

MailStore Cloud

Cloud-native E-Mail-Archivierung
mit höchster Sicherheit



Datenschutz und Datensicherheit haben bei MailStore seit jeher höchste Priorität. MailStore Cloud überzeugt in der Hinsicht durch ein 3-stufiges Sicherheitskonzept.

1. Sicherheitsmechanismen bei der Anwendung von MailStore Cloud

MailStore Cloud verfügt über Mechanismen, die bei der Verwendung der Software für maximale Sicherheit sorgen.

- Rollenbasierte Zugriffsrechte und Multi-Faktor-Authentifizierung
- Manipulationssichere Protokollierung sämtlicher Vorgänge
- Verschlüsselung der E-Mail-Daten bei Übertragung oder Speicherung im Archiv
- Zugriff auf archivierte Daten nur über Administratoren und dedizierte Benutzer
- Kein Zugriff auf archivierte Daten durch Mitarbeiter von MailStore, OpenText oder Mitarbeitern des Rechenzentrums und etwaigier Subunternehmer

Durch die MailStore bekannten Archivierungsoptionen, Aufbewahrungsrichtlinien und Löschfunktionen, sowie der Legal Hold-Funktion und Auditor-Zugriffsmöglichkeiten ist MailStore Cloud DSGVO und IDW PS 880 (GoBD) zertifiziert.

MailStore Cloud wird fortlaufend weiterentwickelt und neue Sicherheits- und Archivierungs-features regelmäßig implementiert, um den hohen Sicherheitsstandard aufrechtzuerhalten und bei Bedarf auszubauen.

MailStore Cloud

Cloud-native E-Mail-Archivierung
mit höchster Sicherheit



2. Überwachung und Sicherheit der MailStore Cloud

MailStore Cloud verfügt über eine Reihe von Vorkehrungen, welche die Anwendung vor Einflüssen von außerhalb schützen. Dazu gehören neben Firewalls und einem Web Application Gateway auch Schutz vor DDos Attacks. Durch das „gehärtete“ Betriebssystem ist die Angriffsfläche bereits minimiert.

Darüber hinaus wird die Software von OpenText Mitarbeitern 24×7 überwacht und regelmäßig Security Scans und Penetration Tests durchgeführt. Den aktuellen Status können Sie hier einsehen: <https://status.opentext.com>.

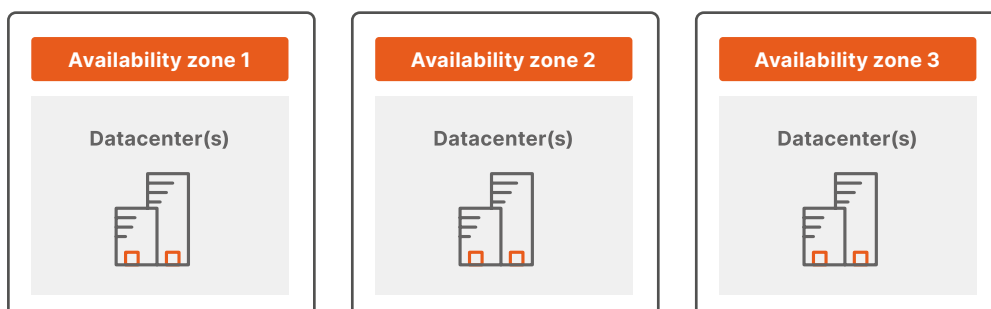
Regelmäßige Backups mit Restore-Funktion (Disaster Recovery) sorgen für zusätzliche Sicherheit.

3. Sicherheitskonzept des Rechenzentrums und der Infrastruktur

MailStore Cloud wird im Microsoft Azure Rechenzentrum Frankfurt - Azure Region Germany West Central bereitgestellt wird. Um höchste Sicherheit zu bieten, verfügt das Rechenzentrum über mehrere Sicherheitsebenen und -vorkehrungen, die durch bestimmte Prozesse im Betriebsanlauf unterstützt werden.

Netzwerkinfrastruktur, Datenredundanz, Disaster Recovery

Microsoft Azure Rechenzentren verfügen über hochleistungsfähige Netzwerkverbindungen für eine schnelle und zuverlässige Datenübertragung. Es gibt redundante Netzwerkpfade, um Ausfälle zu vermeiden. Das Azure Rechenzentrum West Central besteht aus drei einzigartigen, physisch getrennten Standorten oder „Zonen“ innerhalb einer einzigen Region, um die Verfügbarkeit durch lokal redundanten Speicher zu maximieren (Verfügbarkeit: 99,9999999999%). Mithilfe von Disaster Recovery können im Ernstfall Daten wiederhergestellt werden.



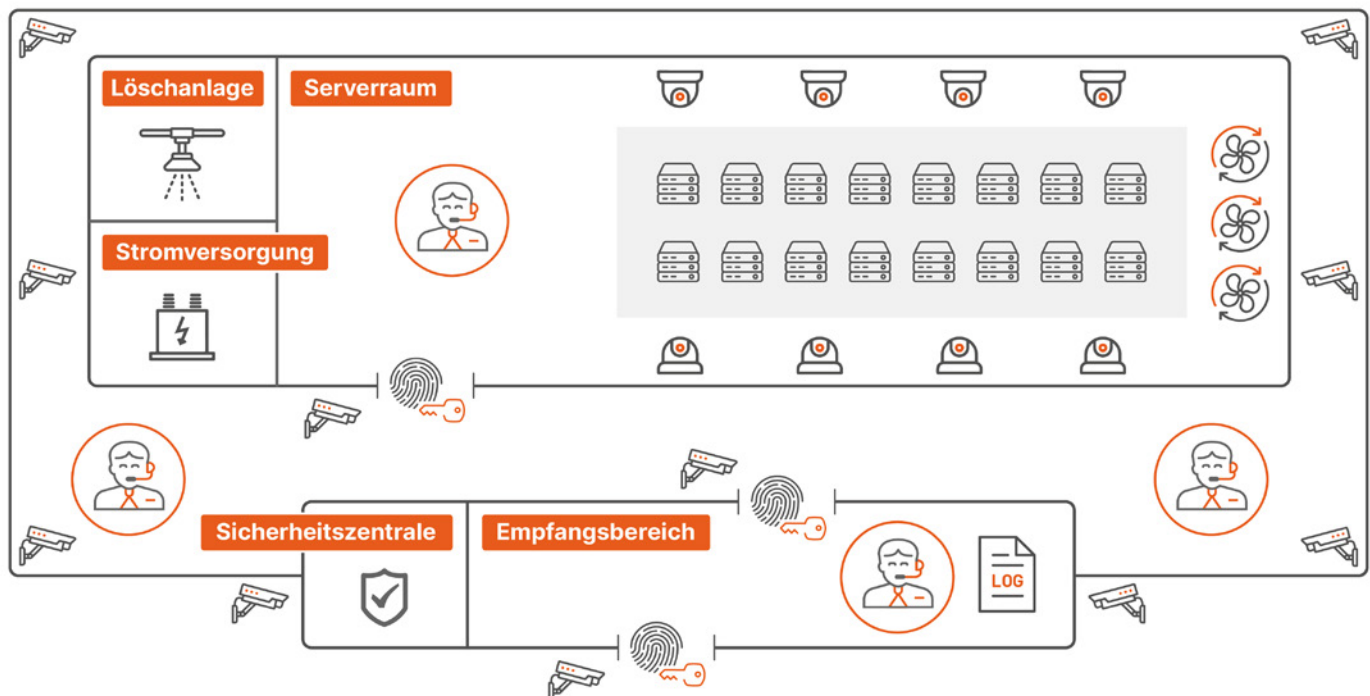
MailStore Cloud

Cloud-native E-Mail-Archivierung
mit höchster Sicherheit



Physische Barrieren

Das Gelände des Rechenzentrums ist von hohen Zäunen aus Stahl und Beton umgeben. In regelmäßigen Abständen sorgen Kameras für eine lückenlose Überwachung des Außengeländes.



Zugang zum Gelände und Protokollierung

Der Zugang zum Gelände ist mehrfach gesichert. Der Eintritt in den Empfangsbereich und der Zugang zum Innengelände ist nur über biometrische Scanner möglich. Überwachungskameras und Sicherheitspersonal sorgen für eine dauerhafte Überwachung dieser Bereiche.

Besucher müssen sich vorher anmelden, und neben der persönlichen Identifizierung auch einen Besuchsgrund nennen. Sicherheitspersonal begleitet den Besucher über die gesamte Dauer des Aufenthalts. Jeder Besuch wird in einem Logbuch dokumentiert.

MailStore Cloud

Cloud-native E-Mail-Archivierung
mit höchster Sicherheit



Zugang zum Gelände und Protokollierung

Der Zugang zum Gelände ist mehrfach gesichert. Der Eintritt in den Empfangsbereich und der Zugang zum Innengelände ist nur über biometrische Scanner möglich. Überwachungskameras und Sicherheitspersonal sorgen für eine dauerhafte Überwachung dieser Bereiche.

Besucher müssen sich vorher anmelden, und neben der persönlichen Identifizierung auch einen Besuchsgrund nennen. Sicherheitspersonal begleitet den Besucher über die gesamte Dauer des Aufenthalts. Jeder Besuch wird in einem Logbuch dokumentiert.

Serverraum

Der Zutritt zum Serverraum ist streng bewacht und gesichert. Neben einer lückenlosen Kameraüberwachung und patrouillierendem Sicherheitspersonal gewähren biometrische Scanner nur autorisiertem Personal den Zutritt zum Serverraum.

■ Stromversorgung

Das Rechenzentrum verfügt über ein redundantes Stromversorgungssystem, inklusive Notstromgeneratoren und ununterbrochene Stromversorgung (USV), um bei Stromausfällen den Betrieb aufrechtzuerhalten.

■ Brandschutz

Moderne Brandschutzsysteme, wie Gaslöschanlagen, sind installiert, um im Falle eines Brandes die Hardware zu schützen, ohne die Infrastruktur zu beschädigen.

■ Klimatisierung

Der Serverraum ist voll klimatisiert, um die Hardware vor Überhitzung zu schützen und eine optimale Betriebstemperatur zu gewährleisten. Die hochentwickelten Kühlsysteme sind redundant ausgelegt, um mögliche Ausfälle der Kühlung kompensieren zu können. Zudem gibt es spezielle Belüftungssysteme zur Optimierung der Luftzirkulation.

■ Videoüberwachung

Die einzelnen Server Racks sind videoüberwacht. Kameras filmen sowohl die Vorderseite als auch die Hinterseite der Racks für eine optimale Überwachung.

MailStore Cloud

Cloud-native E-Mail-Archivierung
mit höchster Sicherheit



Zertifizierungen

Germany C5:2020 – Ein Audit-Standard des BSI (Bundesamt für Sicherheit in der Informationstechnik), der insbesondere für öffentliche Stellen sowie Unternehmen mit hohen Sicherheitsanforderungen in Deutschland relevant ist. Azure nutzt hierfür einen kombinierten Bericht mit **SOC 2 Type 2** (AICPA), der auch C5:2020 einschließt.

- **ISO 27001:2022** – International anerkannter Standard für Informationssicherheitsmanagement.
- **ISO 22301** (Business Continuity) – Gewährleistet Resilienz und Ausfallsicherheit gegenüber Störungen oder Unterbrechungen
- **ISO 9001** (Qualitätsmanagement) – Für konsistente und prozessbasierte Qualität in Betrieb und Management.
- **PCI DSS** – Ein Standard zur Absicherung von Kartendaten, relevant z. B. bei Payment Services.
- **SOC 1 / SOC 2 / SOC 3** – Prüfberichte zur internen Kontrolle (SOC 1) sowie Sicherheit, Verfügbarkeit, Integrität etc. (SOC 2, SOC 3).

MailStore Software GmbH

Clörather Str. 1-3
41748 Viersen
Deutschland

E-Mail: sales@mailstore.com
Telefon: +49 (0)2162 - 50299-0
Fax: +49 (0)2162 - 50299-29