Actisis IT consulting

Ihr zuverlässiger IT-Dienstleister

Möglichkeiten der E-Mail Archivierung

Dr. Andreas Heuer
Actisis GmbH, Trier

Überblick

- Einführung in die Thematik
- Lösungsszenarien
  - Appliance
  - Service
  - Software / Module für bestehende Systeme
- Funktionalitäten eines E-Mail Archivs
- Revisionssichere Archivierung

Motivation für E-Mail-Archivierung

- Erfüllung rechtlicher Anforderungen
- Compliance Regelungen
- Schutz vor E-Mail-Datenverlust
- Schutz vor Überlastung von E-Mail-Servern
  - Archiv kostengünstiger als Mail-Server
  - Retrieval einfacher als von Backups
- Sicherung von „Unternehmenswissen“

Aufbewahrungspflicht / Handelsbrief

- Pflicht des Kaufmanns Daten, Handelsbriefe und Belege über bestimmte Zeiträume aufzubewahren:
  - **10 Jahre**: Bücher, Buchungsbelege, Inventare, Bilanzen, Lageberichte
  - **6 Jahre**: Handelsbriefe, Geschäftsbriefe, E-Mails und andere digitale Dokumente
- Alles was mit dem Betrieb eines Kaufmannes zu tun hat, ist ein Handelsbrief, gleich ob er papiergestützt oder elektronisch **versandt oder empfangen** wird.

Privatsphäre / Postgeheimnis

- Automatische Abspeicherung und der Zugang zu privaten E-Mails von Mitarbeitern könnte das Postgeheimnis verletzen - E-Mails gehören per Definition zu der Kategorie „Brief“
- Lösungsansätze:
  - Kennzeichnungspflicht von E-Mails eine faktische Lösung
  - Private Nutzung des Email-Systems verbieten
  - Alle E-Mails als Geschäftsmails definieren -vertragliche Vereinbarung mit den Mitarbeitern

E-Mail-Management / Mitarbeiter

- Welche E-Mails (Dokumente) sind aufbewahrungspflichtig?
  - SOX, Basel II, SEC
  - GDPdU (*Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen*), GOB (*Grundsätze der ordnungsgemäßen Buchführung*)
  - anderen Vorschriften
  - keine Aufbewahrungspflicht
- Umgang mit E-Mails, Verteilerlisten, CC- und BCC-Felder, Attachments, Lesebestätigung, …
- Richtlinie zur E-Mail Archivierung (Geschäftsleitung)

Ziel: Integrierte E-Mail Archivierung

- E-Mails als Teil einer Menge mit einem Prozess verbundener elektronischer Dokumente
- Archivierung im Kontext zu einem Vorgang gehöriger Daten
- Wiederauffindbarkeit und Verfügbarkeit für alle berechtigten Nutzer
- Anwendung des Document-Lifecycle-Management

Ansätze zur E-Mail Archivierung

- Lösungen auf Client oder Server Basis
- Appliances
- Services (ASP / SAAS)
- Module für
  - Dokumentenmanagementsysteme
  - CRM Systeme
  - ERP Systeme
  - Enterprise Content Management (ECM)

Client oder Server Lösung

- Serverseitige Archivierung
  - E-Mails komplett vor der Zustellung archivierbar.
  - Genügt gesetzlichen Nachweispflichten.
  - Nachrichten können nicht absichtlich entfernt oder unabsichtlich gelöscht werden.
- Clientseitige Archivierung:
  - Durch den Nutzer gesichtet, bewertet und abgelegt
  - Genauere Klassifikation
  - Engere Verbindung zum jeweiligen Geschäftsprozess
  - Nachweispflicht für Vollständigkeit des Archivs
- Viele Produkte unterstützen sowohl client- als auch serverseitige Archivierung

Appliances

- „Out of the Box"-Lösung, die neben den Mail-Server gestellt wird
- Pro:
  - Compliance-tauglich; Kopie aller ein- und ausgehenden E-Mails vorhanden
  - Vergleichsweise preiswert
  - Ohne großen Aufwand zu installieren
- Contra:
  - Oft geringerer Funktionsumfang als reine Softwarelösungen
  - Weniger Anpassungsmöglichkeiten
  - Geringere Unterstützung des Endanwenders (geringere Integrationstiefe)
  - Geringere Integration mit anderen Anwendungsdaten
- Zusatzmodule (Anti-Spam, Virenscan etc.) verfügbar

Services (ASP / SAAS)

- E-Mail Archivierung als Dienstleistung
- Pro:
  - Compliance tauglich; lückenlose Archivierung aller E-Mails vor Zustellung
  - Schnell und problemlos zu realisieren
  - Einfacher Betrieb (Outsourcing)
  - Gute Skalierung mit Unternehmensgröße
- Contra:
  - Zugang über das Internet
  - Vertrauensfrage / rechtliche Situation
  - Zum Teil eingeschränkter Funktionsumfang
- Zusatzmodule verfügbar

Module für Dokumentenmanagement / CRM /ERP / ECM

- Pro:
  - Umfassende Integration der E-Mail Archivierung mit:
    - ✓ Vorgängen und Kontexten
    - ✓ Anderen Daten (strukturiert / unstrukturiert)
  - Flexibilität
  - Optionales Document Lifecycle Management
  - System(e) oft ohnehin schon vorhanden
- Contra:
  - Aufwendiger als reine E-Mail Archivierung
  - Hohe Komplexität
  - Kostenintensiv (Integration, Anpassung)

Funktionalitäten eines E-Mail Archivs

- Verarbeitung vor / bei der Archivierung
- Speicherung der E-Mails
- Retrieval von E-Mails aus dem Archiv
- Entsorgung alter E-Mails
- Schutzfunktionen für das Archiv
- Optionale Funktionalitäten / Ergänzungen

Verarbeitungsschritte im Archivierungsprozess

- Virenscan
- Filtern
- Volltextindizierung
- Kategorisierung

Qualität des Archivs wird verbessert

Speicherung der E-Mails

- Originalgetreu und unverändert auf elektronischem Medium
  - ➢ Veränderbare Medien:
    - ✓ organisatorisch und softwaretechnisch sichergestellt sein: E-Mails sind unverändert*, nicht löschbar
  - ➢ WORM bei entsprechenden Sonderregeln / Vorgaben
- Eindeutiger und unveränderbarer Indexeintrag für jede E-Mail
- Verfügbarkeit für die vorgeschriebene Dauer
- „Single Instance" Konzept
  - ➢ E-Mails
  - ➢ Attachments

* 1. Eindeutige Signatur für jedes Dokument bzw. Hashwerte von Dokumenten
2. Prozess der Signierung dokumentiert und damit eindeutig nachvollziehbar

Speicherung - Konzepte

- Rein auf rechtliche Regelungen fokussiert:
  - Kopie ziehen
  - Original dem Anwender überlassen
- Archiv als unendliche Mailbox
  - Migration aus Mailbox in das Archiv bei Erreichen bestimmter Schwellwerte
  - Platzhalter in Mailbox
- Aus Mailbox in das Archiv verschieben

Elektronische Signaturen / Verschlüsselung

- Signierte E-Mails
  - Ggf. Prüfprotokoll für Signatur
  - Archivierung der Signatur in Abhängigkeit vom Signaturverfahren
    - ✓ Message als Ganzes
    - ✓ Signatur separat
- Verschlüsselte E-Mails
  - Archivierung in entschlüsselter Form
  - Archivierung in verschlüsselter Form
    - ✓ Weitergabe z.B. an Finanzbehörden fordert Entschlüsselung
- Signierte verschlüsselte E-Mails
  - Archivierung in verschlüsselter Form zwecks Erhalt der Signatur

Retrieval

- Gesetzliche Archivierungspflicht:
  - E-Mails schnell auffindbar für Prüfer
  - Elektronisches Originalerscheinungsbild
  - Einschränkung auf Prüfgebiet (Unternehmensinteresse)
- Anwenderorientierte Archivierungssysteme:
  - Den Standard Mail-Client ergänzende Suchmasken
  - Rückladen in das E-Mail System
  - Retrieval mehr als einer E-Mail (Ordner, Gruppe etc.)
  - Hervorhebung von Schlagworten
- Zusätzliche Arbeitschritte beim Retrieval:
  - Prüfung auf Viren oder Würmer, die zum Archivierungszeitpunkt nicht detektiert wurden

Entsorgung archivierter E-Mails

- E-Mails die länger als vorgeschrieben archiviert werden, können in eine Prüfung einbezogen werden
- Bei Archivierung zwecks Erfüllung rechtlicher Vorgaben / Compliance E-Mails **automatisch** nach Ablauf der Frist durch das System löschen lassen.
- Anwenderorientiertes Archivsystem:
  - Langzeitarchiv
  - Speicherplatz erweitern
  - Bzw. Auslagerung auf preiswerteres Archivmedium

Schutzfunktionen des Archivs

- Authentisierung
  - Eigenes Login
  - Arbeitsplatz Account
  - Mail Client
- Zugriffsschutz
  - Vertreter
  - Nachfolger
  - Vorgesetzte
  - Revisoren / Auditoren
- Protokollierung von
  - Anfragen
  - Aktionen
- Verschlüsselung der archivierten Daten*
  - Geheimschutz
  - Personendaten

* Key Lifecycle Mgmt. System

Optionale Archiv-Komponenten

- Push Mail Services / Mobile Geräte
- Instant Messaging
- Indizierung
  - Nachrichtenkopf, -körper
  - komprimierte / verschlüsselte Dateien
  - Office Dateien
- Automatische Verschlagwortung
- Kategorisierung
  - Kunden, Projektgruppe/Verteiler
  - Klassifikation (vertraulich)
- Integration mit anderen Anwendungen

Revisionssichere Archivierung

Ein Archivsystem arbeitet revisionssicher, wenn vom Eingang eines Dokuments in das Archiv über den Transport bis zur endgültigen Speicherung und darüber hinaus sichergestellt ist, dass das Dokument weder verloren gehen kann noch verändert wird.

Merksätze zur revisionssicheren Archivierung*

1. Jedes Dokument muss **unveränderbar** archiviert werden
2. Es **darf kein Dokument** auf dem Weg ins Archiv oder im Archiv selbst **verloren gehen**
3. Jedes Dokument muss mit geeigneten Retrievaltechniken **wieder auffindbar** sein
4. Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist
5. Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können
6. Jedes Dokument muss in genau der **gleichen Form, wie es erfasst wurde**, wieder angezeigt und gedruckt werden können
7. Jedes Dokument muss **zeitnah wiedergefunden** werden können
8. Alle **Aktionen im Archiv**, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu **protokollieren**, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist
9. Elektronische Archive sind so auszulegen, dass eine **Migration** auf neue Plattformen, Medien, Softwareversionen und Komponenten **ohne Informationsverlust** möglich ist
10. Das System muss dem Anwender die Möglichkeit bieten, die **gesetzlichen Bestimmungen** (BDSG, HGB/AO etc.) sowie die **betrieblichen Bestimmungen** des Anwenders hinsichtlich Datensicherheit und Datenschutz **über die Lebensdauer des Archivs** sicherzustellen

* vom Verband Organisations- und Informationssysteme

Fachliche & Organisatorische Kriterien

- Ordnungsmäßigkeit
- Vollständigkeit
- Sicherheit des Gesamtverfahrens
- Schutz vor Veränderung und Verfälschung
- Sicherung vor Verlust
- Nutzung durch Berechtigte
- Einhaltung von Aufbewahrungsfristen
- Dokumentation der Verfahren
- Nachvollziehbarkeit
- Prüfbarkeit
- Testverfahren

Zusammenfassung – Technik

- Appliance / Services ASP bzw. SAAS
  - Compliance-tauglich
  - Preiswert
  - Einfach zu integrieren
  - Eingeschränkter Leistungsumfang
  - Vertrauensfrage im Fall der Services
- Software / Server / ECM
  - Mächtiger Funktionsumfang / Ganzheitlicher Ansatz
  - Document Life Cycle Management
  - Erheblicher Integrationsaufwand

Fazit

- Rechtliche / Compliance Gebenheiten bestimmen Mindestanforderungen
- Technische Ausgestaltung abhängig von den Gegebenheiten im Unternehmen:
  - Appliance
  - Service
  - Software (Spezialsoftware, CRM, ECM etc.)
  - Pflichtenheft für die Auswahl einer passenden Lösung
- Organisatorische Ausgestaltung
  - Richtlinie zur E-Mail Archivierung
  - Prozesse, Dokumentation, Nachvollziehbarkeit
  - Mitarbeiter (Umgang mit E-Mails, Private E-Mails)
  - Kategorisierung, Zuordnung zu Vorgängen, Löschen

Leistungen der Actisis GmbH

- E-Mail Archivierung
  - Beratung allgemein (Prozesse, Richtlinien etc.)
  - Erstellung von Pflichtenheften
  - Durchführung von Auswahlverfahren
  - Audits (Compliance / Sicherheit)
- IT-Sicherheit
  - Beratung / Konzepte
  - Policies & Standards
  - Audits
  - Penetration Tests