Praktischer Einsatz von E-Mail-Gateways zur Sicherung der E-Mail-Kommunikation

Secorvo White Paper

Version 1.0
Stand 20. Juli 2004

Holger Mack, Dr. Markus Michels

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

CA	Certification Authority
HTTP	Hypertext Transmission Protocol
LDAP	Lightweight Directory Access Protocol
PGP	Pretty Good Privacy
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PSE	Personal Security Environment
S/MIME	Secure Multipart Mail Extension
SSL	Secure Socket Layer

Historie

Version	Datum	Änderung	Autor
1.0	20.07.04	Erste Version	M. Michels, H. Mack

1 Summary/Abstract/Management Summary

Die Verwendung von E-Mail-Gateways zur Sicherung der E-Mail-Kommunikation wird derzeit von vielen Organisationen als Alternative zu klassischen Ende-zu-Ende-Lösungen in Betracht gezogen. Bei solchen Lösungen wird die Verschlüsselung, Entschlüsselung und die Signierung von E-Mails sowie die Verifikation einer Signatur für E-Mails von oder zu einem externen Kommunikationspartner auf einem zentralen E-Mail-Gateway durchgeführt.

Es zeigt sich, dass die Sicherung von E-Mail auf der Basis eines E-Mail-Gateways gegenüber dem Ende-zu-Ende Ansatz einige Vorteile besitzt, wie z.B. die Durchführung von zentralen Inhalts- oder Virenprüfungen und die Umsetzung von Vertretungsregelungen. Andererseits wird die Sicherung der internen Strecke, d.h. vom E-Mail Client des Nutzers bis zum E-Mail-Gateway, von den meisten Produkten nicht abgedeckt und muss bei Bedarf anderweitig, z.B. durch Nutzung von Funktionalitäten der E-Mail Infrastruktur, erfolgen.

Sind die externen Kommunikationspartner bzw. deren Organisation langfristig vorher bekannt, sollte die Nutzung gesicherter Kommunikation relativ problemlos möglich sein. Vom Ende-zu-Ende Ansatz bekannte mögliche Probleme und Herausforderungen (wie z.B. Interoperabilität, die Bereitstellung von Zertifikaten für externe Kommunikationspartner oder die Verwendung verschiedener Sicherungsprotokolle für eine E-Mail) bleiben aber bestehen.

Bei einer ad hoc Kommunikation mit einem externen Kommunikationspartner auf der Basis zertifikatsbasierter Verschlüsselung (wie z.B. PGP oder S/MIME) nimmt der E-Mail-Gateway Administrator eine aktive Rolle wahr. Dies ist unerwünscht, da dies i.a. zu Verzögerungen führen wird und ggf. hohen zentralen Aufwand verursachen kann. Bei Lösungen auf Basis des Ende-zu-Ende Ansatzes gibt es diese aktive Rolle des Administrators nicht, da diese Aufgaben vom Nutzer selbst durchgeführt werden müssen. Eine reibungslose gesicherte ad hoc Kommunikation ist deshalb in der Regel nicht zu erwarten. Möglicherweise lässt sich dieses Problem durch die Verwendung von alternativen Verschlüsselungstechniken (passwort-basierte Verschlüsselung, gesicherte E-Mail über eine Web-Infrastruktur) lösen.

2 Motivation

In Unternehmen und Behörden ist die Nutzung von E-Mail für die interne Kommunikation, die Kommunikation mit Partnern und Lieferanten sowie für Workflows heute selbstverständlich geworden. Vor allem bei dem Versenden über das Internet sind E-Mails verschiedenen Bedrohungen ausgesetzt:

- Oftmals werden sensitive Informationen per E-Mail versendet, deren Vertraulichkeit gewahrt werden muss.
- Bei manchen versendeten Informationen muss die Authentizität des Senders sowie eine etwaige Veränderung der Daten zumindest für den Empfänger erkennbar sein.
- Unerwünschte E-Mails (Spam), Viren, Würmer und Trojanische Pferde können die Verfügbarkeit der E-Mail-Infrastruktur bedrohen oder einem Angreifer Zugang zu internen Netzen ermöglichen.

Mit anderen Worten: Die Sicherheit der E-Mail-Infrastruktur sowie der E-Mail-Kommunikation ist für Unternehmen und Behörden ein wichtiges Thema.

Viele Unternehmen und Behörden haben inzwischen Maßnahmen gegen Viren (Einsatz von zentralen und lokalen Virenscannern) und Spam (Einsatz von sog. E-Mail-Filter-Produkten) ergriffen. Hingegen wird weiterhin nur ein Bruchteil des E-Mail-Verkehrs gegen unbefugtes Lesen und Verändern geschützt übertragen, obwohl viele E-Mail-Clients bereits entsprechende Funktionen integriert haben und eine Vielzahl von Lösungen auf dem Markt vorhanden sind.

In diesem Beitrag wird daher das Hauptaugenmerk auf den Schutz der Inhalte der E-Mail-Kommunikation gelegt, d. h. die Gewährleistung der Sicherheitsziele Vertraulichkeit, Integrität und Authentizität von E-Mail-Nachrichten durch den Einsatz von Verschlüsselung und digitalen Signaturen. Eine gesicherte oder geschützte E-Mail gewährleistet mindestens eines dieser Sicherheitsziele. Andere Aspekte der E-Mail-Sicherheit wie z. B. die Sicherheit von E-Mail-Servern oder der Schutz vor Viren werden nur dann betrachtet, wenn sie Auswirkungen auf eine Lösung zur Sicherung der E-Mail-Kommunikation haben.

Ein Grund für die geringe Verbreitung von geschütztem E-Mail-Verkehr ist auch darin zu finden, dass der in den meisten Projekten verfolgte sog. Ende-zu-Ende-Ansatz in der Praxis manche Probleme aufwirft.

In dem Ende-zu-Ende-Ansatz wird die Verschlüsselung, Entschlüsselung und die Signierung von E-Mails sowie die Verifikation der Signatur einer E-Mail auf dem lokalen Anwenderrechner durchgeführt. Dadurch ist es möglich, dass E-Mails durchgängig von Sender zum Empfänger in geschützter Form versendet werden (daher der Name „Ende-zu-Ende-Ansatz“). Dies gilt auch für den E-Mail-Verkehr im internen Netz. Auf dem Anwenderrechner müssen entweder vorhandene Fähigkeiten des E-Mail-Clients verwendet[1] oder ein sog. Plug-In installiert werden, welches die entsprechenden Funktionen ergänzt. Nutzer entscheiden für jede E-Mail, ob und in welcher Weise diese gesichert wird. Dies setzt eine Mitwirkungsbereitschaft und ein ggf. durch Schulungen vermitteltes Know-how der Nutzer voraus.

Die Umsetzungen dieses Ansatzes haben in Praxis zu manchen Problemen geführt, z. B.:

---

[1] Zum Beispiel unterstützen MS Outlook oder Lotus Notes den Austausch gesicherter E-Mail auf Basis des Austauschformats S/MIME.

- Zentrale Inhalts- oder Virenprüfungen können für verschlüsselte E-Mails im Allgemeinen nicht durchgeführt werden.[2]
- Vertretungsprozesse sind schwierig umzusetzen, da Vertreter verschlüsselte E-Mails nur dann lesen können, wenn sie Zugriff auf den geheimen Schlüssel des Empfängers der E-Mail haben.
- Häufig sind aufwändige Message- oder Key-Recovery-Maßnahmen notwendig, um im Notfall (z. B. bei Verlust des geheimen Schlüssels durch den Nutzer) den Zugriff auf die verschlüsselten E-Mails zu ermöglichen.
- Die eingesetzte Technik erweist sich oft als fehleranfällig und komplex, insbesondere wenn Komponenten verschiedener Hersteller eingesetzt werden, die nicht optimal verzahnt sind.
- E-Mail Plug-Ins sind Ergänzungen des jeweiligen E-Mail-Clients und müssen für jede neue Version des E-Mail-Clients angepasst und getestet werden. Dadurch steht möglicherweise nicht für alle (künftig) eingesetzten Versionen eines E-Mail-Clients ein E-Mail Plug-In zur Verfügung. Häufig unterstützen die E-Mail-Clients oder Plug-Ins nur eines der verbreiteten Sicherheitsprotokolle (PGP, S/MIME). Dadurch ist die Funktionalität der Lösung von vornherein eingeschränkt.
- Ein Schlüsselmanagement muss aufgebaut werden, meist in Form einer Public Key Infrastruktur (PKI). Dies ist oft sehr aufwändig und komplex. Die Prozesse für Schlüsselerzeugung, Schlüsselverteilung und -wiederherstellung sowie die Verwaltung von Vertrauensbeziehungen müssen für jeden Benutzer umgesetzt werden, was die Mitarbeiter z. T. überfordert und oft hohen zentralen Aufwand verursacht.
- Insbesondere die gesicherte Kommunikation mit externen Nutzern erweist sich als schwierig. Denn z. T. verfügen diese nicht über eine entsprechende Sicherheits-Infrastruktur. Selbst beim Vorliegen entsprechender Infrastrukturen (wie z. B. E-Mail-Clients mit S/MIME Funktionalitäten und der Ausstattung der Nutzer mit Zertifikaten) ist die Initialisierung des gesicherten E-Mail-Verkehrs (d. h. die Ausstattung des Kommunikationspartners mit den eigenen Zertifikaten) schwer handhabbar.
- In heterogenen Umgebungen treten immer noch Interoperabilitätsprobleme auf.

Auch aus diesen Gründen wird von Unternehmen und Behörden in E-Mail-Sicherheits-projekten in letzter Zeit vermehrt ein anderer Ansatz verfolgt: der Einsatz einer E-Mail-Gateway-Lösung. In dieser Lösung werden die Verschlüsselung, Entschlüsselung und die Signierung von E-Mails sowie die Verifikation einer Signatur für E-Mails von oder zu einem externen Kommunikationspartner auf einem oder mehreren zentralen E-Mail-Gateways durchgeführt.

In erster Linie geht es bei dieser Lösung darum, die externe Strecke (d. h. die Strecke vom E-Mail-Gateway zum Kommunikationspartner) zu sichern. Auf die Installation eines E-Mail Plug-Ins auf dem Anwenderrechner sowie die Ausgabe von Schlüsseln und Zertifikaten an die einzelnen Anwender kann verzichtet werden. Die Regeln, die festlegen, wie eine E-Mail an einen bestimmten Kommunikationspartner geschützt wird, können meist zentral vorgegeben werden. Wegen der Analogien zum Umgang mit Briefen in vielen Organisationen wird diese Art der Lösung häufig auch als „Virtuelle Poststelle“ bezeichnet.

---

[2] Grundsätzlich ist es möglich, das auch Ende-zu-Ende Lösungen diese Prüfungen ermöglichen. Den Autoren ist jedoch nur eine Ende-zu-Ende Lösung bekannt, die diese Eigenschaft aufweist.

In diesem Whitepaper wird die E-Mail-Gateway-Lösung in Hinblick auf ihre Vor- und Nachteile untersucht. Insbesondere sollen die folgenden Fragen beantwortet werden:

- Welche Vorteile bietet die Umsetzung der E-Mail-Gateway-Lösung? Insbesondere: Welche der oben genannten Nachteile in Umsetzungen der Ende-zu-Ende-Lösung können vermieden werden?
- Welche spezifischen Nachteile haben Umsetzungen der E-Mail-Gateway-Lösung und wie können diese Nachteile begrenzt oder überwunden werden?

Die Untersuchung konzentriert sich nicht auf eine theoretische Betrachtung der Möglichkeiten der Lösung, sondern diskutiert einige Aspekte, die bei der praktischen Umsetzung zu berücksichtigen sind.

In Kapitel 3 wird die E-Mail-Gateway Lösung näher beschrieben und in Kapitel 4 die Anforderungen an ein E-Mail-Gateway Produkt geschildert. In Kapitel 5 werden die Vor- und Nachteile des Ansatzes diskutiert.

3 Zentrale E-Mail-Gateways

3.1 Architektur und Prinzip

Die E-Mail-Gateways werden im internen Netz einer Organisation entweder als eigenständige Server oder als Aufsatz für vorhandene E-Mail-Server eingesetzt. Sie werden dabei so innerhalb der E-Mail-Infrastruktur platziert, dass nach außen gesendete und von außen kommende E-Mails über diese Server geleitet werden.[3] Die gesuchte Lösung muss dabei skalierbar sein (z. B. durch Clustering- und Load-Balancing-Mechanismen), um Kapazitäten und Verfügbarkeitsanforderungen der vorhandenen E-Mail-Infrastruktur gewährleisten zu können.

Im Folgenden wird zwischen *internen Nutzern*, die an das internen Netz angeschlossen sind und *externen Kommunikationspartnern*, die nicht an das interne Netz angeschlossen sind, unterschieden.

In den meisten E-Mail-Gateway-Produkten werden die von den internen Nutzern im Klartext gesendeten E-Mails nach vorher zentral festgelegten Regeln verschlüsselt und/oder signiert (siehe Bild 1). Der Nutzer kann die Regeln durch Eingabe von Schlüsselworten im E-Mail-Header („Betreff-Zeile“) für jede E-Mail verändern bzw. beeinflussen. Die genaue Umsetzung der Regeln auf dem E-Mail-Gateway sowie Einflussmöglichkeiten durch den Nutzer müssen abhängig von der gewünschten Policy und den Produkteigenschaften definiert werden. Bei einzelnen E-Mail-Gateway-Produkten entscheiden ausschließlich die Nutzer, ob und wie die Nachricht gesichert wird.

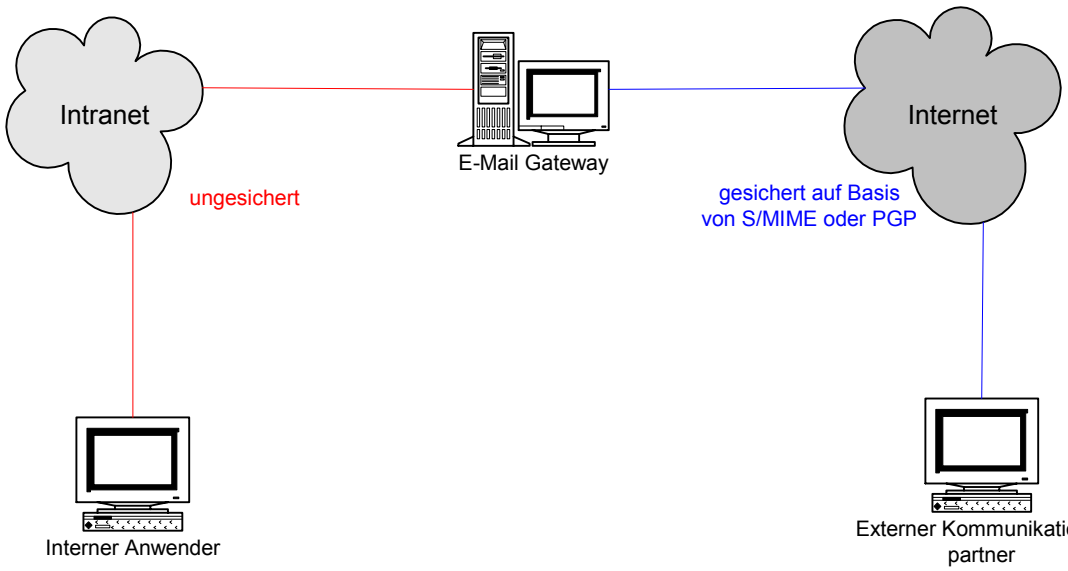

Bild 1: Basisarchitektur „E-Mail-Gateway“

Möchte ein interner Nutzer gesichert kommunizieren können, so werden entweder bei der Initialisierung oder später bei Bedarf Schlüssel und Zertifikate für den Nutzer erzeugt und

[3] In den meisten Fällen werden E-Mail-Gateways am Übergang zwischen dem internen Netzwerk und dem Internet eingesetzt. Es ist auch denkbar, solche Gateways intern einzusetzen, um spezielle sensitive Bereiche abzusichern.

zentral beim E-Mail-Gateway hinterlegt. Zusätzlich sammelt das E-Mail-Gateway die Zertifikate der externen Kommunikationspartner.

Sendet der interne Nutzer an einen externen Kommunikationspartner eine Nachricht, die auf Basis einer zentral beim E-Mail-Gateway eingestellten Regel signiert und verschlüsselt werden soll, so sendet der Nutzer die E-Mail ab, ohne eine Einstellung für die Verschlüsselung oder Signatur vornehmen zu müssen. Das E-Mail-Gateway empfängt die E-Mail und erkennt anhand der zentral eingestellten Regel, dass diese verschlüsselt und signiert werden soll. Die Signatur erfolgt mit dem zentral hinterlegten privaten Schlüssel des Nutzers. Sofern der öffentliche Schlüssel des Empfängers vorhanden ist, kann das E-Mail-Gateway die E-Mail auch verschlüsseln und absenden. Anschließend wird die gesicherte E-Mail an den externen Kommunikationspartner gesendet.

Eine signierte und verschlüsselte Nachricht von einem externen Kommunikationspartner an einen internen Nutzer wird vom E-Mail-Gateway empfangen und entschlüsselt. Ist das Zertifikat des externen Kommunikationspartners im E-Mail-Gateway vorhanden, so kann auch die Signatur geprüft werden, sofern das Zertifikat als vertrauenswürdig eingestuft wird. Die nun im Klartext vorliegende E-Mail kann nun ggf. auf Viren und Inhalt geprüft werden. Anschließend wird sie an den internen Nutzer weitergeleitet.

3.2 Ausgestaltung der Lösung

Im Folgenden sollen einige wichtige Aspekte beschrieben werden, die bei Verwendung einer Lösung auf Basis eines E-Mail-Gateways im Vorfeld geklärt werden müssen. Dazu zählen

- ob und ggf. wie die interne Strecke (Strecke vom internen Anwender zum E-Mail-Gateway) gesichert werden soll,
- ob für alle internen Nutzer ein gemeinsamer Schlüssel genutzt werden soll (sog. Firmenschlüssel) oder ob für jeden Nutzer mindestens ein eigener Schlüssel generiert wird,
- woher die Schlüssel und Zertifikate der internen Nutzer bezogen werden,
- wie die Zertifikate der externen Kommunikationspartner in das E-Mail-Gateway importiert werden können und
- welche Sicherungsprotokolle (z. B. S/MIME, PGP, Passwort-basierte Verschlüsselung) verwendet werden sollen.

Die Lösung hängt dabei von den Randbedingungen (z. B. welche Sicherheitsprotokolle externe Kommunikationspartner einsetzen) und Bedrohungsszenarien ab (z. B. ob Angriffe auf das interne Netzwerk als unwahrscheinlich gelten).

3.2.1 Sicherung der internen Strecke

Eine reine E-Mail-Gateway-Lösung sieht keine Sicherung der internen Kommunikation vor. Eine Sicherung der internen Strecke kann je nach vorhandener Infrastruktur und verwendetem E-Mail-Gateway-Produkt auf verschiedene Weise ergänzt werden:

- Ein E-Mail-Gateway-Produkt ermöglicht auch die Sicherung der internen Strecke. Dazu müssen die Anwenderrechner der Nutzer mit zusätzlicher Client-Software und/oder benutzerspezifischen Schlüsseln und Zertifikaten ausgestattet werden.
- Die spezifischen Verschlüsselungsmechanismen der E-Mail-Infrastruktur (z. B. mittels Portverschlüsselung in Domino/Notes, SMTP über SSL bei Microsoft Exchange) können

genutzt werden, um die interne Strecke zu schützen. Der Vorteil dieser Methode ist, dass die Anwenderrechner der Nutzer nicht mit zusätzlicher Client-Software und/oder benutzerspezifischen Schlüsseln und Zertifikaten ausgestattet werden müssen.

Je nach Umsetzung der internen Verschlüsselung sind dabei nur Teile der internen Kommunikation gesichert (z. B. Kommunikation zwischen Client und E-Mail-Server, unverschlüsselte Ablage auf dem E-Mail-Server).

3.2.2 Schlüssel und Zertifikate der internen Anwender

Für die internen Anwender werden Schlüsselpaare für die Signatur und die Entschlüsselung von E-Mails im E-Mail-Gateway benötigt. Es werden entweder ein unternehmensweiter oder benutzerspezifische Schlüssel verwendet:

- *Unternehmensweiter Schlüssel*: Es wird für alle Nutzer ein unternehmensweiter Schlüssel verwendet. Die unternehmensweiten Schlüsselpaare werden durch eine im E-Mail-Gateway integrierte PKI erzeugt, von einer bereits im Unternehmen vorhandenen PKI erzeugt oder von einem PKI-Dienstleister bezogen. Externen Kommunikationspartnern wird das unternehmensweite öffentliche Zertifikat zur Verfügung gestellt, um eine gesicherte Kommunikation zu ermöglichen.
- *Anwenderspezifische Schlüssel*: Für jeden internen Anwender werden eigene Schlüssel erzeugt und die öffentlichen Schlüssel in einem für Externe zugänglichen Verzeichnis zur Verfügung gestellt. Die meisten E-Mail-Gateway-Produkte können so konfiguriert werden, dass die Generierung der Schlüssel durch eine im E-Mail-Gateway integrierte PKI erfolgt. Alternativ können die Schlüssel und Zertifikate von einer bereits im Unternehmen vorhandenen PKI erzeugt oder von einem PKI-Dienstleister bezogen und manuell in das E-Mail-Gateway importiert werden.

Bei der Wahl des unternehmensweiten Schlüssels ist zu beachten, dass externe Kommunikationspartner – je nach gewähltem Produkt der Externen – ggf. nicht in der Lage sind, eine E-Mail per S/MIME an interne Anwender zu versenden, da in einigen E-Mail Plug-Ins bzw. E-Mail-Clients die im Zertifikat enthaltene E-Mail-Adresse mit der E-Mail-Adresse des Empfängers übereinstimmen muss. In einigen E-Mail-Clients oder Plug-Ins kann dieses Problem aber durch Modifikation der Konfiguration bzw. durch Ändern der Mailadresse des Empfängers gelöst werden. Der damit verbundene Aufwand kann aber für manchen externen Kommunikationspartner inakzeptabel sein.

Bei der Verwendung von anwenderspezifischen Schlüsseln sind diese Probleme nicht zu erwarten. Allerdings entsteht durch die Erzeugung und Verwaltung dieser Schlüssel gegenüber der Lösung mit einem unternehmensweiten Schlüssel ein z. T. erheblicher Mehraufwand. Sind mehrere E-Mail-Gateways in einem Cluster im Einsatz, müssen alle E-Mail-Gateways Zugriff auf die Schlüssel bekommen, z. B. durch Replikationsmechanismen oder den Einsatz eines gemeinsamen Verzeichnisses, in dem die Schlüssel und Zertifikate hinterlegt sind. Zudem müssen externe Kommunikationspartner auf die Zertifikate der internen Nutzer zugreifen können.

3.2.3 Zertifikate der externen Kommunikationspartner

Damit interne Anwender verschlüsselte Nachrichten an externe Kommunikationspartner versenden können, müssen die Zertifikate des Empfängers im E-Mail-Gateway vorhanden sein. Je nach verwendetem Produkt gibt es verschiedene Mechanismen. Dazu zählen:

- Der manuelle Import von Zertifikaten in das E-Mail-Gateway.

- Das Laden von Zertifikaten aus einem vorkonfigurierten Verzeichnis.
- Der automatische Import von Zertifikaten aus E-Mails in das E-Mail-Gateway.

Je nach E-Mail-Gateway-Produkt wird die Vertrauenswürdigkeit der Zertifikate auf verschiedene Weise überprüft:

- Der Administrator setzt die Zertifikate explizit als vertrauenswürdig. Dadurch entfällt eine weitere Prüfung.
- Die Zertifikate werden automatisch überprüft. Dazu ist es erforderlich, dass das zugehörige Root CA Zertifikat als vertrauenswürdig bekannt ist, bzw. ein Vertrauenspfad zur eigenen Root CA vorhanden ist. Zudem müssen die zugehörigen Sperrlisten aus vorkonfigurierten Verzeichnissen geladen werden können.

Manche E-Mail-Gateway-Produkte ermöglichen es auch externen Kommunikationspartnern, vorhandene Zertifikate über eine Web-Seite in das E-Mail-Gateway zu importieren oder sich neue Zertifikate vom E-Mail-Gateway ausstellen zu lassen.

Sind mehrere E-Mail-Gateways in einem Cluster im Einsatz, müssen alle E-Mail-Gateways Zugriff auf die Zertifikate der externen Kommunikationspartner bekommen, z. B. durch Replikationsmechanismen oder den Einsatz eines gemeinsamen Verzeichnisses, in dem die Zertifikate hinterlegt sind.

3.2.4 Sicherungsprotokolle

Es muss festgelegt werden, welche Sicherungsprotokolle verwendet werden sollen. Die meisten E-Mail-Gateway-Produkte unterstützen PGP und S/MIME. Zur Kommunikation mit externen Kommunikationspartnern ohne entsprechende PKI-Sicherheitsinfrastruktur kann es nützlich sein, auch auf Basis von alternativen Verschlüsselungssystemen sicher kommunizieren zu können. Dabei kommen Passwort-basierte Verschlüsselungssysteme oder eine gesicherte Web-basierte E-Mail-Infrastruktur in Frage.

Passwort-basierte Verschlüsselungssysteme zeichnen sich dadurch aus, dass ein Passwort für die Verschlüsselung verwendet wird, das nur dem Sender und dem Empfänger der verschlüsselten Nachricht bekannt ist. Der externe Kommunikationspartner muss dabei mit einem entsprechenden Verschlüsselungssystem ausgestattet sein. Soll eine E-Mail vom internen Nutzer zum externen Kommunikationspartner gesendet werden, wird meist das zu verwendende Passwort im E-Mail-Betreff-Feld der E-Mail vom internen Nutzer ergänzt. Das E-Mail-Gateway entfernt dieses Passwort im E-Mail-Betreff-Feld der E-Mail und verwendet es zur Verschlüsselung der E-Mail. Der interne Nutzer teilt dem externen Kommunikationspartner das Passwort z. B. per Telefon mit.

Damit diese Art der Verschlüsselung auch beim Versand von E-Mails vom externen Kommunikationspartner zum internen Nutzer funktioniert, muss das E-Mail-Gateway das verwendete Passwort kennen und der Kommunikationsbeziehung zuordnen können. Zur Zeit kann bei den meisten Produkten allerdings nur der Weg von Innen nach Außen auf diese Weise geschützt werden.

Eine Web-basierte E-Mail-Infrastruktur bietet das Versenden und Empfangen der E-Mail über den Web-Browser an. Die Sicherung der Strecke erfolgt über SSL mit Serverauthentifikation. Interne Nutzer authentifizieren sich über vorhandene Nutzer-IDs und Passwörter. Externe Kommunikationspartner authentifizieren sich über Passwörter, die ihnen z. B. per Telefon oder SMS zugesendet werden.

3.3 Prozesse

Die Prozesse unterteilen sich in Prozesse zur Administration des E-Mail-Gateways und solche mit Nutzerbeteiligung.

3.3.1 Administration des E-Mail-Gateways

Die E-Mail-Gateways werden von E-Mail-Gateway-Administratoren verwaltet. Deren Aufgaben sind:

- die Konfiguration der Verbindung des E-Mail-Gateways,
- die Einstellung zentraler Regeln für die Signierung sowie die Ver- und Entschlüsselung von E-Mails,
- die Einstellung von Workflows, z. B. für den Fall, dass für externe Kommunikationspartner keine Zertifikate im E-Mail-Gateway hinterlegt sind,
- die Konfiguration von Verzeichnissen für den Zertifikatsimport,
- der manuelle Zertifikatsimport von externen Kommunikationspartnern,
- die Generierung von Schlüsseln und Zertifikaten für interne Nutzer.

Hinzu kommt die Auditierung, die von unabhängigen Auditoren durchgeführt werden sollte.

Einige E-Mail-Gateway-Produkte unterstützen auch Rollenkonzepte, so dass Administratoren nur bestimmte Aufgaben wahrnehmen können. Es ist insbesondere sinnvoll, dass eine spezielle Auditorenrolle vorhanden ist, mit der nur lesend auf Protokollierungsdaten zugegriffen werden kann.

3.3.2 Prozesse mit Nutzerbeteiligung

Die internen Nutzer verwenden nach wie vor ihren üblichen E-Mail-Client. Das Senden und Empfangen von E-Mail erfordert meist keine zusätzliche Tätigkeit von ihnen. Bei den meisten E-Mail-Produkten können sie aber die zentral im E-Mail-Gateway eingestellten Regeln überschreiben, so dass eine bestimmte E-Mail an externe Kommunikationspartner verschlüsselt und/oder signiert wird oder nicht, indem sie ein entsprechendes Schlüsselwort (z. B. „crypt“) im Betreff-Feld der E-Mail ergänzen. Dieses Schlüsselwort wird vom E-Mail-Gateway erkannt und die entsprechende Operation durchgeführt. Es wird aber nicht an den Kommunikationspartner weitergeleitet.

Sendet der interne Nutzer eine E-Mail an einen externen Kommunikationspartner, so wird die E-Mail an das E-Mail-Gateway weitergeleitet. Dort wird sie gemäß den zentral eingestellten oder vom Nutzer eingegebenen Regeln gesichert:

- Soll die Nachricht signiert werden, so muss ein Unternehmensschlüssel oder für den interne Nutzer ein eigenes Schlüsselpaar vorhanden sein. Liegt beides nicht vor, so muss – je nach Konzept – ein solcher Schlüssel „on-the-fly“ erzeugt werden oder die Operation abgebrochen werden. Bei Abbruch der Operation wird dann ein in den zentralen Regeln einstellbarer Workflow (z. B. Benachrichtigung des E-Mail-Administrators) ausgeführt. Andernfalls wird die Nachricht signiert.
- Soll die Nachricht mit PGP oder S/MIME verschlüsselt werden, so muss das Zertifikat des Empfängers vorhanden sein oder aus einem Verzeichnis geladen werden können. Liegt es nicht vor, wird ein in den zentralen Regeln einstellbarer Workflow (z. B.

Aufforderung des Empfängers, sein Zertifikat an das E-Mail-Gateway zu senden) ausgeführt. Andernfalls wird die Nachricht verschlüsselt.

- Soll die Nachricht mit Passwort-basierter Verschlüsselung gesichert werden, so führt das E-Mail-Gateway die Operation aus, sofern das Passwort bekannt ist oder in der E-Mail mitgeliefert wird.

Je nach Produkt, Kommunikationspartner und den organisatorischen Prozessen muss der interne Nutzer bei Herstellung einer neuen Kommunikationsbeziehung einbezogen werden (z. B. Beschaffung der Schlüssel der externen Partner, Beantragen der Einrichtung einer neuen Kommunikationsbeziehung, Schlüsselwechsel des Partners etc.). Vor allem bei der Prüfung der Authentizität von Schlüsseln ist der Administrator oft auf die Unterstützung des internen Nutzers angewiesen.

Für den externen Kommunikationspartner besteht im Normalfall kein Unterschied zu einer Ende-zu-Ende-Lösung. Beim Empfänger kann entweder eine Client-basierte oder auch eine Server-basierte Lösung zum Einsatz kommen. Voraussetzung ist der Einsatz eines zu S/MIME oder PGP kompatiblen Produkts. Bei der Verwendung der Passwort-basierten Lösung ist es bei einigen E-Mail-Gateway-Produkten notwendig, dem externen Kommunikationspartner ein entsprechendes Produkt zur Verfügung zu stellen. Diese Passwort-basierten Verfahren sind meist proprietär und setzen daher die Verwendung von Produkten des gleichen Herstellers voraus.

Ein Sonderfall tritt ein, wenn speziell ausgewählte Nutzer zusätzlich in der Lage sein sollen, E-Mails mit einer Ende-zu-Ende Lösung zu verschlüsseln (z. B. in besonders kritischen Fällen). In diesem Fall sollte das E-Mail-Gateway in der Lage sein, verschlüsselte E-Mail von internen Nutzern als verschlüsselt zu erkennen und diese nicht zusätzlich zu sichern. Sendet der externe Kommunikationspartner eine E-Mail an einen internen Nutzer, führt er zunächst die Sicherungsoperation durch. Dann wird die gesicherte E-Mail an das E-Mail-Gateway weitergeleitet, in dem sie gemäß den zentral eingestellten Regeln verarbeitet werden:

- Soll der Kommunikationspartner die E-Mail mit PGP oder S/MIME verschlüsseln, muss er dazu im Besitz des dem Nutzer zugeordneten Zertifikats sein. Dies erhält er entweder direkt vom internen Nutzer oder über ein Verzeichnis. Verschlüsselte E-Mails werden vom E-Mail-Gateway entschlüsselt und an den internen Nutzer weitergeleitet.
- Vom externen Kommunikationspartner signierte E-Mails werden vom E-Mail-Gateway überprüft und das Ergebnis der Prüfung der E-Mail angehängt, sofern Zertifikate der externen Kommunikationspartner im E-Mail-Gateway vorhanden sind bzw. aus der E-Mail extrahiert werden können. Zudem muss die Vertrauenswürdigkeit der Zertifikate geprüft werden. Dies setzt in der Regel voraus, dass das E-Mail-Gateway das als vertrauenswürdig eingestufte Ausstellerzertifikat des Zertifikats des externen Kommunikationspartners kennt und auf eine entsprechende Sperrliste zugreifen kann. Bei der Verwendung des Austauschformats S/MIME enthält die signierte Nachricht das Zertifikat des Senders. Die meisten E-Mail-Gateways sind in der Lage, das Zertifikat aus der E-Mail zu extrahieren, so dass das Zertifikat im E-Mail-Gateway nicht vorhanden sein muss. Die E-Mail und das Ergebnis der Signaturprüfung werden an den internen Nutzer weitergeleitet.
- Das Senden von E-Mails des externen Kommunikationspartners an einen internen Nutzer, die mit Passwort-basierter Verschlüsselung gesichert sind, ist grundsätzlich möglich. Allerdings wird die Speicherung und Verwaltung des Passworts bei den meisten E-Mail-Gateway-Produkten z. Zt. nicht unterstützt. Um externen Kommunikationspartnern ohne PKI-Sicherheitsinfrastruktur das Senden gesicherter E-Mails zu ermöglichen, könnte die E-Mail z. B. über einen SSL-gesicherten Web-Server an den internen Nutzer gesendet werden.

4 Marktüberblick

Es werden verschiedene E-Mail-Gateway-Produkte angeboten. Diese lassen sich in zwei Klassen unterteilen.

Eine Klasse *E-Mail-Gateway mit integrierten Schutz der internen Strecke* (mit dem Vertreter Entrust Messaging Server) zeichnet sich dadurch aus, dass

- der Schutz der internen Strecke Teil der angebotenen Lösung ist,
- eine Sicherung der E-Mail-Kommunikation auch zwischen zwei internen Nutzern möglich ist,
- zusätzliche Client-Software (E-Mail Plug-In) im Rechner des Nutzers installiert bzw. bei Lotus Notes eine angepasste Mailschablone verwendet werden muss und
- auf zentrale Regeln für die Sicherung der E-Mails verzichtet wird (d. h. die Nutzer entscheiden über die Sicherung).

Der Unterschied zu Ende-zu-Ende Lösungen besteht in erster Linie darin, zentrale Viren- und Inhaltsprüfungen zu ermöglichen und die Komplexität der Sicherungsoperationen (z. B. Zertifikatsverwaltung) auf dem Client zu reduzieren.

Die andere Klasse *E-Mail-Gateway ohne integrierten Schutz der internen Strecke* (Vertreter sind z. B. BCC Mail Protect Gateway, C1 Secure Mail Gateway, Glück & Kanja CryptoEx Business Gateway, Group IQ Suite, ICC JULIA MailOffice, TFS Secure Messaging Server, Tumbleweed MS Secure Redirect und Utimaco Secure Mail Gateway) zeichnet sich dadurch aus, dass

- der Schutz der internen Strecke anderweitig erreicht werden muss (siehe Kapitel 2.2),
- die Sicherung der E-Mail-Kommunikation zwischen zwei internen Nutzer durch das E-Mail-Gateway in der Regel nicht möglich ist,
- zentrale Regeln für die Sicherung der E-Mails verwendet werden (die der Nutzer ggf. überschreiben kann) und
- der E-Mail-Client nicht angepasst werden muss.

Bei Analyse und Test einiger E-Mail-Gateway-Produkte fiel auf, dass

- die untersuchten Produkte die meisten der grundlegenden gewünschten Anforderungen erfüllen, in wichtigen Details (z. B. Beziehen von Zertifikaten, Integration in die E-Mail-Infrastruktur) aber deutliche Unterschiede aufweisen,
- einige Produkte bei Lasttests Probleme aufwiesen (wie z. B. Absturz oder Nichtauslieferung von E-Mails), und
- einige Produkte unausgereift wirkten, was möglicherweise darauf zurückzuführen ist, dass sie noch nicht sehr lange auf dem Markt erhältlich sind.

Die technische Prüfung eines E-Mail-Gateway-Produkts sollte auf Basis der zuvor festgelegten und priorisierten Anforderungen sowie von Tests in der Testumgebung der eigenen Organisation erfolgen.

Es gibt je nach Hersteller unterschiedliche Lizenzkostenmodelle für E-Mail-Gateway-Produkte:

- Bei allen Herstellern sind die Kosten abhängig von der Nutzeranzahl und werden pro Nutzer ausgewiesen. Je höher die Nutzeranzahl, desto niedriger sind die Kosten pro Nutzer.
- Bei einigen Herstellern werden zusätzlich (fixe) Kosten für jedes verwendete E-Mail-Gateway erhoben. Auch bei Verwendung mehrerer E-Mail-Gateways ist diese Summe bei hoher Nutzerzahl meist zu vernachlässigen. Sie führt aber bei niedriger Nutzerzahl zu einem eher hohen Preis für die Lizenz der Software.

Zu beachten ist, dass der Begriff Nutzer unterschiedlich interpretiert wird. Unter einem Nutzer werden in jedem Fall die internen Nutzer verstanden, die mit Schlüsseln und Zertifikaten ausgestattet werden. Zum Teil zählen jedoch auch die externen Kommunikationspartner dazu, für die im E-Mail-Gateway nur ein Zertifikat gespeichert ist. Um eine Vergleichbarkeit der Kosten zu erreichen, sollte der Nutzerbegriff mit dem Hersteller geklärt werden

5 Diskussion

Werden die Erwartungen mit den Anforderungen an E-Mail-Gateway-Lösungen verglichen, so ergibt sich ein differenziertes Bild. Vorteile des Ansatzes sind:

- Zentrale Inhalts- oder Virenprüfungen können für gesicherte E-Mails durchgeführt werden.
- Die Umsetzung von Vertretungsprozessen ist möglich.
- Die Nutzer sind i. a. weniger stark in die Sicherung von einzelnen E-Mails involviert.
- Die Verwendung von Client-Software wie E-Mail Plug-Ins ist zumindest für die Klasse der E-Mail-Gateways ohne Schutz der internen Strecke überflüssig.

Nachteile sind:

- Bei den meisten E-Mail-Gateways werden die Schlüssel der Nutzer zentral im E-Mail-Gateway gespeichert und ausgehende E-Mails interner Nutzer vom E-Mail-Gateway signiert, ohne den Nutzer in den Signaturprozess zu involvieren. Die Aussagekraft von Signaturen in signierten E-Mails ist daher eher gering.
- Die interne Strecke wird von den meisten E-Mail-Gateways nicht geschützt. Dies muss anderweitig erreicht werden.

Die Eignung und Funktionsfähigkeit der Lösung hängt stark von der Art der Kommunikationspartner ab.

Sind die externen Kommunikationspartner bzw. deren Organisation langfristig vorher bekannt, so können die notwendigen Vorarbeiten vom E-Mail-Gateway-Administrator im Vorfeld vorgenommen werden. Vorarbeiten sind z. B.

- der Import des Root CA Zertifikats des Kommunikationspartners,
- die Überprüfung des Root CA Zertifikats,
- die Festlegung des Root CA Zertifikats als vertrauenswürdig,
- der Import der Zertifikate der externen Kommunikationspartner in das E-Mail-Gateway oder
- die Anbindung eines externen Verzeichnisses, in dem sich die Nutzerzertifikate und die Sperrlisten befinden.

Haben zusätzlich die externen Kommunikationspartner automatisierten Zugriff auf die Zertifikate der internen Nutzer, so steht der relativ problemlosen gesicherten Kommunikation per E-Mail nichts im Wege. Vom Ende-zu-Ende-Ansatz bekannte mögliche Probleme und Herausforderungen bleiben aber bestehen. Dazu zählen

- die Interoperabilität der Sicherungsprotokolle (S/MIME, PGP) zwischen Sender und Empfänger. Nicht alle Implementierungen unterstützen auch die optionalen Teile des standardisierten Sicherungsprotokoll; auch Implementierungsfehler oder unterschiedliche Auslegungen des Standards können zu Problemen führen.
- die Bereitstellung von Zertifikaten für externe Kommunikationspartner, insbesondere bei Verwendung von individuellen Nutzerschlüsseln. Hierzu muss in der Regel ein Verzeichnis betrieben werden, auf das Externe zugreifen können.

- die Verwendung verschiedener Sicherungsprotokolle für eine E-Mail, wenn diese an verschiedene Empfänger gesendet wird. Dies wird insbesondere dann schwierig, wenn die E-Mail an interne Nutzer und externe Kommunikationspartner gesendet wird und für die Sicherung der internen Strecke Sicherungsmechanismen der E-Mail Infrastruktur (z.B. die Lotus Notes eigene Verschlüsselung) eingesetzt werden. Ggf. muss hingenommen werden, dass die E-Mails an interne Nutzer allenfalls auf der Transportschicht (z.B. per Notes Portverschlüsselung) gesichert werden. In jedem Falle sollte gewährleistet sein, dass das verwendete E-Mail-Gateway-Produkt die Verwendung verschiedener Sicherungsprotokolle für eine E-Mail an verschiedene externe Kommunikationspartner unterstützt.

Zu beachten ist, dass der interne Nutzer in viele Vorarbeiten nicht involviert ist. Dies gilt auch für den externen Kommunikationspartner, sofern seine Organisation (z. B. ein Administrator) diese Aufgabe wahrnimmt.

Werden die externen Kommunikationspartner jedoch ad hoc festgelegt und soll eine zertifikatsbasierte Verschlüsselung erfolgen (z. B. PGP oder S/MIME), so ist die aktive Mitarbeit des E-Mail-Gateway-Administrators erforderlich, denn er muss das Root CA Zertifikat oder das Benutzerzertifikat prüfen und als vertrauenswürdig markieren, sofern die Lösung ein Mindestmaß an Sicherheit bieten soll. Zudem sind eine aktive Mitarbeit und entsprechende Kenntnisse des externen Kommunikationspartners erforderlich. Neben der Bereitstellung des Root CA Zertifikats muss er dem E-Mail-Gateway auch sein persönliches bzw. sein unternehmensweites Zertifikat zur Verfügung stellen.

Bei einer ad hoc Kommunikation kann diese Aufgabe i. a. nicht an dessen Organisation delegiert werden. Der interne Nutzer muss zusätzlich ggf. bei der Authentizitätsprüfung und bei Vertrauensentscheidungen beteiligt sein, da häufig nur er oder sie den direkten Kontakt zum externen Kommunikationspartner hat. Durch die erforderliche Mitarbeit des E-Mail-Gateway-Administrators und die notwendigen Prozesse ergibt sich notwendigerweise eine Verzögerung in der Kommunikation, die gerade bei ad hoc Kommunikation mit dringendem Bedarf unerwünscht ist. Es muss auch geklärt werden, wie die Prüfung des Root CA Zertifikats durch einen E-Mail-Gateway-Administrator vorgenommen werden kann.

Eine Alternative wäre es, auf die Beteiligung des E-Mail-Gateway-Administrators zu verzichten. Dies würde bedeuten, dass die manuelle Prüfung des Root CA Zertifikats sowie der manuelle Import von Schlüsseln und Zertifikaten wegfallen müsste. Dies hieße aber, dass alle z. B. aus E-Mails oder Verzeichnissen importierten Schlüssel automatisch als vertrauenswürdig gelten und anschließend benutzt würden. Angreifer könnten sich selber Schlüssel und Zertifikate für den anzugreifenden externen Kommunikationspartner generieren und in das E-Mail-Gateway einstellen. Wären sie in der Lage, E-Mails an diesen externen Kommunikationspartner abzufangen und zu sich umzuleiten, könnten sie damit dem internen Nutzer eine falsche Identität vorspiegeln. Insofern ist diese Alternative nicht sinnvoll, sofern die Lösung ein Mindestmaß an Sicherheit bieten soll.

Soll bei der ad hoc Kommunikation mit externen Kommunikationspartnern eine Passwort-basierte Verschlüsselung genutzt werden, so kann u. U. auf eine aktive Rolle des E-Mail-Gateway-Administrators verzichtet werden. Voraussetzung wäre aber die Einstellung einer zentralen Regel, nach der für alle Kommunikationspartner, für die kein Zertifikat hinterlegt ist, die Passwort-basierte Verschlüsselung angewendet werden soll. Allerdings muss gewährleistet sein, dass die Empfänger die verschlüsselte Nachricht lesen können (d. h. über das ent-sprechende Verschlüsselungssystem verfügen) und diese nicht durch einen E-Mail-Filter blockiert wird. Letzteres ist z. B. leicht möglich, falls die verschlüsselte Nachricht in einem selbstextrahierenden Format (z.B. exe) vorliegt.

Nutzer und externe Kommunikationspartner müssen sich zudem auf ein Passwort einigen. Bei vielen verschiedenen Kontakten kann das erforderliche Passwortmanagement die Nutzer überfordern. Dadurch ist ersichtlich, dass auch die Passwort-basierte Verschlüsselung nicht unproblematisch ist. Zudem kann sie für die E-Mails vom externen Kommunikationspartner zum internen Nutzer nur dann eingesetzt werden, wenn der externe Kommunikationspartner Verschlüsselungen durchführen und das Passwort im E-Mail-Gateway hinterlegt werden kann, z. B. dadurch, dass sich das E-Mail-Gateway die Passwörter speichert und eine entsprechende Regel für die Kommunikationsbeziehung generiert. Diese Technik wird aber bislang von keinem der untersuchten Produkte verwendet.

Eine alternative Möglichkeit wäre es, E-Mails über einen SSL-gesicherten Web-Server auszutauschen. Dies würde aber bedeuten, dass einer oder beide Kommunikationspartner die eigene E-Mail-Infrastruktur nicht mehr für diese Kommunikation verwenden. Dies wird nicht bei allen Organisationen akzeptiert bzw. bei externen Kommunikationspartnern (insbesondere bei komplexen Workflows) durchsetzbar sein.