NETSEC.CO
THE NETWORK SECURITY COMPANY

E-Mail Sicherheit

Factsheet

Beschreibung

Obwohl E-Mail ein sehr unsicheres Medium ist, erfolgt ein grosser Teil der Korrespondenz mit Kunden und Partnern darüber. So werden vertrauliche Informationen unverschlüsselt über das Internet übertragen. Falls die so übermittelten Informationen in falsche Hände geraten, kann dies zu einem Reputationsverlust oder sogar zu einem Strafverfahren führen.

Die digitale Signatur von ausgehenden E-Mails erhöht die Reputation des Absenders erheblich und stellt sicher, dass der Inhalt nicht verändert wurde.

Lösung

Technisch ist es heute problemlos möglich, E-Mails zu verschlüsseln, so dass die Vertraulichkeit gewährt ist. Allerdings sind die meisten Lösungen kompliziert in der Anwendung und verursachen einen grossen administrativen Aufwand.

Mit dem Cloud Service von **CLEANMAIL** steht ein sehr einfach zu nutzender Dienst zum sicheren Austausch von E-Mails zur Verfügung.

Vorteile

- transparente Lösung – keine lokale Software und Zertifikate notwendig
- das Arbeiten mit E-Mails ändert sich nicht
- verschlüsselte E-Mails können auch auf mobilen Geräten gelesen werden
- automatische digitale Signatur für alle ausgehenden E-Mails
- automatische Verschlüsselung ausgehender E-Mails bei Bedarf
- automatische Entschlüsselung eingehender E-Mails
- einfache und sichere Lösung für Empfänger ohne Zertifikat
- Zertifikate werden auf Wunsch für neue Benutzer automatisch erstellt
- Schweizer Software, in der Schweiz betrieben, Zertifikate eines CH Trust Centers

Kompatibilität

CLEANMAIL ist mit den allermeisten E-Mail Systemen kompatibel, insbesondere mit Exchange (*on premise* und als MS 365 Service) und Outlook.

Preise

Grundpreis pro Monat	CHF 30*	*ab 10 Benutzern inkl.
pro Benutzer und Monat	CHF 12	

Technische Beschreibung

CLEANMAIL ist ein Cloud Service der in den Datenfluss des E-Mail Systems eingebunden wird. Ausgehende E-Mails werden vom E-Mail Server zum **CLEANMAIL** Service weitergeleitet. Dieser signiert das E-Mail automatisch digital. Falls das benötigte Zertifikat noch nicht vorliegt, wird es automatisch beim Trust Center gelöst.

Falls gewünscht, wird das E-Mail verschlüsselt. Dies kann vom Benutzer gesteuert werden (über einen Hinweis im Betreff oder über die Option *vertraulich*).

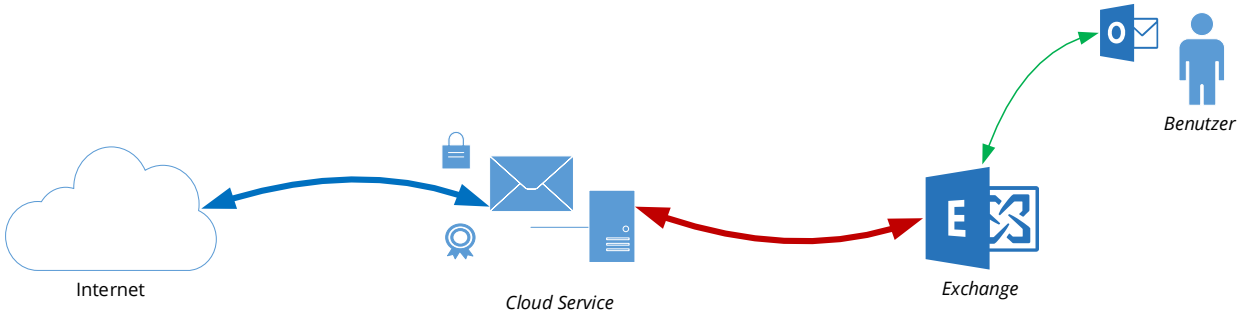
Um ein E-Mail an einen bestimmten Empfänger verschlüsselt zu senden, wird ein E-Mail Zertifikat des Empfängers benötigt. Dieses wird übermittelt, wenn dieser ein signiertes E-Mail verschickt.

Nebst der Verschlüsselung und der digitalen Signierung von E-Mails führt **CLEANMAIL** auch SPAM- und Malwareprüfungen durch.

Einbindung in den E-Mail Datenfluss

Um **CLEANMAIL** in den Datenfluss einzubinden, wird der MX Record auf den Cleanmail Server umgestellt. Eingehende E-Mails werden dann direkt zum Cleanmail Service geleitet. Nachdem **CLEANMAIL** ein E-Mail bearbeitet hat, wird dieses an den Exchange Server weitergeleitet und so dem Benutzer zugestellt.

Für ausgehende E-Mails wird auf dem Exchange Server ein Connector eingerichtet. Dadurch werden die E-Mails an den **CLEANMAIL** Service geschickt. Dieser führt die notwendigen Operationen aus und schickt dann das E-Mail an den gewünschten Empfänger.



Die Verbindung zwischen **CLEANMAIL** und Exchange erfolgt verschlüsselt (TLS).

Funktion von Cleanmail

CLEANMAIL führt folgende Operationen aus:

- ausgehende E-Mails werden immer digital signiert
- ausgehende E-Mails werden verschlüsselt, falls sie vom Absender markiert wurden
- eingehende E-Mails werden entschlüsselt, falls sie verschlüsselt waren
- alle E-Mails werden auf SPAM geprüft
- alle E-Mails werden auf Schadsoftware geprüft

Grundsystem

CLEANMAIL basiert auf SEPP**MAIL**, einem Schweizer Produkt für E-Mail Sicherheit.

Zertifikate

Für den Austausch verschlüsselter und digital signierter E-Mails wird ein E-Mail Zertifikat benötigt. Dieses wird vom **CLEANMAIL** Service automatisch beim Schweizer *Trust Center* QuoVadis über eine sogenannte *managed PKI* bezogen.

Option für Empfänger ohne E-Mail Zertifikat

Um jemandem ein verschlüsseltes E-Mail zu schicken, das direkt im Outlook geöffnet werden kann, muss der Absender im Besitz des E-Mail Zertifikates des Empfängers sein. Dies ist oft nicht der Fall, da ein solches gar nicht vorhanden ist.

Für diesen Fall bietet **CLEANMAIL** die Option GINA an. Der Ablauf ist dann wie folgt:

- Der Absender **A** schickt ein verschlüsseltes E-Mail an den Empfänger **E**
- **CLEANMAIL** stellt fest, dass kein Zertifikat vorliegt
- **CLEANMAIL** legt das E-Mail auf dem GINA Server ab und erzeugt zwei E-Mails
    - eines wird an **A** geschickt mit dem Initialpasswort für **E**
    - eines wird an **E** geschickt mit einem Link zum E-Mail auf dem GINA Server
- **A** muss nun das Initialpasswort auf einem sicheren Kanal an **E** übermitteln
- **E** kann über den Link auf GINA zugreifen und sich dort mit dem Initialpasswort anmelden; dieses muss sofort geändert werden
- **E** hat nun einen sicheren Zugriff (https) auf das verschlüsselte E-Mail
- **E** kann nun über GINA antworten und weitere E-Mails empfangen

der Passwortaustausch ist nur beim ersten verschlüsselten E-Mail erforderlich

Verwaltung

Die Verwaltung des **CLEANMAIL** Services erfolgt über ein Web Interface. Über dieses können folgende Funktionen ausgeführt werden.

- Anzeige von Statistiken (Anzahl ein- / ausgehende E-Mails, SPAM, Malware, ...)
- Anzeige von Benutzern, die den Service nutzen
- Suche und Anzeige von ein- und ausgehenden E-Mails (nur Randdaten)
- Zugriff auf Quarantäne (dort werden als SPAM erkannte E-Mails zurückgehalten) und Freigabe von E-Mails falls erforderlich

Der Zugriff erfolgt über Administratorenkonten, die mit MFA geschützt werden können.