Sicherheitskonzept

Details zu Datensicherung

01.04.2021

www.aeb.com

Inhalt

1 Grundsätzliches zum Dokument

Dieses Dokument dient der Beschreibung von Datensicherungsmaßnahmen, die AEB vornimmt, um das Wiederherstellen von Daten zu ermöglichen.

Es fasst die zum Thema passende Informationen aus dem „Sicherheitskonzept“ der AEB zusammen und vertieft diese. Sie finden das Sicherheitskonzept in dem AEB TrustCenter (https://www.aeb.com/TrustCenter)

Als IT-Service Provider/Cloud Anbieter ist es für AEB eine Selbstverständlichkeit, Maßnahmen zu ergreifen, die für Kundendaten in unseren Rechenzentren eine hohe Verfügbarkeit sicherstellen.

Die Maßnahmen, die AEB vornimmt umfassen sowohl physische, organisatorische als auch virtuelle Maßnahmen zur Datensicherung.

Das Backup-Konzept von AEB ist in der ISO 27001 Zertifizierung beinhaltet und wird jährlich wiederkehrend auditiert. Außerdem wird es auch im Rahmen des ISAE3402 Reports jährlich geprüft.

AEB ist berechtigt, die erforderlichen Maßnahmen anzupassen, um das vereinbarte Sicherheitsniveau weiter zu verbessern und auf Stand der Technik zu halten. Die hier dargestellten Maßnahmen sind - wenn nicht anders vereinbart - übergreifend im Sinne für alle Kunden gleich ausgelegt.

Dieses Dokument dient ausschließlich der Beschreibung der Datensicherungsmaßnahmen und berücksichtigt nicht Daten, die aufgrund von Aufbewahrungsfristen archiviert wurden.

Die in diesem Dokument dargelegten Informationen sind, wie beschrieben, für alle Kunden der AEB allgemein gültig. Genaue Informationen finden Sie in Ihren Leistungsvereinbarungen und Servicebeschreibungen.

Sollten Sie weitere Fragen hierzu haben, können Sie sich an die Ihnen bekannten Ansprechpartner der AEB wenden.

2 Datensicherungsmaßnahmen im Überblick

Um die Verfügbarkeit der Daten zu gewährleisten, besitzt AEB räumlich getrennte Rechenzentren. AEB spiegelt oder kopiert Teile der Daten in einem jeweils separaten Rechenzentrum, um die Datensicherung und Verfügbarkeit zu gewährleisten.

Neben diesen physischen Maßnahmen setzt AEB auch auf virtuelle Datensicherung, um eine möglichst hohe Verfügbarkeit zu erreichen. Ergänzt werden diese Maßnahmen um Live Maßnahmen, die kurzfristige auch Wiederherstellungen ermöglichen.

2.1 Physische und virtuelle Maßnahmen zur Datensicherung

Zu den physischen und virtuellen Sicherungsmaßnahmen, die AEB einsetzt gehören:

- Hohe Verfügbarkeit durch Virtualisierung und Storagespiegelung für wichtige Anwendungen inklusive Instant Recovery Funktionalität
- Virtuelle Maschinen werden bei einem Serverausfall auf anderen Servern neue gestartet, um längere Unterbrechungen zu vermeiden
- Regelmäßiges Backup auf Server-Festplatten
  - Sicherung oder Kopieren der Daten auf den Server-Festplatten: Überschreibungsschutz auf Festplatten beträgt mindestens sechs Tage
- Regelmäßiges Kopieren der Sicherung von den Festplatten auf LTO-Bänder in ein räumlich getrenntes Datacenter
  - Überschreibungsschutz auf den Bändern beträgt vier Wochen
  - Automatische AES 256-bit Verschlüsselung der Bänder zum Schutz vor unbefugtem Zugriff
  - Wöchentliche Auslagerung der Bänder in einen Standort an einer anderen Lokation
- Anwendung eines strengen Rollenkonzeptes für die Zugangsbeschränkung zu den Backups
- Die Datensicherung und das Zurückspielen der Daten werden regelmäßig getestet. Diesbezügliche Tests, deren Ergebnisse und daraus abzuleitende Maßnahmen werden dokumentiert

2.2 Live Maßnahmen zur Datensicherung

Da die virtuellen und physischen Maßnahmen zur Datensicherung grundsätzlich nur nach einer Datenkorruption zum Einsatz kommen, greift die AEB auf Live Maßnahmen zur Datensicherung zurück, welche zum Wiederherstellen eines vorherigen Zustands dienen.

Dabei werden folgende Maßnahmen getroffen:

- Doppelte Speicherung der Datenbank LogFiles in räumlich getrennten Datacentern
- Wiederherstellung bis zu 2 Stunden rückwirkend möglich
- Die Speicherung und das Wiederherstellen von Datenbanken werden regelmäßig getestet. Diesbezügliche Tests, deren Ergebnisse und daraus abzuleitende Maßnahmen werden dokumentiert