Security Insider

eBook

E-Mail-Verschlüsselung im Unternehmen

Alternativen zur Public Key Infrastructure und Integration von cloud-basierten Lösungen in die Unternehmens-IT

Vogel Business Media

Inhalt

Vogel IT-Medien GmbH
August-Wessels-Str. 27, 86156 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel-it.de
Erscheinungstermin: Februar 2013
Titelbild: beermedia - Fotolia.com

Vogel Business Media

Alternative Lösungen zur E-Mail-Verschlüsselung

Verschlüsselte Mails vom Server bis zum Smartphone

Alternative Verschlüsselungslösungen ermöglichen eine durchgehende E-Mail-Verschlüsselung, die sich auch mit mobilen Endgeräten nutzen lässt.

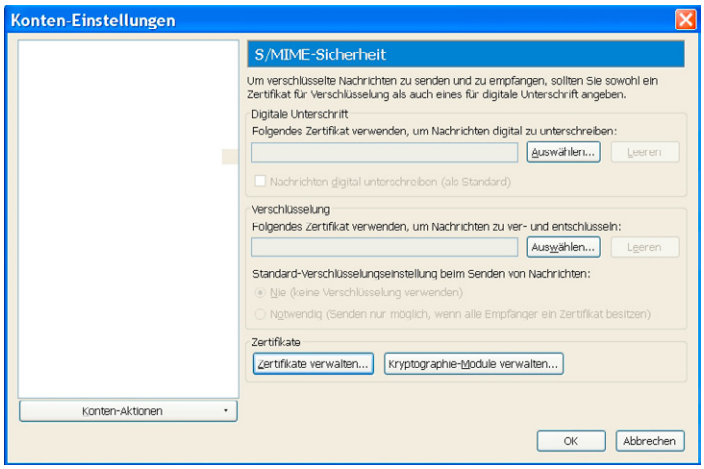
Die meisten Unternehmen schreiben vor, dass jede E-Mail mit vertraulichem Inhalt zu verschlüsseln ist. Trotzdem werden immer noch zahlreiche E-Mails ohne jede Verschlüsselung verschickt. Laut der Ponemon-Studie „The State of Email Encryption“ gehen 69 Prozent der Unternehmen davon aus, dass ihre Mitarbeiter keine E-Mail-Verschlüsselung einsetzen.
Um das zu ändern, sollten sich Unternehmen der typischen Probleme der E-Mail-Verschlüsselung annehmen:

- E-Mail-Verschlüsselung gilt als kompliziert und aufwändig.
- E-Mails werden auch mobil oder im Home-Office bearbeitet.
- Nicht jeder Geschäftspartner oder externe Mitarbeiter verfügt über eine eigene Verschlüsselungslösung, um die E-Mails entschlüsseln zu können.

Damit sich die E-Mail-Verschlüsselung durchsetzen lässt, müssen Unternehmen deshalb an alle Endgeräte und Nutzertypen denken und eine möglichst einfache Verschlüsselungslösung suchen.

1. Alternativen zur PKI im Unternehmen

Klassische Lösungen zur E-Mail-Verschlüsselung wie PGP setzen den Aufbau und Betrieb einer Public Key Infrastructure (PKI) voraus. Bei S/MIME (Secure / Multipurpose Internet Mail Extensions) benötigt jeder E-Mail-Nutzer ein digitales Zertifikat zur Verschlüsselung. Da die meisten Nutzer die an sich wenigen, erforderlichen Schritte zur Einrichtung der E-Mail-Zertifikate ablehnen, empfiehlt sich eine zentrale, serverseitige Verschlüsselungslösung, die keine Vorbereitung seitens der Nutzer erforderlich macht.



Gängige E-Mail-Clients wie Mozilla Thunderbird unterstützen die E-Mail-Verschlüsselung nach S/MIME, wobei die Nutzer allerdings digitale Zertifikate benötigen. Auch mit anderen klassischen Verschlüsselungslösungen wie PGP können nicht alle Kommunikationspartner erreicht werden.

E-Mail-Adresse als öffentlicher Schlüssel

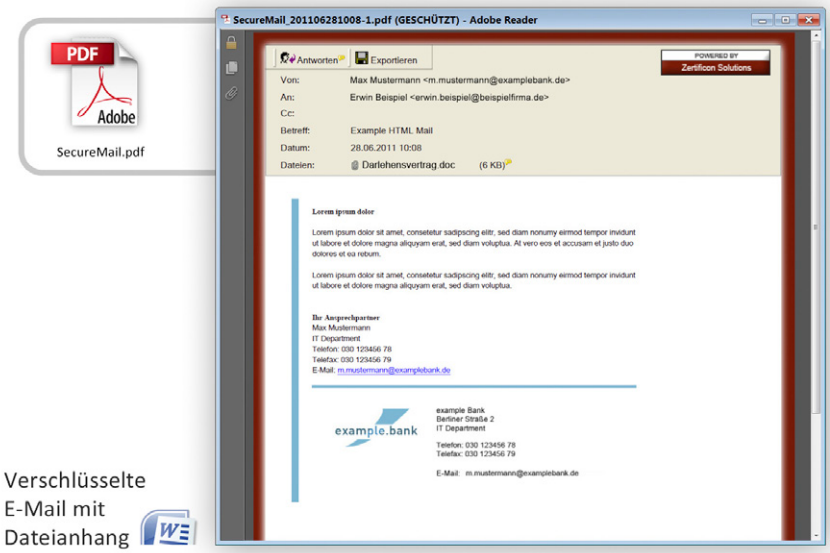
Die identitätsbasierte Verschlüsselung (IBE, Identity-based Encryption) zum Beispiel bei FortiMail Identity Based Encryption oder bei Trend Micro Email Encryption nutzt die Tatsache, dass jeder E-Mail-Nutzer auch ohne Zertifikat bereits ein eindeutiges Merkmal besitzt, seine E-Mail-Adresse. Diese wird bei IBE zum öffentlichen Schlüssel. Der zentrale Verschlüsselungsserver generiert aus den E-Mail-Adressen der Nutzer die privaten Schlüssel. Anstelle eines speziellen Clients benötigen die Empfänger einer verschlüsselten Nachricht nur einen Webbrowser, um die Dekodierung der E-Mail zu bewerkstelligen. Zur Verschlüsselung wird allerdings ein Plug-In für den Mail-Client Outlook vorausgesetzt. Im Vergleich zu einer PKI-basierten Lösung sollen sich die Aufwände mit IBE um 78 Prozent senken lassen, so die Enterprise Strategy Group.

2. Jedem seine E-Mail-Verschlüsselung

Für Unternehmen, die eine eigene PKI betreiben, aber auch mit Geschäftspartnern oder freien Mitarbeitern ohne klassische Verschlüsselungslösung sicher per E-Mail kommunizieren wollen, bietet sich eine Hybrid-Verschlüsselungslösung an. Eine solche Lösung unterstützt sowohl Verfahren wie PGP und S/MIME als auch eine SSL-Verschlüsselung für E-Mails und passwortgeschützte E-Mails.

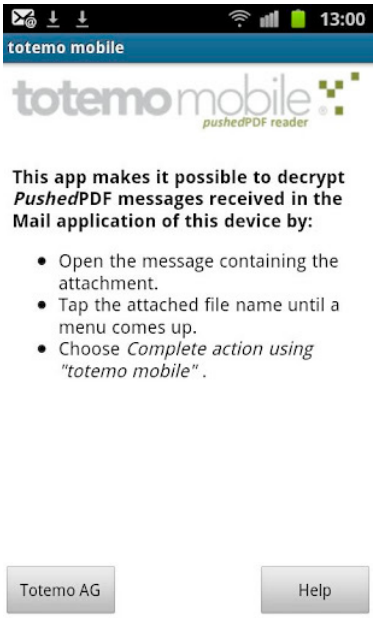
Browser als Entschlüsselungsgehilfe

Möglich ist solch eine breite Unterstützung von Verschlüsselungsverfahren für E-Mails zum Beispiel bei dem Z1 SecureMail Gateway mit Z1 WebSafe (browserbasiert), Z1 KickMail (verschlüsselter HTML-Anhang) und Z1 KickMail-PDF (verschlüsselter PDF-Anhang), bei dem Totemo TrustMail Secure Messaging Gateway, zusammen mit Totemo TrustMail WebMail und Registered Pushed-PDF für Totemo TrustMail, oder bei iQ.Suite Crypt in Verbindung mit iQ.Suite WebCrypt Pro oder WebCrypt Live, die sich jeweils für Kommunikationspartner ohne Unterstützung von PGP oder S/MIME eignen.



Mit dem Zertificon Z1 Gateway lassen sich verschlüsselte E-Mails je nach Ausstattung des Empfängers auch als verschlüsselte PDF-Datei oder als verschlüsselter HTML-Anhang verschicken. Der Empfänger braucht dann keine eigene, lokale Verschlüsselungslösung für die Entschlüsselung (Bild: Zertificon Solutions).

In einer solchen Konstellation können E-Mail-Nutzer mit klassischer Verschlüsselungslösung auch mit solchen Anwendern verschlüsselte E-Mails austauschen, die nur einen Webbrowser und einen einfachen Mail-Client zur Verfügung haben. Die E-Mail enthält dann zum Beispiel einen Link, der im



Smartphone-Nutzer können mit der App Registered PushedPDF verschlüsselte E-Mails als PDF-Datei öffnen und bearbeiten, wenn diese mit Totemo TrustMail verschickt wurden (Bild: Totemo AG).

Browser SSL-verschlüsselt mit dem richtigen Passwort geöffnet werden kann. Die E-Mail-Verschlüsselung erreicht dadurch auch externe Projektpartner oder aber Mitarbeiter im Home-Office, ohne große Anforderungen an die IT-Infrastruktur zu stellen.

3. Mobile E-Mail-Nutzer einbinden

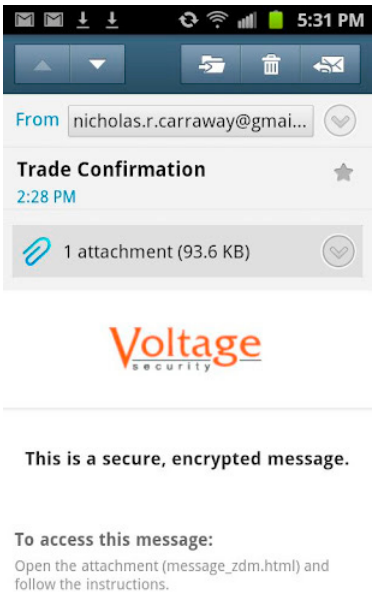
Fast 60 Prozent der Smartphone-Nutzer in Deutschland, Großbritannien, Frankreich, Italien und Spanien nutzen ihr mobiles Endgerät für private und berufliche E-Mails, so die Studie comScore MobiLens (Oktober 2012). Ohne Einbindung der mobilen Nutzer kann eine durchgehende E-Mail-Verschlüsselung also nicht gelingen. Mobile Nutzer müssen zum einen in die Lage versetzt werden, verschlüsselte E-Mails auf ihrem Smartphone zu entschlüsseln, zum anderen muss es aber auch möglich sein, vom Smartphone aus selbst verschlüsselte E-Mails zu verschicken.

Mit der App zur mobilen Verschlüsselung

Die Voltage SecureMail Mobile Edition zum Beispiel ermöglicht Ent- und Verschlüsselung für Android-, BlackBerry- und iPhone-Nutzer. Dazu integriert sich die Lösung in die auf den Smartphones laufenden E-Mail-Clients. Eingehende, verschlüsselte E-Mails lassen sich verschlüsselt beantworten, neue E-Mails können mit dem Befehl „Send Secure“ und nach Anmeldung am Verschlüsselungsserver erstellt und sicher verschickt werden. Mit der totemo mobile pushed PDF Reader-App für iOS- und Android-Geräte können verschlüsselte Nachrichten auf dem Smartphone geöffnet und bearbeitet werden, wenn diese über das Totemo TrustMail Secure Messaging Gateway verschickt wurden. Bei Verwendung von WebMail für Totemo TrustMail reicht ein mobiler Browser auf dem Smartphone, um die verschlüsselten E-Mails auch mobil öffnen zu können.

Fazit

Alternative Verschlüsselungslösungen vereinfachen somit das Ausrollen der Verschlüsselung, auch für mobile Nutzer und für Nutzer ohne eigenen Verschlüsselungsclient. Eine weitere Herausforderung bei der Umsetzung der E-Mail-Verschlüsselung ist die notwendige Administration. Gerade für kleine und mittlere Unternehmen, die die E-Mail-Verschlüsselung nicht selbst betreiben wollen, gibt es aber eine ganze Reihe von cloud-basierten Lösungen. Darum geht es im zweiten Teil dieses Ratgebers zur E-Mail-Verschlüsselung. *Oliver Schonschek*



Mit der App Voltage SecureMail können verschlüsselte E-Mails geöffnet und neue E-Mails verschlüsselt werden. Dadurch lassen sich auch mobile Nutzer in die unternehmensweite Mail-Verschlüsselung einbeziehen (Bild: Voltage Security).

Cloud-basierte Lösungen zur E-Mail-Verschlüsselung

E-Mail-Verschlüsselung aus der Cloud

Cloud-Dienste vereinfachen die E-Mail-Verschlüsselung für kleine und mittlere Unternehmen. Ohne eigene Administration geht es aber nicht.

Für Unternehmen, die die E-Mail-Verschlüsselung nicht selbst betreiben wollen oder können, gibt es eine ganze Reihe von cloud-basierten Lösungen (siehe Kasten). Im Idealfall verwenden die E-Mail-Nutzer dann einfach ihr gewohntes Mail-Programm, ohne sich um die Verschlüsselung der Nachrichten kümmern zu müssen. Die Verschlüsselung der vertraulichen Nachrichten übernimmt die Cloud-Lösung ebenso wie die Entschlüsselung eingehender E-Mails.

In der Praxis zeigt sich allerdings, dass auf die eigene Administration und meist auch auf die E-Mail-Nutzer trotz Cloud-Unterstützung einige Aufgaben zukommen. Für das Unternehmen beginnt dies bereits mit der Auswahl des richtigen Cloud-Anbieters, es geht weiter mit der Einrichtung der E-Mail-Anbindung und der Nutzer, mit der Definition der Verschlüsselungsrichtlinien und mit der Einbindung der E-Mail-Empfänger und schließt auch die Überwachung des genutzten Cloud-Dienstes ein. Trotzdem kann eine E-Mail-Verschlüsselung aus der Cloud je nach Anbieter eine sehr wertvolle Hilfe bei der Umsetzung der Verschlüsselung elektronischer Nachrichten sein, wenn die folgenden Punkte beachtet werden.

1. Kosten im Vergleich zum Eigenbetrieb

Bei der Suche nach einer E-Mail-Verschlüsselung aus der Cloud spielen natürlich die Kostengesichtspunkte eine wichtige Rolle. Bei einer Cloud-Lösung entfallen die Anschaffungs-, Installations-, Betriebs- und Wartungskosten einer E-Mail-Verschlüsselungslösung. Nur die Nutzungsgebühr des Cloud-Anbieters bei der Kostenbetrachtung zu berücksichtigen, wäre allerdings zu kurz gedacht.
Zum einen verbleiben nicht zu unterschätzende Administrationsaufgaben. Dazu gehören die Verknüpfung des

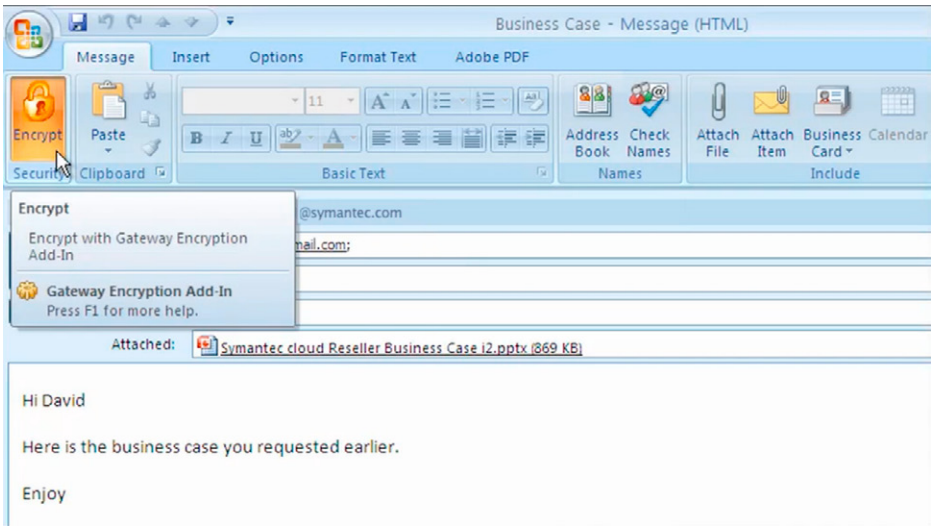
Coud-basierte Lösungen zur E-Mail-Verschlüsselung
Barracuda Email Security Service
CipherCloud
GBS WebCrypt Live
Hosted ZixGateway Service
McAfee SaaS Email Encryption
Proofpoint Encryption
SEPPmail Secure E-Mail
Symantec E-Mail Boundary Encryption.cloud
Symantec Policy based Encryption.cloud
Trend Micro Hosted Email Encryption
Voltage SecureMail Cloud
Websense Cloud Email Security Encryption

Mail-Dienstes mit der Verschlüsselungslösung in der Cloud (Routing), die Einrichtung der Nutzer und Gruppen und die Definition der gewünschten Verschlüsselungsrichtlinien, die vorgeben, welche Art von E-Mails verschlüsselt werden soll. Einen internen Aufwand erzeugt auch die Schulung der E-Mail-Nutzer, abhängig davon, wie selbst erklärend die Cloud-Lösung ist und ob sie in das bekannte E-Mail-Programm integriert werden kann.

Wie bei anderen Cloud-Lösungen auch sollte das Kostenmodell der passenden Anbieter genau hinterfragt werden. Zu klären ist insbesondere, wie viele Nutzer und Nachrichten in einer bestimmten Nutzungsgebühr bereits enthalten sind. Dabei sollte nicht vergessen werden, dass der Leistungsumfang der verschiedenen Cloud-Dienste sehr unterschiedlich ausfällt. Lösungen wie Barracuda Email Security Service enthalten neben der cloud-basierten E-Mail-Verschlüsselung zum Beispiel auch einen Schutz gegen Spam und Malware.

2. Anforderungen aus dem Datenschutz

Eine E-Mail-Verschlüsselung aus der Cloud soll insbesondere auch dabei helfen, personenbezogene Daten in E-Mails zu schützen. Deshalb müssen die Vorgaben aus den Datenschutzgesetzen Beachtung finden. Cloud-Dienste stellen in aller Regel eine Form von Auftragsdatenverarbeitung dar, so dass Anbieter und Cloud-Dienst einer sogenannten Auftragskontrolle nach Bundesdatenschutzgesetz unterzogen werden müssen. Dabei stellt sich auch die Frage, wo die Daten verschlüsselt und entschlüsselt werden und wo die Schlüssel der Nutzer geschützt aufbewahrt werden.



Verschiedene Anbieter wie Symantec bieten eine Outlook-Erweiterung, so dass die Nutzer in ihrer gewohnten Mail-Umgebung die E-Mail-Verschlüsselung aktivieren können (Bild: Symantec-Demo).

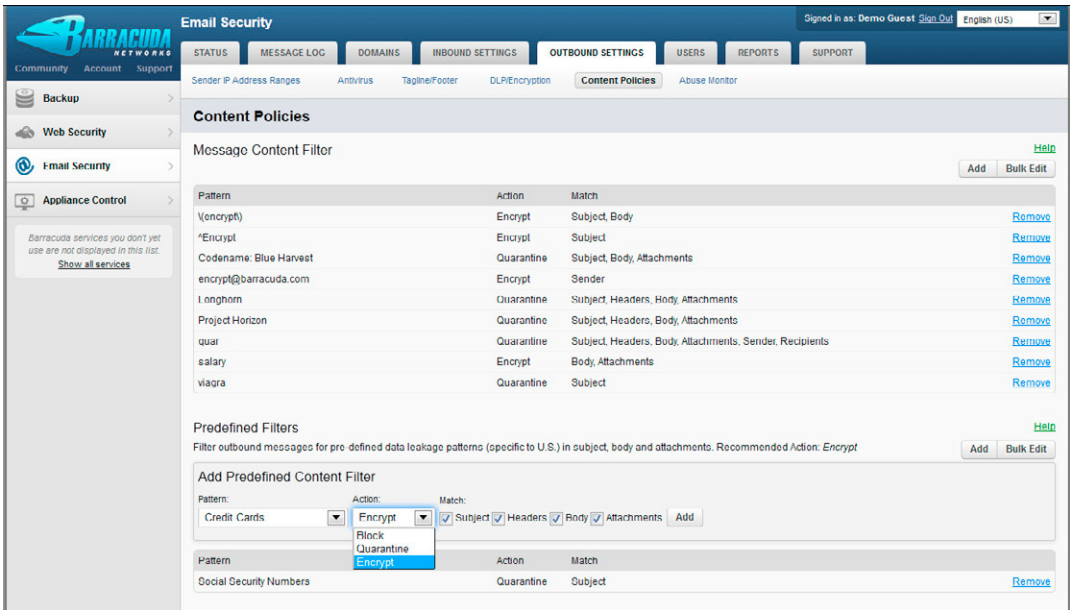
3. Unterstützte E-Mail-Lösungen

Die Wahl der passenden Cloud-Lösung zur E-Mail-Verschlüsselung hängt auch davon ab, welche E-Mail-Lösung genutzt wird. So gibt es zum Beispiel bei den Cloud-Diensten von Symantec und Voltage eine spezielle Outlook-Erweiterung, so dass die Nutzer die Verschlüsselung innerhalb der gewohnten Mail-Umgebung aktivieren können.
Wer zum Beispiel Gmail nutzt, kann die im Standard aktivierte HTTPS-Verschlüsselung von Google nutzen oder aber eine zusätzliche Cloud-Verschlüsselung speziell für Gmail-Nutzer verwenden, wie sie zum Beispiel CipherCloud for Gmail bietet.

4. Richtlinien und Administration

Gerade für kleine und mittlere Unternehmen ist es wichtig, nicht nur die Nutzung, sondern auch die Administration der E-Mail-Verschlüsselung so weit wie möglich zu vereinfachen. Vordefinierte Richtlinien als Basis der Verschlüsselung helfen bei der Einrichtung der E-Mail-Verschlüsselung. So stehen zum Beispiel bei der McAfee SaaS E-Mail-Sicherheitslösung zahlreiche, vordefinierte Richtlinien zur Verfügung, die die Definition eigener E-Mail-Policies erleichtern.

Eine richtlinienabhängige E-Mail-Verschlüsselung hilft generell bei der Automatisierung und damit bei der Durchsetzung der Verschlüsselung, während eine manuell aktivierte Verschlüsselung immer noch von der erfolgreichen Sensibilisierung der Nutzer abhängt. Neben expliziten Verschlüsselungsregeln abhängig von Absender, Inhalt, Dateianhang und Empfänger kann auch eine Zwangsverschlüsselung für den kompletten E-Mail-Verkehr durchgesetzt werden, ein Option, auf die zum Beispiel Symantec verweist.



Über eine Web-Konsole können die Administratoren des Anwenderunternehmens eigene Richtlinien zur E-Mail-Verschlüsselung definieren. Die Verschlüsselung findet dann entsprechend automatisch in der Cloud statt (Bild: Barracuda Networks-Demo).

5. Anbindung von Partnern und Empfängern

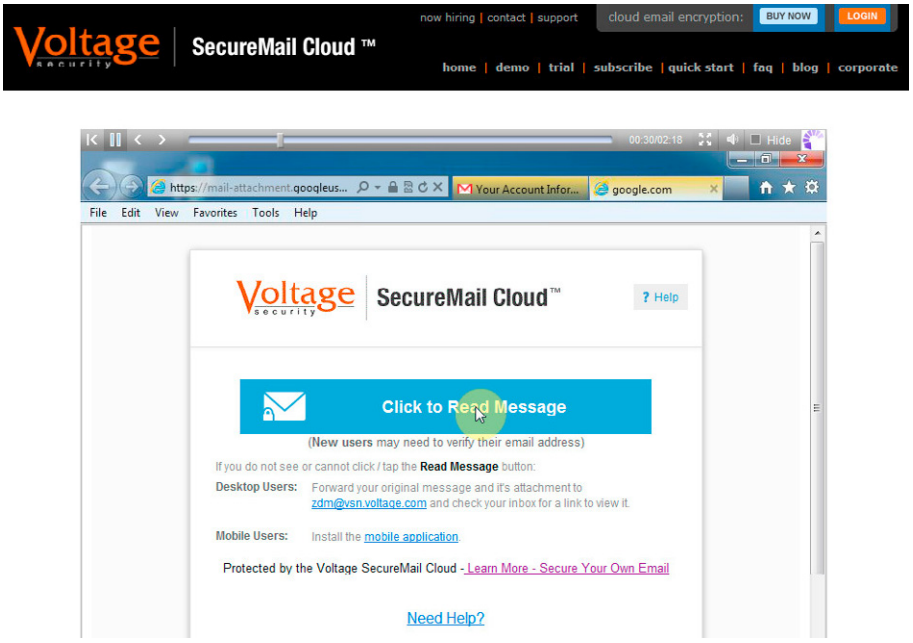
Wenn die E-Mail-Verschlüsselung für eine definierte Absender- und Empfängergruppe zur Verfügung stehen soll, lassen sich alle vorgesehenen Nutzer einrichten, wie dies zum Beispiel bei Symantec E-Mail Boundary Encryption.cloud vorgesehen ist.

Anders sieht es aus, wenn es möglich sein soll, an jeden möglichen Empfänger verschlüsselte E-Mails zu schicken. Damit der Empfänger seine Nachrichten auch entschlüsseln kann, bieten die meisten Lösungen, darunter Symantec Policy based Encryption.cloud, Proofpoint Encryption oder Voltage SecureMail Cloud, eine spezielle Weboberfläche für die Empfänger an, Proofpoint zum Beispiel den Secure Reader. Der Empfänger enthält jeweils eine Nachricht, dass für ihn eine

verschlüsselte E-Mail vorliegt und muss sich dann (in der Regel) kostenlos für den Web-Dienst anmelden, der dann die Entschlüsselung der Nachricht vornimmt.

6. Reporting und Verfügbarkeit

Wie bei jedem ausgelagerten Dienst besteht auch bei einer E-Mail-Verschlüsselung aus der Cloud prinzipiell das Risiko, dass der Cloud-Dienst einmal nicht zur Verfügung steht. Für das ZixData Center, in dem der Hosted ZixGateway Service betrieben wird, wird zum Beispiel eine Verfügbarkeit von 99,99 Prozent angegeben.



Empfänger einer verschlüsselten E-Mail finden zum Beispiel einen Link in einer Mail-Benachrichtigung, der sie zu einem Web-Portal führt (Bild: Voltage Security-Demo).

Grundsätzlich sollte die garantierte Verfügbarkeit der cloud-basierten E-Mail-Verschlüsselung (Service Level Agreements) ebenso hinterfragt werden wie das Notfall-Verfahren, wenn eine E-Mail verschlüsselt verschickt werden soll, der Dienst aber nicht verfügbar ist. Neben einer eindeutigen Fehlermeldung in diesem Fall sollte generell ein aussagekräftiges Reporting zur Verfügung stehen, so dass das Anwenderunternehmen prüfen kann, ob die E-Mail-Verschlüsselung auch wie gewünscht und vereinbart funktioniert.

Verschlüsselung aus der Cloud hat Zukunft

Wenn die Anbieter den Administrationsaufwand auf Seiten des Anwenderunternehmens weiter reduzieren und die Cloud-Sicherheit zuverlässig gewährleisten, wird die E-Mail-Verschlüsselung aus der Cloud zweifellos weiter an Bedeutung gewinnen. Mobile Endgeräte, BYOD und die generelle Zunahme an Cloud-Nutzung werden die Nachfrage nach einer flexiblen und einfachen E-Mail-Verschlüsselung erhöhen. Gartner erwartet, dass bis 2015 zehn Prozent der IT-Sicherheitsfunktionen von Unternehmen aus der Cloud stammen werden. Daran dürfte die E-Mail-Verschlüsselung einen spürbaren Anteil haben.

Oliver Schonschek

Hybrid-Ansatz zur E-Mail-Verschlüsselung

Interne E-Mail-Sicherheit für externe Cloud-Dienste

E-Mails aus der Cloud und Verschlüsselung aus dem eigenen Netzwerk, dieser Hybrid-Ansatz kombiniert die Cloud-Vorteile mit der internen Sicherheit.


Bild: Scanrail - Fotolia.com

Als größtes Hindernis bei der weiteren Verbreitung von Cloud Computing gelten die Sicherheitsbedenken, wie zum Beispiel das Kompetenzzentrum Trusted Cloud betont. Viele Unternehmen verzichten auf die Flexibilität und Kostenvorteile einer Cloud-Lösung, weil sie fürchten, die Datenschutzanforderungen nicht erfüllen zu können. Gerade bei E-Mail-Diensten liegt es auf der Hand, dass personenbezogene Daten von möglichen Sicherheitslücken einer Cloud-Implementierung betroffen sein könnten. E-Mail-Adressbücher mit Kontaktdaten und E-Mail-Nachrichten mit vertraulichem Inhalt bedürfen im Outsourcing eines besonderen Schutzes.

Cloud-Mail zusätzlich zum eigenen Mailserver

Doch auch Unternehmen, die lieber einen eigenen Mailserver betreiben, können mit den möglichen Risiken von Cloud-basierter Mail in Berührung kommen. Cloud-Dienste aus dem CRM-Bereich haben in aller Regel eine E-Mail-Funktion. Business-Intelligence- oder Sicherheitslösungen aus der Cloud übertragen zumindest Berichte per E-Mail, eine ebenfalls nicht unkritische E-Mail-Anwendung.

Es hilft dann scheinbar wenig, wenn man die E-Mails von dem eigenen Mailserver sicher verschlüsselt, die E-Mails aus den Cloud-Lösungen aber nicht im eigenen Verschlüsselungskonzept berücksichtigt sind.

Insourcing statt Outsourcing

Es ist aber möglich, die interne E-Mail-Verschlüsselung auch für die E-Mails aus bestimmten Cloud-Lösungen zu verwenden. Anstatt die E-Mail-Verschlüsselung im Outsourcing in die Cloud zu verlagern, holt man die Verschlüsselung der Cloud-Mails in das eigene Unternehmen. Tatsächlich

erwarten verschiedene Analysten eine Zunahme eines solchen Insourcings, wenn Unternehmen glauben, die Schwierigkeiten der Cloud-Sicherheit nicht bewältigen zu können.

Umleitung zur Verschlüsselung

Lösungen wie PerspecSys PRS MTA, Teil des PerspecSys Cloud Data Protection Gateway, verbinden die Nutzung von Cloud-Diensten mit dem Einsatz der internen E-Mail-Sicherheit. Grundsätzlich nimmt ein Mail Transfer Agent (MTA) die E-Mails der Absender entgegen und sorgt für das Routing zu den Empfängern.

Bei PerspecSys PRS MTA stellt der MTA letztlich die gewünschte Verknüpfung zwischen Cloud-Vorteilen und interner E-Mail-Sicherheit her. Die von dieser Lösung unterstützten Cloud-Dienste wie Salesforce.com erhalten durch PerspecSys PRS MTA Zugang zu dem internen Mailserver des Anwenderunternehmens. Die für die E-Mail-Dienste der Cloud-Lösung erforderlichen Kontaktdaten müssen dann zum Beispiel nicht in der Cloud-CRM-Lösung vorgehalten werden.

In Verbindung mit dem PRS MTA Server kann der Mail Transfer Agent sicherstellen, dass alle entsprechenden Cloud-Mails des Unternehmens durch den eigenen E-Mail-Server geleitet werden. Dabei können alle E-Mail-Richtlinien zum Einsatz kommen, neben der E-Mail-Verschlüsselung auch die Suche nach Malware und Spam. Im Prinzip sorgt der MTA also dafür, dass die E-Mails aus den Cloud-Lösungen so behandelt werden, als seien sie von einem internen E-Mail-Client erstellt worden.

Insourcing für die einheitliche E-Mail-Verschlüsselung

Die Integration von eigenem Mailserver und Cloud-Dienst macht eine durchgehende, einheitlich definierte E-Mail-Verschlüsselung möglich. Voraussetzung ist jedoch, dass auch wirklich alle genutzten Cloud-Dienste über den Mail Transfer Agent angeschlossen werden können. Ausnahmen führen letztlich zu möglichen Brüchen im Verschlüsselungskonzept.

Bei der Definition der E-Mail-Richtlinien sollte zudem daran gedacht werden, dass sie auch für die E-Mail-Funktionen der Cloud-Dienste gelten sollen, also auch zum Beispiel die dort geltenden Anforderungen an Verfügbarkeit berücksichtigen müssen.

Insourcing nur mit sauberer Integration

Wenn eine sichere E-Mail aus der Cloud-Anwendung verschickt werden soll, muss die Verbindung zum internen Mailserver stehen. Dies sollte bei dem Monitoring und der Kontrolle des Mailservers ebenfalls bedacht werden. Wenn der Fall eintritt, dass keine sichere E-Mail-Funktion für den Nutzer des Cloud-Dienstes zur Verfügung steht, muss dies auch durch eine entsprechende Fehlermeldung ersichtlich sein und in dem Reporting für den Cloud-Dienst zu finden sein.

Fazit

Eine interne E-Mail-Sicherheit für externe Cloud-Dienste stellt hohe Anforderungen an die Integration zwischen Mailserver und Cloud. Werden diese nicht erfüllt, würden die möglichen Sicherheitsprobleme aus der Cloud gegen handfeste Integrationsprobleme eingetauscht. *Oliver Schonschek*