CLEARSWIFT
MIMEsweeper™
Simplifying content security

FACTSHEET

Email-Verschlüsselung

Komfortable Verschlüsselung für Clearswift MIMEsweeper for SMTP

Sicherer Email-Verkehr mit CompanyCRYPT Encryption

Die Herausforderung

Bei ungeschütztem Email-Verkehr besteht die Gefahr, dass Nachrichten auf ihrem Weg zum Empfänger von Dritten gelesen, abgefangen, manipuliert und weitergeleitet werden. Mangelndes Gefahrenbewusstsein führt immer wieder dazu, dass Firmengeheimnisse per Email verbreitet werden oder vertrauliche Daten verloren gehen. Unternehmen werden deshalb zunehmend durch Gesetze und Richtlinien verpflichtet, den Schutz ihres Email-Verkehrs sicher zu stellen.

COMPANYCRYPT®
The encryption module for MIMEsweeper

Gefahr durch Inhalte verschlüsselter Emails

Die Verschlüsselung von Emails und die Nutzung von digitalen Signaturen sind hilfreich, wenn es um den Schutz vertraulicher Daten geht, doch diese Technologien verursachen auch neue Sicherheitsprobleme.

Wenn eine verschlüsselte Email empfangen oder versendet wird, muss gewährleistet sein, dass sie keinerlei Gefahren wie bösartigen Code, Viren oder unautorisierte Übertragungen vertraulicher Informationen enthält (auch die Keys für die Verschlüsselung selbst zählen dazu).

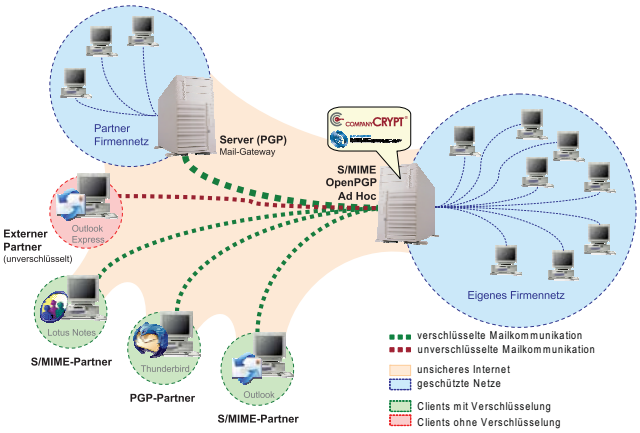
MIMEsweeper ist so konzipiert, dass es führende Verschlüsselungstechnologien zur Bereitstellung von Gateway-Signierung, Ver- und Entschlüsselung sowie Richtlinien-basierter Verwaltung von Gefahren, die mit verschlüsselten Emails einhergehen, unterstützt.

Bei verschlüsselten Emails kann der Inhalt nicht auf Gefahren untersucht werden. Daher müssen eingehende geschützte Emails zuerst entschlüsselt werden, ehe MIMEsweeper eine Content Analyse durchführen kann. Beim Versenden prüft MIMEsweeper vertrauliche Emails auf Sicherheitsrisiken, bervor diese zur Verschlüsselung weitergeleitet werden. Übertragungen, die nach den Richtlinien als vertraulich eingestuft sind, werden automatisch verschlüsselt, nachdem sie von der Content Analyse frei gegeben wurden.

Die Lösung

Durch CompanyCRYPT werden vertrauliche Emails der Mitarbeiter zentral und ohne ihr Zutun verschlüsselt und gesetzeskonform versendet. Neben einer personalisierten Email-Signierung und -Verschlüsselung ist auch die Signierung per Firmenschlüssel im Sinne einer hausinternen Poststelle möglich.

Durch die nahtlose Integration von CompanyCRYPT in den MIMEsweeper wird die Überprüfung verschlüsselter Inhalte durch Virenscanner, Anti-Spamfilter und Content-Scan Engine möglich. Nur so können Sicherheitsrichtlinien auch auf verschlüsselte Emails angewendet werden.



Ihre Checkliste für die Wahl Ihrer Verschlüsselung

1. **Wählen Sie eine Lösung, die transparent und ohne Anwenderinteraktion arbeitet**, weil die Aktivierung gern vergessen wird und Sie Ihre User so nicht zusätzlich schulen müssen

2. **Entschlüsseln Sie bereits am Gateway**, weil nur so Content-Analyse, Virenschutz und Unternehmensrichtlinien auch auf verschlüsselte Inhalte und unternehmensweit angewendet werden können.

3. **Setzen Sie auf mehrere, internationale Standards**, weil Sie so flexibel und offen für die von Ihrem Kommunikationspartner angewendete Methode sind und Sie beide Standards (OpenPGP und S/MIME) nutzen können.

4. **Wählen sie zusätzlich zu den Standardverfahren eine weitere Technik zur Ad Hoc-Verschlüsselung**, falls der externe Partner kein PGP oder S/MIME nutzt oder bei spontanem Verschlüsselungsbedarf vereinbarte Sicherheitsniveaus eingehalten werden müssen.

5. **Wählen Sie eine Lösung mit komfortabler Anwendersteuerung zur Durchsetzung richtliniengesteuerte Verschlüsselung**, weil nur so Anforderungen nach Revisionssicherheit und flexibler Aktivierung von Vertraulichkeit erreichbar sind.

6. **Für eine einfache Administration muss sich Encryption optimal in das Content Security System integrieren,** a) damit durch eine Verschlüsselungslösung Ihre Mailinfrastruktur nicht komplexer wird oder Single-Points-of-Failure entstehen, b) damit Richtlinienmanagement und Verschlüsselung sich von einem Punkt aus administrieren lassen und c) damit keine weitere Hardware für Encryption benötigt wird.

7. **Setzen Sie granulare Verschlüsselungsrichtlinen für unterschiedliche Usergruppen ein** z.B. policy-basierte Methoden bei Anwendern oder Systemen mit offensichtlicher Verschlüsselungspflicht oder Site2Site Verschlüsselung um mit ganzen Mail-Domains zu verschlüsseln und nutzen Sie die Möglichkeit, die Gateway-Verschlüsselung bei sensiblen Dokumenten als Sender selber zu aktivieren.

CLEARSWIFT
MIMEsweeper™
Simplifying content security

FACTSHEET

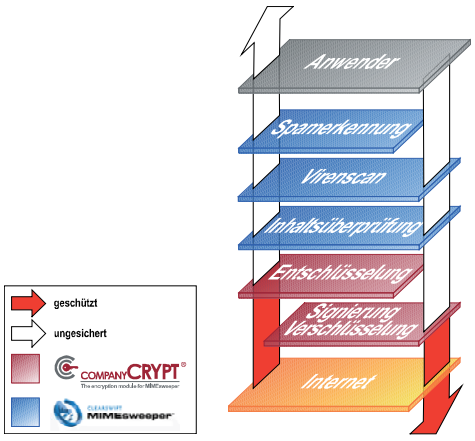
Email-Verschlüsselung

Einfache Integration in MIMEsweeper

- Nahtlose Integration direkt im Content Security-Gateway MIMEsweeper for SMTP ohne zusätzliche Hardware
- Ermöglicht die vollständige Anwendung aller Security-Policies inklusive Inhaltsüberprüfung, Virenschutz und Anti-Spam auch auf verschlüsselte Emails
- Zentrales webbasiertes Management auf dem MIMEsweeper
- Beliebig skalierbar durch MIMEsweeper-Clustering

Highlights

- Automatische Ver- und Entschlüsselung, zentral und ohne Interaktion der Benutzer.
- Vollständige Unterstützung der Standards S/MIME und OpenPGP
- Ad Hoc Encryption zur sofortigen Verschlüsselung auch an Kommunikationspartner ohne Verschlüsselungstechnologie
- Umfassende Signaturprüfung und Signierung von Emails mit User oder Firmenschlüssel
- Geringer Administrationsaufwand durch automatisierte Schlüsselerzeugung (onboard CA), selbständiger Schlüsselaustausch und vollautomatischer Keyimport
- Intelligente Verschlüsselungsszenarien, wie Best Effort, garantieren optimale Nutzung von Email-Verschlüsselung ohne Konfigurationsaufwand
- Gesetzeskonforme Verschlüsselung der Emails
- Support von Domänen-, Team- und Gatewayzertifikaten



FAQs

Auf welchen MIMEsweeper-Systemen kann CompanyCRYPT installiert werden?

CompanyCRYPT arbeitet mit allen Versionen der Software MIMEsweeper for SMTP zusammen.

Benötigt der Empfänger auch CompanyCRYPT um verschlüsselte Emails empfangen zu können?

Nein er benötigt nicht speziell CompanyCRYPT. Jede Email-Lösung, die eine der beiden Standards S/MIME oder OpenPGP unterstützt, ist für eine gesicherte Kommunikation geeignet – egal ob Gateway- oder Desktop-Lösung

Welche zusätzlichen Anforderungen gibt es für System-Hardware?

Da CompanyCRYPT direkt auf den MIMEsweeper-Servern installiert wird, ist keine zusätzliche Hardware erforderlich.

Wie kann ich verschlüsseln, wenn mein Kommunikationspartner noch keine Verschlüsselungstechnik einsetzt?

Falls Ihr Partner weder mit S/MIME oder OpenPGP arbeitet, nutzt CompanyCRYPT ein Ad Hoc-Verfahren. Hierbei werden die Informationen mit einem hochsicheren AES-Verschlüsselungsalgorhythmus geschützt und als selbstentpackendes Archiv übertragen.

Kann ich vorhandene PGP-Schlüssel und Zertifikate mit CompanyCRYPT weiter benutzen?

Ja, Ihre vorhandenen Zertifikate und Schlüssel, die Sie z. B. bereits bei einem Trustcenter erworben haben, lassen sich problemlos importieren. Da CompanyCRYPT eine eigene Onboad-CA besitzt, ist auch die Erstellung von neuen Schlüsseln und Zertifikaten ohne zusätzliche Kosten möglich.

Secure Internet Traffic

Secure Internet Traffic
S.I.T. GmbH & Co. KG
Goseriede 4, D-30159 Hannover
Tel. +49 511 89 997-10
Fax +49 511 89 997-12
Email: info@companycrypt.com
www.companycrypt.com

Kontakt Clearswift

05-08

USA
100 Marine Parkway, Suite 550
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

Spanien
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón, Madrid
Tel: +34 91 7901219 / +34 91 7901220 | Fax: +34 91 7901112

Australien
Level 5, Suite 504, 165 Walker Street,
North Sydney, New South Wales, 2060
Tel : +61 2 9424 1200 | Fax : +61 2 9424 1201

Großbritannien
1310 Waterside, Arlington Business Park, Theale,
Reading, Berkshire, RG7 4SA
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Deutschland
Amsinckstrasse 67, 20097 Hamburg
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

Japan
Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku
Tokyo 105-0011
Tel : +81 (3) 5777 2248 | Fax : +81 (3) 5777 2249