

Astaro Mail Archiving

Verfahrensdokumentation v1.0

Einführung

Astaro Mail Archiving (AMA) bietet die Archivierung von E-Mails als Dienstleistung der Astaro Services AG (Astaro) an. Hierbei werden zu archivierende E-Mails an den zentral über das Internet erreichbaren Archivierungsdienst verschlüsselt übergeben. Die E-Mails werden daraufhin indexiert, archiviert und für autorisierte Benutzer-Anfragen durch den Kunden jederzeit verfügbar gemacht.

Als cloud-basierte Lösung bietet AMA große Vorteile in Bezug auf Verwaltung, Skalierbarkeit, Verfügbarkeit und Sicherheit. Astaro hat langjährige Erfahrung mit Fragen der Internetsicherheit. Mit dieser umfassenden Expertise hat Astaro einen ganz besonderen Anspruch auf die Sicherstellung des Datenschutzes, Zugriffsschutz und Verfügbarkeit von AMA.

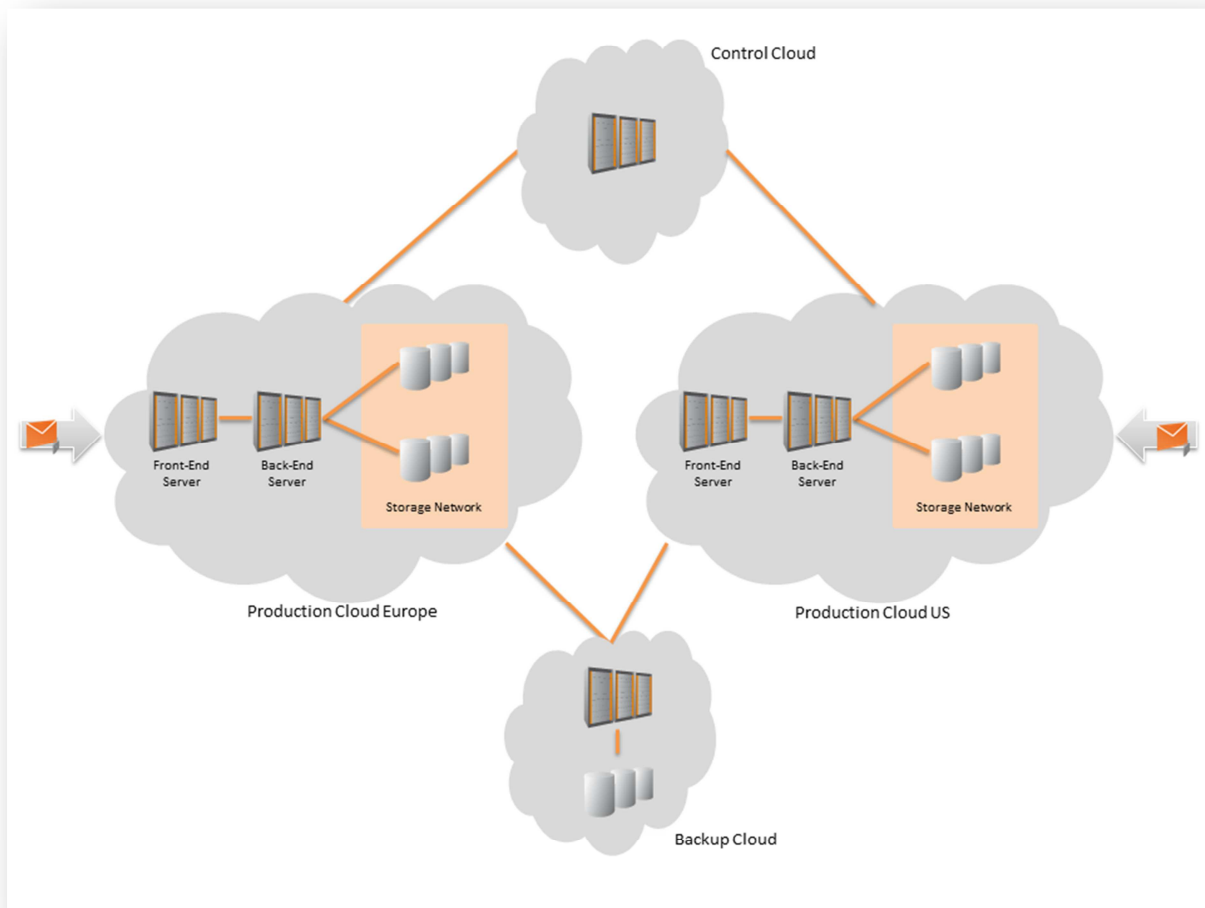
Dieses Dokument erläutert die internen Abläufe und Strukturen von AMA sowie Schutzmaßnahmen zum umfassenden Daten- und Zugriffsschutz.

Inhalt

1. Übersicht	2
1.1 Production Cloud.....	2
1.2 Backup Cloud	3
1.3 Control Cloud	3
1.4 Zugangsschutz	3
2. Prozesse	4
2.1 Datenübermittlung & Verarbeitung.....	4
2.2 Datenspeicherung	4
2.3 Datenzugriffe (User/Export/Löschung).....	4
3. Ausfallschutz & Verfügbarkeit.....	4

1. Übersicht

Die AMA-Infrastruktur setzt sich aus einer Vielzahl von Servern zusammen, die unterschiedliche Aufgabenbereiche bearbeiten.



Astaro unterscheidet hierbei zwischen Production-, Backup- und Control-Cloud welche in jeweils getrennten Hosting-Umgebungen physikalisch und geographisch getrennt arbeiten. Diese Trennung wird auch zur Gewaltenteilung eingesetzt, um Zugriffe und Daten maximal zu schützen.

Dieses Kapitel skizziert die Aufgaben der unterschiedlichen Cloud-Komponenten, bevor auf die einzelnen Prozesse weiter eingegangen wird.

1.1 Production Cloud

Astaro unterhält zwei eigenständige AMA-Infrastrukturen in den Regionen USA und Europäische Union (EU). Dabei wird sichergestellt, dass Daten eines Kunden in der EU-Region jederzeit vollständig und ausschließlich in einem EU Mitgliedsstaat gespeichert werden. Kunden aus den USA oder anderen Nicht-EU-Staaten, nutzen die AMA-Infrastruktur in den USA. Dabei gelten auch dort die gleichen Prozesse, Richtlinien und technischen Maßnahmen. Zu keinem Zeitpunkt werden Daten zwischen den Regionen ausgetauscht.

In jeder Region existiert eine komplette, redundante Produktionsumgebung. Die hochskalierbaren Server-Instanzen der Production-Cloud können jederzeit erweitert werden und sind zuständig für die Annahme, Verarbeitung sowie verschlüsselte Speicherung der E-Mails.

Innerhalb der Produktionsumgebung sind Daten-Zugriffe über die physikalischen Einzelsysteme im Rechenzentrum nicht möglich. Alle Zugriffe müssen über die Control-Cloud erfolgen. Kundenschlüssel für die kryptographische Verarbeitung der zu archivierenden E-Mails sind ausschließlich in der Control-Cloud gespeichert und Zugriff wird im System nur zum Verarbeitungszeitraum temporär gewährt.

Innerhalb der Production-Cloud werden Frontend-Server, Backend-Server sowie ein separates Storage-Network unterschieden. Alle Server arbeiten mit verschlüsselten Datenpartitionen deren Schlüssel zentral in der Control-Cloud gespeichert werden und nur zur Laufzeit übertragen werden.

Bei der Verarbeitung von Kunden E-Mails ist zusätzlich der kundenspezifische Schlüssel zur Ver- und Entschlüsselung von E-Mails nötig. Hierbei wird sichergestellt, dass dieser ausschließlich auf geschlossenen, nicht von außerhalb erreichbaren Backend-Servern abgelegt ist. Zugriffe erfolgen über spezielle Programm-Schnittstellen ausschließlich zur Laufzeit.

1.2 Backup Cloud

Die Backup-Cloud wird - geographisch von beiden Produktionsregionen getrennt - innerhalb der EU betrieben. In dieser weiteren Sicherheitsstufe werden alle archivierten Nachrichten automatisch gesichert. Die hier gespeicherten Daten sind zu jedem Zeitpunkt verschlüsselt.

1.3 Control Cloud

Eine für die Einhaltung von Datenschutzrichtlinien wichtige Komponente ist das Kontrollsystem. Dieses arbeitet ebenfalls in einer separaten Control-Cloud. Zentrale Aufgaben sind der Zugriffsschutz, Verwaltung und Hoheit über Datenschlüssel sowie Überwachung des Gesamt-Systems.

1.4 Zugangsschutz

Astaro hat umfangreiche Mechanismen zum Schutz sowohl des physischen Zugangs zu den Cloudsystemen als auch des Datenzugriffs implementiert. Das vertraglich entsprechend gebundene Astaro Betriebspersonal wurde – im Rahmen der gesetzlich erlaubten Möglichkeiten – einer Überprüfung unterzogen und sorgfältig ausgewählt.

In der Production-Cloud ist ein physischer Zugang zu den einzelnen Systemen nur dem dortigen Betriebspersonal möglich. Durch zentrale Verwaltung aller Datenzugriffe über die Control-Cloud ist vor Ort kein Zugriff auf die Daten oder eine gerichtlich autorisierte Herausgabe an Dritte möglich.

In der Backup-Cloud ist der physische Zugang zu den einzelnen Systemen nur dem dortigen Betriebspersonal möglich. Durch die reine Sicherung bereits verschlüsselter Daten kann in keinem Fall eine Verarbeitung der gespeicherten Daten oder die gerichtlich autorisierte Herausgabe an Dritte erfolgen.

In der Control-Cloud sind der physische Zugang sowie der Zugriff ebenfalls nur ausgewähltem Astaro Betriebspersonal möglich. Eine Herausgabe von Datenschlüsseln bzw. Freigabe des Datenzugriffs an Dritte kann ausschließlich im Rahmen legitimer Rechtsmittel erfolgen.

2. Prozesse

2.1 Datenübermittlung & Verarbeitung

E-Mail Nachrichten werden vom E-Mail Server des Kunden verschlüsselt an die Production-Cloud von AMA übertragen. Eine Annahme unverschlüsselter Daten wird von AMA nicht unterstützt!

Während des Annahmeprozesses sind die Daten vor Verlust und unberechtigten Zugriffen jederzeit durch eine redundante und verschlüsselte Warteschlange geschützt.

Während der Verarbeitungsphase werden die E-Mails indiziert, komprimiert und danach mit dem jeweiligen Kundenschlüssel einzeln verschlüsselt. Hierbei ist zu beachten, dass jedem Kunden ein eigener Schlüssel zugewiesen ist, die Archivdaten also immer mandantengenau abgelegt werden können. Ein versehentlicher, kundenübergreifender Zugriff auf E-Mails ist daher nicht möglich.

2.2 Datenspeicherung

Die endgültige Speicherung der archivierten Daten erfolgt verschlüsselt und redundant in hochverfügbaren Speichersystemen der jeweiligen Cloud-Region. Parallel zur Speicherung wird zum maximalen Schutz der Kundendaten eine verschlüsselte Sicherungskopie jeder archivierten E-Mail in der Backup-Cloud angelegt.

2.3 Datenzugriffe (User/Export/Löschung)

Auf archivierte E-Mails kann auf verschiedene Weisen zugegriffen werden:

- Durch berechtigte und authentifizierte End-Benutzer (bspw. Recherchezwecke)
- Durch berechtigte und authentifizierte Auditoren (bspw. zur Löschanforderung)
- Durch automatische AMA-Prozesse zur zuverlässigen Löschung von E-Mails nach Ablauf der Aufbewahrungspflicht
- Durch Exportanforderung des Archivs durch den Kunden.

Eine Authentisierung von Benutzern erfolgt entweder über Anmeldeserver des Kunden oder alternativ über lokale Benutzerdatenbanken des AMA-Systems. In allen Fällen ist zum Zugriff auf archivierte Daten der gesicherte Schlüssel zur Entschlüsselung von E-Mails nötig, welcher nur auf Backend-Servern temporär und über definierte Programmschnittstellen angefordert werden kann.

3. Ausfallschutz & Verfügbarkeit

Alle Systeme in AMA sind redundant ausgelegt und geographisch verteilt. Regelmäßige, automatische Datensicherungen gewähren darüber hinaus einen erweiterten Schutz vor unvorhergesehenen Ereignissen. Die redundante und hochskalierbare Systemarchitektur sorgt für eine ständige Verfügbarkeit und flexible Skalierung bei steigenden Anforderungen. Sowohl benötigte Server- als auch Speicherressourcen werden hierbei automatisch angepasst und gewährleisten ein performantes Zugriffsverhalten.

Wartungsarbeiten werden in der Regel so ausgeführt, dass Archivzugriffe nicht behindert werden. Bei Arbeiten, die eine kurzfristige Abschaltung von AMA erfordern, werden diese nach Ankündigung wenn möglich außerhalb der Hauptgeschäftszeiten erfolgen.