Security Concept

Details on data backup measures

April 1, 2021

www.aeb.com

Contents

1 About this document

This document describes data backup measures AEB takes to enable data recovery.

As an IT service provider/cloud provider, it is a matter of course for AEB to take measures that ensure high availability of customer data in our data centers.

The measures AEB takes include physical, organizational, and virtual backup measures.

AEB's backup concept is included in the ISO 27001 certification which is audited annually. It is also audited annually as part of the ISAE3402 report.

AEB is entitled to adapt the necessary measures in order to further improve the agreed security level and to maintain the state of the art. The measures outlined here are, unless otherwise stipulated, general in nature in that they are the same for all customers.

This document is intended solely to describe the data backup measures and does not take into account data that has been archived due to retention periods.

This document is provided with a version and a date.

The information set forth in this document is generally applicable to all AEB customers. You can find more detailed information in your service agreements.

If you have any further questions, please contact your usual AEB representative.

2 Overview of data backup measures

To ensure data availability, AEB has physically separated data centers. AEB mirrors or copies parts of the data to a separate data center to ensure data backup and availability.

In addition to these physical measures, AEB also relies on virtual data backup to achieve the highest possible availability. These measures are complemented by live measures that also enable short-term recoveries.

2.1 Physical and virtual backup measures

The physical and virtual backup measures AEB employs include:

- High availability through virtualization and storage mirroring for important applications including instant recovery functionality
- Virtual machines are restarted on other servers in case of server failure to avoid longer interruptions
- Regular backup to server hard disks
  - Backup or copy of data on the server hard disks: Overwrite protection on hard disks is at least six days
- Regular copying of the backup from the hard disks to LTO tapes in a physically separate data center
  - Overwrite protection on the tapes is four weeks
  - Automatic AES 256-bit encryption of tapes to protect against unauthorized access
  - Weekly relocation of the tapes to a site at another location
- Application of a strict role concept for access restriction to the backups
- Data backup and restore are tested regularly. The tests, their results, and measures to be derived are documented

2.2 Live data backup measures

Since the virtual and physical data backup measures are generally only used after a data corruption, AEB resorts to live data backup measures, which are used to restore a previous state.

The following measures are taken:

- Double storage of database log files in physically separated data centers
- Recovery possible up to 2 hours retrospectively
- The storage and recovery of databases are tested regularly. The tests, their results, and measures to be derived are documented