Die virtuelle Poststelle

Prof. Dr. Norbert Pohlmann

Fachhochschule Gelsenkirchen

Fachbereich Informatik

Neidenburger Straße 43

45877 Gelsenkirchen

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Trotz vielfältiger Möglichkeiten den Mailverkehr im Internet mitzulesen, sind heutzutage immer noch weniger als 5% aller E-Mails verschlüsselt. Doch kaum eine andere Internetanwendung erfreut sich einer vergleichbaren Akzeptanz und Verbreitung, ungeachtet der mangelhaften Sicherheit. Nicht ohne Grund steht das Thema E-Mail-Sicherheit deshalb ganz oben auf der To-do-Liste vieler Unternehmen.

E-Mails haben in vielen Bereichen die traditionelle Kommunikation per Telefon, Brief oder Fax abgelöst. Bis auf wenige isolierte PGP- und S/MIME-Inseln, gibt es in der Praxis kaum fundierte Konzepte für unternehmensweite und -übergreifende E-Mail Sicherheitslösungen. Die Ursache für die zögerliche Umsetzung sind die hohen Kosten für die Infrastruktur durch Clientsoftware, Token, Lesegeräte, Rollout, Helpdesk, Migration und Zertifikatsmanagement.

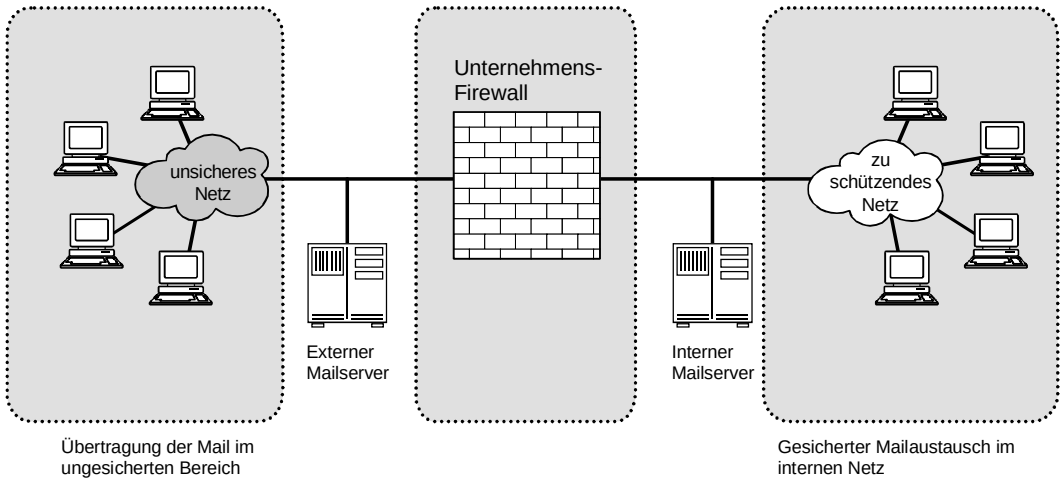
Das im Folgenden beschriebene Umsetzungskonzept des Secure-E-Mail-Gateway stellt eine neuartige, pragmatische Lösung zur Sicherung des kompletten E-Mail-Verkehrs bereit. Aufgrund des zentralen Ansatzes ist diese den herkömmlichen End-to-End-Lösungen hinsichtlich Kosten und Leistungsfähigkeit weit überlegen. Als Erweiterung der bereits genutzten E-Mail-Server übernimmt das Secure-E-Mail-Gateway die Aufgabe einer "virtuellen Poststelle“, die für die Vertraulichkeit (Verschlüsselung), Integrität und Verbindlichkeit (Signatur) des gesamten E-Mail-Verkehrs sorgt.

Secure-E-Mail-Gateway

Clientbasierte End-to-End Lösungen für E-Mail Sicherheit haben sich – obwohl seit langem verfügbar - in der Praxis kaum durchgesetzt. Neben hohen Kosten und aufwendiger Administration kranken diese Konzepte an vier charakteristischen Problemfeldern, für die es innerhalb dieser Konzepte bis heute keine überzeugenden Lösungen

gibt. Neben der immer noch mangelhaften Interoperabilität der Lösungen, die sich immer dann als besonderes Handicap erweist, wenn der eigentlich sensible externe E-Mail-Verkehr geschützt werden soll, sind dies die Message-Recovery-Problematik, die Schwierigkeit der Abbildung interner Vertreter-Policies und die Viren-Problematik.

Clientbasierte Konzepte sind individuelle Konzepte, d.h. sie benötigen so viele Schlüssel wie Mitarbeiter im Unternehmen sind. Scheidet ein Mitarbeiter aus dem Unternehmen aus, muss gewährleistet sein, dass berechtigte Personen, die an diesen Mitarbeiter gerichteten oder von ihm bereits erhaltenen E-Mails, lesen und beantworten können. Die Schlüssel der Mitarbeiter müssen bei diesen Konzepten entweder an zentraler Stelle hinterlegt werden, oder jede E-Mail muss zusätzlich mit einem Hauptschlüssel - also doppelt - verschlüsselt werden. Die gleiche Problematik gilt für die Vertretung bei Abwesenheit des Mitarbeiters. Bei der Prüfung verschlüsselter Mails auf Virenbefall sind aufwendige Umverschlüsselungen erforderlich, da Anti-Viren-Programme nur Klartext analysieren können.



Übersicht: Standard Mail Server System

An dieser Stelle setzt das Konzept des Secure-E-Mail-Gateways an. Die Aufstellung an zentraler Stelle im E-Mail-Verkehr erlaubt die Anwendung einer zentralen Unternehmens-Policy hinsichtlich der Verteilung von E-Mails sowie der Anwendung von kryptographischen Operationen. Dies wird unterstützt durch die Möglichkeit, kryptographische Schlüssel innerhalb des Secure-E-Mail-Gateways gesichert speichern zu können. Hierzu kann zusätzlich ein Hardware-Sicherheitsmodul integriert werden, welches ein Höchstmaß an Sicherheit für die (kryptographischen) Schlüssel garantiert.

I. Systemübersicht

Dem Gateway-Ansatz folgend, befindet sich das Secure-E-Mail-Gateway immer an zentraler Stelle im Netzwerk, dem “Common Point of Trust“. Die Secure-E-Mail-Gateway Lösung entschlüsselt und verifiziert eingehende E-Mails und ist in der Lage, hinausgehenden E-Mail-Verkehr zu verschlüsseln und zu signieren. Das Secure-E-Mail-Gateway muss auf einem sicheren Betriebssystem laufen und die Sicherheitsfunktionen müssen sicher eingebunden werden, damit keine Angriffe über das Netz oder das Betriebssystem stattfinden können [1].

Durch seine Funktion als “virtuelle Poststelle“ bietet das Secure-E-Mail-Gateway Vertraulichkeit (Verschlüsselung), Integrität und Verbindlichkeit (Signatur) für den gesamten E-Mail-Verkehr. Auf der Gegenseite kann ebenfalls ein Secure-E-Mail-Gateway stehen oder eine entsprechende Client-Software, um die Sicherheitsfunktionen zu realisieren. Steht keine dieser Komponenten auf der Gegenseite zur Verfügung, kann das Secure-E-Mail-Gateway verschlüsselte, selbstextrahierende Dateien zuschikken, die mittels Passphrase wieder entschlüsselt werden können. Sicherer E-Mail-Verkehr zwischen allen Kommunikationspartnern ist die Anforderung, die auf diese Weise realisiert wird [2].

II. Funktionsweise

Das Secure-E-Mail-Gateway stellt eine Erweiterung der genutzten E-Mail-Server dar. Definierte Benutzergruppen aber auch Einzelanwender können damit ihre E-Mail automatisch vor dem Versand signieren und/oder verschlüsseln lassen.

Über Regeln wird der virtuellen Poststelle mitgeteilt, wann eine E-Mail signiert und/oder verschlüsselt werden soll. Entweder sind diese Regeln als Sicherheitsrichtlinien fest in der virtuellen Poststelle definiert, dann hat der Mitarbeiter keinen zusätzlichen Aufwand, oder der Mitarbeiter kann über die Betreffzeile die Aktionen in der virtuellen Poststelle steuern. Das Ergebnis bekommt der Empfänger dann angezeigt.

Mögliche Aktionen können sein:

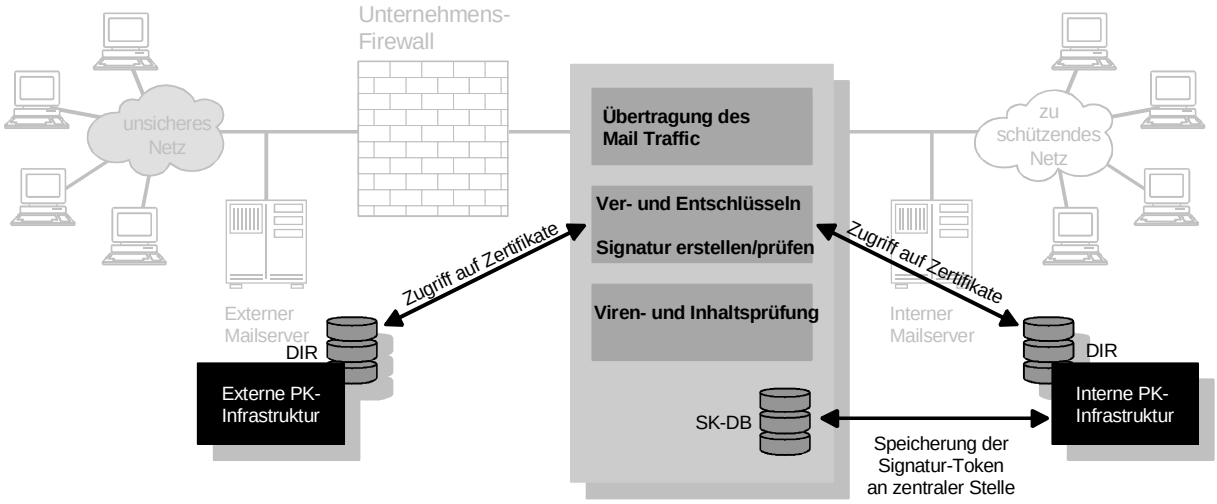
{sign} Die Mail wird signiert.

{crypt} Die Mail wird verschlüsselt.

{trust} Die Mail wird signiert und verschlüsselt.

Der Empfänger erkennt dann die Aktionen in der Betreffzeile: {signed}, {encrypted}, {trusted}.

Die Mitarbeiter brauchen keine zusätzliche Software, um die Dienste der virtuellen Poststelle nutzen zu können, denn das Secure-E-Mail-Gateway ist in den E-Mail-Versand integriert.



Allgemeine Funktionsweise der virtuellen Poststelle

Durch die Speicherung der Übermittlungsbestätigung ist der Nachweis der Kommunikation gegeben. Ein Mitarbeiter des Unternehmens, der verschlüsselte E-Mails erhält, sieht diese aufgrund der automatisch ablaufenden Entschlüsselung immer im Klartext, er selbst muss diesen Vorgang nicht aktiv einleiten, für ihn sind diese Vorgänge transparent.

Es gibt keine zusätzlichen Anforderungen an den Client und damit auch keine Kosten, die typischerweise hier entstehen (Ausstattung, Schulung, Wartung, Updates, etc.). Liegt das Zertifikat eines bestimmten Empfängers bereits dem Unternehmen vor, so kann beim Versand der E-Mail diese automatisch verschlüsselt und verschickt werden. Falls das Zertifikat nicht vorliegt, kann das Secure-E-Mail-Gateway die notwendigen Zertifikate auch über externe und interne Directory Server abrufen. Die Speicherung der empfangenen Zertifikate erfolgt sinnvoller Weise an zentraler Stelle, denn dann kann die Verschlüsselung auch erfolgen, wenn der Versender von E-Mails persönlich bis zu diesem Zeitpunkt noch keine direkte Kommunikation mit dem Empfänger aufgenommen hat, sondern nur ein Kollege oder eine andere Abteilung im Unternehmen. Die Verifikation der Zertifikate erfolgt ebenfalls an zentraler Stelle im Unternehmen. Damit ist ein Common Point of Trust, eine gemeinsame Vertrauensbasis, gegeben.

An eben dieser zentralen Stelle, erfolgt auch die Festlegung der Regeln, nach denen das Secure-E-Mail-Gateway die ein- bzw. ausgehenden Mails für einzelne Empfänger oder ganze Gruppen behandelt. Neben den Standards wie S/MIME, ISIS-MTT oder PGP, ist das Secure-E-Mail-Gateway auch in der Lage die E-Mail mit einem symmetrischen Verschlüsselungsverfahren zu verschlüsseln. Ein kleines Programm, welches eine selbstextrahierende, verschlüsselte Datei produziert, kommt hier zum Einsatz. Auf der Empfängerseite kann dann z.B. eine einfache Software zur Verfügung gestellt werden, die in der Lage ist, den Inhalt und die Anhänge der E-Mail wieder zu entschlüsseln. Organisationen sind durch diese verschiedenen Alternativen in der Lage, sowohl mit großen Partnerunternehmen (die ebenfalls Gateways einsetzen), Außendienstlern, kleineren Unternehmen und Dienstleistern, kurz: mit der ganzen Welt sicher zu kommunizieren. Der pragmatische Ansatz ist hier, eine einfache Verschlüsselung von E-Mails bereit zu stellen, die auch dann funktioniert, wenn auf der Empfängerseite keine Standards wie S/MIME, ISIS-MTT oder PGP zur Verfügung stehen (z.B. bei AOL).

Zentrale Sicherheitsfunktionen

Verschlüsselung	Digitale Signatur
Die E-Mails können während der Übertragung im Internet nicht im Klartext gelesen werden, gezielte Manipulationen sind nicht möglich.	Bietet eine Gewährleistung der Datenunversehrtheit und der Verbindlichkeit.

Zeitstempeldienste

Signaturen sind durch die Einbindung so genannter Zeitstempeldienste erweiterbar. Die Zeitstempelfunktionalität bedeutet jedoch mehr als nur ein elektronischer „Post-Eingangsstempel“. Ein Zeitstempel ist der eindeutige Beleg darüber, wann ein Dokument in einer bestimmten Form vorgelegen hat. Sobald an dem digital „zeitgestempelten“ Dokument Veränderungen vorgenommen werden, sind diese nachprüfbar. Workflow-Systeme, E-Mail-Korrespondenz und Archivierungssysteme profitieren durch Zeitstempelfunktionaliäten.

Zeitstempeldienste erlauben den Nachweis der Authentizität und Integrität von Daten zu einem bestimmten Zeitpunkt. Ereignisse wie zum Beispiel der Eingang von Bestellungen, Online-Auktionsgeboten oder Online-Brokerage-Aktivitäten werden mittels des Time-Stamping-Systems mit einer offiziellen Zeitangabe versehen.

III. Vorteile der „virtuellen Poststelle“

Ein wesentliches Argument für den Einsatz von Secure-E-Mail-Gateways ist der geringe Aufwand hinsichtlich der erforderlichen PKI-Infrastrukturen. Organisationen steht nun ein pragmatischer und ausbaufähiger Weg offen, um das Thema PKI und E-Mail-Sicherheit bedarfsgerecht umzusetzen. Durch den zentralen Ansatz beim Secure-E-Mail-Gateway sind PKI-Funktionalitäten schnell und einfach zu implementieren und einzusetzen [3].

Eingangsstempel

Die Sicherstellung der Unveränderbarkeit von Daten erfolgt bisher nur über sehr aufwändige Archivierungsverfahren (WORM, Bandlösungen, etc.), die zudem keine hundertprozentige Sicherheit bieten. Bei dem Secure-E-Mail-Gateway läuft die Sicherung der Daten im Hintergrund mit Hilfe von Zeitsignaturen automatisch ab.

Vertretungsregelung

Da die Entschlüsselung beim Secure-E-Mail-Gateway zentral durchgeführt wird, kann nach der Entschlüsselung die E-Mail automatisch und im Klartext an den Vertreter umgeleitet werden, bzw. der Vertreter kann auch im Auftrag verschlüsseln/signieren, ohne dass Token und PIN der zu Vertretenden genutzt werden müssen.

Zentrale Viren- und Inhaltsprüfung

Mit der Hilfe eines Secure-E-Mail-Gateway ist es weiterhin möglich an zentraler Stelle Viren- und Inhaltsüberprüfung, gemäß der Unternehmenspolicy, durchzuführen. Die eingehende E-Mail wird zunächst zentral entschlüsselt und danach überprüft.

Unterstützung mehrerer Standards und Methoden

Im Secure-E-Mail-Gateway können an zentraler Stelle sehr einfach mehrere Standards (z.B. S/MIME, ISIS-MTT oder PGP) und Methoden (symmetrische Verschlüsselungsverfahren und PKI-orientierte) unterstützt werden.

Anwenderfreundlich

Entscheidende Vorteile sind die deutlich reduzierte Komplexität durch die Realisierung an zentraler Stelle und die hohe Benutzerfreundlichkeit, da keine zusätzliche Software auf der Anwenderseite bedient und geschult werden muss. Umständliche dezentrale Rollout-Planungen und hoher Wartungsaufwand (keine Wartung von Software auf Anwenderseite z.B. Updates, Patches, ..) entfallen ebenso. Gleichzeitig ist die „Message-Recovery“-Problematik gelöst. Weiterhin besteht die Möglichkeit die E-

Mail-Sicherheit Remote zu administrieren und diese Dienstleistung kostengünstig outzusourcen.

Maximale Sicherheit bei reduzierten Kosten

Im Unternehmen wird die Anzahl der benötigten Zertifikate deutlich reduziert und die Abbildung und Einhaltung der Security Policy konsequent umgesetzt. Sicherheit ist nicht länger Entscheidung des Anwenders. Die erhöhte Interoperabilität mit externen Systemen bringt dem Unternehmen entscheidende Impulse, eine wichtige Hemmschwelle entfällt.

In der folgenden Tabelle sind die Vor- und Nachteile von einer Client- und Gateway-Lösung dargestellt:

Anwendung	**Zentral/Gateway**	**Client**
Bedienkomfort	+	-
Sign./Verschl. von großen Mailvolumina	+	-
Elektronische Signatur	+	+
Qualifizierte Signatur	-	+
Umsetzung der Unternehmenspolicy	+	**o (Vertrauen auf Anwender)**
Vertreterregelung	+	-
Recovery	+	**o (nur wenn Anwender mit Unternehmens-Schlüssel mitverschlüsselt)**
Mails mit hoher interner Vertraulichkeit	-	+
Virenscanning, Inhaltsprüfung	+	-

Hinweis:

Bei der Notwendigkeit qualifizierte Signaturen durchzuführen und eine hohe End-to-End-Vertrauenswürdigkeit zu erzielen, kann auf eine Clientsoftware nicht verzichtet werden. Betrachtet man die in der Regel wenigen Arbeitsplätze (Geschäftsleitung,

Prokuristen, Einkäufer, ...), bei denen dies notwendig ist, stellt die Hybridlösung einen pragmatischen, kostengünstigen und anwenderorientierten Weg zur Erhöhung von Sicherheit und Vertrauenswürdigkeit im E-Mail-Verkehr dar. Ansonsten hat das Secure-E-Mail-Gateway enorme Vorteile.

IV. Fazit

Der pragmatische Ansatz des Secure-E-Mail-Gateway als Plattform zur Absicherung von Unternehmenswerten ist gerade deshalb sinnvoll, weil die Standards bei unterschiedlichen Herstellern nicht zustande kommen oder zu lange dauern, weil sie passgenau sind, zukunftssicher und ein sehr gutes Kosten-/Nutzenverhältnis haben. Hier liegt der Return on Investment von IT-Sicherheit in der Akzeptanz auf breiter Basis durch ihre Nutzer. Dieser einfache Grundschutz für die E-Mail-Sicherheit hat sich in der Praxis schnell bewährt. Organisationen werden in die Lage versetzt, schnell, flexibel und bedarfsgerechte Sicherheit zu erzielen, ohne ein hohes Investment in die benötigte Infrastruktur zu tätigen [4].

Literatur

[1] N. Pohlmann: "Firewall Systeme – Sicherheit für Internet und Intranet" 5. aktualisierte und erweiterte Auflage. Bonn: MITP-Verlag 2003.

[2] A. Philipp, N. Pohlmann, B. Weiss: „Security Gateway – Plattform zur Absicherung von Unternehmensnetzen", in "Enterprise Security", Hrsg.: Patrick Horster, IT Verlag, 2002

[3] N. Pohlmann: „Nutzen und Chancen von Public-Key-Infrastrukturen", in "Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung", Hrsg.: Patrick Horster, IT Verlag, 2002

[4] H. Blumberg, N. Pohlmann: "Der IT-Sicherheitsleitfaden“, ISBN 3-8266-0940-9, MITP-Verlag, Bonn 2004