10 | 19 Sonderdruck für Ciphermail

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Verschlüsselung mit Ciphermail

www.it-administrator.de

Verschlüsselung mit Ciphermail

Schlüsselverwalter

von Thomas Zeller

Mit einem Encryption Gateway kann der Administrator die automatische Ver- und Entschlüsselung von E-Mails steuern und das Schlüsselmaterial zentral verwalten. Das reduziert den Supportaufwand und schont die Nerven der Anwender – denn sie bekommen von der Verschlüsselung gar nichts mit. Ciphermail ist ein leistungsfähiges Encryption Gateway aus den Niederlanden. Wir stellen das System und dessen Inbetriebnahme vor.

Quelle: Oleg Sinitsa – 123RF

Damit vertrauliche Informationen auch dann vertraulich bleiben, wenn sie per E-Mail versendet werden, empfiehlt sich der Einsatz einer Lösung zur E-Mail-Verschlüsselung. Mit (Open) PGP und S/MIME stehen dafür seit Jahren etablierte und sichere Standards zur Verfügung. Die Benutzer sind beim Einsatz dieser Technologien am Desktop jedoch häufig überfordert und mit der Unterstützung von Clients für mobile Geräte steht es ebenfalls nicht zum Besten. Es ist daher naheliegend, die Verschlüsselung über ein Encryption Gateway zu realisieren. Hier kommt Ciphermail - vormals unter dem Namen Djigzo bekannt – ins Spiel.

Große Auswahl an Encryption-Standards

Ciphermail unterstützt die folgenden Verschlüsselungsstandards:

- TLS
- S(ecure)/MIME
- OpenPGP
- PDF encrypted E-Mail

Während TLS der Sicherung des Transportwegs bei der Übertragung von Nachrichten zwischen Mailservern dient, bieten S/MIME und OpenPGP eine Verschlüsselung der E-Mail selbst. Für die Verschlüsselung und Signatur setzen beide Verfahren auf ein asymmetrisches Verschlüsselungsverfahren beziehungsweise eine Public-Key-Infrastruktur (PKI). Während S/MIME mit X.509 Zertifikaten arbeitet, nutzt OpenPGP ein eigenes (und zu älteren PGP-Versionen abwärtskompatibles) Schlüsselformat.

Beide Standards setzen voraus, dass auf Sender- und Empfängerseite jeweils ein Schlüsselpaar bestehend aus öffentlichem und privatem Schlüssel respektive Zertifikat vorliegt. Ist dies nicht gewährleistet, kann Ciphermails PDF-Verschlüsselung als "symmetrisches" Verschlüsselungsverfahren eine gute Alternative darstellen. Dabei werden Inhalt und Attachments von E-Mails in eine passwortgeschützte PDF-Datei verpackt, der Empfänger muss zum Öffnen und Lesen der Nachricht das zugehörige Passwort eingeben.

Optional kann Ciphermail mithilfe eines Zusatzmoduls auch einen Webmailer bereitstellen, bei dem der Empfänger zum Abrufen der Nachrichten lediglich einen Webbrowser benötigt. Ciphermail verfügt zudem über ein eingebautes Modul zur Data Leakage Prevention (DLP). Mit diesem lässt sich der ausgehende E-Mail-Verkehr auf Schlüsselbegriffe (Text) oder mit Hilfe von Regular Expressions untersuchen.

Blick in die Systemarchitektur

Das Ciphermail-Gateway basiert auf den Open-Source-Komponenten Postfix, OpenJDK, ANT und Tomcat und unterstützt mit PostgreSQL, MySQL/MariaDB und Oracle gleich drei relationale Datenbanksysteme. Es läuft auf Ubuntu, Debian, RedHat, CentOS und SUSE. Die DEB- und RPM-Packages wurden laut Hersteller unter Ubuntu 16.04, Debian 9, RedHat/CentOS 7 und dem SuSE Linux Enterprise Server 12 getestet. Die Installation kann entweder als virtuelle Appliance (auf Basis eines CentOS-Systems) oder mithilfe von Distributionspaketen auf einem bestehenden Linux-System erfolgen. Anwender anderer Distributionen bedienen sich dagegen der TAR- beziehungsweise Source-Pakete, die der Entwickler im Downloadbereich der Ciphermail-Webseite [1] bereitstellt.

Für die Installation in Cloudumgebungen wie Microsoft Azure oder Amazon Web Services existieren derzeit noch keine nativen Versionen. Soll Ciphermail in der Cloud laufen, können Sie stattdessen eine Linux-VM und die entsprechenden Distributions- beziehungsweise Installationspakete nutzen. Die Lizenzierung erfolgt dabei analog zur On-Premises-Installation.

Bild 1: Ciphermail unterstützt zahlreiche Methoden für die E-Mail-Verschlüsselung. Diese werden global definiert und können dann für jeden Benutzer individuell angepasst werden.

Wahl des Betriebsmodus

Vor der Installation von Ciphermail steht die Überlegung, wie Sie das Encryption Gateway in das E-Mail-Routing integrieren wollen. Ciphermail kennt drei verschiedene Betriebsmodi:

Die einfachste Möglichkeit ist die direkte Zustellung. In diesem Szenario wird das Gateway zwischen dem internen Mailserver (etwa Exchange) und dem Internet platziert. Der interne Mailserver routet Nachrichten an externe Empfänger an Ciphermail, das den Ziel-Mailserver mithilfe von MX Lookups identifiziert und die E-Mails entsprechend ausliefert. Umgekehrt nimmt Ciphermail E-Mails für Empfänger der konfigurierten E-Mail-Domains aus dem Internet entgegen und routet die Nachrichten dann an den internen Mailserver weiter.

Die zweite Option: In vielen Unternehmensnetzwerken ist bereits ein E-Mail-Relay oder Frontend-Server vorhanden, zum Beispiel eine Firewall oder ein E-Mail-Relay beim Internetprovider. Ciphermail kommt in diesem Fall zwischen dem internen Mailserver und dem E-Mail-Relay zum Einsatz. Letzteres übernimmt in diesem Fall die Zustellung der Nachrichten per MX Lookup und nimmt E-Mails aus dem Internet entgegen. Ciphermail kann sich dabei per SASL (Simple Authentication and Security Layer) am E-Mail-Relay beziehungsweise Frontend-Server authentifizieren.

Eine dritte Variante findet sich, wenn ein Virenscanner zum Einsatz kommt. In verschlüsselten E-Mails kann naturgemäß keine Virenprüfung durchgeführt werden. Kommt ein Scanserver zum Einsatz, liefert der interne Mailserver seine E-Mails daher zunächst an den Virenscanner, der sie dann an das Ciphermail-Gateway weiterleitet.

Dieses kümmert sich wiederum um die Zustellung per MX Record oder leitet E-Mails wie oben beschrieben an ein weiteres E-Mail-Relay oder einen Frontend-Server weiter.

Für diesen Workshop haben wir die virtuelle Enterprise-Appliance im internen Netzwerk installiert und als E-Mail-Relay für den internen Mailserver eingetragen. Die E-Mail-Zustellung an externe Empfänger übernimmt in unserem Test-Setup ein Smarthost im Internet. Ciphermail meldet sich per SASL-Authentifizierung am Smarthost an.

Schnelles Setup mit virtueller Appliance

Haben Sie sich entschieden, in welchem Setup Sie Ciphermail betreiben wollen, installieren Sie das Encryption-Gateway an der entsprechenden Position im E-Mail-Fluss. Am schnellsten sind Sie dabei mit der virtuellen Appliance am Start. Die Community Edition steht in einer Version für VMware und Hyper-V auf der Ciphermail-Webseite zum Download bereit [2].
Unternehmen, die eine Professional- oder Enterprise-Lizenz erworben haben, erhalten dagegen ein Login für das Supportportal und können die Enterprise-Version von Ciphermail dort herunterladen. Die virtuelle Appliance für VMware (ESX & ESXi ab Version 5, VMware Workstation oder VMware Player) läuft problemlos auch unter Virtualbox beziehungsweise KVM – Ciphermail lässt sich zum Testen also schnell mithilfe eines Desktop-Hypervisors aufsetzen.

Aus Sicherheitsgründen bezieht die virtuelle Appliance nicht automatisch per DHCP eine IP-Adresse. Nach dem Start der VM müssen Sie sich daher zunächst in der Konsole mit dem Benutzernamen und Passwort "sa" einloggen, um die Netzwerkkonfiguration vorzunehmen. Dank eines textbasierten Konfigurationsmenüs gehen diese Schritte leicht von der Hand. Wählen Sie im Menü "Config / Keyboard" zunächst einen deutschen Tastaturtreiber und stellen Sie unter "Config / Timezone" die Zone "Europe/Berlin" ein. Danach wählen Sie "Config / Network" und wählen die angebotene Ethernet-Schnittstelle (in unserem Fall "enp0s17") aus. Entscheiden Sie, ob Ciphermail die Netzwerkkonfiguration per DHCP beziehen soll oder tragen Sie IP-Adresse, Gateway, Netzmaske und Broadcast manuell ein.

Nachdem Sie die Konfiguration per "Apply" aktiviert haben, können Sie sich unter der URL "https://<IP-Adresse>" mit dem Benutzernamen und Passwort "admin" in die Weboberfläche von Ciphermail einloggen. Als erste Amtshandlung sollten Sie unter "Admin / Add Admin" einen personalisierten Admin-User mit den Berechtigungen "ROLE_ADMIN" und "ROLE_LOGIN" anlegen. Da sich der Default-Admin-User leider nicht deaktivieren lässt, sollten Sie diesem aus Sicherheitsgründen ein langes und komplexes Passwort zuweisen. Ciphermail bietet verschiedene Admin-Rollen an – so können Sie im Bedarfsfall weitere Admins mit beschränkten Rechten hinzufügen.

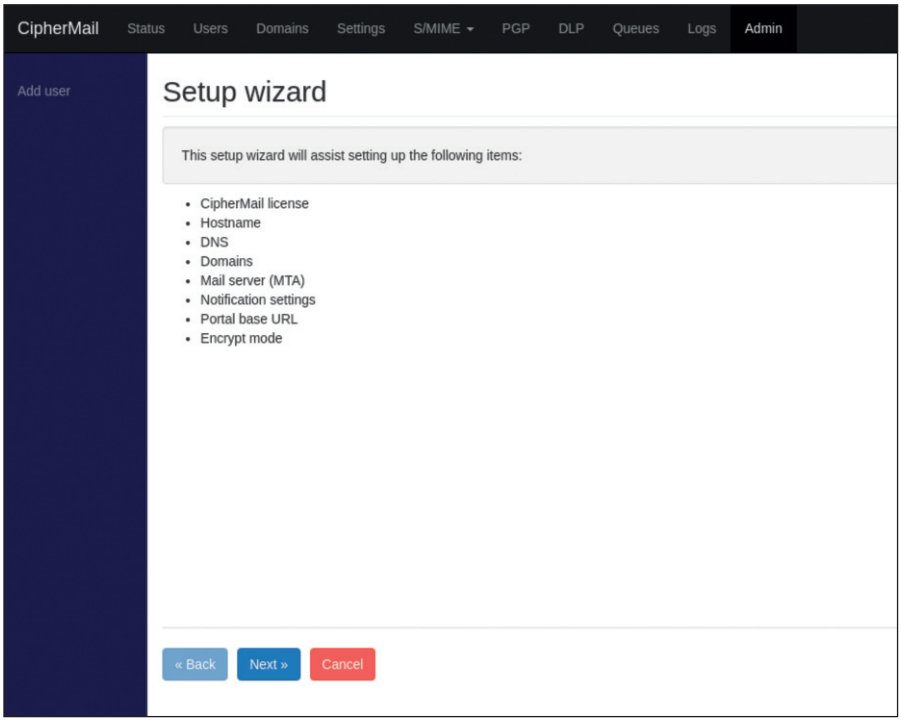

Bild 2: Ciphermail bietet eine Reihe von Wizards, mit denen Grundfunktionen und Verschlüsselung schnell eingerichtet sind.

Konfiguration per Wizard

Nach dem ersten Login erschlägt die Vielzahl der angebotenen Optionen. So fördert ein Klick auf das Admin-Menü gleich elf Submenüs zu Tage, die ihrerseits wiederum bis zu elf Unterpunkte enthalten. Daher empfiehlt es sich, die Grundkonfiguration mit Hilfe der Wizards durchzuführen. Wählen Sie zunächst das Menü "Admin / Other / Wizards" und klicken Sie unter "Category" auf "Setup Wizards". Markieren Sie in der Liste den "Initial Set-up Wizard" und klicken Sie dann auf "Start Wizard".

Ciphermail fragt nun in mehreren Dialogen alle erforderlichen Parameter ab, um eine valide Grundkonfiguration für den Mail Transfer Agent (MTA) und das E-Mail-Routing zu erzeugen. Im letzten Dialog des Wizards können Sie den Default-Encryption-Modus einstellen, hier sollten Sie zunächst "No Encryption" wählen und den Assistenten abschließen. Möchten Sie für das Web-GUI und den SMTP-Server ein offizielles SSL/TLS-Zertifikat nutzen, führt Sie der TLS/SSL-Import-Wizard schrittweise durch den Installationsprozess.

Aktivierung der Verschlüsselungsmethoden

Im Anschluss starten Sie den "Encryption Setup Wizard", mit dessen Hilfe Sie die Verschlüsselungsverfahren festlegen können, die Ciphermail für die E-Mail-Verschlüsselung verwenden soll. Aktivieren Sie hier am besten alle drei angebotenen Verfahren: S/MIME, PGP und PDF Encryption. Bei der Frage zum PDF Encryption Mode sollten Sie sich zunächst für "Send to originator" entscheiden. Mit dieser Einstellung erzeugt Ciphermail für jedes verschlüsselte PDF ein neues Passwort und sendet es an den Verfasser der E-Mail. Dieser kann das Passwort dann auf einem sicheren Kanal an den Empfänger übermitteln. Die anderen Methoden (Static und OTP) behandeln wir noch.

Da wir ausgehende E-Mails per Default nicht verschlüsseln, benötigen wir nun noch einen Mechanismus zum "Triggern" der Verschlüsselung. Dafür legen Sie im Dialog "Encryption subject trigger" ein Keyword für die Betreffzeile, zum Beispiel "#crypt", fest. Findet Ciphermail diesen Begriff in der Betreffzeile einer ausgehenden E-Mail, verschlüsselt es die betreffende E-Mail. Setzen Sie das Häkchen bei "Remove Match", entfernt Ciphermail das Trigger-Wort anschließend wieder aus dem Betreff, sodass es beim Empfänger nicht sichtbar ist.

Haben Sie alle drei Verschlüsselungsverfahren aktiviert, nutzt Ciphermail zur Verschlüsselung standardmäßig die folgende Reihenfolge:

1. S/MIME
2. PGP
3. PDF
4. Webmail

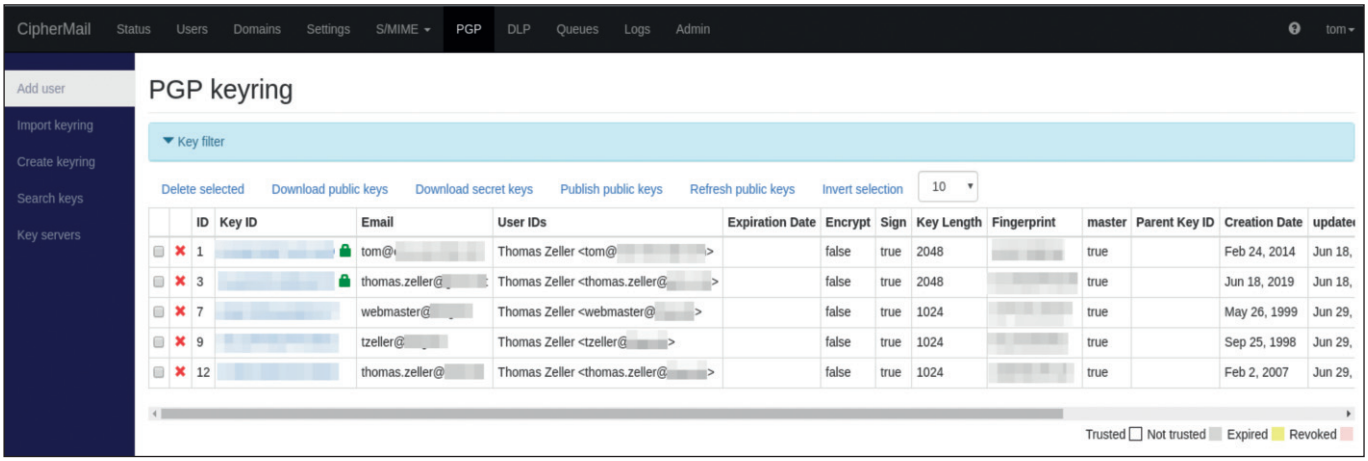

Bild 3: PGP-Schlüsselbünde können entweder direkt auf Ciphermail erstellt oder importiert werden. Keyrings mit privatem Schlüssel kennzeichnet Ciphermail mit einem grünen Schloss-Symbol.

Bild 4: Auskunftsfreudig – Ciphermail schreibt ausführliche und lesbare Logdateien.

Ist für einen Empfänger ein S/MIME-Zertifikat vorhanden, verwendet Ciphermail also primär diese Verschlüsselungsmethode. Liegt weder ein S/MIME-Zertifikat noch ein PGP-Key vor und findet Ciphermail das Trigger-Wort in der Betreffzeile, wird die E-Mail vor dem Versand per PDF-Encryption verschlüsselt. Diese Reihenfolge ist vom Hersteller vorgegeben, lässt sich aber prinzipiell über den Mailflow-Mechanismus auch an die eigenen Bedürfnisse anpassen. Der Mailflow ist in der Konfigurationsdatei "/usr/share/djigzo/conf/james/SAR-INF/config.xml" hinterlegt und in der Dokumentation [3] beschrieben. Die meisten Organisationen werden sich damit aber wohl nicht auseinandersetzen müssen. Denn Ciphermail erlaubt es, für jeden Empfänger individuell festzulegen, welches Verschlüsselungsverfahren es bevorzugt nutzen soll.

E-Mail-Routing mittels Testmail überprüfen

Bevor wir nun das E-Mail-Routing zum ersten Mal testen, müssen wir noch die Authentifizierung per SASL an unserem Smarthost im Internet aktivieren. Dazu legen Sie den Smarthost zunächst mit seinem Hostnamen oder IP-Adresse unter "Admin / MTA / SASL / Add password" an und tragen die erforderlichen Credentials ein.

Für den Versand einer Testmail nutzen Sie dann am besten den integrierten SMTP-Client unter "Admin / Other / Send email", um den internen Mailserver zu umgehen. Den Versand der Testmail können Sie dann live über "Logs / MTA" mitverfolgen. Wenn dieser Schritt erfolgreich war, senden Sie eine weitere Testmail über Ihren internen Mailserver und überprüfen, ob Ciphermail diese korrekt routet.

Schlüssel und Zertifikate importieren oder generieren

Die asymmetrischen Verschlüsselungsverfahren S/MIME und PGP arbeiten jeweils mit einem öffentlichen und einem privaten Schlüssel. Diese müssen Sie auf dem Ciphermail-Gateway hinterlegen, damit es die Ver- und Entschlüsselung und das Signieren von Nachrichten anstelle des Benutzers vornehmen kann. Für die Verwendung von S/MIME müssen Sie zunächst entscheiden, ob Sie Ihre Benutzer mit offiziellen oder selbstsignierten Zertifikaten ausstatten wollen. Offizielle S/MIME Zertifikate können Sie entweder bei Resellern wie der PSW Group oder direkt bei einer Certificate Authority (CA) wie GlobalSign oder Comodo erwerben.

Für den Einsatz kommerzieller Zertifikate spricht, dass sich auf Empfängerseite die Zertifikatsgültigkeit anhand der Signatur der CA überprüfen lässt. Entscheiden Sie sich dagegen für den Betrieb einer eigenen CA und die Ausgabe selbstsignierter Zertifikate, ist auf Seiten des Empfängers die Gültigkeit der Zertifikate nur dann überprüfbar, wenn dort zuvor Ihre Root-CA hinterlegt wurde. Ciphermail bringt eine eigene CA mit, deren Einrichtung die Dokumentation unter [4] beschreibt.

Lizenzierung und Preise

Das Ciphermail-Gateway steht in drei verschiedenen Versionen zur Verfügung.

Die kostenfreie Open-Source-Community-Edition bietet die grundlegenden Verschlüsselungs- und DLP-Funktionen und erlaubt den Betrieb für ein unlimitierte Anzahl an Benutzern. Support und verschiedene Komfort- und Personalisierungsfunktionen sind in dieser Version nicht enthalten. In der Lizenz für die Professional-Edition (4500 Euro im ersten Jahr, 1500 Euro in jedem weiteren) ist bereits ein Support-Paket enthalten. Gegen Aufpreis lässt sich der Webmail-Messenger an das Gateway anbinden.

Kunden mit Enterprise-Lizenz (9500 Euro im ersten Jahr) erhalten Silver-Support und können Enterprise-Features wie HSM-Module, Remote-CA-Konnektoren und externe Datenbanken inklusive HA-Clustering für Oracle beziehungsweise den Galera Cluster für MySQL nutzen. Der Webmail-Messenger ist in der Enterprise-Lizenz kostenfrei enthalten. Für kleinere Unternehmen hat der Hersteller eine preiswertere SME-Edition angekündigt. Der deutsche Ciphermail-Partner und Linux-Systemhaus in-put bietet indes vorinstallierte Appliances mit Ciphermail in der Community-Edition zu einem Preis ab 700 Euro an.

Listing: Entscheidungsprozess bei der Verschlüsselung

```
INFO The subject contains the "must encrypt" trigger for the sender and will therefore be
  encrypted; Recipients: [info@company.xy]
INFO must encrypt mail attribute is set; Recipients: [info@company.xy]
INFO There are no valid S/MIME encryption certificates for the recipient(s); Recipients:
  [info@company.xy]
INFO There are valid PGP encryption keys for recipient(s); Recipients: [info@company.xy]
INFO Trying to PGP/MIME sign the message; Recipients: [info@company.xy]
INFO Message was PGP/MIME signed. Hash algorithm: SHA256; Recipients: [info@company.xy]
INFO Trying to PGP/MIME encrypt the message; Recipients: [info@company.xy]
INFO Message was PGP/MIME encrypted. Encryption algorithm: AES-128; Compression algorithm: ZLIB;
  Add integrity packet: true; Recipients: [info@company.xy]
```

Haben Sie dagegen ein oder mehrere offizielle S/MIME-Zertifikate für Ihre eigenen Benutzer bei einer CA erworben, importieren Sie diese über "S/MIME / Certificate Store / Import Certificates + Import keys" in den Zertifikatsspeicher von Ciphermail. Die Professional- und Enterprise-Versionen verfügen zusätzlich über eine integrierte Schnittstelle, mit deren Hilfe Sie externe CAs auch direkt anbinden können. Die Schnittstelle unterstützt derzeit folgende Anbieter: CSR, Global Sign EPKI und Intellicard EPKI (Enterprise PKI).

Bei CSR handelt es sich um einen sogenannten "certificate request handler". Dieser generiert statt eines Zertifikats einen privaten Schlüssel und einen PKCS#12-Zertifikats-Request, der an eine Remote-CA mit CSR-Unterstützung übermittelt wird. Die CA stellt auf Basis des Requests ein S/MIME Zertfikat aus. Dieses müssen Sie anschließend manuell in den Ciphermail Zertifikatsspeicher importieren. Komfortabler geht das, wenn Sie über einen EPKI-Account bei GlobalSign oder Intellicard verfügen. Die Beantragung / Ausstellung und der Import von Zertifikaten erfolgen dann vollautomatisch. E-Mail-Zertifikate externer Empfänger enthalten nur den öffentlichen Schlüssel, daher ist in diesem Fall nur der Menüpunkt "Import Certificates" relevant.

Die Aktivierung der PGP-Verschlüsselung auf Ciphermail ist im Vergleich zu S/MIME weniger komplex, da der PGP-Standard keine offiziellen Zertifizierungsstellen vorsieht. Stattdessen werden die Schlüsselpaare – bei PGP Keyrings genannt – einfach am Client erzeugt und über die Funktion "PGP / Import keyring" in Ciphermail importiert. Enthält der Keyring neben dem öffentlichen auch einen privaten Schlüssel, muss der Admin beim Import das zugehörige Passwort angeben.

Auch im Fall von PGP gilt, dass Sie für externe E-Mail-Empfänger nur den öffentlichen Schlüssel importieren müssen. Haben Ihre internen Benutzer bisher noch keinen PGP-Keyring, erzeugen Sie diesen über "PGP / Create Keyring". Für jeden Keyring müssen Sie eine E-Mail-Adresse angeben, die von PGP als UserID zur Identifikation des Schlüssels Verwendung findet. Weitere E-Mail-Adressen fügen Sie im Bedarfsfall später in der Schlüsselverwaltung hinzu.

PDF-Verschlüsselung konfigurieren

Mit der PDF-Verschlüsselung können Sie Nachrichten auch für Empfänger verschlüsseln, die weder S/MIME noch PGP unterstützen. Sowohl den Text der E-Mail als auch die Dateianhänge verpackt Ciphermail dann in eine passwortgeschützte PDF-Datei und verschickt sie als Anhang an den Empfänger. Das Passwort zum Öffnen des PDFs wird von Ciphermail generiert und Sie müssen es auf einem sicheren Weg (zum Beispiel telefonisch) an den Empfänger übermitteln.

Alternativ kann Ciphermail das Passwort automatisch per SMS an den Empfänger senden. Für den SMS-Versand nutzt Ciphermail bekannte Provider wie Clickatell, twilio und eCall, bei denen Sie ein Kontingent an SMS-Nachrichten im Prepaid-Verfahren erwerben. Die Zugangsdaten des SMS Providers hinterlegen Sie dann zusammen mit dem API-Key unter "Admin / SMS / SMS transport / Configure". Bei Einsatz der PDF-Verschlüsselung sollten Sie beachten, dass der Betreff der E-Mail nicht codiert wird und er daher keine sensiblen Informationen enthalten sollte.

Die globalen Einstellungen für die PDF-Verschlüsselung nehmen Sie im Menü "Settings / PDF" vor. In der Pro/Enterprise-Version können Sie hier beispielsweise eine zusätzliche Titelseite mit Kontaktdaten und Unternehmenslogo einfügen. Optional kann die ursprüngliche E-Mail im EML-Format ebenfalls in das verschlüsselte PDF aufgenommen werden. Diese Funktion erlaubt es dem Empfänger, die Nachricht unverschlüsselt im Originalformat in seinem E-Mail-Client zu speichern.

Da manche PDF-Reader den Zugriff auf bestimmte Attachments blockieren – der Acrobat Reader blockt beispielsweise den Zugriff auf angehängte ZIP-Dateien –, kann Ciphermail Dateianhänge umbenennen. Fügen Sie Ihrer PDF-verschlüsselten E-Mail zum Beispiel die Datei "document.zip" hinzu, benennt Ciphermail diese in "document.zip.RENAME" um. Der Empfänger kann das ZIP-File dann lokal speichern und nach dem Rückbenennen in "document.zip" normal öffnen.

Benutzer anlegen und verwalten

Nachdem Sie die globalen Parameter für die E-Mail-Verschlüsselung konfiguriert und die Zertifikate sowie Schlüssel Ihrer

Link-Codes

[1] Ciphermail Distribution Packages
j0z11

[2] Ciphermail Virtual Appliances
j0z12

[3] Dokumentation: State Diagram
j0z13

[4] Dokumentation: Built-in CA
j0z14

E-Mail-Sender- und -Empfänger importiert haben, bestimmen Sie nun, welches Verschlüsselungsverfahren Ciphermail für externe Adressaten nutzen soll. Dazu legen Sie über "User / Add user" einen neuen Benutzer mit seiner E-Mail-Adresse an. Findet Ciphermail für diese Adresse ein S/MIME-Zertifikat und/oder einen PGP-Key, wird dieser automatisch in die Benutzerkonfiguration übernommen.

Für jeden neu angelegten Benutzer werden die zuvor global festgelegten Einstellungen gesetzt und "vererbt" (inherit). Diese Vererbung können Sie individuell für jeden Benutzer ein- oder ausschalten und auf diese Weise ein bestimmtes Verschlüsselungsverfahren aktivieren. Folgendes Beispiel soll die Arbeitsweise von Ciphermail verdeutlichen:

Für den externen E-Mail Empfänger "info@company.xy" wurde ein PGP-Key erstellt. In der Benutzerverwaltung sind die Verschlüsselungsverfahren S/MIME, PGP und PDF über die Vererbung aktiviert, das Schlüsselwort zum Triggern der Verschlüsselung (#crypt) ist ebenfalls über die Vererbung gesetzt. Senden Sie nun eine E-Mail an "info@company.xy" und nehmen den Begriff "#crypt" in die Betreffzeile auf, sendet Ciphermail diese E-Mail per PGP Signatur/Verschlüsselung an den Empfänger.

Der gesamte Entscheidungsprozess wird ausführlich dokumentiert und ist über das Logfile "Logs / MPA" nachvollziehbar. Das Listing "Entscheidungsprozess bei der Verschlüsselung" verschafft hier (in verkürzter Darstellung) einen ersten Überblick.

Ciphermail hat also automatisch den hinterlegten PGP-Key für die Verschlüsselung der Nachricht verwendet. Möchten Sie für diesen Benutzer dagegen die Verwendung der PDF-Verschlüsselung erzwingen, würden Sie in der Benutzerverwaltung in der Sektion "PGP" die Häkchen bei der Vererbung (inherit) und Aktivierung (enabled) entfernen.

Fazit

Ciphermail bietet eine sehr gute Unterstützung für die E-Mail-Verschlüsselung mit S/MIME, PGP und PDF und kann mithilfe der DLP-Funktion den Abfluss vertraulicher Daten per E-Mail verhindern. Das System lässt sich leicht in bestehende E-Mail-Routing-Szenarien integrieren und unterstützt auch Konfigurationen mit externem Mailserver wie Office 365 / Exchange online.

Bereits die kostenfreie Community-Edition bietet Gateway-basierte E-Mail-Verschlüsselung für eine unlimitierte Anzahl von Sendern und Empfängern, die Professional- und Enterprise-Editionen bringen zusätzlich interessante Funktionen wie professionellen Support, einen Updateservice, HA-Clustering und den Webmail-Messenger mit. Leider ist die Benutzeroberfläche derzeit nicht auf Deutsch verfügbar und bietet keine Suchfunktion für Einstellungen und Konfigurationsdialoge. Wer etwas Einarbeitungsaufwand in Kauf nimmt, erhält mit Ciphermail aber ein äußerst zuverlässiges und individuell konfigurierbares Encryption-Gateway. *(ln)*