

Zentrale Lösungen zur e-Mail Security

Dr. Torsten Johr

Whitepaper

Juli 2010

Bei all seiner Attraktivität ist e-Mail ein ausgesprochen unsicheres Medium. Gerade im Unternehmenseinsatz ist eine Absicherung durch Verschlüsselung und Signatur zwingend notwendig. Dies war allerdings bisher in den meisten Unternehmen auf Grund der Komplexität des Themas und der unzureichenden Ausbildung der meisten Anwender auf diesem Gebiet nicht möglich. Abhilfe schaffen hier zentrale Verschlüsselungsgateways.

Gefahren

Mit der zunehmenden Nutzung des Internets ist eine entsprechende Verlagerung der Kommunikation auf elektronische Medien einhergegangen. In immer stärkerem Ausmaß wird e-Mail für Bestellungen, Werbung, Angebotsübermittlung, Auftragsbestätigungen, Rechnungen u.v.a.m. verwendet. Dies gilt sowohl für Geschäfte zwischen Unternehmen und Endkunden, als auch für die Kommunikation zwischen Unternehmen oder Unternehmensteilen. Allerdings ist SMTP, das Standardprotokoll für die e-Mail-Übermittlung über das Internet, niemals für den sicheren Transport vertraulicher Daten konzipiert worden. Vielmehr imitiert dieses Protokoll seit seiner ersten Definition im August 1982 den klassischen Versand mittels einer Postkarte. Kennzeichnend sind hier insbesondere die fehlende Authentisierung (und damit die leichte Fälschbarkeit) des Absenders, ein fehlender Schutz der Vertraulichkeit des Textes und der fehlende Schutz der Integrität des Textes. Hieran hat sich auch durch die zwischenzeitlich erfolgten Anpassungen an die technische Entwicklung nichts geändert. Dementsprechend hat die e-Mail-Kommunikation die gleichen prinzipiellen Sicherheitsprobleme wie eine Kommunikation per Postkarte:

- Sensible Informationen können in unbefugte Hände gelangen.
- Die übermittelten Informationen könnten gefälscht worden sein.
- Dritte könnten e-Mails mit gefälschtem Absender verschicken.

Im Unterschied zur klassischen „snail mail“ lassen sich Erzeugung, Manipulation und Mithören von e-Mails allerdings sehr einfach automatisieren. Außerdem entstehen in vielen Fällen selbst beim massenhaften Versand von e-Mails keine zusätzlichen Kosten für den Absender. All dies hat zur Folge, dass die eben genannten Probleme des elektronischen Versands um ein Vielfaches häufiger auftreten als im klassischen Postverkehr und sich somit auch die entstehenden Probleme vervielfachen.

Beispiele hierfür lassen leicht finden. Bspw. ist ein gängiges Hilfsmittel bei der Verbreitung von Würmern, das Adressbuch eines befallenen Rechners auszulesen und Kopien des Wurms an die dort aufgeführten Kontakte zu schicken. Als vorgeblicher Absender wird, um die e-Mail vertrauenswürdiger erscheinen zu lassen, oft der Eigner des befallenen Rechners verwendet. Ein anderes Beispiel für gefälschte Absender ist das bekannte Phishing. Hier wird versucht, die Empfänger durch gefälschte e-Mails zu gefährlichen Handlungen zu verleiten (z.B. zur Preisgabe von PINs, zum Besuch präparierter Webseiten usw.). Diese e-Mails erscheinen meist so täuschend echt, dass ein Erkennen der Fälschungen auch für Experten nicht immer leicht ist (Abbildung 1). Eine weitere Angriffsmöglichkeit ist, falsche Informationen unter fremdem Namen zu verschicken, dies ist neben Anderen auch diversen Bundesministerien widerfahren. Durch derartige Angriffe kann besonders für kommerzielle Nutzer von e-Mail ein nennenswerter Schaden entstehen – entweder direkt oder in Form eines Imageverlustes.

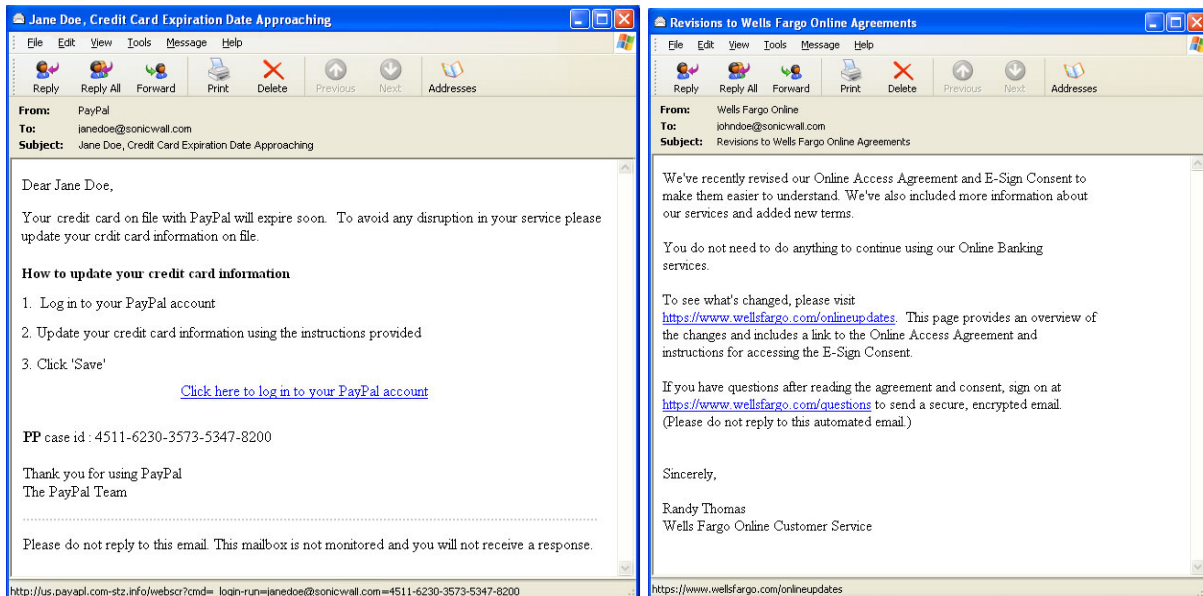


Abbildung 1: Beispiele für tatsächlich verschickte e-Mails. Inhalt, Qualität des Textes, Absenderdomänen geben keinen eindeutigen Hinweis, welche der beiden e-Mails gefälscht (links) und welche echt ist (rechts). Quelle: www.sonicwall.com/phishing

Gegenmaßnahmen

Die möglichen Gegenmaßnahmen sind seit Langem bekannt: Natürlich sind alle vertraulichen Informationen zu verschlüsseln. Hierdurch wird ein effizienter Schutz gegen das Abhören von Übertragungen erreicht. Als Schutz gegen das Verfälschen von e-Mails sollten generell elektronische Signaturen eingesetzt werden. Dabei müssen diese nicht unbedingt im juristisch strengen Sinn einer qualifizierten oder fortgeschrittenen Signatur eingesetzt werden. In vielen Fällen reicht es vollkommen aus, die e-Mails mit einem zuverlässigen Herkunftsnachweis zu versehen, quasi einer Art elektronischem Briefpapier (wobei der Herkunftsnachweise durch eine elektronische Unterschrift meist sehr viel zuverlässiger sein dürfte als ein Stück bedruckten Papiers). Soll dieser Herkunftsnachweis aber tatsächlich einen Schutz gegen den Versand gefälschter e-Mails durch Dritte (z.B. Phishing-Angriffe auf Kunden) bieten, so muss sicher gestellt sein, dass die Kommunikationspartner auch wissen, wie eine korrekte e-Mail auszusehen hat. Das bedeutet, dass das Layout einschließlich der Signatur immer gleich zu sein hat. Eine nur gelegentliche Signierung von e-Mails funktioniert nicht – die Kommunikationspartner werden nur dann bei einer nicht signierten, sonst aber sehr echt aussehenden e-Mail misstrauisch werden, wenn e-Mails aus dieser Quelle immer signiert sind.

(Nicht-) Einsatz kryptografischer Techniken

Die notwendigen Techniken zur Implementierung dieser Sicherheitsmaßnahmen stehen mit S/MIME und PGP seit etlichen Jahren zur Verfügung. Beide Verfahren verwenden Methoden der asymmetrischen Verschlüsselung, d.h. es existieren unterschiedliche Schlüssel zum Ver- und Entschlüsseln. Anders als bei symmetrischen Verschlüsselungsverfahren liegt hierdurch das primäre Problem nicht im sicheren (d.h. nicht mitgehörten) Austausch des Schlüssels, sondern in der Beurteilung der Vertrauenswürdigkeit der übermittelten Schlüssel. PGP und S/MIME unterscheiden sich im Wesentlichen in den Verfahren, die genutzt werden, um die Vertrauenswürdigkeit der verwendeten Schlüssel zu garantieren. Während S/MIME hier ein strikt hierarchisches Modell benutzt (es gibt zentrale Verifikationsstellen, die diese Aufgaben auch nach unten delegieren können), verwendet PGP ein Verfahren auf Peer-Basis (möglichst viele Bekannte bestätigen, dass dies mein Schlüssel ist). Beide Verfahren sind weit verbreitet und in den gängigen e-Mail-Browsern entweder nativ (S/MIME) oder durch Plugins (PGP) verfügbar. Einer allgemeinen Nutzung von Signatur und Verschlüsselung steht also nichts entgegen – sollte man meinen. Leider sieht die Realität anders aus. Obwohl zahlrei-

che Unternehmen ihre Arbeitsplätze mit entsprechenden Programmen ausgerüstet haben, ist die tatsächliche Nutzung von Verschlüsselung beim e-Mail-Versand kaum verbreitet. Von einer flächendeckenden Nutzung von kryptografischen Signaturen kann schon gar keine Rede sein, sie werden so gut wie nie genutzt. Hieran haben auch Pflichten zur Übertragungsverschlüsselung, die in den letzten Jahren in verschiedenen Bereichen eingeführt wurden, nichts ändern können. Die Anwender verfügen hierdurch zwar über die Möglichkeiten zur Verschlüsselung und Signatur, verwenden diese aber nur, wenn sie es müssen.

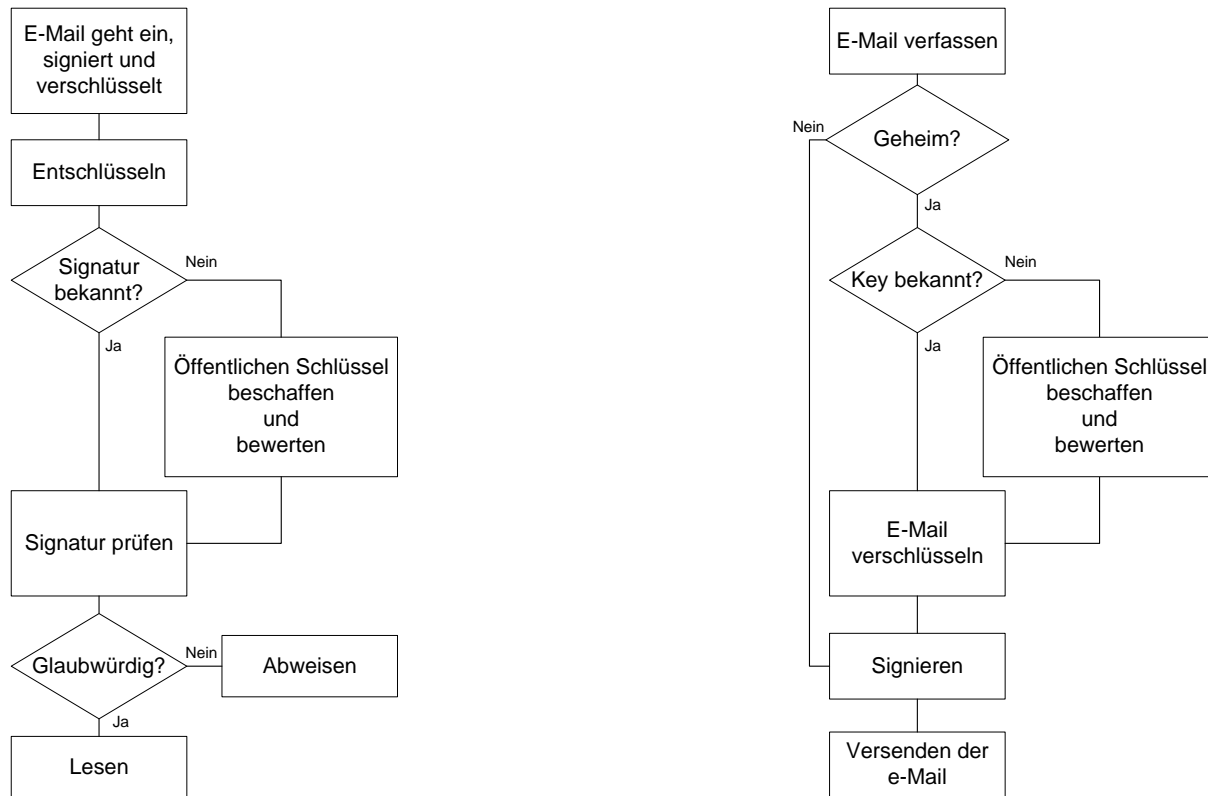


Abbildung 2: Entscheidungen bei Empfang / Versand verschlüsselter / signierter e-Mails

Die wesentliche Schwierigkeit bei der Nutzung kryptografischer Techniken ist, dass der eigentliche Aufwand in der Verwaltung und Bewertung der Schlüssel sowie der Definition und Pflege einer durchgängigen Nutzungsstrategie liegt (s. Abbildung 2). Trifft eine verschlüsselte e-Mail bei einem Empfänger ein, so ist der Umgang damit noch relativ einfach. Der Umgang mit einer signierten e-Mail ist jedoch bedeutend schwieriger: Der Anwender muss sich ggf. den öffentlichen Schlüssel seines Kommunikationspartners besorgen, die Echtheit dieses Schlüssels mit Hilfe vertrauenswürdiger Unterschriften oder einer Prüfung des Fingerabdruckes verifizieren und dann die Unterschrift prüfen. Ähnlich komplex sind die notwendigen Schritte beim Versand einer e-Mail. Zunächst muss der Anwender entscheiden, ob die Informationen verschlüsselt werden müssen oder offen über das Internet versendet werden dürfen, anschließend sind die notwendigen Schlüssel zu besorgen. Diese Entscheidung ist dann besonders schwierig, wenn nur für einige der Empfänger keine Schlüssel verfügbar sind. In diesem Fall müsste sich der Versender zunächst die öffentlichen Schlüssel dieser Personen beschaffen oder, falls dies nicht möglich ist, auf den Versand an diese Personen verzichten.

Die Erfahrung zeigt jedoch, dass in solchen Fällen häufig aus Bequemlichkeit auf die Verschlüsselung verzichtet wird. Ein derartiges Verhalten ist in einem Unternehmen natürlich nicht tolerierbar. Aus diesem Grunde existieren üblicherweise Richtlinien zum korrekten Umgang mit kryptografisch behandelten e-Mails. Diese in einem nur mittelgroßen Unternehmen bei allen Anwendern und Arbeitsplatzrechnern anzuwenden und durchzusetzen ist aber ein

gigantisches Problem, dessen Lösung ohne intensive Schulung aller Nutzer von e-Mail nicht möglich ist. Derartige Schulungen dürften in den allermeisten Umgebungen zu aufwändig sein. Ein unqualifizierter Einsatz solcher Techniken führt aber, da die Nutzer sich in falscher Sicherheit wiegen, meist zu einer Verringerung der Sicherheit. Faktisch ist ein sicherer e-Mail-Verkehr (hinsichtlich Vertraulichkeit und Integrität) in den meisten Unternehmen derzeit nicht gewährleistet.

Die Lösung: Zentrale Verschlüsselung

Da die Schulung aller in Frage kommenden Anwender zumeist keine Option ist, verbleibt als mögliche Lösung des Problems nur eine, die zentral administrierbar und für die Anwender weitestgehend transparent ist (s. Abbildung 3). In diesem Fall würden sowohl die generelle Politik im Umgang mit e-Mails (z.B.: An wen wird verschlüsselt? Werden unverschlüsselte e-Mails akzeptiert? Müssen e-Mails signiert werden?) als auch die Bewertung der verwendeten Schlüssel den Anwendern ab- und zentral von einigen wenigen speziell ausgebildeten Administratoren vorgenommen. Dieses Vorgehen spart einerseits Ausbildungskosten und erhöht andererseits auf Grund der so durchgesetzten einheitlichen Policy die Sicherheit im e-Mail-Verkehr stärker, als es bei individuellen Bewertungen / Entscheidungen durch (auch entsprechend geschulte) Endanwender der Fall wäre.

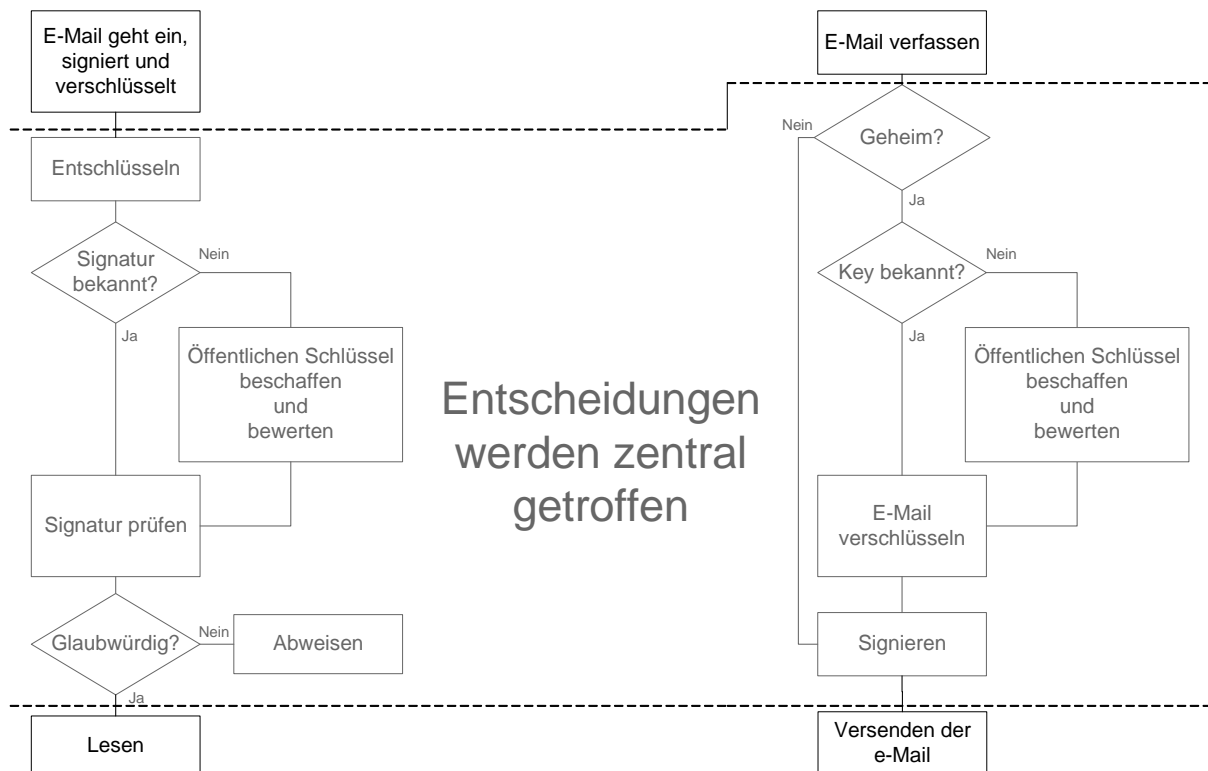


Abbildung 3: Zentrale Verschlüsselung / Signatur: Alle ausgegrauten Schritte werden den Anwendern ab- und vom zentralen Gateway übernommen.

Basisanforderungen an zentrale Lösungen

Zahlreiche Anbieter bieten entsprechende zentralisierte Lösungen zur Absicherung des e-Mail-Verkehrs an. Tabelle 1 zeigt einen Überblick über eine Auswahl solcher Produkte (erhebt aber keinen Anspruch auf Vollständigkeit).

Name	Hersteller	Betriebssystem	Technik	Protokolle	PKI
<i>Axway Secure Messenger</i>	Axway www.axway.com	Windows	Gateway	S/MIME, PGP, Webmail, aktiver Inhalt im Anhang	Extern
BCC <i>MailProtect</i>	BCC Unternehmensberatung GmbH www.bcc.biz	Notes Plugin	Gateway	S/MIME, PGP, AES verschl. ZIP	Intern
<i>Ironport Encryption Appliance</i>	Cisco Systems Inc. www.ironport.com	Appliance	Gateway	S/MIME, PGP, aktiver Inhalt im Anhang	Extern
<i>Julia MailOffice</i>	ICC Solutions GmbH www.ICCSec.com	Software Appliance	Gateway	S/MIME, PGP, Webmail, PDF	Intern
<i>PGP Universal Gateway EMail</i>	PGP Corporation www.pgp.com	Software-Appliance	Gateway	S/MIME, PGP, Webmail, PDF	Intern
SeppMail	SEPPmail AG www.SEPPmail.com	Appliance	Gateway	S/MIME, PGP, aktiver Inhalt im Anhang	Intern
<i>Z1 Secure Mail Gateway</i>	Zertificon GmbH www.zertificon.com	Appliance	Gateway	S/MIME, PGP, Webmail, PDF	Intern

Tabelle 1: Überblick zu Secure e-Mail Lösungen (Stand: 7/2010)

Allerdings ist nicht jede Lösung in jeder Umgebung gleich sinnvoll. Zentrale Lösungen für Unternehmen sollten gewisse Voraussetzungen erfüllen, um praktikabel zu sein: Zunächst muss der administrative Aufwand an beiden Enden des Kommunikationsweges minimal gehalten werden. Diese Forderung schließt in den meisten Fällen Lösungen am Endgerät, bspw. zentral administrierbare Browserplugins, aus, da Betrieb und Wartung von Software auf den Endgeräten in mittleren und größeren Umgebungen einen nicht unerheblichen Aufwand mit sich bringen. Dieser lässt sich durch den Einsatz eines Gateways, auf dem die gesamte kryptografische Behandlung der e-Mail vorgenommen wird, minimieren. Als willkommenen Nebeneffekt schafft ein solches Gateway die Möglichkeit, auch verschlüsselt übertragene Nachrichten vor der Übertragung an das Endgerät auf Viren und aktive Inhalte zu untersuchen. Außerdem können bei der Nutzung eines zentralen Gateways auch Smartphones (bspw. Blackberry-Geräte in Verbindung mit einem unternehmenseigenen Blackberry Enterprise Server) ohne jede Anpassung von dieser Lösung profitieren¹. Weiterhin muss gewährleistet sein, dass die Kommunikationspartner nicht zwingend über dasselbe Produkt zur Verschlüsselung verfügen müssen. Es muss im Gegenteil möglich sein, an der sicheren Kommunikation auch mit anderen Secure Mail Programmen sowie mit den gängigen Standardmailprogrammen teilnehmen zu können. Dies bedeutet, dass eine gute Lösung sowohl PGP als auch S/MIME standardkonform unterstützen muss.

Eine Beschränkung auf einen der beiden genannten Standards ist zumindest in Europa derzeit noch nicht möglich. Zwar hat im Unternehmensbereich die Nutzung von PGP stark abgenommen, doch kann bei der Kommunikation mit Privatanwendern und kleineren Unternehmen nicht auf PGP verzichtet werden. E-Mail-Software, die für Verschlüsselung und Signatur proprietäre Schlüsselformate verwendet, ist in Umgebungen mit einem geschlossenen Benutzerkreis zumeist gut geeignet, da diese Tools über sehr elegante Lösungen zur

¹ Hierbei wird vorausgesetzt, dass die Kommunikation zwischen Smartphone und Unternehmensnetz bereits verschlüsselt erfolgt.

Schlüsselverteilung verfügen. In den sehr viel häufigeren Umgebungen aber, in denen die Gruppe der potentiellen Kommunikationspartner nicht geschlossen ist, sondern ständigen Wechseln unterliegt und auch keine Einflussmöglichkeit auf die von den Kommunikationspartner verwendeten Werkzeuge besteht, ist nach unserer Erfahrung eine Lösung auf der Grundlage offener und verbreiteter Standards die praktikablere Lösung.

Meist das Optimum: Gateway mit S/MIME und PGP

Nach unseren Erfahrungen ist also ein dediziertes Secure Mail Gateway mit S/MIME- und PGP-Unterstützung in den meisten Unternehmens-Umgebungen die optimale Lösung zur Absicherung des e-Mail-Verkehrs. Ein derartiges, in Abbildung 4 skizziertes, System bietet, für die Anwender weitestgehend transparent, die Möglichkeit, die e-Mail-Kommunikation zu verschlüsseln und zu signieren. Über eine zentrale Administrationsschnittstelle ist bei allen gängigen Lösungen eine sehr fein granulare Justierung der e-Mail-Behandlung möglich, bspw. kann zu bestimmten Zielen bevorzugt verschlüsselt, optional aber auch im Klartext übertragen werden, zu anderen Zielen wird grundsätzlich verschlüsselt oder, falls dies fehlschlägt, der Verkehr blockiert und in der Kommunikation mit einem dritten Empfänger werden nicht nur ausgehende Nachrichten zwangsweise verschlüsselt, sondern es wird auch eingehender Verkehr nur akzeptiert, wenn dieser signiert und/oder verschlüsselt war. Hier bleiben bei der Absicherung der Kommunikation kaum Wünsche offen. Durch die Verwendung der standardisierten Protokolle PGP und S/MIME ist dabei der Aufbau gesicherter Kommunikation mit praktisch jedem Gesprächspartner möglich, egal, ob die Gegenseite ebenfalls über ein Gateway verfügt oder nicht. Auf Grund der standardmäßigen Implementierung von S/MIME in den gängigsten e-Mail-Programmen Outlook, Windows Live Mail, Windows Live Mail und Mozilla Thunderbird ist sogar eine gesicherte Verbindung mit Endanwendern, die einen Standard-Home-PC, verwenden möglich.

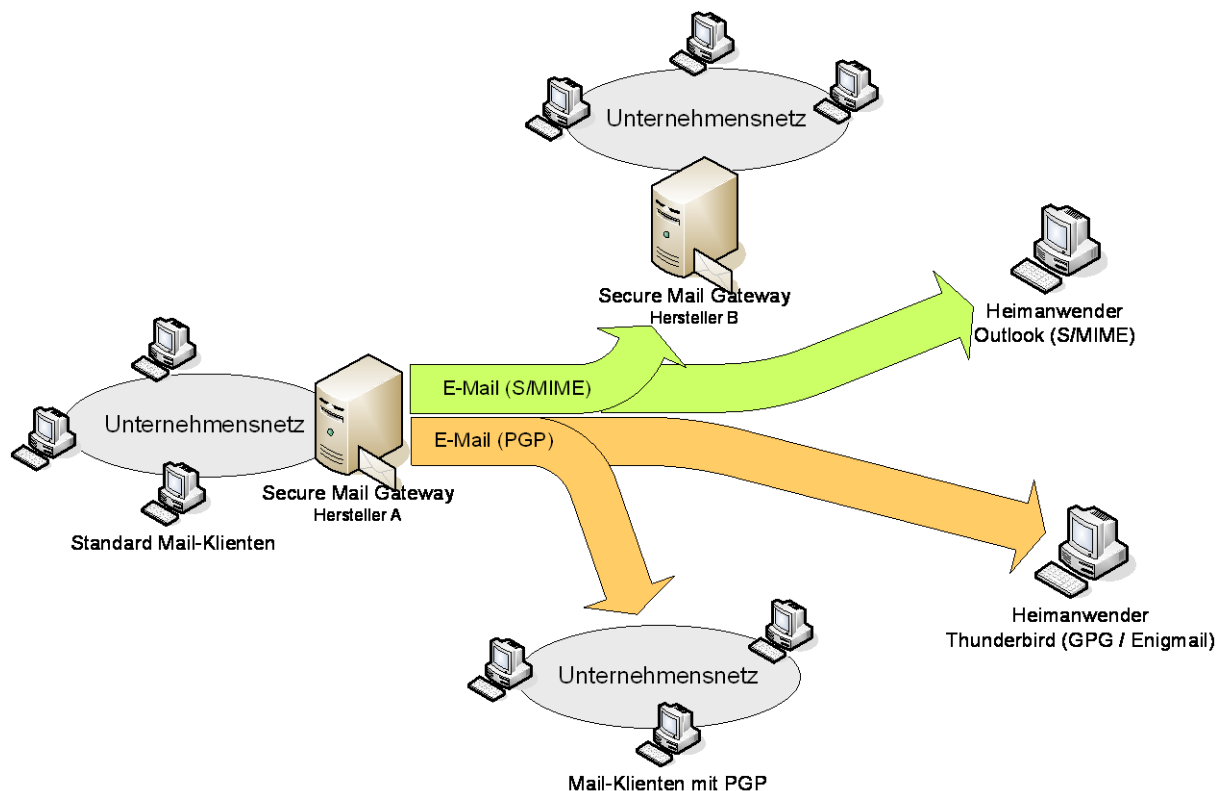


Abbildung 4: Einsatz von Secure Mail Gateways in einer Standardumgebung

Schlüsselbeschaffung

Gateways mit Unterstützung für S/MIME und PGP übernehmen i.A. sämtliche für Verschlüsselung und Signatur notwendige Arbeiten (Abbildung 5). Dies beginnt mit der Suche nach passenden Schlüsseln. Durch Zugriff auf öffentliche Schlüsselserver (sowohl PGP als auch S/MIME) sind die Gateways in der Lage, sich benötigte öffentliche Schlüssel, die lokal noch nicht verfügbar sind, selbsttätig zu beschaffen. Nach dem Download erfolgt eine Gültigkeitsprüfung der Schlüssel, bevor sie schließlich verwendet werden. Die Schlüssel werden als gültig eingestuft, wenn sie mit einem als vertrauenswürdig eingestuftem Schlüssel unterschrieben wurden und diese Unterschrift nicht abgelaufen ist. Je nach gefundenem Schlüssel wird dann das geeignete Kryptofieverfahren ausgewählt. So kann es auch passieren, dass bei Versand einer zu verschlüsselnden e-Mail ein Teil der Empfänger die Nachricht PGP-verschlüsselt, ein anderer Teil diese aber im S/MIME-Format erhält. Der Absender bekommt hiervon i.A. nichts mit.

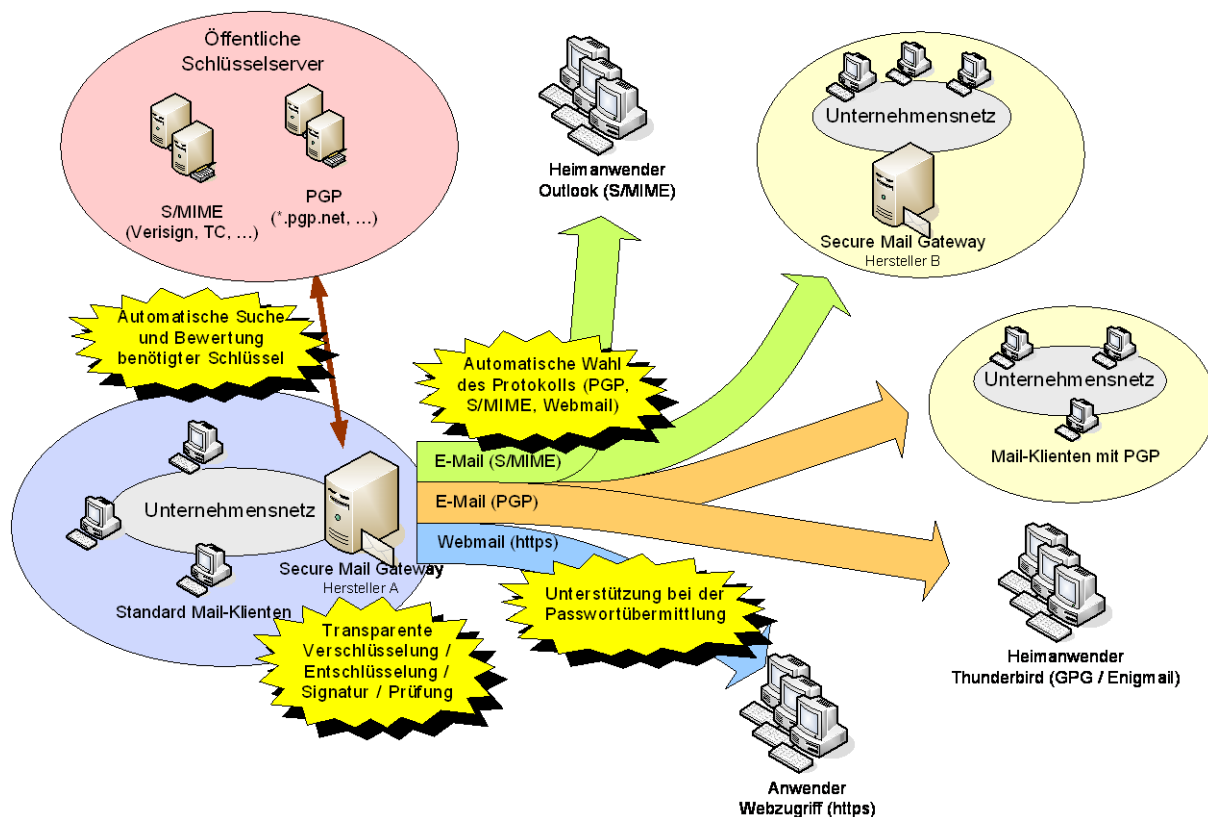


Abbildung 5: Einsatz eines Secure Mail Gateways mit Modulen zur automatische Schlüsselbeschaffung und Webmailzugang („pull-Modul“)

Etwas komplexer verläuft die Auswahl der privaten Schlüssel. Die auf dem Markt befindlichen Produkte gehen hier zwei verschiedene Wege: Einerseits können sie extern erzeugte Schlüsselpaare und Zertifikate verwenden, die in das Gateway geladen und bestimmten Nutzern oder Nutzergruppen zugewiesen werden. Andererseits verfügen die meisten der gängigen Gateways (s. Tabelle 1) über eine eigene interne PKI (*public key infrastructure*) und erzeugen so bei Bedarf selbsttätig Schlüsselpaare und Zertifikate nach dem X.509v3-Standard für die Anwender.

Beide Ansätze haben Vor- und Nachteile. Die Verwendung externer Schlüssel und Zertifikate ist wesentlich einfacher zu handhaben, aber auch sehr viel unflexibler. Diese Lösung ist nur dann nutzbar, wenn lediglich wenige verschiedene Schlüssel verwendet werden. Dies bedeutet aber nicht, dass nur wenige verschiedene Anwender das Gateway verwenden können. Vielmehr ist die Nutzung von Gruppenschlüsseln möglich, d.h. die e-Mails aller Support-Mitarbeiter werden mit dem Schlüssel *support@example.com* signiert. Dagegen ist die Be-

nutzung einer in das Gateway integrierten PKI zwar flexibler und in Umgebungen, in denen viele individuelle Schlüssel benötigt werden, sehr viel leichter einsetzbar, doch darf nicht vergessen werden, dass eine PKI auch zahlreiche administrative Aufgaben, wie bspw. die Pflege von Rückruflisten (*certificate revocation lists*, CRLs), mit sich bringt, die einen erheblichen Mehraufwand bedeuten. Die Unterstützung, die die PKIs der Gateways hier bieten ist meist nicht so umfangreich, wie man sie sich wünschen würde. Es muss jeweils im Einzelfall entschieden werden, welche Lösung für eine bestimmte Umgebung geeigneter ist. Grundsätzlich gilt aber, dass ein Gateway seine Stärken immer dann ausspielen kann, wenn Ent- / Verschlüsselung und Signierung vollkommen automatisch ablaufen. Dies ist aber mit individualisierten Schlüsseln nur unter massiven Aufwänden und bei Einschränkungen der Vertraulichkeit möglich. Das liegt schlicht daran, dass in solchen Fällen entweder Schlüssel und Passwort auf dem Gateway abgelegt werden müssen oder alternativ das Gateway bei Bedarf eine Nachricht an den Schlüsselbesitzer schickt und um Eingabe des Passwortes (bspw. per https-Schnittstelle) bittet. Beides ist, da entweder aus Sicherheitsgründen nicht akzeptabel oder schlicht unkomfortabel, nicht zu empfehlen.

Allerdings besteht ein Bedarf für individualisierte Schlüssel in der Mehrzahl der Umgebungen nur für sehr wenige Anwender, z.B. die Mitglieder der Geschäftsführung. Meist ist es nur wichtig, dass die Nachrichten verschlüsselt übertragen werden und die Empfänger sicher sein können, dass die e-Mails tatsächlich aus diesem Unternehmen oder dieser Abteilung stammen. In solchen Fällen reichen Gruppenschlüssel also völlig aus. Für die Mitarbeiter, für die die Notwendigkeit besteht, persönliche Schlüssel zu benutzen, sollte auf die klassischen Mailprogramme wie Outlook, Mozilla Thunderbird usw. zurückgegriffen werden, die dies meist gut unterstützen. Diese Mischung aus persönlicher Verschlüsselung am Endgerät für einige Anwender und Gatewayverschlüsselung für die große Masse der Anwender ist problemlos möglich.

Verschlüsselung ohne Schlüssel

Bei den bisher beschriebenen Lösungen wird vorausgesetzt, dass alle Teilnehmer an der Kommunikation über kryptografische Schlüssel verfügen. Dies ist aber (nicht nur) in Unternehmensumgebungen nicht immer der Fall. Ist der Empfänger mit eigenen Mitteln nicht in der Lage, die Nachricht zu entschlüsseln, so muss auf andere Lösungen zurückgegriffen werden. Der traditionelle Weg war hier häufig die Erzeugung eines (ggf. selbst entpackenden) verschlüsselten Archivs. Da aber ausführbare Dateien und Archive von e-Mail-Filtern völlig zu Recht als potentiell gefährlich herausgefiltert werden, werden meist kleinere oder größere Tricks eingesetzt, um solche Daten an den Prüfinstanzen vorbei zu mogeln. Es ist klar, dass dies keine wünschenswerte Lösung ist. Besteht häufiger die Notwendigkeit verschlüsselte Daten an Personen ohne Entschlüsselungsmöglichkeiten zu versenden, sollte deshalb das Gateway um eine entsprechende Lösung ergänzt werden. Hierfür existieren zwei Ansätze:

Hersteller wie bspw. die Totemo AG oder die Zertificon GmbH setzen auf die Nutzung der in Quasi-Standard-Werkzeugen (https-fähige Webbrowser, PDF-Reader) vorhandenen Verschlüsselungsmöglichkeiten. Sie bieten als Alternativen zur Benutzung von PGP oder S/MIME einen https-Webmailer oder die Möglichkeit des Mailversands in Form eines verschlüsselten PDF-Dokumentes an. Emails können so für mögliche Angreifer unlesbar an die Empfänger übertragen werden, ohne dass diese hierzu zusätzliche Infrastruktur beschaffen müssen. Als sicherer Antwortkanal stellen diese Anbieter i.A. ihren https-Webmailer zur Verfügung.

Ein Nachteil dieser Verfahren ist, dass die Vertraulichkeit der Nachrichten nur bei einer fehlerfreien Nutzung der Leseprogramme durch den Empfänger gewährleistet ist. Prüft ein Empfänger nicht sorgfältig das korrekte Zustandekommen der https-Verbindung zum Webmailer, so sind Man-in-the-Middle-Angriffe möglich, bei denen das Kennwort für den Webmailer abgehört werden kann. Genauso sind auch Angriffe auf die PDF-Lesesoftware denkbar (bspw., durch Ausnutzung von Fehlern in der JavaScript-Verarbeitung).

Insgesamt ist das Risiko eines Vertrauensbruchs beim Einsatz dieser Methoden sicherlich etwas höher als bei ausschließlicher Verwendung von PGP oder S/MIME, es ist aber in der überwiegenden Mehrzahl der Fälle sicherlich tragbar und kann durch geeignete Informationen in den Emails zur Anmeldung eines neuen Benutzers weiter reduziert werden.

Einen deutlich anderen Weg beschreiten Hersteller wie die SeppMail AG oder Cisco/IronPort, die zur Ver-/Entschlüsselung aktive Inhalte in die Benachrichtigungsmail einfügen. Hier wird zur Verschlüsselung proprietäre Software (geschrieben in JavaScript oder Java) eingesetzt. Das Entschlüsselungsprogramm wird dem Empfänger verschlüsselt zugestellt, zur Entschlüsselung dient sein Kennwort. Dieses Kennwort verlässt somit, anders als bei den Webmail-Lösungen niemals den Rechner des externen Nutzers. Diesem Vorteil steht allerdings ein gravierender Nachteil entgegen: Der Nutzer muss Fremdsoftware auf seinem Rechner ausführen. Ein Angreifer könnte somit eine Phishing-Mail erzeugen, die ein von ihm erzeugtes Schadskript (bspw. einen Trojaner oder ein Skript, das das eingegebene Passwort per Email versendet) enthält. Klassische Schutzmechanismen wie das Sperren von JavaScript an der Firewall sind hier wirkungslos, da dieser Schutz ja zur Nutzung dieser Verschlüsselungstechnik abgeschaltet werden muss. Da Emails bekanntermaßen sehr einfach gefälscht werden können und dies häufig für den unbedarften Nutzer auch nicht erkennbar ist, birgt diese Verschlüsselungsmethode u.E. ein recht hohes Risiko für Angriffe durch Schadsoftware.

In jedem Fall muss die Nutzung dieser nicht PGP oder S/MIME nutzenden Verfahren vom Versender nicht explizit angefordert werden. Das Gateway entscheidet autonom auf Grund einer bestehenden Policy („Diese e-Mails müssen verschlüsselt werden“) und der verfügbaren Schlüssel, welche Verschlüsselungsmethode (S/MIME, PGP oder Ersatzverfahren) verwendet wird (siehe auch Abbildung 5). Lediglich beim ersten e-Mail-Versand an einen Empfänger ohne kryptografische Schlüssel ist zur Übermittlung der Authentisierungsinformationen ein zusätzlicher (telefonischer, brieflicher) Kontakt notwendig. Dieses Verfahren ist für den Absender vollkommen transparent, hat aber für den einige Nachteile:

- Es existiert keine Signatur des empfangenen Dokumentes, nachträgliche Änderungen des ausgelieferten Textes durch den Absender sind möglich.
- Es können bestehende Standardabläufe durch diese „untypische“ Art der Auslieferung unterbrochen werden. Antworten sind auf diese Art ohnehin kaum möglich.
- Die Archivierung der empfangenen verschlüsselten PDF-Dateien ist schwierig.

Diese Verfahren können eine sehr sinnvolle Ergänzung zum Secure Mail Gateway sein, wobei allerdings zusätzliche Maßnahmen zum Schutz der externen Anwender (wie bspw. eine gute Information zum korrekten Verhalten) getroffen werden müssen. Als eigenständige Lösung machen sie nur Sinn, wenn ein Absender regelmäßig sehr viele E-Mails an sehr viele Empfänger verschickt (z.B. periodischer Massenversand von Rechnungen).

Fazit

Mit den inzwischen recht zahlreich verfügbaren Gateway-Lösungen zur kryptografischen Behandlung von e-Mails ist die Chance gestiegen, dass in Unternehmensumgebungen sichere e-Mail-Kommunikation endlich den Stellenwert erhält, den sie verdient. Durch die Verlagerung sämtlicher Schlüsselverwaltungs- und -bewertungsaufgaben auf ein zentrales Gateway, das von einigen entsprechend ausgebildeten Administratoren verwaltet wird, ist eine für die Standardanwender völlig transparente und zentral gesteuerte Einhaltung von Unternehmenspolicies zur Verschlüsselung und Signatur realisierbar.

Der dafür zu zahlende Preis, der entweder im Betrieb einer kleinen, weitgehend automatisierten PKI oder in der Verwendung von Gruppenschlüsseln besteht, ist im Vergleich mit den gewonnenen Vorteilen in den allermeisten Umgebungen ausgesprochen gering. Es bleibt zu hoffen, dass sich angesichts solcher sehr einfachen Lösungen zunehmend Unternehmen

ihrer Verantwortung gerecht werden und die e-Mail-Kommunikation durch standardmäßigen Einsatz von Signatur und Verschlüsselung sicherer machen.

Dr. Torsten Johr ist als IT-Security Consultant bei der GAI NetConsult GmbH tätig.

*Die **GAI NetConsult GmbH** ist ein bundesweit tätiges unabhängiges Software- und Consulting-Unternehmen mit besonderer Expertise in den Bereichen IT-Sicherheit, Software-Entwicklung und Integration. Das Angebot umfasst dabei die qualifizierte Beratung, sowie die Konzeption und Realisierung individueller Aufgabenstellungen bis zur Einführung und Betreuung im laufenden Betrieb. Zum Kundenstamm der GAI NetConsult gehören vorwiegend Unternehmen aus den Branchen Energieversorgung, Finanzdienstleistung, Chemie/Pharma sowie Öffentliche Verwaltungen und Bundesinstitute. Nachgewiesenes fachliches Know-how, weithin beachtete Publikationen sowie eine Vielzahl von Beiträgen auf exponierten Fachkongressen und nicht zuletzt exzellente Kundenreferenzen unterstreichen die Positionierung des Unternehmens als einen der führenden Dienstleister für „Sichere eBusiness-Lösungen“.*