SEPPMAIL

Sichere **E-Mail-** und **Datenkommunikation** für Unternehmen und Behörden

E-Mail ist das Kommunikationsmedium Nr. 1. Gesetzliche Vorgaben sowie zunehmende kriminelle Versuche, über E-Mails Zahlungsströme zu manipulieren, stellen Unternehmen vor eine große Aufgabe: den geeigneten Schutz der zu übertragenden E-Mails, personenbezogenen Daten und sensiblen Informationen.

KUNDENHERAUSFORDERUNGEN

1. COMPLIANCE

- Einhaltung gesetzlicher Regelungen (z.B. SOX, HIPPA, PCI, EU-DSGVO etc.), regulatorischer Standards und freiwilliger Kodizes

2. KOSTEN / ZEIT

- Modernisierung bestehender Technologien wie z.B. Ersatz von physikalischer Post oder Fax
- Digitalisierung von Geschäftsprozessen

3. UMFELD / IMAGE

- Verschlüsselte Kommunikation ist oftmals Voraussetzung der Kunden, Geschäftspartner etc.
- E-Mail-Signatur steht für Qualität und Authentizität

EINE Appliance – EIN Management – VIER Lösungen

- Patentierte GINA-Technologie für die spontane, verschlüsselte Übertragung von vertraulichen E-Mails auf jedes Endgerät
- Automatische und einfache Verwaltung der Zertifikate von Certificate Authorities (CAs) über Konnektoren in der Basislizenz
- Ressourcenschonende Firmware, schnelle Installation, einfache Versionspflege
- Vier Lösungen in einer Appliance – unabhängig von der jeweiligen Nutzerzahl

E-MAIL VER- UND ENTSCHLÜSSELUNG

Verschlüsseln verhindert das Mitlesen durch unbefugte Dritte und gewährleistet Vertraulichkeit.

- Verschlüsseln aller als vertraulich gekennzeichneten E-Mails
- Automatische Auswahl der geeigneten Verschlüsselungstechnologie (S/MIME –> openPGP –> Domainverschlüsselung –> GINA-Technologie)

USPs

- Patentierte GINA-Technologie für die Spontankommunikation
- Bewährt benutzerfreundliche Bedienung
- Einfache Administration und Integration

E-MAIL-SIGNATUREN UND AUTOMATISCHE ZERTIFIKATSVERWALTUNG

E-Mail-Signaturen verifizieren die Quelle und schließen Manipulationen aus.

- Automatische Prüfung eingehender E-Mails mit Signaturen
- Einsammeln der öffentlichen Schlüssel und sofortige Verschlüsselung bei ausgehenden E-Mails
- Transparente Verwaltung, Erneuerung und Revozierung der Zertifikate

USPs

- Vollautomatische Nutzung und einfache Verwaltung der Zertifikate

LARGE FILE TRANSFER (LFT)

Oft ist die Größe einer E-Mail beschränkt und der Aufwand bei Übertragung per FTP hoch.

- Große Dateien einfach mit LFT ohne zusätzliche Systeme und Accounts übertragen
- Optionaler Passwortschutz

USPs

- Gewohnte Umgebung
- Geringer Aufwand für den Anwender
- Speicherzeit ist einstellbar – keine „Altdaten“ auf der Appliance

ZENTRALES E-MAIL-SIGNATUREN- UND DISCLAIMER MANAGEMENT

In Unternehmen existiert eine Vielzahl an E-Mail-Footern, und der Disclaimer der E-Mail muss rechtskonform sein.

- Professionelle, einheitliche und CI-konforme E-Mail-Signaturen
- Einheitlicher Unternehmens-Disclaimer
- Verknüpfung von statischen mit dynamischen Inhalten

USPs

- Informationen nur an der richtigen Stelle verwenden
- Automatisches Ausfüllen dynamischer Inhalte

SEPPMAIL

Features der **SEPPmail Appliances**

SIGNATUR

- Lernfunktion der Zertifikate aus eingehenden, signierten E-Mails
- Prüffunktion für signierte E-Mails mit entsprechendem Betreff-Tagging
- Optional: Entfernen von Signaturen nach Prüfung
- Automatische Signatur aller ausgehender E-Mails mit hinterlegten Nutzerzertifikaten

ZERTIFIKATS- UND SCHLÜSSELVERWALTUNG

- Integrierte CA für das Erstellen von Schlüsselmaterial
- Anbinden von akkreditierten CAs via Konnektoren
- Automatische Verwaltung der konnektorbezogenen Zertifikate
- Import von vorhandenem Schlüsselmaterial
- Erstellen von OpenPGP-Schlüsselpaaren

VERSCHLÜSSELUNG

- Ver- und Entschlüsseln via S/MIME oder OpenPGP
- Frei anpassbares Regelwerk
- Domain-Verschlüsselung mit S/MIME oder OpenPGP, SEPPmail Managed Domainservice für automatisches Verschlüsseln zwischen SEPPmail Appliances
- Verschlüsselte Spontankommunikation via TLS GINA
  - Flexibel anpassbar an Corporate Identity
  - SMS-Versand von Passwörtern
  - Self Service Password Management
- Interne E-Mail-Verschlüsselung über Outlook-Add-In

LARGE FILE TRANSFER

- Einfaches Versenden großer Datenmengen
- Trennen von E-Mail und Anhang per Outlook-Add-In
- Verschlüsselter oder unverschlüsselter Empfang über GINA-Technologie – ohne Größenbeschränkung, Passworteingabe oder zusätzlichen Empfängeraccount
- Einstellbare Verweildauer
- Einstellbare Schwellwerte für einen automatischen LFT-Versand
- API für den automatisierten Datenimport

ZENTRALES E-MAIL-SIGNATUREN- UND DISCLAIMER MANAGEMENT

- Erstellen von Templates für mehrere parallele Disclaimer (pro E-Mail-Domain)
- Signaturdaten für Grußformel aus LDAP/AD
- Zentrales Management der E-Mail-Signaturen und Disclaimer
- Korrektes Positionieren innerhalb der E-Mail

BASISSYSTEM

- Appliance als Hardware oder virtuelle Instanz für VMware/ESX, Hyper Visor, KVM, Hyper-V, Azure
- Unabhängig vom Mailserver und -client
- Ressourcenschonend
- Firmware auf OpenBSD basierend
- Multidomain- und mandantenfähig
- Mehrsprachig: Deutsch, Englisch u.v.m.

ADMINISTRATION

- Intuitive Weboberfläche und zentrale Benutzerverwaltung
- Keine Installation auf dem Mailclient notwendig
- Optional: Outlook-Add-In für noch einfachere Bedienung per MSI
- Anbindung an Drittsysteme möglich (z.B. LDAP/Active Directory (AD), SNMP/Nagios, SOAP/REST, HSM)

BACKUP UND HIGH AVAILABILITY

- Keine E-Mail-Daten auf der Appliance -> minimale Backupgröße
- Wiederherstellung der Appliance aus Backup
- Optional: Queueless-Betrieb
- Clusterfähig (Multimaster, Geocluster)
- Integrierte Loadbalancer-Funktion

ANTIVIRUS / ANTISPAM

- SpamAssassin
- ClamAV
- Diverse Filter
- Anbinden von Scan-Instanzen via ICAP

SEPPmail GINA Technologie vs. WebServer und pdf-Verschlüsselung	pdf-Verschl.	Normales „secure Webmail“	Selbsextrahierendes Archiv	Spezieller Client	GINA
Empfänger kommt mit Standardkomponenten aus (Mail-Client / Browser / Internet)	Nur bedingt (Mobile Endgeräte!)	Ja	-	-	
Passwortwechsel möglich	-	Ja	-	-	
Sichere Antwort möglich	-	Ja	-	Ja	
Mail wird sofort und vollständig ausgeliefert	Ja	-	Ja	Ja	
Corporate Identity individuell anpassbar	Ja	Ja	-		
Empfänger kann seinen öffentlichen Schlüssel hinterlegen	-	Ja	-		
Empfänger kann vorgängig sein Wunschpasswort hinterlegen	-	Ja	-		**Ja**
Appliance hält keine Nutzerdaten	Ja	-	-		
Phishing Resistent	Ja	-	Ja	Ja	
Resistent gegen Brute Force Attacken	-	Ja	-	Ja	
„E-Mail als Einwurf-Einschreiben“; Lesebestätigung möglich	-	Ja	-	-	
Passwort Selfservice	-	Ja	-		
Two-Factor Authentication	-	-	-	Ja	
Queless Betrieb (kein Datenverlust bei Ausfall)	-	-	-	-	