



Email Encryption für InterScan™ Messaging Hosted Security

Trend Micro Incorporated ↩

- ➔ Ein Überblick über den zusätzlichen Service zur Verschlüsselung von E-Mails bei der gehosteten E-Mail-Sicherheitslösung von Trend Micro

Warum verschlüsseln?

Die heutigen Anforderungen an Datenschutz und Geheimhaltung zwingen Unternehmen aller Größenordnungen und Branchen dazu, wichtige Daten in E-Mails sorgfältig zu sichern. Oft müssen bestimmte Arten von Daten verschlüsselt werden, wie z. B. Kreditkartennummern, geistiges Eigentum und Kundendaten. Unternehmen müssen auch die vertraulichen E-Mails bestimmter Gruppen (z. B. Geschäftsleitung, Personal- oder Rechtsabteilungen) zuverlässig schützen.

Viele Unternehmen entscheiden sich für richtlinienbasierte Verschlüsselung, da Daten anhand von Content-Filter-Regeln, die bestimmte Inhalts- oder Benutzergruppen erkennen, automatisch verschlüsselt werden. Die Verschlüsselung wird ausgeführt, sobald die Regeln ausgelöst werden. Bei der richtlinienbasierten Verschlüsselung sind Unternehmen nicht darauf angewiesen, dass Benutzer wichtige Inhalte selbstständig sichern.

Einführung in Email Encryption for InterScan Messaging Hosted Security

Trend Micro bietet Email Encryption als einen zusätzlichen Service für InterScan Messaging Hosted Security. Es ist nahtlos in den Content-Filter des gehosteten E-Mail-Sicherheitservice von Trend Micro integriert, der vor Spam, Viren und unerwünschten Inhalten schützt. Trend Micro Email Encryption verwendet identitätsbasierte Verschlüsselung (IBE), um jeden Benutzer mit einer E-Mail-Adresse zu schützen. Dieser Ansatz macht die mühsame Vorregistrierung und Zertifikatsverwaltung der herkömmlichen Public Key Infrastructure (PKI) Technologie mit dynamischer Schlüsselerzeugung überflüssig. Verschlüsselte Inhalte werden wie jede andere E-Mail vom Absender an den Empfänger übertragen.

Weitere Informationen über andere E-Mail-Verschlüsselungslösungen von Trend Micro finden Sie unter <http://de.trendmicro.com/de/products/enterprise/email-encryption/index.html>

Die Funktion von TLS

TLS, also der Schutz der Transportschicht, ist eine Verschlüsselungsart, die von vielen Anbietern gehosteter Sicherheit verwendet wird. TLS verschlüsselt die E-Mail-Pipeline, aber nicht die E-Mail selbst. Zusammen mit einem gehosteten E-Mail-Verschlüsselungsservice kann TLS eine wichtige Funktion zukommen, ist als eigenständige Lösung jedoch unzuverlässig. Damit die Pipeline sicher ist, müssen sowohl der sendende als auch der empfangende Server TLS aktivieren. Dies kann für die Server des E-Mail-Empfängers nicht garantiert werden, da E-Mails auf ihrem Weg zum Zielempfänger oft über mehrere ISP-Server geleitet werden und dabei auch die Schutzkette unterbrochen wird. Diese Form von TLS reicht nicht aus, um E-Mail-Inhalte zu schützen. Siehe Abbildung 1.



Abbildung 1: TLS schützt nur einen Teil der Strecke, über die Daten geleitet werden, und wird möglicherweise nicht durchgängig unterstützt.

Richtlinienbasierte E-Mail-Verschlüsselung aktivieren

Email Encryption ist in den Content-Filter von InterScan Messaging Hosted Security integriert, das flexible und unkomplizierte Filteroptionen für fast alle Arten von Inhalten bietet. Administratoren legen einfach Content-Filterregeln fest, deren Aktion die Verschlüsselung ist.

Kunden schützen ihre E-Mails auf der Strecke zwischen ihrem Netzwerk und dem InterScan Messaging Hosted Security Server mit TLS. Trend Micro bietet allen Kunden TLS-Funktionen als Teil des Service, um die Sicherheit bei der Übertragung vom Kundenstandort an den Service zu gewährleisten. Die entsprechenden E-Mails werden dann vom Email Encryption Service gemäß den vom Kunden erstellten Regeln verschlüsselt und sicher an die Empfänger gesendet. (Siehe unten stehende Abbildung 2.)



Abbildung 2: Email Encryption for InterScan Messaging Hosted Security gewährleistet die sichere Zustellung von E-Mails an jeden Benutzer mit einer E-Mail-Adresse.

Um Verschlüsselung als Aktion einer Content-Filterregel festzulegen, führen Administratoren diese fünf einfachen Schritte aus:

1. Sie geben an, dass die Regel für ausgehende E-Mails gilt.
2. Sie bestimmen den Absender/Empfänger der Regel.
3. Sie wählen die Nachrichtenattribute aus (wonach sucht der Filter?).
4. Sie geben „E-Mail verschlüsseln“ als Regelaktion an.
5. Sie benennen die Regel und speichern sie.

Bei der Angabe von Absendern oder Empfängern für eine bestimmte Regel können Administratoren spezifische E-Mail-Adressen verwenden oder eine gesamte Domäne auswählen. Außerdem können Administratoren Ausnahmen zu einer Regel angeben.

Um Inhalte zu ermitteln, erstellen Administratoren einen 'Schlüsselwortausdruck'. Administratoren können eine beliebige Kombination aus Schlüsselwörtern und regulären Ausdrücken verwenden, um einen Schlüsselwortausdruck festzulegen (es stehen vordefinierte Wortlisten und Datenformatwörterbücher zur Verfügung). Dieser wird dann vom Administrator gespeichert und benannt. Der Schlüsselwortausdruck kann auf mehrere Regeln angewendet werden (u. a. für unterschiedliche Gruppen oder Nachrichtenattribute, wie beispielsweise Betreffzeile, E-Mail-Text oder -Kopfzeile oder Anhangsinhalt).

Nach der Festlegung der Nachrichtenattribute müssen Administratoren die Verschlüsselung als Regelaktion angeben, indem sie die Option „Nachrichten nicht ausfiltern“ auswählen und auf die Aktion *E-Mail verschlüsseln* klicken, wie in unten stehender Abbildung 3 angezeigt.

All messages triggering rule will be logged.

Intercept

- Do not intercept messages
- Delete entire message
- Deliver now
- Quarantine
- Change recipient to

Modify

- Clean cleanable viruses, delete those that cannot be cleaned
- Delete attachment
- Insert stamp in body
- Tag Subject
- Encrypt email

Monitor

- Send notification
- BCC

Abbildung 3: Die Option „E-Mail verschlüsseln“ als Aktion auswählen

Anwendungsbeispiele:

- 1) Administratoren können Datenformatwörterbücher für Kreditkarten- oder Sozialversicherungsnummern mit Client-Namenslisten oder Kontonummern kombinieren, um E-Mails mit vertraulichen Daten zu kennzeichnen, wie es häufig durch Richtlinien gefordert wird.
- 2) Schlüsselausdrücke für Wörter wie 'verschlüsseln' oder 'vertraulich' können die Verschlüsselung von E-Mails erleichtern.

Nachdem *E-Mail verschlüsseln* als Regelaktion festgelegt wurde, muss die Regel vom Administrator nur noch benannt und gespeichert werden. Nach dem Erstellen der Regel kann sie bearbeitet oder kopiert werden, wobei Letzteres die Erstellung einer ähnlichen Regel vereinfacht, da Administratoren die kopierte Regel einfach durch Einfügen der gewünschten Änderungen bearbeiten.

Auswirkungen von Email Encryption auf den Empfänger

Empfänger der verschlüsselten E-Mail erhalten eine E-Mail-Benachrichtigung in Form eines versiegelten, elektronischen Umschlags. Empfänger können ihre eigene Version des Trend Micro Email Encryption Clients herunterladen oder ihren Webbrowser zum Lesen und Beantworten verwenden, ohne zusätzliche Software zu installieren. Unten stehende Abbildung 3 zeigt das Beispiel einer E-Mail, die an den Empfänger gesendet wird, und das Beispiel eines HTML-Dateianhangs, der einen Link zum Webbrowser enthält, wo die verschlüsselte E-Mail angezeigt werden kann.

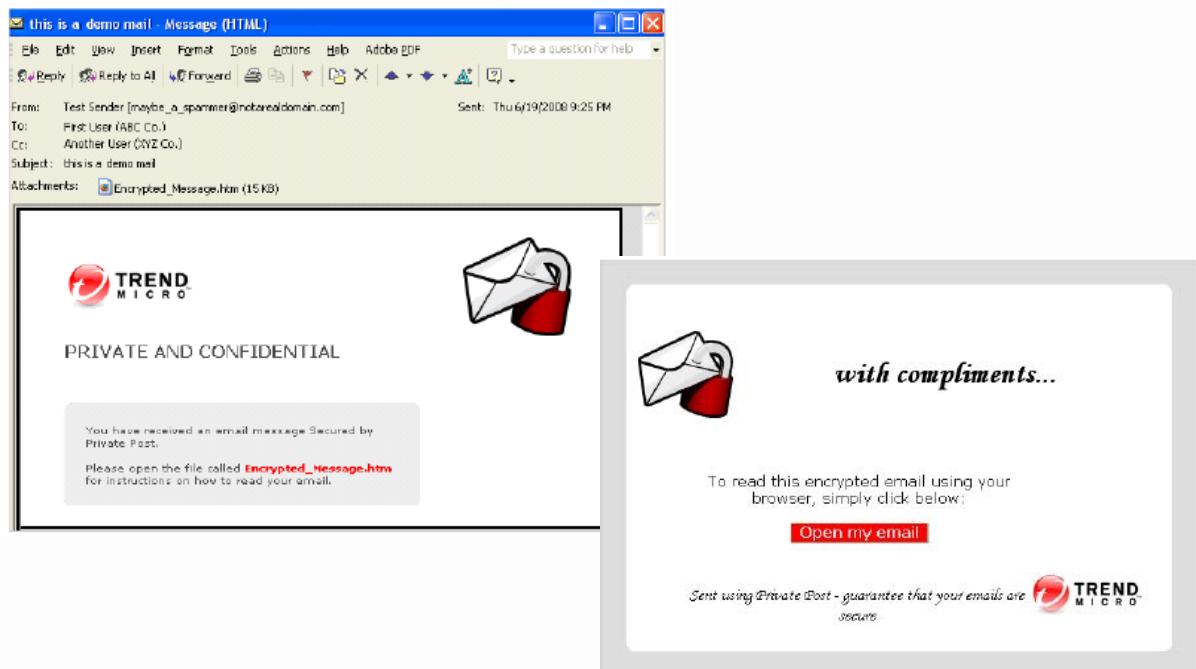


Abbildung 4: Auswirkungen von Email Encryption auf den Empfänger: Verschlüsselter E-Mail-Umschlag und Browser-Zugriff

Email Encryption aktivieren

Trend Micro Email Encryption for InterScan Messaging Hosted Security ist nur als zusätzlicher Service für die Advanced-Version mit Filter für den ausgehenden Datenverkehr verfügbar. Diese Option steht Advanced-Kunden ohne Aufpreis zur Verfügung und kann während der Testphase oder der Registrierung angefordert werden.

Die Aktivierungsoptionen für Email Encryption hängen vom Status der InterScan Messaging Hosted Security Lizenz ab, wie unten stehende Tabelle 1 zeigt.

Email Encryption für InterScan Messaging Hosted Security

InterScan Messaging Hosted Security – Lizenzstatus	Email Encryption – Lizenzoptionen
Erworben	Kann Email Encryption testen oder erwerben. <ul style="list-style-type: none">• Siehe „Eine kostenfreie Testphase von Email Encryption starten“.• Siehe „Email Encryption erwerben“.
In Testphase	Kann Email Encryption nur kostenfrei testen. <ul style="list-style-type: none">• Siehe „Eine kostenfreie Testphase von Email Encryption starten“.

Tabelle 1: Email Encryption – Aktivierungsoptionen

Eine kostenfreie Testphase von Email Encryption starten

Unternehmen können Email Encryption zusammen mit einer Testversion von InterScan Messaging Hosted Security Advanced kostenfrei testen, indem sie im Formular zur Beantragung der Testversion Email Encryption auswählen. Das Formular befindet sich auf der Webseite des Service. Wurde InterScan Messaging Hosted Security bereits erworben oder befindet sich in der Testphase, kann eine kostenfreie Testversion von Email Encryption über die Service-Konsole im Bereich Administration > Lizenzen beantragt werden. (Siehe unten stehende Abbildung 4.)

Email Encryption erwerben

Um diesen Email Encryption Service zu erwerben, muss auch InterScan Messaging Hosted Security Advanced mit Filter für ausgehenden Datenverkehr erworben werden. Unternehmen können während der Testphase des Advanced-Service auch Email Encryption kostenfrei testen. Email Encryption kann jedoch erst nach dem Kauf von InterScan Messaging Hosted Security erworben werden.

Sowohl InterScan Messaging Hosted Security als auch Email Encryption können über einen Reseller erworben werden. Kontaktdaten von Resellern sind über Links auf der Service-Webseite verfügbar. In einigen Regionen erhalten Kunden einen Registrierungsschlüssel (RK) und müssen sich online registrieren, um einen Aktivierungscode zu erhalten. In anderen Regionen wird direkt nach dem Erwerb ein Aktivierungscode ausgegeben. In jedem Fall muss der Kunde den Aktivierungscode in der InterScan Messaging Hosted Security Konsole im Bereich **Administration > Lizenzen** eingeben, um den Service zu starten. **(Siehe unten stehende Abbildung 4.)**

Licenses (Activate an Account) ?

If you have a **Registration Key**, [register online](#) to get an Activation Code.

Activation Type:

Trial Activation
Service Name Email Encryption ▼
(An Activation Code is not required to activate a trial)

Purchase Activation
Service Name Email Encryption ▼
Activation Code
(Insert Activation Code provided by email to activate purchase)

Abbildung 4: Email Encryption – Lizenzaktivierung

Email Encryption für InterScan Messaging Hosted Security

Beachten Sie, dass die Überprüfung Ihres Antrags auf eine Test- oder Vollversion von Email Encryption und die Freischaltung Ihres Kontos durch Trend Micro 24 bis 48 Stunden dauern können. Nach der Aktivierung wird Email Encryption als verfügbare Regelaktion beim Hinzufügen oder Bearbeiten einer Regel im InterScan Messaging Hosted Security Richtlinienfenster angezeigt.

Fazit

Bei der richtlinienbasierten Verschlüsselung sind Unternehmen nicht darauf angewiesen, dass Benutzer wichtige Inhalte selbstständig sichern. Die Verschlüsselung wird beim Auslösen einer Content-Filterregel ganz automatisch angewendet, um die Einhaltung von Geheimhaltungs- und Datenschutzanforderungen zu gewährleisten.

Trend Micro bietet eine richtlinienbasierte E-Mail-Verschlüsselungslösung, die sich nahtlos in den Content-Filter von InterScan Messaging Hosted Security integriert. Administratoren aktivieren einfach ein Kontrollkästchen, um Verschlüsselung als eine Regelaktion festzulegen. Die flexible Email Encryption Lösung von Trend Micro setzt identitätsbasierte Verschlüsselung (IBE) ein und macht die mühsame Vorregistrierung und Zertifikatsverwaltung der Public Key Infrastructure (PKI) Technologie überflüssig. Mit Trend Micro Email Encryption ist es einfach, Inhalte sicher zu verschlüsseln.

WP02_IMHSEncrypt_090219DE. ©2009 by Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo, InterScan und Private Post sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und den darin beschriebenen Produkten ohne vorherige Benachrichtigung durchzuführen.