

Secure Email

Vertrauliche und authentische Kommunikation, transparent für den User

Email ist wie Postkarte?

Da der Versand einer Email viel schneller und kostengünstiger vor sich geht als der einer Postkarte, zielt die Aussage "Email ist wie Postkarte" auf die mangelnde Vertraulichkeit beider Transportwege. Tatsächlich ist die normale Email aber noch schlechter dran: Sie ist nicht unterschrieben, und jemand könnte in ihr unterwegs "herumradieren". Eine Email-Übertragung im Klartext verbietet sich deshalb für sensible, z.B. personenbezogene Daten oder Know-how-Inhalte.

Die normale Email-Kommunikation kann also die üblichen Schutzziele der Informationssicherheit, nämlich

- Vertraulichkeit,
- Integrität und
- Authentizität

nicht erfüllen. Dabei sind asymmetrische Verschlüsselungsverfahren, die diesem Mangel abhelfen, seit langem bekannt. Mit S/MIME und OpenPGP haben sich dafür auch zwei Standards herausgebildet, die die notwendigen Schlüssel verwalten und von modernen Mailprogrammen automatisch unterstützt werden. Dennoch wird nach wie vor nur ein geringer Anteil des Email-Verkehrs verschlüsselt. Selbst Angebote und Bestellungen werden oft unsigniert und unverschlüsselt übertragen.

Transparente Email-Signierung und -Verschlüsselung

Der Grund für den geringen Gebrauch verschlüsselter Emails ist die Komplexität im Einsatz. Wenn man dies nämlich dem einzelnen Email-Nutzer überlässt, muss er sich um sämtliche Schlüssel seiner Kommunikationspartner kümmern. Das ist aber ein ineffizientes und teures Verfahren, das zudem die Erfüllung einer einheitlichen Firmenpolicy sehr erschwert und sicherheitstechnische Schwächen hat. Dazu gehört, dass wegen der Verschlüsselung kein Viren- und Spamschutz am Gateway greifen kann. Das Verfahren der Wahl für die vertrauliche und authentische Email-Kommunikation ist deshalb das Setzen von digitalen Signaturen sowie die optionale Verschlüsselung am Mailgateway. Das geht vollkommen transparent für den User, er arbeitet ohne Änderung und Beeinträchtigung wie zuvor, und es ist keinerlei Installation auf seinem Rechner erforderlich. Dennoch kann das Verfahren auf User-Zertifikaten aufsetzen, das Zertifikats- und Policy-Management erfolgt jedoch am Gateway bei Pallas. Domain-Zertifikate sind weniger zu empfehlen, da sie zu Kompatibilitätsproblemen führen können und die einzelnen User nicht unterscheiden. Ob eine Email verschlüsselt oder signiert war, erkennt der User an einem eingefügten Kennzeichen im Betreff. Beim Beantworten oder Weiterleiten dieser Email wird das Kennzeichen wieder entfernt.

Pallas setzt auf die Lösung von Zertificon Solutions

Pallas hat das SecureMail Gateway von Zertificon Solutions in seine Mailinfrastruktur integriert und bietet die Leistung, Emails zu signieren und zu verschlüsseln, als Managed Security Service an. Pallas berät und unterstützt auch bei der Integration von Lösungen beim Kunden vor Ort. Zertificon ist einer der führenden Anbieter für die Email-Signierung und -Verschlüsselung.

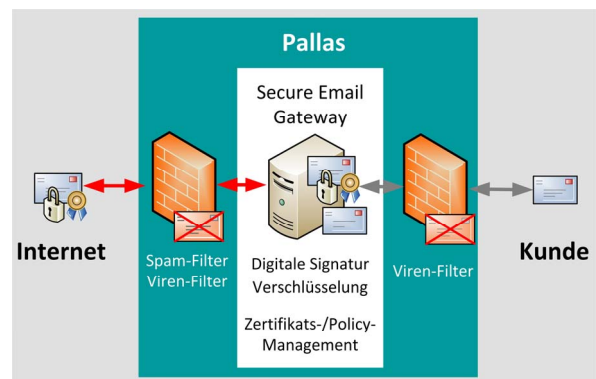
Eine Policy

Jede Policy wird am Gateway einheitlich umgesetzt, hier ein Beispiel:

- Ausgehende Email:
 - Immer signieren
 - Verschlüsseln, falls Empfänger-Zertifikat bzw. PGP-Key bekannt
 - Wenn nicht bekannt, bei voreingestellten Trustcentern und PGP Key-Servern nach Zertifikat/Schlüssel des Empfängers fragen
- Eingehende Email:
 - Signatur des Absenders auslesen und prüfen, falls vorhanden
 - Entschlüsseln, sofern verschlüsselt gesendet
 - Automatischer Import eines gültigen Sender-Zertifikats bzw. PGP-Keys, falls vorhanden

Die Vorteile der Secure Email von Pallas

- Schutz gegen Mitlesen und Manipulieren von Emails
- Einsatz von User-Zertifikaten
- Client-System und Kunden-Mailserver bleiben unverändert
- Investitions- und Betriebskosten entfallen
- Automatische Zertifikatserzeugung für neue Mitarbeiter
- Dito für funktionale Email-Adressen, z.B. für den Rechnungsversand
- Automatische, zentrale Zertifikatsverwaltung, S/MIME und OpenPGP
- Kompatibel zu anderen Produkten (Basis S/MIME oder OpenPGP)
- Transparente Nutzung von Mobile Devices
- Weitere Pallas-Bausteine am Gateway integrierbar (Virenschutz, Spamschutz, AutoFooter)



Hinzu kommt der hohe Standard des Pallas Managed Security Service

- TÜV-Geprüfte Managed Services
- Hochverfügbare, integrierte Betriebslösung
- 24x7-Systemüberwachung
- Incident Management
- Direkter technischer Helpdesk-Support
- Reporting