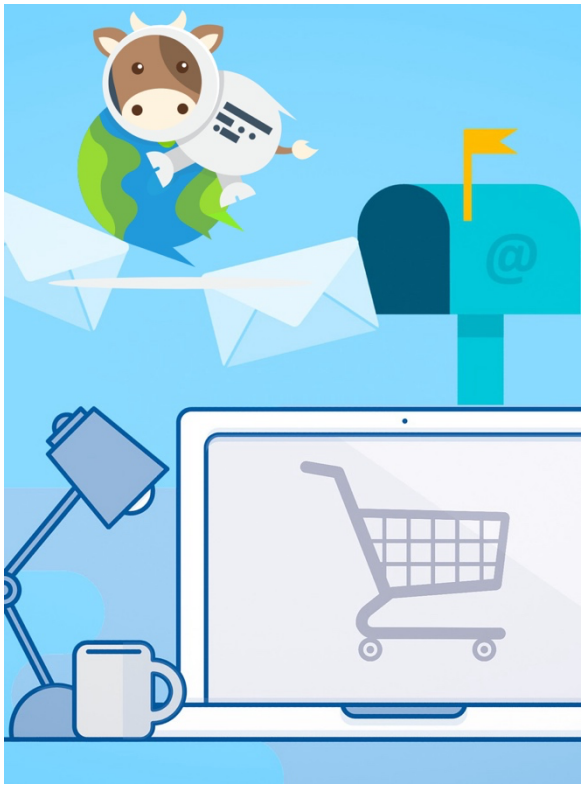
Mailpiler-Verfahrensdokumentation

Enterprise Edition



Vorwort 3
Was ist Mailpiler Enterprise? 3
E-Mails empfangen 3
E-Mails verarbeiten 4
  Parsen der E-Mail 4
  Single Instance Copy 4
  E-Mails und Anhänge speichern 5
E-Mails indizieren 5
Regeln 6
  Archivieren 6
  Aufbewahrungszeit 6
Datensicherheit 6
E-Mails löschen 7
Authentifizierung 7
Auf E-Mails zugreifen 8
Anmerkungen zur grafischen Benutzeroberfläche 9
Auditing 10
Anmerkungen zur GDPR (General Data Protection Regulation) 10
Datensicherung durch Back-ups 11
Der Rechtsrahmen 11
Änderungsverzeichnis für die Verfahrensdokumentation 12

Vorwort

Die Mailpiler-Verfahrensdokumentation wurde im April 2020 geschrieben und orientiert sich an den einschlägigen rechtlichen Anforderungen in der Bundesrepublik Deutschland, insbesondere an den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) sowie den 10 Merksätzen des VOI für eine ordnungsgemäße Aufbewahrung digitaler Dokumente.

Weiterführend Informationen, insbesondere zur allgemeinen Beschreibung, Anwenderdokumentation, technischer Systemdokumentation und Betriebsdokumentation unter http://www.mailMailpiler.org/wiki/current:index .

Was ist Mailpiler Enterprise?

Mailpiler Enterprise (https://www.mailpiler.de/) ist eine Anwendung zur E-Mail Archivierung.

E-Mails empfangen

Mailpiler empfängt E-Mails über das SMTP Protokoll. Der Mailpiler-SMTP Daemon ist auf Port 25 voreingestellt (der Wert kann konfiguriert werden) und akzeptiert alle E-Mails von jedem Remote SMTP Client der Port 25 erreichen kann.

Es ist möglich den SMTP Zugang zum Mailpiler-SMTP Daemon über hosts.allow und hosts.deny Dateien (mit Hilfe von TCP_Wrappern) zu beschränken. Auch geeignete Firewall Regeln können sicherstellen dass keine unberechtigten Hosts E-Mails ans Archiv senden können.

Zu beachten ist dass der Mailpiler-SMTP Daemon alle Verbindungen selbstständig zulassen kann, aber kein offenes Relay ist. Er empfängt E-Mails, sendet aber keine.

Mailpiler-SMTP erstellt syslog-Meldungen der SMTP Transaktionen mit veränderbarem Datenumfang, zum Beispiel Remote Host IP Adresse, Datum und Zeit, Envelope Sender, Nachrichtengröße und weist der SMTP Transaktion eine eindeutige ID zu.

Typische syslog Einträge für eine SMTP Transaktion (die quelloffene Version hat kein Customer Label):

Apr 18 07:45:08 myarchive Mailpiler-smtp[481]: connected from 172.21.0.8:40910 on fd=7 (active connections: 2)

Apr 18 07:45:08 myarchive Mailpiler-smtp[481]: received: 06L4YG5CJVVYXVK0, customer=aaa, from=sender@aaa.fu, size=29083, client=172.21.0.8, fd=7

Apr 18 07:45:08 myarchive Mailpiler-smtp[481]: disconnected from 172.21.0.8 on fd=7, reason=finished (3 active connections)

Anzumerken ist dass der Verbosity Wert in Mailpiler.conf erhöht werden kann um wortreiche Einträge zu ermöglichen.

Der Mailpiler-SMTP Daemon schreibt die E-Mail während einer SMTP Transaktion in eine temporäre Datei im Verzeichnis /var/Mailpiler/tmp. Der Dateiname entspricht der internen ID (06L4YG5CJVVYXVK0 im oben genannten Beispiel). Die Zugriffsberechtigungen auf Verzeichnis und Datei erlauben nur dem Benutzer Mailpiler Zugriff auf diese Datei. (Zu beachten ist dass der Root Benutzer ausdrücklich Zugang zum gesamten System hat.)

Nachdem die E-Mail sorgfältig auf die Festplatte geschrieben wurde sendet der Mailpiler-SMTP Daemon die interne ID an den SMTP Client mit einer 250 OK Antwort, z.B. 250 OK <06L4YG5CJVVYXVK0>.

Im Fall eines Fehlers während der SMTP Transaktion sendet der Mailpiler-SMTP Daemon einen entsprechenden Fehlercode an den SMTP Client und protokolliert ihn mit einer syslog-Meldung um sicherzustellen dass keine E-Mail verloren geht.

Der Mailpiler-SMTP Daemon unterstützt die STARTTLS SMTP Erweiterung. E-Mails sind so verschlüsselt während sie über das Netzwerk übertragen werden.

E-Mails verarbeiten

Der Mailpiler-SMTP Daemon legt neue E-Mails im Mailpiler TMP Verzeichnis (/var/Mailpiler/tmp) ab. Der Mailpiler Daemon liest dieses Verzeichnis und verarbeitet neue E-Mails so schnell wie möglich. Nach der Verarbeitung der neuen E-Mail wird die temporäre Datei von der Festplatte entfernt.

Parsen der E-Mail

Mailpiler parst die E-Mail und extrahiert die Metadaten, z.B. Absender, Empfänger, Datum, Größe, Message ID, ebenso wie die Metadaten der Anhänge (z.B. Dateiname, Größe, etc.). Alle Metadaten werden in die Mailpiler MySQL Datenbank geschrieben.

Single Instance Copy

Mailpiler speichert die E-Mail als einmalige Kopie, auch wenn sie mehrmals ans Archiv gesendet wird. Mit Bezug auf RFC 2822 sollte jede Nachricht ein Message-ID Feld haben. Der Message-ID Header hat für Mailpiler eine hohe Bedeutung. Mailpiler nutzt diesen, für eine verschickte E-Mail eindeutigen Wert, um festzustellen ob die Nachricht ein Duplikat und schon im Archiv ist. In diesem Fall verwirft Mailpiler das Duplikat und erstellt eine syslog-Meldung dass es sich bei der E-Mail um ein Duplikat handelt.

Mailpiler dedupliziert auch den Anhang. Der Anhang wird vom E-Mail Body extrahiert und separat gespeichert. Die E-Mail wird transparent zusammengesetzt bevor sie dem Benutzer dargestellt wird.

Wenn die Mitarbeiter einer Firma beispielsweise das Firmelogo in der E-Mail Signatur verwenden, wird das Firmenlogo nur in einer Kopie im Archiv gespeichert.

E-Mails und Anhänge speichern

Mailpiler verdichtet jede gespeicherte Datei (E-Mails und Anhänge) mit zlib um weiteren Platz auf der Festplatte zu sparen. Nachdem die Dateien verdichtet wurden verschlüsselt sie der Blowfish Algorithmus. Zugang zum 128 bit Chiffrierschlüssel hat nur der Benutzer Mailpiler. Ohne den Chriffrierschlüssel kann selbst ein priviligierter Benutzer den Inhalt der E-Mails nicht wieder herstellen.

Anzumerken ist dass Mailpiler E-Mails und Anhänge auch an einen S3 kompatiblen Object Store senden kann. In diesem Fall werden nur die verschlüsselten Daten an den S3 Object Store gesendet.

Außer dem verdichten und verschlüsseln findet keine weitere Veränderung des Formats statt. Eine Word Datei wird nicht in eine Textdatei oder eine PDF Datei konvertiert. Anhänge werden in Ihrem ursprünglichen Format gespeichert. Es findet auch keine Kodierung statt, z.B. bleibt ein base64 kodierter Anhang als base64 kodiert gespeichert.

Alle temporären Dateien werden entfernt nachdem E-Mail und Anhänge gespeichert wurden. Im Fall eines internen Fehlers wird die Datei Mailpiler-smtp created zur späteren Sichtung im Fehlerverzeichnis (/var/Mailpiler/error) gespeichert.

Die grafische Benutzeroberfläache stellt dem Administrator die Anzahl der fehlerhaften E-Mails dar.

Mailpiler erstellt auch syslog-Meldungen zu den Ergebnissen seiner Aktionen. Der Status kann ‘stored, ‘discarded’, ‘duplicate’ oder ‘error’ sein. Der log Eintrag für eine erfolgreich gespeicherte E-Mail:

Apr 13 18:11:36 a455f3977b50 Mailpiler[836]: 1/aaa-ABFPBO56SDC73TB6: 400000005e9ab00e034d67d400832338dd28, size=29080/12352, attachments=2, reference=, message-id=<6YLOQLOLF7R07WVJE1FS64QTW1U7FF5OMM0Y67XE@myhost.aaa.fu>, retention=2557, delay=0.04, delays=0.01/0.01/0.00/0.00/0.02/0.00, status=stored

E-Mails indizieren

Mailpiler nutzt die Software eines Drittanbieters (Sphinx Search) um ein durchsuchbares Archiv darstellen zu können. Der Parser extrahiert Textinformationen aus E-Mail und Anhängen sowie einige Informationen aus den E-Mail Headern, z.B. Betreff, Absender, Empfänger, Datum und Message ID. Die zu indizierenden Textdaten werden in eine MySQL Tabelle (sph_index) geschrieben.

Der Sphinx Indizierer wird regelmäßig aufgefordert den sph_index table zu lesen und aktualisiert die Sphinx Index Dateien. Nachdem der sph_index table verarbeitet wurde entfernt der Indexer alle verarbeiteten Reihen aus der Tabelle. Die Klartext Daten befinden sich bis zu 30 Minuten im sph_index table.

Das Sphinx Datenverzeichnis hat 0700 Zugriffsrechte um sicherzustellen das nur der Mailpiler Benutzer Zugang zu den Index Daten hat.

Zu beachten ist dass die MySQL Tabellen und die Sphinx Datenbank nicht verschlüsselt sind.

Regeln

Archivieren

Administratoren können Regeln einrichten um bestimmte E-Mails nach Betreff, Größe, Absender, Empfänger usw. zu verwerfen. Nachdem die E-Mail geparst wurde, iteriert Mailpiler die Archivregeln und prüft ob die gegebene E-Mail gegen diese verstößt. In diesem Fall verwirft Mailpiler die E-Mail und erstellt eine syslog-Meldung zu Vorgang und einschlägiger Regel. Ein Beispiel:

Apr 18 07:43:41 myarchive Mailpiler[836]: 1/aaa-S22SZU3URP71GW9T: discarding: archiving policy: *customer=fictive,domain=,from=newsletters@aaa.fu,to=,subject=,body=,size0,att.name=,att.type=,att.size0,spam=-1,days=0*

Apr 18 07:43:41 myarchive Mailpiler[836]: 1/aaa-S22SZU3URP71GW9T: 400000005e9aafb70dd6464400fe5a46aa1d, size=110529/0, attachments=1, reference=, message-id=<20151120041635.1D16E68BB67DD947@aaa.fu>, retention=0, delay=0.00, delays=0.00/0.00/0.00/0.00/0.00/0.00, status=discarded

Aufbewahrungszeit

Jede archivierte Nachricht erhält beim speichern von Mailpiler einen Wert zur Aufbewahrungszeit. Der Zeitstempel zur Aufbewahrungszeit wird in der Metadaten Tabelle gespeichert. Der Vorgabewert befindet sich im *default_retention_days* Parameter im Mailpiler.conf. Aber dieser Wert kann durch die Regeln zur Aufbewahrungszeit übersteuert werden.

Es ist wichtig zu verstehen dass der Wert zur Aufbewahrungszeit der bereits gespeicherten Nachrichten weder durch Änderung des Werts zur Aufbewahrungszeit in der Mailpiler Config Datei noch durch die Regeln zur Aufbewahrungszeit revidiert werden kann. Die neuen Werte zur Aufbewahrungszeit beziehen sich ausschließlich auf neue Nachrichten.

Der kalkulierte Wert zur Aufbewahrungszeit (in Tagen) wird mit syslog-Meldungen protokolliert.

Administratoren sollten sich nach den Vorgaben der Firma und Branche richten wenn sie die Werte zur Aufbewahrungszeit für das Archiv einrichten.

Datensicherheit

Neben der Blowfish Verschlüsselung stellen die Datei- und Verzeichniszugriffsrechte sicher dass nur der Benutzer Mailpiler Zugang zu den gespeicherten E-Mails und Anhängen hat.

Ein SHA256 Hash Wert wird beim speichern der E-Mails und Dateien für diese erstellt und gespeichert. Beim Abruf der E-Mail aus dem Archiv wird ihr SHA256 Hash Wert berechnet und mit dem in der MySQL Datenbank gespeicherten Hash Wert verglichen. Wenn es keine

Übereinstimmung gibt wird dem Benutzer mitgeteilt dass die abgerufene Nachricht nicht mit der gespeicherten Nachricht übereinstimmt.

Mailpiler speichert mehrere Zeitstempel in der Metadaten Tabelle, z.B. wenn die Nachricht gesendet wurde, wenn sie zugegangen ist und archiviert wurde, ebenso wie die Aufbewahrungszeit.

Es sei angemerkt das Mailpiler Enterprise keinem Anwender erlaubt, auch nicht den Administratoren, irgendeine archivierte Nachricht zu verändern.

E-Mails löschen

Mailpiler sichert Nachrichten bis Ihre Aufbewahrungszeit abgelaufen ist. Mit einem täglichen Vorgang bereinigt Mailpiler veraltete oder anderweitig unerwünschte Nachrichten (s.u. Anmerkungen zur GDPR).

Die Anwendung zur Bereinigung stellt eine Anfrage an die Metadaten Tabelle um herauszufinden welche E-Mails aufgrund ihrer Zeitstempel zur Aufbewahrungszeit vom Archiv entfernt werden sollen. Dann entfernt es diese physisch vom System und aktualisiert die Spalte ‘deleted’ in den Metadaten. Die Spalte ‘deleted’ weist Sphinx Search an die gelöschten E-Mails von den Suchergebnissen auszuschließen.

Angemerkt sei dass Anhänge der zu löschenden E-Mails, welche auch mit anderen E-Mails verbunden sind, nicht gelöscht werden um die Integrität der verbleibenden E-Mails sicherzustellen.

Es mag Fälle geben in denen die E-Mails einer Person erhalten bleiben sollen, auch nach Ablauf der Aufbewahrungszeit. Administratoren können diese E-Mail-Adressen in die Sperrfristen Tabelle in der grafischen Benutzeroberfläche eintragen. Die Anwendung zur Bereinigung wird diese E-Mails dann ausschließen, unabhängig vom Ablauf der Aufbewahrungszeit.

Authentifizierung

Die grafische Benutzeroberfläche erlaubt nur nach Authentifizierung Zugriff auf die E-Mails. Der Administrator des Archivs kann verschiedene Methoden zur Authentifizierung einrichten, z.B. eine lokale Datenbank, LDAP, Active Directory, Azure AD, Single Sign-On (SS0), usw. Auch die Zweifaktoren Authentifizierung wird unterstützt um die Sicherheit zu erhöhen. In diesem Fall werden die Codes zur Wiederherstellung in der Mailpiler MySQL Datenbank gespeichert.

Alle Login Versuche werden mit syslog-Meldungen protokolliert. Im folgenden ein erfolgreicher Login über eine LDAP Datenbank:

```
Apr 18 10:31:50 myarchive Mailpiler-webui[432]: ldap query: base
dn='ou=usersF,dc=nodomain',
filter='(&(objectClass=inetOrgPerson)(mail=jim@fictive.com))', attr='', 1 hits

Apr 18 10:31:50 myarchive Mailpiler-webui[432]: ldap auth against
'ldap.fictive.com', dn: 'cn=Jim Jones,ou=usersF,dc=nodomain', result: 1
```

Apr 18 10:31:50 myarchive Mailpiler-webui[432]: ldap query: base dn='ou=usersF,dc=nodomain', filter='(|(&(objectClass=inetOrgPerson)(mail=jim@fictive.com))(&(objectClass=posixGroup)(memberuid=jim@fictive.com))(&(objectClass=posixGroup)(memberuid=cn=Jim Jones,ou=usersF,dc=nodomain)))', attr='', 2 hits

Apr 18 10:31:50 myarchive Mailpiler-webui[432]: ldap auth result against ldap.fictive.com / generic_ldap: 1

Apr 18 10:31:50 myarchive Mailpiler-webui[432]: username=jim@fictive.com, customer=fictive, event='logged in', ip=172.20.0.1

Hier ein fehlgeschlagener Login Versuch:

Apr 18 10:38:07 myarchive Mailpiler-webui[431]: ldap query: base dn='ou=usersF,dc=nodomain', filter='(&(objectClass=inetOrgPerson)(mail=jim@fictive.com))', attr='', 1 hits

Apr 18 10:38:07 myarchive Mailpiler-webui[431]: ldap auth against 'ldap.fictive.com', dn: 'cn=Jim Jones,ou=usersF,dc=nodomain', result: 0

Apr 18 10:38:07 myarchive Mailpiler-webui[431]: ldap auth result against ldap.fictive.com / generic_ldap: 0

Apr 18 10:38:09 myarchive Mailpiler-webui[431]: username=jim@fictive.com, customer=fictive, event='login failed', ip=172.20.0.1

Die grafische Benutzeroberfläche unterstützt CAPTCHA um Brute Force Login Angriffe zu verlangsamen. Single Sign-On (SSO) unterstützt den passwortlosen Zugang.

Auf E-Mails zugreifen

Mailpiler ermöglicht dem Anwender über eine webbasierte grafische Benutzeroberfläche Zugriff auf die E-Mails. Die Sphinx Suchmaschine stellt die Suchergebnisse in Sekunden bereit, unter der Bedingung dass Ihr genügend Resourcen zugeteilt wurden um die Anfragen zu bedienen.

Für den das Archiv bedienenden virtuellen Host sollten die Administratoren TLS einrichten um die maximale Sicherheit zu gewährleisten. Die Administratoren sollten die grafische Benutzeroberfläche auch durch weitere Maßnahmen sichern, z.B. indem sie den Zugang auf eine Bandbreite von IP Adressen beschränkt.

Die grafische Benutzeroberfläche verfügt über eine integrierte Zugangskontrolle um auszuschließen dass ein Anwender auf die Nachrichten anderer Anwender zugreift. Auditoren
können jede archivierte E-Mail der Organisation einsehen. Wenn ein solcher Anwender nicht benötigt wird kann er gelöscht werden. Ab Version 1.4.9 wird bei Installation des Archivs kein Anwender mit Auditorenrechten mehr automatisch erstellt.

Anzumerken ist dass Auditoren Gruppen in Mailpiler's grafischer Benutzeroberfläche erstellen können. Gruppen können genutzt werden um Zugriffsrechte auf E-Mails anderer E-Mail-Adressen zu gewähren. Eine typische Anwendung von Gruppen besteht darin Zugang zu den E-Mails einer Verteilerliste zu gewähren.

Anwender können frei wählbare Suchanfragen stellen. Aber die grafische Benutzeroberfläche wendet automatisch einen Filter an um den Zugang auf eigene E-Mails zu beschränken.

Dieser Filter wird basierend auf der E-Mail-Adresse des Anwenders erstellt. Alle Suchanfragen werden mit syslog-Meldungen protokolliert, z.B.

Apr 18 10:51:42 myarchive Mailpiler-webui[433]: sphinx query: 'SELECT id FROM fictive_main1,fictive_dailydelta1,fictive_delta1 WHERE MATCH(' (@from jimXfictiveXcom | @to jimXfictiveXcom) ') ORDER BY `sent` DESC LIMIT 0,20 OPTION max_matches=1000' in 0.00 s, 15 hits, 15 total found

Anmerkungen zur grafischen Benutzeroberfläche

Anwender können Ihre eigenen E-Mails kennzeichnen oder mit Bemerkungen versehen. Diese Metadaten werden in der MySQL Datenbank gespeichert, indiziert und sind suchbar. Jeder Anwender kann nur auf seine eigenen Kennzeichnungen und Bemerkungen zugreifen.

Anwender können Suchanfragen speichern. Die gespeicherten Suchanfragen werden in der MySQL Datenbank und memcached gespeichert, sofern memcached Unterstützung freigeschaltet ist.

Das Administrator Benutzerkonto (z.B. admin@local) wird nur für den Administrator Mailpiler verwendet. Es ist kein Benutzerkonto mit Sonderrechten, insbesondere nicht mit Zugang auf die E-Mails aller anderen Anwender. Aus diesem Grund können Administratoren nicht auf das Suchmenü zugreifen.

Anwender mit Administratorenrechten können auf System Statistiken, Accounting Summary und Audit logs zugreifen, Benutzer / Gruppen Einstellungen bearbeiten sowie Regeln setzen, etc. .

Anwender können eigene E-Mails in der eigenen Mailbox wieder herstellen. Die grafische Benutzeroberfläche stellt die ausgewählten E-Mails wieder her indem sie sie an den Smarthost sendet. Zurzeit ist dieser Verkehr nicht verschlüsselt. Aber Administratoren können ein lokales SMTP Relay am Localhost einrichten und dann 127.0.0.1 als Smarthost nutzen. Unter der Voraussetzung dass der Smarthost auf das verschlüsselte Senden konfiguriert wurde, verlassen die wiederhergestellten E-Mails das Archiv nicht als Klartext.

Anwender können Ihre E-Mails als Zip oder Eml Datei herunterladen. Diese Dateien werden im Verzeichnis /var/Mailpiler/www/tmp erstellt und sofort gelöscht nachdem sie an den Anwender gesendet wurden. Die Zip und Eml Dateien sind nicht verschlüsselt.

Auditing

Die grafische Benutzeroberfläche protokolliert was die Anwender machen und wann sie aktiv sind. Jede Aktivität des Anwenders zieht einen Audit Eintrag nach sich, welchen die grafische Benutzeroberfläche in der Audit MySQL Datenbank speichert. So entsteht eine Prüfkette zu jeder Anwenderaktivität, z.B. Suche nach E-Mails, Ansicht einer E-Mail, Herunterladen einer E-Mail etc. Die grafische Benutzeroberlfäche speichert auch Log In und Log Out des Anwenders.

Die folgenden Informationen werden protokolliert:

- Zeitstempel
- Benutzername (E-Mail)
- Aktion (z.B.. ansehen, suchen, herunterladen)
- IP-Adresse
- Seriennummer der Nachricht – sofern vorhanden
- eventuelle Beschreibung

Administratoren und Auditoren können die Audit Aufzeichnungen durchsuchen und die Prüfketten als CSV Datei exportieren.

Auditing ist per Voreinstellung aktiviert. Aber Administratoren können Auditing wenn nötig deaktivieren.

Anmerkungen zur GDPR (General Data Protection Regulation)

Mailpiler erlaubt über die Einstellungen in der config-site.php Datei die Konfiguration von ENABLE_DELETE und ermöglicht Auditoren so bestimmte E-Mails aus dem Archiv zu entfernen, z.B. wenn der Anwender eine E-Mail mit personenbezogenen Daten erhält.

Mit Hilfe der Data Officer Anwendung kann der Auditor zu löschende Nachrichten kennzeichnen. Der Data Officer akzeptiert das Löschen der Nachricht und entfernt sie oder weist die Löschanfrage ab.

Der Auditor muss eine kurze Erklärung abgeben und begründen warum er die ausgewählte Nachricht löschen will. Der Data Officer muss begründen warum er die Löschung ablehnt. Beide Aktivitäten werden in der MySQL Datenbank “deleted” protokolliert. Zu beachten ist dass der Data Officer berechtigt ist zu löschende E-Mails zu sichten bevor er die Nachrichten löscht. So soll sichergestellt werden dass es sich um eine berechtigte Anfrage handelt.

Eine Nachricht die aus der grafischen Benutzeroberfläche entfernt wurde wird ausgegraut um diesen Vorgang sichtbar zu machen. Aber die Nachricht befindet sich noch im Archiv. Nur die Lösch Anwendung entfernt die gespeicherte Nachricht und Ihre Anhänge physisch von der Festplatte. Mehr zum Thema Löschen von E-Mails im Abschnitt “E-Mails löschen” weiter oben.

Datensicherung durch Back-ups

Der Archiv Administrator ist für das Erstellen regelmäßiger und sicherer Backups der archivierten Daten, unter Berücksichtigung der Anforderungen der Firma und der betreffenden Branche, verantwortlich.

Der Rechtsrahmen

Der Rechtsrahmen für die E-Mail Archivierung unterscheidet sich von Land zu Land und von Branche zu Branche. Lassen Sie sich rechtlich beraten wenn Sie verpflichtet sind E-Mails zu archivieren.

Im folgenden eine nicht abschließende Liste von Rechtsquellen zum Thema revisionssichere E-Mail Archivierung.

- Handelsgesetzbuch §§ 238, 239, 257 HGB
- Ordnungsvorschriften des $147 AO
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- Umsatzsteuergesetz (UStG)
- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetze (LDSG)
- Gesetz zur Kontrolle und Transparenz Unternehmensbereich (KonTraG)
- Telekommunikationsgesetz (TKB)
- Aktiengesetz (AG)
- Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)
- General Data Protection Regulation (GDPR)
- Signature Act §15
- Sarbanes-Oxley Act (SOX)
- Federal Rules of Civil Procedure (FRCP)
- Basel II Direktive

Änderungsverzeichnis für die Verfahrensdokumentation

Erstellt am 2020.04.20.