

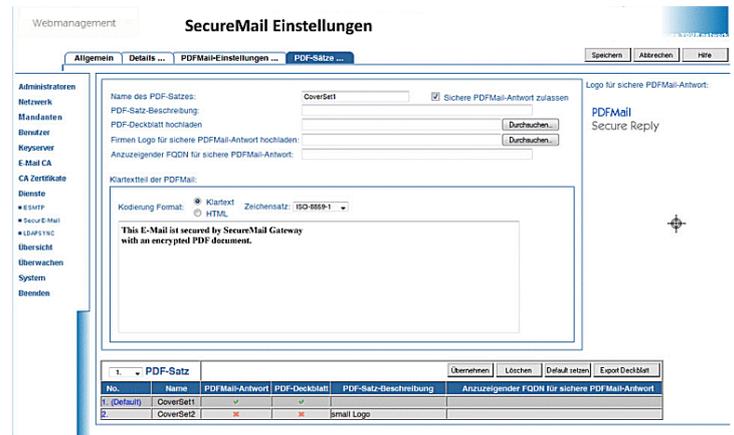
WARUM E-MAIL-KOMMUNIKATION EINEN BESONDEREN SCHUTZ BENÖTIGT

Die E-Mail ist die mit Abstand am häufigsten verwendete Anwendung im Internet und löst die herkömmliche Kommunikation per Briefpost und Telefon immer mehr ab. Nach Angaben des Statistischen Bundesamtes im Januar 2013 werden jeden Tag weltweit rund 89 Milliarden geschäftliche E-Mails verschickt. Der Nachteil bei der E-Mail-Kommunikation besteht jedoch primär darin, dass es kein Briefgeheimnis und somit auch keine Vertraulichkeit gibt. Während bei der Postkarte das geringe Risiko, dass die Mitarbeiter der Post die Urlaubsgrüße lesen könnten, den meisten bekannt ist, so sind die möglichen Risiken des Mitlesens durch unberechtigte Dritte bei E-Mails um ein Vielfaches höher - und oft unbekannt. Denn E-Mails passieren auf ihrem Weg durch das weltweite Internet viele Stationen, an denen sie abgefangen, von Unbefugten gelesen und auch verändert werden können. An diesen Stationen und auf Servern werden alle E-Mails, darunter auch geschäftsrelevante, vertrauliche und somit schützenswerte Informationen, verarbeitet. Sensible Informationen können dadurch rasch in die falschen Hände gelangen, wenn sie ungeschützt, d. h. ohne geeignete Mechanismen zur Absicherung, übermittelt werden. Wer eine E-Mail erhält, kann zudem nicht sicher sein, dass deren Inhalt so empfangen wird, wie er vom Sender ursprünglich abgeschickt wurde. Denn wer sich unbefugten Zugang zu fremden Servern verschaffen und E-Mails lesen kann, ist damit ebenso in der Lage auch deren Inhalte zu verändern oder zu verfälschen. Betroffen hiervon sind dabei nicht nur der Text oder Dateianhang einer E-Mail, sondern auch die Absenderangaben. Auf diese Weise können leicht falsche Identitäten vorgetäuscht werden, was zu verheerenden Folgen führen kann.

Daher stellt die Kommunikation mit E-Mail für jedes Unternehmen und für jede Organisation ein ernst zu nehmendes Sicherheitsrisiko dar. Und das nicht erst seit Bekanntwerden der NSA-Affäre.

SECUREMAIL GATEWAY BIETET OPTIMALEN SCHUTZ FÜR IHRE E-MAIL-KOMMUNIKATION

SecureMail Gateway ebnet auf einfachste Weise den Weg zur Implementierung einer organisationsweiten, einheitlichen E-Mail-Sicherheitsrichtlinie (Security Policy). Der Einsatz von Signatur und Verschlüsselung lässt sich dabei zuverlässig und konform zu der jeweiligen Unternehmens-



richtlinie integrieren und umsetzen. Das System unterstützt die Nutzung von Firmenverzeichnissen, wie beispielsweise von Active Directory (AD). Dabei kann pro Regel nicht nur eine einzelne Aktion, wie z. B. die Verschlüsselung einer ausgehenden E-Mail, definiert werden, sondern Regeln lassen sich auch verketteten. Dadurch kann eine E-Mail beispielsweise in einem ersten Verarbeitungsschritt an ein Archivsystem geleitet, um im Anschluss daran dann verschlüsselt, digital signiert und zugestellt zu werden. Durch den Einsatz von bewährten und anerkannten Standards sowohl bei den verwendeten Verschlüsselungs- als auch Signaturverfahren (S/MIME, OpenPGP und PDFMail) kann *SecureMail Gateway* die Interoperabilität einer geschützten E-Mail-Kommunikation mit Geschäftspartnern im höchsten Maße garantieren.

WIE FUNKTIONIERT SECUREMAIL GATEWAY?

SecureMail Gateway ist eine virtuelle Appliance und lässt sich ganz einfach an zentraler Stelle in die SMTP-Kette integrieren. Die serverbasierte E-Mail-Sicherheitslösung verwaltet und verarbeitet digitale Zertifikate sowie Rückruflisten (CRLs) völlig automatisch. Alle ein- und ausgehenden E-Mails werden transparent anhand von definierten Regeln durch sichere und anerkannte Verschlüsselungsverfahren ver- und entschlüsselt bzw. digital signiert, ohne dass ein Mitarbeiter in seinem Arbeitsprozess gestört oder behindert wird.

Über die Zusatzfunktion *PDFMail* können verschlüsselte E-Mails auch an Empfänger gesendet werden, die nicht über eine zertifikatsbasierte Infrastruktur (PKI) verfügen. Hierbei benötigt der Empfänger lediglich einen PDF-Reader.

TECHNISCHE DATEN

AUSFÜHRUNGEN

- Virtuelle Appliance; Betriebssystem: CentOS

UNTERSTÜTZTE MAILSERVER

- SMTP-basiertes Verschlüsselungs-Gateway; unterstützt alle bekannten Mailserverssysteme; (sowohl Senden als auch Empfangen von E-Mails erfolgen ausschließlich über SMTP).

INSTALLATION / INBETRIEBNAHME

- Einfache und schnelle Integration in die bestehende IT-Infrastruktur
- Unterstützt nahezu alle E-Mailsysteme.
- Erfordert keine Clientinstallationen.
- Beliebig skalierbar und nahezu unbegrenzt einsetzbar.
- Hochverfügbar einsetzbar (Clustering).

VERSCHLÜSSELUNGSSTANDARDS

- Asymmetrische Verschlüsselungsverfahren: RSA, DSA, El Gamal
- Symmetrische Verschlüsselungsverfahren: RC2, RC4, AES, AES192, AES256, DES, 3DES, Blowfish, Twofish, Cast5
- Hashverfahren: MD2, MD5, MDC2, SHA, SHA-1, RipeMD160

PROTOKOLLE & SICHERHEITSSTANDARDS

- SMTP(S), ESMTP, TLS, HTTP(S), SSH, SCP, FTP, MTA, NTP, SMNP, LDAP(S), AD, OCSP, HKP, S/MIME, OpenPGP, PDFMail, X.509, PEM, DER, PKCS #7, PKCS #12, CRL, OpenPGP keys, PGP/MIME, PGP/Inline

SPRACHEN

- deutsch, englisch, französisch, weitere auf Nachfrage

Sie haben noch weitere Fragen?
Zögern Sie nicht, uns zu kontaktieren!



FUNKTIONSUMFANG

- Effektiver Schutz vor Datenspionage
- Einfache Integration und Verwaltung
- Serverbasierte Absicherung der extern geführten E-Mail-Kommunikation
- Höchste Interoperabilität zu anderen Systemen
- Generiert automatisch digitale Zertifikate und Schlüssel für S/MIME und OpenPGP
- Ermöglicht die gesicherte Anbindung externer Kommunikationspartner auch ohne eigene Sicherheitsinfrastruktur durch PDFMail
- Transparenz für den Absender durch automatische Ver- und Entschlüsselung (S/MIME und Open-PGP) des ein- und ausgehenden E-Mail-Verkehrs
- Gewährleistet die Authentizität und Integrität von E-Mails durch digitale Signaturverfahren
- Enthält zentrale Public Key Infrastruktur (PKI)
- Zentrale Umsetzung interner Sicherheitsrichtlinien
- Einfache Anbindung an zentrale Verzeichnisdienste (z. B. LDAP, Active Directory)
- Zentrale und rollenbasierte Administration
- Granular einstellbare Sicherheitsfunktionen
- Unterstützt wirkungsvoll die Einhaltung von Compliance-Vorschriften
- Optimaler Schutz von personenbezogenen Daten bei der Kommunikation mit E-Mails
- Erfordert keine Mitarbeiterschulungen
- Erfordert keine Client-Installationen
- Sehr geringe Betriebs- und Wartungskosten (TCO)
- Kann auch hochverfügbar betrieben werden (Clustering)
- Ermöglicht eine einfache Anbindung an Data Leakage Prevention Systeme (DLP / ILP)
- Einfache Integration von externen Virenscannern
- Smartphone-kompatibel
- Auch als multimandantenfähige Version für Managed Service Provider (MSP) verfügbar

COMPLIANCE

- SecureMail Gateway unterstützt Sie aktiv dabei, dass Ihr E-Mail-System die Bedingungen des Datenschutzes erfüllt und konform zu aktuellen Complianceanforderungen ist.
- **Deutschland:** konform zu BDSG und weitere
- **International:** Basel II, PCI, HIPPA, EuroSOX, Sarbanes Oxley Act und weitere