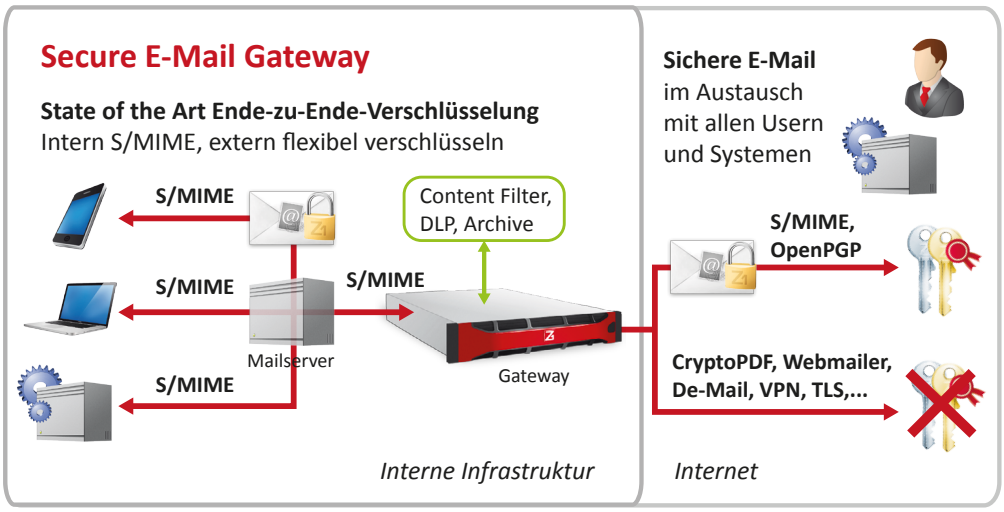

Abb. 7: Ende-zu-Ende-Verschlüsselung mit flexibler Umverschlüsselung auf dem Gateway

Ende-zu-Ende-Verschlüsselung mit Ausstellung von X.509-Zertifikaten

Wenn Ende-zu-Ende-Verschlüsselung gewünscht ist, aber kein Zertifikat für den Empfänger gefunden wird, gibt es Programme, die direkt selbst als CA agieren.

Um die adhoc Ende-zu-Ende-Verschlüsselung zu erzwingen, versorgt Alices spezieller Zertifikatsserver Bob mit einem on-the-fly erzeugten Schlüsselpaar. Alice lässt also neben dem X.509-Zertifikat auch Bobs privaten Schlüssel ausstellen und sendet Bob beides zu. Der private Schlüssel muss dabei in irgendeiner Weise gesichert übertragen werden. Alice kann Bob nun mit dem in Echtzeit erstellten Schlüsselpaar eine verschlüsselte E-Mail senden. So weit, so gut.

Das X.509-Zertifkat bleibt im Einsatz allerdings auf Alice und Bob beschränkt, da dem Zertifikat offiziell nicht getraut wird und es im Kontakt mit anderen Zertifikatsservern und Mail-Clients nicht verifiziert werden kann. Die PKI-Sicherheitsstandards sind nicht erfüllt, denn Alice hat Zugriff auf Bobs privaten Schlüssel. Zusätzlich handelt es sich um weniger als ein Class 1 Zertifikat, da die E-Mail-Adresse von Bob nicht bestätigt wurde.

Bob wurde eine Public Key Infrastructure „aufgezwungen“, ob er das Zertifikat einfach nutzen kann, hängt von den Administrationsrechten in seinem Mail-Client ab. Die Lösung ist auf S/MIME beschränkt, auch Bobs bekannter öffentlicher OpenPGP-Schlüssel würde ihm nichts nutzen. Und sollte Bob mehrere Kontakte zu Firmen pflegen, die solche Zertifikate spontan selbst ausstellen, hat er bald einen reichlichen Zertifikatsbestand. Eine Aufklärung über die eingeschränkte Nutzung der Pseudo-Zertifikate ist deshalb unbedingt notwendig.

Die Lösung kann nur ein Kompromiss sein, wenn der Zugriff auf das Mailsystem nicht gegeben ist.

Ende-zu Ende-Verschlüsselung mit flexibler Umverschlüsselung

Moderne Secure E-Mail Gateways mit Erweiterungen ermöglichen eine Verknüpfung zwischen interner und externer E-Mail-Verschlüsselung, sodass E-Mails nicht nur über das Internet, sondern auch innerhalb der firmeninternen Netze in verschlüsseltem Zustand übertragen werden (siehe Abb. 7). 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, weshalb sich die Vertrauensfrage auf externen Zertifikatsservern und Mail-Clients nicht stellt.

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 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 nach S/MIME, OpenPGP, CryptoPDF, 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 greifen die Schnittstellen für Antivirus, Antispam, DLP, Archivierung etc.

Secure E-Mail Gateways können mit echter Ende-zu-Ende-Verschlüsselung kombiniert werden, die vielleicht in einem kleinen Empfängerkreis durchaus gewünscht ist.

Kriterien für eine solide Vertrauensbasis

Strikte Gesetze zum Datenschutz, Geheimdienste ohne den Auftrag zur Wirtschaftsspionage und ohne direkten Einfluss auf Internetservices und IT-Technologieanbieter – solche Rahmenbedingungen sind auch in Europa nicht überall vorhanden. In Deutschland jedoch kann IT-Security ohne Hintertüren gebaut werden.

Bei proprietären IT-Security Lösungen ist neben dem zu prüfenden Vertrauen in die Hersteller eben auch das jeweilige Produktionsland zu berücksichtigen. Weiterhin sollte man bedenken, dass Sender und Empfänger die gleiche Lösung nutzen müssen und dann an die Geräte gebunden sind, auf denen die Software installiert ist.

Die Zukunft für Secure E-Mail Gateways – Made in Germany – ist sicher

Mit der Kombination aus interner und externer Verschlüsselung ist das Gateway-Konzept für die Zukunft gerüstet. Einige Hersteller punkten zusätzlich mit Erweiterungen, die neben der sicheren E-Mail-Übertragung beispielsweise den sicheren Transfer großer Dateien integrieren.

Wer sich mit der Investition in eine Verschlüsselungslösung beschäftigt, sollte sich neben der Abwägung nach dem Herstellerland und der Kernfrage, ob Sicherheit oder Compliance im Vordergrund steht, vor allem die Frage stellen, wie groß und heterogen das Feld der möglichen externen Kommunikationspartner ist, mit denen die vertrauliche Kommunikation gepflegt werden soll.

Quellenangabe:

(1) http://www.golem.de/news/verschluesselung-was-noch-sicher-ist-1309-101457-3.html
(2) https://www.globaltrustpoint.com

Das White Paper ist auch erschienen in:
IT-Sicherheit 2/2014, Datakontext, Verlagsgruppe Hüthig Jehle Rehm. S. 41-45