Link: https://www.tecchannel.de/a/automatische-verschluesselung-mit-e-mail-gateways,1762105

Zentrale E-Mail-Verschlüsselung statt Desktop-Security

Automatische Verschlüsselung mit E-Mail Gateways

Datum: 02.07.2008
Autor(en): Klaus Manhart

E-Mail Gateways verschlüsseln und signieren Mails automatisch – der Anwender kommt ganz ohne Krypto-Lösung aus. Mit E-Mail Gateways können Unternehmen eine sichere E-Mail-Lösungen installieren.

Trotz vielfältiger Sicherheitsprobleme und der einfachen Möglichkeiten, den E-Mail-Verkehr im Internet mitzulesen scheuen viele Unternehmen den Aufwand, vertrauliche elektronische Post zu verschlüsseln und zu signieren. Eine sichere E-Mail-Lösung steht zwar bei vielen Unternehmen auf der To-Do-Liste, doch mit der Umsetzung hapert es. Laut einer Studie der Sicherheitsexperten des unabhängigen **Ponemon-Instituts**[1] verfügten 2007 lediglich 26 Prozent der deutschen Unternehmen über eine Verschlüsselungsstrategie.

Die Ursache für die zögerliche Einführung von E-Mail-Sicherheit liegt zum einen in der mangelnden Akzeptanz von Mitarbeitern und Kommunikationspartnern. Zum anderen schlagen der hohe Administrationsaufwand und Kosten für die Infrastruktur zu Buche – Client-Software, Lesegeräte, Helpdesk und Zertifikatsmanagement belasten Administratoren und den Firmenetat.

Diese Probleme lassen sich vor allem auf das vorherrschende clientbasierte Sicherheitskonzept zurückführen. Bei diesem so genannten End-to-End-Ansatz wird die Verschlüsselung, Entschlüsselung und das Signieren von E-Mails sowie deren Verifikation auf dem lokalen Anwenderrechner durchgeführt. Jeder PC muss hierfür mit einem sicheren E-Mail-Client mit Kryptografie-Funktion ausgestattet werden.

Die Krypto-Fähigkeit bringt die Mail-Software entweder von Haus aus mit – wie etwa Outlook - oder sie wird über Plug Ins nachgerüstet. In der Regel werden alle Mitarbeiter über eine zentrale Public Key Infrastruktur (PKI) mit eigenen und fremden Schlüsseln versorgt, die sie auf ihren PCs dezentral verwalten. Auf diese Weise ist es möglich, dass E-Mails durchgängig vom Sender zum Empfänger in geschützter Form versendet werden können – daher der Name „End-to-End“.

1. Problematische End-to-End-Verschlüsselung

End-to-End-Verschlüsselung am Arbeitsplatz ist effizient und schützt die Nachrichten auch innerhalb eines Firmennetzwerks vor unerlaubtem Zugriff. Doch diese individuelle Lösung hat auch eine ganze Reihe gravierender Nachteile.

So sind clientbasierte Securitykonzepte nur mit viel Aufwand und hohen Administrationskosten realisierbar – die Installation von PlugIns auf den Rechnern von Sendern und Empfängern ist dabei noch das geringste Übel. Kosten entstehen auch durch die Schulung von Mitarbeitern. Schließlich braucht es auch nutzerseitig einige Kenntnisse über Verschlüsselungs- und Signaturverfahren. Außerdem funktioniert der zentrale Antivirenscanner nicht mehr, da die E-Mails auch für ihn verschlüsselt sind.

Wird die End-to-End-Verschlüsselung mit der Einführung einer unternehmensweite PKI verknüpft – wie dies in vielen Fällen geschieht – wird die Komplexität zusätzlich verschärft. Die Schlüssel der Mitarbeiter müssen bei dem Individualansatz entweder an zentraler Stelle hinterlegt werden oder jede E-Mail muss zusätzlich, also doppelt, mit einem Hauptschlüssel verschlüsselt werden.

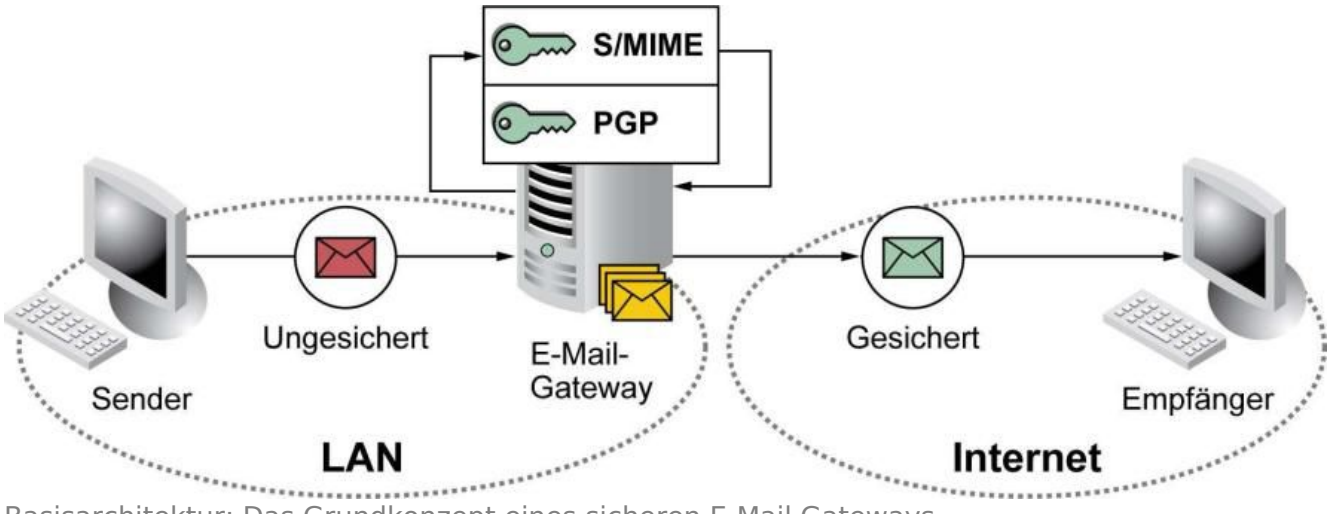
Mit die gravierendste Schwachstelle der End-to-End-Verschlüsselung ist die mangelnde Umsetzung der unternehmensweiten Sicherheitspolicy. Schließlich bleibt jedem Mitarbeiter individuell die Entscheidung überlassen, wie diszipliniert er die Regeln für die Verschlüsselung und Signierung vertraulicher Informationen einhält. Die Sicherheitspolitik eines Unternehmens lässt sich mit individuell ausgerichteten Konzepten daher nicht konsequent umsetzen.

2. Secure E-Mail Gateways

Diesen Risiken und Nachteilen entgeht man mit einer serverseitigen Verschlüsselungslösung, einem Secure E-Mail Gateway. Alle kryptografischen Vorgänge wie Verschlüsseln und Signieren werden hier vom individuellen Desktop-PC in ein dediziertes Mail Gateway verlagert.

Das Gateway befindet sich dabei an zentraler Stelle im Unternehmensnetzwerk und wird entweder als eigenständige Server oder als Aufsatz für vorhandene E-Mail-Server eingesetzt. Wegen der Analogien zum Umgang mit Briefen in Organisationen wird diese Art der Lösung häufig auch als „virtuelle Poststelle“ bezeichnet.

Im Gegensatz zu einer Einzelplatzlösung nimmt ein sicheres Mail Gateway alle wichtigen kryptografischen Vorgänge für Mitarbeiter und bestimmte Nutzergruppen transparent vor: Die virtuelle Poststelle verschlüsselt und signiert ausgehende E-Mails und entschlüsselt und verifiziert den eingehenden E-Mail-Verkehr. Das alles erfolgt automatisch und einheitlich gemäß den Unternehmensrichtlinien.



Basisarchitektur: Das Grundkonzept eines sicheren E-Mail Gateways.

Die Mitarbeiter haben somit keinen Mehraufwand: Die Gateway-Anwender können ihre E-Mails wie gewohnt empfangen und versenden, ohne dass sie dazu irgendwelche zusätzlichen Tätigkeiten ausüben müssen. Auch auf Seite der Kommunikationspartner sind die Anforderungen minimal – sie kommen gegebenenfalls ganz ohne kryptografische Software aus. Ein E-Mail Gateway gewährleistet damit Vertraulichkeit, Integrität und Verbindlichkeit bei E-Mails deutlich besser als isolierte Insellösungen.

3. Sichere Mails versenden

Alle Secure Mail Gateways unterstützen zumindest die Verschlüsselungsstandards S/MIME und PGP bzw. OpenPGP. Die öffentlichen und privaten Schlüssel der Sender und die öffentlichen Schlüssel der Empfänger bzw. deren Zertifikate speichert das Gateway.

Über Regeln wird der virtuellen Poststelle mitgeteilt, wann eine E-Mail signiert oder verschlüsselt werden soll. Solche Regeln können zum Beispiel auf bestimmte Schlüsselwörter im Inhalt und Betreff reagieren oder auf bestimmte Mail-Empfänger. Meist sind diese Regeln als Sicherheitsrichtlinien fest im Gateway definiert, so dass der Mitarbeiter keinen zusätzlichen Aufwand hat.

Versendet ein Mitarbeiter eine E-Mail, empfängt das E-Mail Gateway die Sendung und erkennt anhand der eingestellten Regel, dass diese verschlüsselt oder signiert werden soll. Das Signieren erfolgt mit dem zentral hinterlegten privaten Schlüssel des Nutzers, die Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers. Anschließend wird die gesicherte E-Mail an den externen Kommunikationspartner gesendet.

Der umgekehrte Weg, das Empfangen verschlüsselter Mails, funktioniert analog. Empfangene, geschützte Mails verifiziert und entschlüsselt das Gateway automatisch und gibt die Mails mit einem passenden Kommentar - im Betreff oder einem spezifischen Header - an die Adressaten weiter. Empfangene, verschlüsselte Mails sieht der Mitarbeiter also immer sofort im Klartext.

Ist das Zertifikat des externen Kommunikationspartners im E-Mail Gateway vorhanden, so kann auch die Signatur geprüft werden. Liegt das Zertifikat nicht vor, kann das Gateway die notwendigen Zertifikate über externe und interne Serviceanbieter abrufen.

4. Entschlüsseln ohne Krypto-Software

Steht dem Empfänger kein Schlüssel bzw. Zertifikat zur Verfügung, gibt es alternative Methoden. Verbreitet ist die Hinterlegung der Nachricht auf einem sicheren Webserver oder die Zusendung verschlüsselter, selbstextrahierender Dateien, die mittels Passphrase wieder entschlüsselt werden. Im ersten Fall erhält der Empfänger eine Benachrichtigungs-Mail und kann mit einem Passwort die verschlüsselte Mail per https-Verbindung vom Webmailer abrufen.

Das folgende Beispiel illustriert den Ablauf bei Verschlüsselung mit Passphrase mit dem **SEPPmail Secure E-Mail Gateway**[2]:

- Der Sender verschickt seine als vertraulich markierten E-Mails wie gewohnt mit seinem Mailprogramm
- SEPPmail generiert ein Passwort, das an den Sender zurückgeschickt wird.
- Das Passwort gibt der Sender dem Empfänger seiner E-Mails bekannt, beispielsweise telefonisch, per SMS oder als Fax.
- Die Verschlüsselung der E-Mail erledigt SEPPmail automatisch im Hintergrund.

- Der Empfänger erhält eine E-Mail mit der Information und Aufforderung zur Passworteingabe.
- Nach Überprüfung der Eingabe wird die Nachricht automatisch entschlüsselt und kann im Mailprogramm wie gewohnt abgespeichert werden.

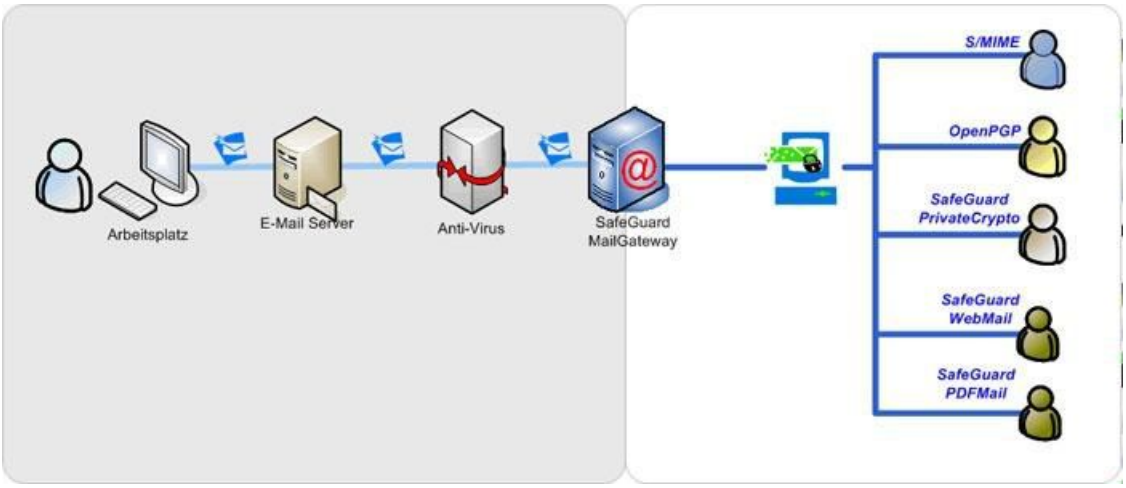
Sicherheit per Push: Die Hardware-Appliance SEPPmail bietet eine 2-Faktor-Authentifikation per Mail und Passwort. (Quelle: Zoe-One GmbH)

5. Vorteile eines zentralen Mail Gateways

Ein sicheres, zentrales E-Mail Gateway bietet Unternehmen mehrere Vorteile. So gewährleistet das Secure Mail Gateway, dass alle ausgehenden E-Mails zu 100 Prozent verschlüsselt und sicher zugestellt werden. Disziplinlosigkeit einzelner Mitarbeiter, Flüchtigkeitsfehler und Unachtsamkeiten beim Verschicken von vertraulichen Informationen werden eliminiert.

Der Installations- und Administrationsaufwand wird erheblich reduziert. Durch den zentralen Ansatz lassen sich PKI-Funktionen schnell und einfach implementieren und einsetzen, der Aufwand ist im Vergleich zu einer End-to-End-Verschlüsselung gering. Zusätzliche, clientbasierte Software mit PlugIns ist nicht nötig.

Der Gateway-basierte Ansatz erleichtert auch die Umsetzung der Security Policy des Unternehmens. Richtlinien, die beispielsweise festlegen, ob E-Mails signiert werden müssen oder welche Mails an welche Empfänger verschlüssel werden müssen, können zentral definiert und verwaltet werden. Auch eine Viren- und Inhaltsprüfung kann zentral gemäß der Unternehmenspolicy erfolgen.



Virencheck: Anders als bei End-to-End-Verschlüsselung kann bei Secure Mail Gateways die Virenprüfung vor dem Mail-Server erfolgen. (Quelle: Utimaco)

Ein weiterer Vorteil: Secure E-Mail Gateway unterstützten in der Regel mehrere Standards - wie S/MIME, ISIS-MTT oder OpenPGP - und Methoden wie symmetrische oder asymmetrische Verschlüsselungsverfahren. Zudem lassen sich die öffentlichen Schlüssel der externen Kommunikationspartner zentral und gesichert auf dem Gateway speichern und verwalten.

6. Nachteile von Mail Gateways – und deren Behebung

Den Vorteilen stehen zwei wesentliche Nachteile von Mail Gateways gegenüber. So ist der Konfigurationsaufwand bei zentralen Gateways im Vergleich zu isolierten End-to-End-Lösungen aufwändiger. Besonders kleinere, sicherheitstechnisch weniger anspruchvolle Firmen, sollten deshalb abwägen, ob nicht eine isolierte Lösung doch besser ist.

Ein großer Schwachpunkt der zentralen Lösung ist die innere Sicherheit. Die interne Strecke wird – anders als bei End-to-End-Lösungen - von den meisten E-Mail Gateways nicht geschützt. Dies muss bei Bedarf anderweitig erreicht werden.

Eine Möglichkeit ist, ein Mail Gateway mit Sicherung der internen Stecke zu installieren. Dazu müssen allerdings die Anwenderrechner mit zusätzlicher Client-Software oder benutzerspezifischen Schlüsseln und Zertifikaten ausgestattet werden – was den Vorteil von zentralen Gateways wieder dahin schmelzen lässt.

Eine bessere Möglichkeit ist, die spezifischen Verschlüsselungsmechanismen der E-Mail-Infrastruktur etwa mittels Portverschlüsselung in Domino/Notes oder SMTP über SSL bei Microsoft Exchange auszunutzen. Vorteil dieser Methode ist, dass die Clients nicht mit zusätzlicher Software oder benutzerspezifischen Schlüsseln und Zertifikaten ausgestattet werden müssen.

7. Marktübersicht Secure E-Mail Gateways

Grundsätzlich lassen sich E-Mail Gateways im internen Netz eines Unternehmens entweder als eigenständige Server oder als Aufsatz für vorhandene E-Mail-Server einsetzen. Im letzten Fall werden sie in bestehende E-Mail-Infrastrukturen wie beispielsweise Microsoft Exchange, Lotus Domino oder GroupWise eingebunden.

In den meisten Fällen werden E-Mail Gateways aber als eigenständige Server am Übergang zwischen dem internen Netzwerk und dem Internet eingesetzt. Hierfür bieten zahlreiche Hersteller inzwischen zentralisierte Gateway-Lösungen an. Die Tabelle gibt einen Überblick über die wichtigsten Produkte.

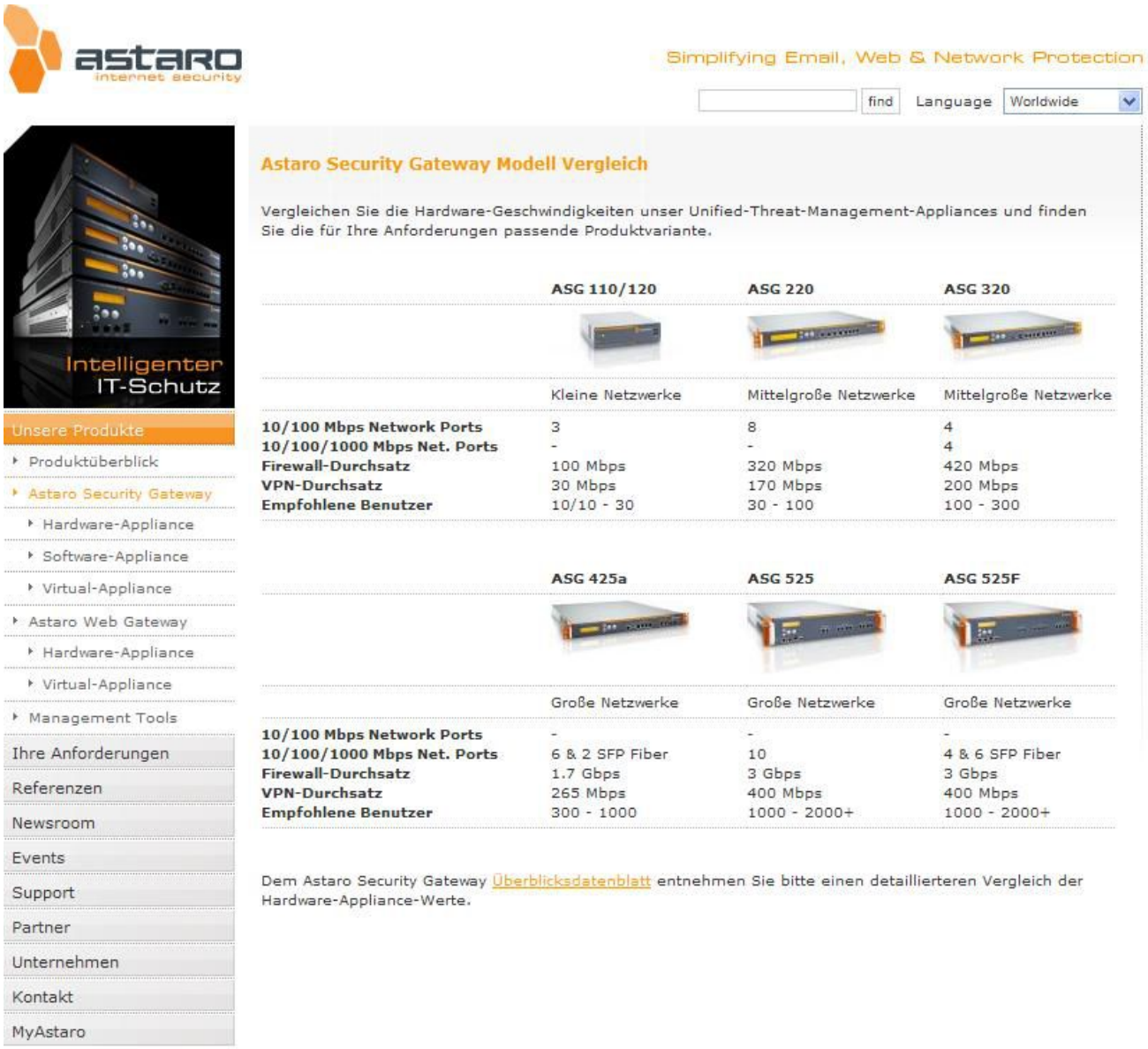
Zentrale Secure E-Mail Gateways im Überblick

Anbieter	**Name des Tools**	**System**	**Standards**	**URL**
Astaro	Security Gateway	Hardware-, Software und Virtual Appliance, Linux	S/MIME, PGP, TLS	**www.astaro.de**[10]
ICC Solutions	Julia Mail Office	Software-Appliance, Linux, Solaris	S/MIME, PGP	**www.iccSec.com**[11]
PGP Corporation	PGP Universal Gateway Email	Software-Appliance, Linux	S/MIME, PGP	**www.pgp.com**[12]
Utimaco	SafeGuard MailGateway	Software-Appliance, Linux	PGP, S/MIME	**www.utimaco.de**[13]
Zertificon	Z1 SecureMail Gateway	Software-Appliance, Linux, Solaris	S/MIME, PGP	**www.zertificon.com**[14]
Zoe-One	SEPPmail Secure E-Mail Gateway	Hardware-Appliance in drei Ausführungen	S/MIME, PGP,TLS	**www.seppmail.ch**[15]

8. Software oder Hardware Appliance?

Die Grundfunktionalität – die kryptografische Behandlung von E-Mails über einen zentralen Server – ist bei allen Systemen ähnlich. Dennoch unterscheiden sie sich im Detail.

Die meisten Systeme laufen unter Linux und sind technisch unterschiedlich realisiert. Gateways wie die von **Astaro**[3] und **Utimaco**[4] werden als Software Appliances geliefert – fertig gepackte und vorkonfigurierte Pakete inklusive Anwendung und Betriebssystem mit wenig Installations– und Konfigurationsaufwand.



Bedarfsgerecht: Astaro bietet Hardware-Appliances für unterschiedlich große Netzwerke. (Quelle: Astaro)

Neben Software-Appliances bietet Astaro alternativ Hardware Appliances für verschiedene Nutzerzahlen an. Bei Hardware-Appliances wird ein vorkonfiguriertes System inklusive Hardware bereitgestellt. Sie sind vor allem für Anwender mit geringen Administrationskapazitäten empfehlenswert. **Zoe-One**[5] liefert sein **SEPPMail-Gateway**[6] ausschließlich in Hardwareform im Desktop oder 19-Zoll-Rack-Format.

Bei allen Herstellern sind die Lizenzkosten abhängig von der Nutzeranzahl und werden pro User ausgewiesen. Je höher die Nutzeranzahl, desto niedriger sind die Kosten pro User. Bei einigen Herstellern werden zusätzlich fixe Kosten für jedes verwendete E-Mail Gateway erhoben. Die Tabelle enthält aus diesen Gründen keine Preise, ein Angebot des Herstellers erhalten Sie auf Anfrage.

Bei der Auswahl ist darauf zu achten, dass die Gateways sowohl S/MIME als auch PGP unterstützen - was alle in der Tabelle aufgeführten Tools auch leisten. Mit diesen Verschlüsselungsstandards sind Anwender immer auf der sicheren Seite – die standardisierten Protokolle gewährleisten eine gesicherte Kommunikation mit praktisch jedem Gesprächspartner.

Alle Lösungen eignen sich auch für kleine Netzwerke zwischen 10 und 50 Mitarbeitern. Bei kleinen Netzen besonders gut bewährt hat sich **Julia MailOffice**[7]. Gut skalierbar sind die Hardware-Appliances Astaro und SEPPMail. Letzteres bietet Server-Racks für Unternehmen mit bis zu 50, 500 und für über 500 Mitarbeiter. Eine skalierbare Lösung für größere Unternehmen ist das PGP Universal Gateway, das z.B. auch Fail-Over-Mechanismen bietet.

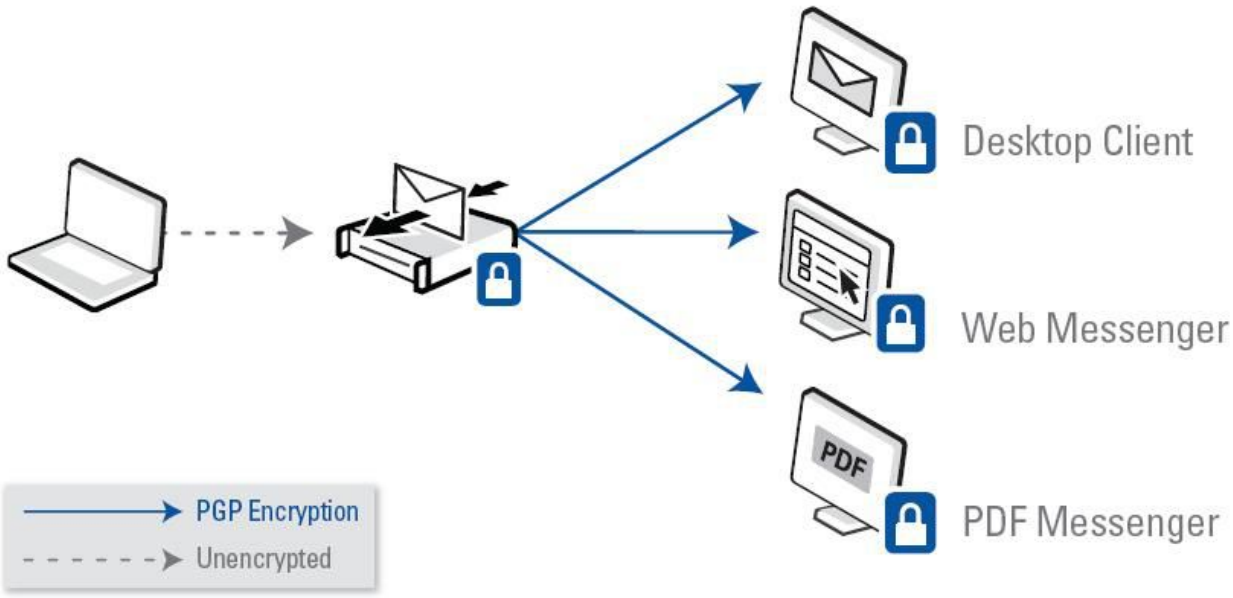
9. Sichere Mails empfangen ohne Krypto-Software

Viele, aber nicht alle, Systeme bieten Alternativen für den Fall, dass der Kommunikationspartner über keine Krypto-Lösung verfügt. Beim **PGP Universal Gateway**[8] hat der Empfänger über das bereits erwähnte Verfahren der passwortgeschützten Website (https) Zugriff auf die Mail.

Die Utimaco Lösung generiert für den Fall, dass die Gegenstelle über keine Krypto-Lösung verfügt, einen Zufallsschlüssel und verschlüsselt die E-Mail mit dem Programm PrivateCrypto. Der Zufallsschlüssel wird an den Absender der E-Mail geschickt, damit dieser ihn „out-of-band“ sicher an den vorgesehenen Empfänger schicken kann.

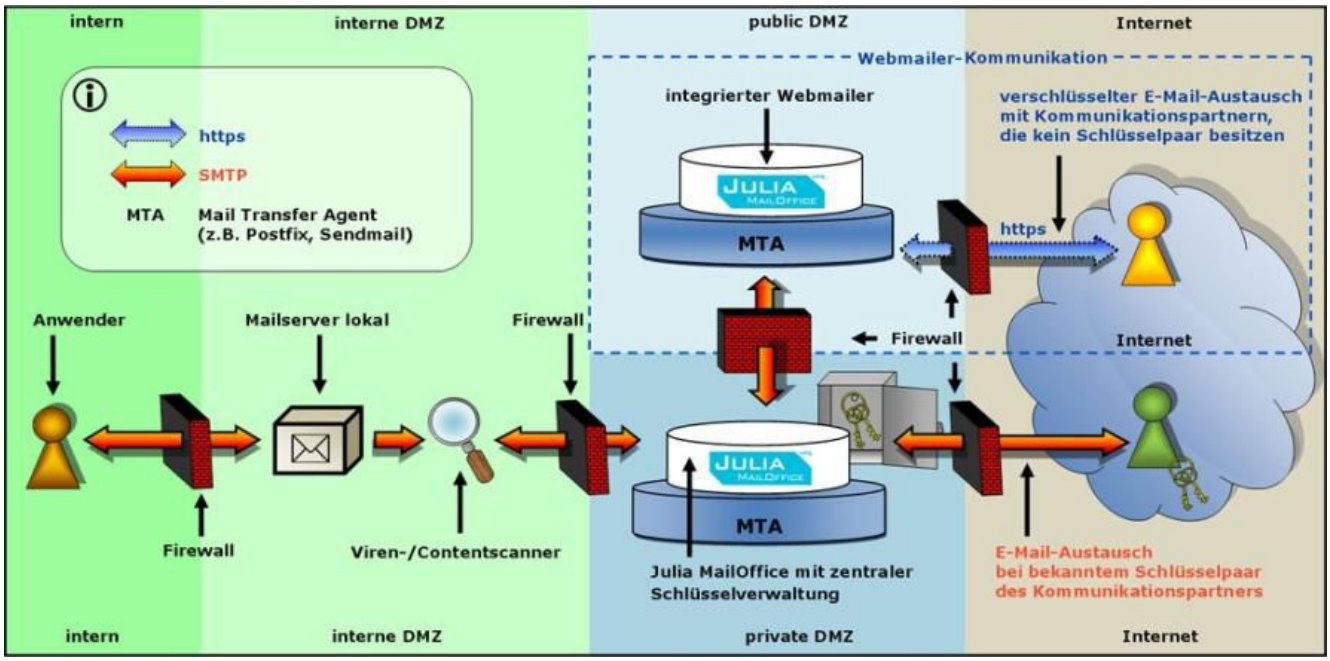
Eine inzwischen recht beliebte und häufig angewandte Methode ist die Verschlüsselung der E-Mail als PDF. Dabei wird die Mail vor dem Versand inklusive deren Anhang in eine PDF-Datei umgewandelt. Diese PDF-Datei wird verschlüsselt und als Attachment per E-Mail an den eigentlichen Empfänger verschickt. Mit dem ihm mitgeteilten Passwort kann er die PDF-Datei öffnen und in den E-Mail Client importieren.

Auch hier entfällt also die Notwendigkeit von Krypto-Software für den Kommunikationspartner. Beim PGP Universal Gateway lässt sich beispielsweise über den PDF Messenger eine als PDF verschlüsselte Mail versenden, Utimaco nutzt das Tool Safeguard PDFMail dafür.



Dreibeinig: Das PGP Universal Gateway liefert vertrauliche E-Mails über eine Client-Software, eine sichere Website oder als PDF aus. (Quelle: PGP)

Über besonders vielfältige Optionen verfügt Julia MailOffice, das von der Bundesregierung im Rahmen des Projektes **BundOnline 2005**[9] genutzt wurde. Hat der Empfänger keine Krypto-Lösung bietet das Gateway alternativ einen Webmailer, auf den die Gegenstelle nach einer E-Mail-Info per https-Link zugreifen kann. Außerdem kann Julia MailOffice eigene Zertifikate erzeugen sowie Mails ebenfalls mittels verschlüsseltem PDF übertragen.

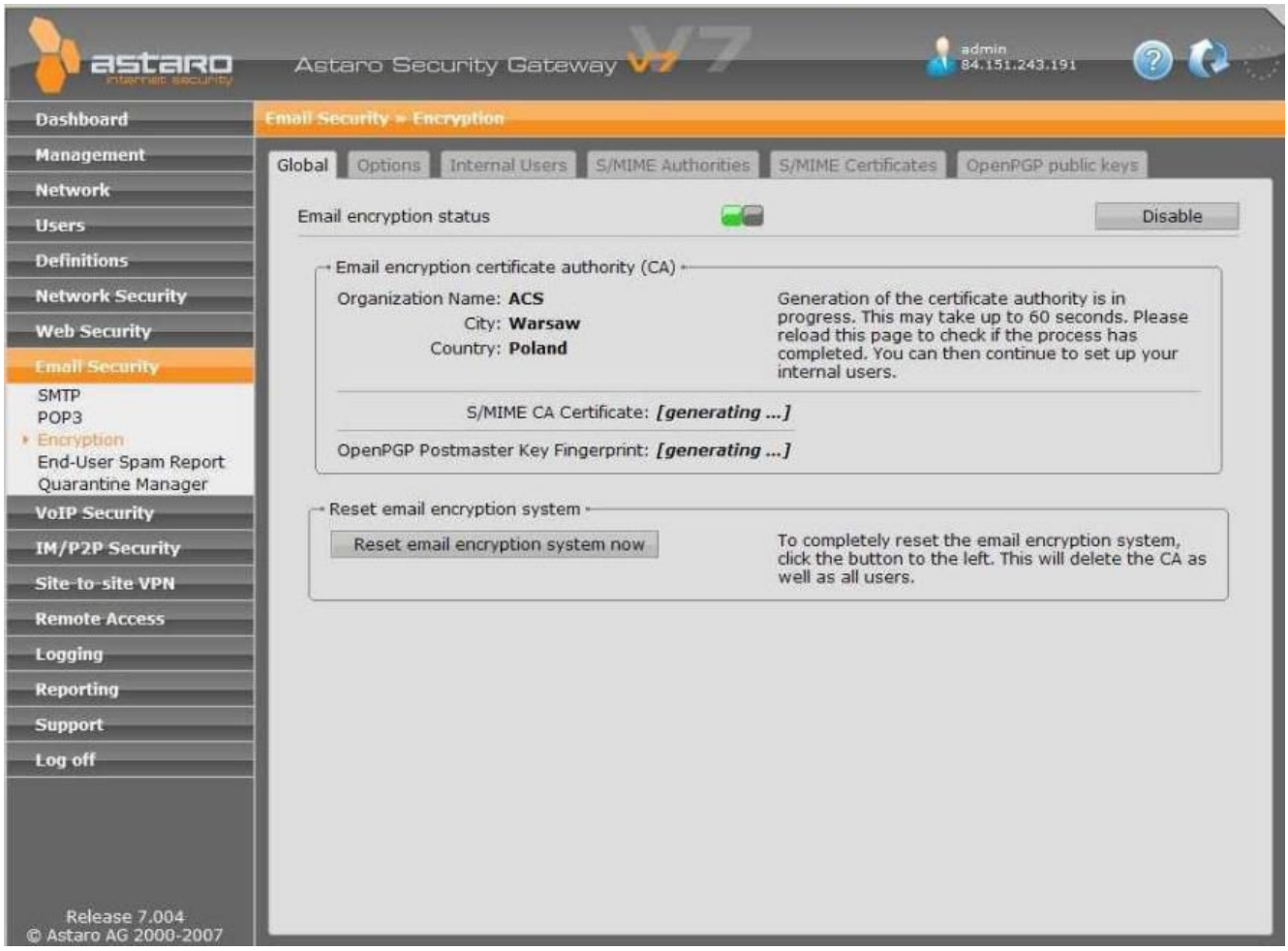


Hoch modular: Individuelle Anforderungen können mit Julia MailOffice leicht umgesetzt werden. (Quelle: ICC Solutions)

10. Beispiel: Verschlüsselung einrichten

- Administratoren eines E-Mail Gateways müssen eine Reihe von Aufgaben bewältigen: Die Konfiguration der Verbindung des E-Mail Gateways,
- die Einstellung zentraler Regeln für die Signierung sowie die Ver- und Entschlüsselung
- und die Definition von Workflows - etwa für den Fall, dass für externe Partner keine Zertifikate im E-Mail Gateway hinterlegt sind.

Viele Tools erlauben die Konfiguration über ein Web-Interface. Über diese zentrale Admin-Schnittstelle ist bei den meisten Tools eine fein granulare Justierung des Mail-Handlings möglich.



Web-Interface: Beim Astaro Security Gateway erfolgt die Konfiguration bequem über ein Web-Interface. (Quelle: Astaro)

Beim Astaro Security Gateway beispielsweise erfolgt die Einrichtung der E-Mail-Verschlüsselung in folgenden Schritten:

Zunächst muss die E-Mail-Verschlüsselung über die grafische Benutzeroberfläche (WebAdmin) aktiviert werden.

Anschließend sind die E-Mail-Adressen der internen Benutzer, deren E-Mails automatisch verschlüsselt bzw. signiert werden sollen, einzugeben. Statt einzelner E-Mail-Adressen können auch komplette Domains angegeben werden. Schlüssel und Zertifikate für alle Benutzer werden daraufhin automatisch generiert und an vordefinierte Key-Server verteilt.

Als letztes sind die E-Mail-Adressen der Empfänger, für die E-Mails immer verschlüsselt werden sollen, einzutragen. Hier kann für jeden Empfänger zusätzlich bestimmt werden, ob E-Mails mit S/MIME oder PGP verschlüsselt oder signiert werden sollen.

Nach diesem Setup erfolgt die Ver-/Entschlüsselung und Signatur von E-Mails automatisch für alle konfigurierten Benutzer. Um auch den Austausch öffentlicher Schlüssel mit anderen Benutzern bzw. Servern zu vereinfachen und die Integration in bestehende PKI-Infrastrukturen zu erleichtern, stehen zusätzliche Mechanismen zur Verfügung, die diese Vorgänge automatisieren.

11. Fazit

Secure E-Mail Gateways sind vor allem für mittlere und größere Unternehmen die bessere Alternative zu herkömmlichen End-to-End-Verschlüsselungslösungen und diesen bezüglich Kosten und Leistungsfähigkeit weit überlegen. Die zentrale Installation im Unternehmen erlaubt die Umsetzung der unternehmensweiten Sicherheitspolitik was die Verteilung von E-Mails und die Anwendung von kryptografischen Verfahren betrifft.

Auf dem Markt sind eine ganze Reihe von Mail Gateways als Software- oder Hardware-Appliances verfügbar. Sie bieten vielfältige Funktionen wie die sichere Speicherung kryptografischer Schlüssel und die Festlegung von Regeln, nach denen das Gateway ein- und ausgehende Mails für einzelne Empfänger oder Gruppen behandeln soll.

Wer mit Kommunikationspartnern ohne Schlüsselmaterial bzw. fehlende Verschlüsselungslösung kommuniziert, sollte unbedingt sicher stellen, dass das Gateway Alternativen wie Webmailer oder die PDF-Verschlüsselung anbietet. (ala)

Links im Artikel:

1 **http://www.ponemon.org/**
2 **http://www.seppmail.ch/**
3 **http://www.astaro.de**
4 **http://www.utimaco.de**
5 **http://www.zoe-one.com/**
6 **http://www.seppmail.ch/**
7 **http://www.iccSec.com**
8 **http://www.pgp.com**
9 **http://www.kbst.bund.de/Content/Egov/Initiativen/Bol/bol.html**
10 **http://www.astaro.de**
11 **http://www.iccSec.com**
12 **http://www.pgp.com**
13 **http://www.utimaco.de**
14 **http://www.zertificon.com**
15 **http://www.seppmail.ch**
