Landesamt für Sicherheit in
der Informationstechnik

LSI-Info T#01

DATENSICHERUNG (BACKUP UND RECOVERY)

EIN GROBER LEITFADEN

Version 1.3 vom: 10.02.2020

Management Summary

Ein gut geplantes, überwachtes und regelmäßig getestetes Backup kann ein helfender Rettungsring bei kritischen Vorfällen in der IT sein und ist für die digitale Daseinsvorsorge unerlässlich.

Ein fehlendes oder fehlerbehaftetes Backup stellt ein großes Haftungsrisiko für IT-Verantwortliche und deren Vorgesetzte dar.

Diese LSI-Info soll einen groben Überblick über Backup-Strategien, Backup-Technologien und damit verbundene rechtliche Aspekte geben

DATENSICHERUNG

Für die Datensicherung müssen technische Maßnahmen und organisatorische Rahmenbedingungen definiert werden.

- Zu den organisatorischen Rahmenbedingungen gehört, dass allen Mitarbeitern der sachgemäße Umgang mit Daten und Dateien und deren Ablageort bekannt sein muss. Es sollte geregelt sein, wie Rücksicherungen (Recoveries) durchzuführen sind.
- Für ein effektives Backup werden die Daten an einer definierten zentralen Stelle abgelegt. Ein Datensicherungskonzept regelt die organisatorischen und technischen Maßnahmen, die es ermöglichen, Daten von einem zeitlich definierten Stand wiederherstellen zu können.

SICHERUNGSMEDIEN

Externe Datenträger stellen die häufigste Form der Sicherheitsmedien dar. Die zu sichernden Daten werden meist in Schwachlastzeiten (z. B. nachts und am Wochenende) auf Magnetbänder oder Festplatten kopiert.

LAGERUNG

Sicherungsmedien müssen räumlich getrennt von den Originaldaten aufbewahrt werden. Es ist unabdingbar, dass die Lagerung in einem getrennten Brandabschnitt - besser in einem anderen Gebäude und im Idealfall an einem anderen Ort (z. B. Bankschließfach) erfolgt. Der Lagerort muss den Ansprüchen an einen Server-Raum genügen.

Bedingt durch die technische Entwicklung, die damit verbundenen Möglichkeiten und aufgrund des Kostendruckes werden Cloud-Backups populärer. Die Sicherungsdaten werden dabei in einen Online-Speicher geladen und dort vorgehalten. Bei der Auswahl eines Anbieters sollte neben den angebotenen Technologien dringend auf dessen Zuverlässigkeit, zum Beispiel durch ISO 27001-Zertifizierung, internationale Verflechtungen wie der CloudAct, einen ausschließlich europäischen Serverstandort, Transport- und Inhaltsverschlüsselung vor der Übertragung sowie vertragliche Regelungen - Auftragsdatenverarbeitung - geachtet werden. Durch ein Backup in der Cloud hat man vorteilhafte räumliche Redundanz und bei Angebot entsprechender Technologien einen zusätzlichen Schutz bei destruktiver Malware wie Verschlüsselungstrojaner. Auf eine ausreichend dimensionierte Internetanbindung, die sich am jeweiligen Backup-Volumen orientiert, ist zu achten. Sofern die Datensicherung ausschließlich in der Cloud erfolgt, empfiehlt sich eine redundante und zuverlässige Internetanbindung. Lösungen, die lediglich die geänderten Blöcke einer Datei - und nicht die komplette Datei - im Rahmen eines inkrementellen Backups sichern, sollten bevorzugt werden, um die notwendige Bandbreite und Übertragungszeit gering zu halten.

SICHERUNGSMETHODEN

Neben den Sicherungsmedien stellt die Kombination der Sicherungsmethode/n für eine zuverlässige Datensicherung eine wichtige Kenngröße dar.

FULL-BACKUP

Beim Full-Backup wird der komplette Datenbestand gesichert. Hierbei wird nicht unterschieden, ob sich die Daten verändert haben. Ein Full-Backup kann einfach realisiert werden und benötigt wenig Komplexität der Backupsoftware. Es ist aber bei großen Datenmengen hinsichtlich des Ressourceneinsatzes, insb. Zeit und Größe der Sicherungsmedien, sehr aufwendig.

INKREMENTELLES BACKUP

Ein inkrementelles Backup baut immer auf der vorangegangenen Sicherung auf. Es werden wiederkehrend nur die Unterschiede zum vorhergehenden (inkrementellen) Backup gesichert. Ein inkrementelles Backup ergibt nur nach einem Full-Backup Sinn, da sonst bei Ausfall eines Mediums in der Sicherungskette eine komplette Wiederherstellung der Daten unmöglich ist. Gebräuchlich ist die Kombination von Full-Backup am Wochenende und inkrementellen Backups an allen Wochentagen.

DIFFERENZIELLES BACKUP

Es werden alle zum letzten Full-Backup veränderten Daten gesichert. Es ist daher nur in Kombination mit einem Full-Backup sinnvoll. Entsprechende Intelligenz muss dabei die Backup-Software mitbringen.

BLOCK-BACKUP

Im Gegensatz zu den voran genannten Sicherungsmethoden werden bei Block-Backups nicht die veränderten Dateien, sondern lediglich die veränderten Blöcke (kleinste Dateneinheiten von Speichermedien) gesichert. Hierdurch kann die Größe der einzelnen Datensicherung minimiert werden.

IMAGING

Das Imaging wird in der Regel bei Sicherungen von Betriebssystemen (Client, Server) angewandt. Es wird eine 1-zu-1-Kopie des Datenträgers auf einem anderen Datenträger erstellt - man spricht hier auch von einem Klon. Mit Hilfe des Klons lässt sich eine Systemumgebung relativ schnell wiederherstellen. Voraussetzung für die Wiederherstellung ist jedoch identische beziehungsweise kompatible Hardware.

SNAPSHOT

Ein Snapshot ist ähnlich dem Imaging. Hier wird jedoch zusätzlich der Systemzustand, also Inhalt und Zustand des Hauptspeichers, gesichert. Im Gegensatz zum Imaging wird der Snapshot jedoch in der Regel auf dem Quelldatenträger gespeichert. Diese Technologie ist bei virtuellen Umgebungen sehr weit verbreitet und wird vor allem vor Systemänderungen eingesetzt.

SPIEGELUNG

Bei einer Spiegelung werden die Daten parallel auf zwei identischen Datenträgern abgelegt. Eine Spiegelung sorgt daher primär für Redundanz. Beachtet werden sollte, dass auch korrumpierte Daten gespiegelt werden.

SERVERBASIERTES BACKUP

Beim serverbasierten Backup werden die Daten im Server selbst oder durch einen anderen Server auf Sicherungsmedien kopiert. Das System wird hierdurch zusätzlich belastet, weshalb Sicherungsaufträge nur in Schwachlastzeiten sinnvoll sind. Weiterhin erweist sich als nachteilig, dass bei einer in den Server integrierten Lösung auch das Sicherungssystem vom Ausfall betroffen ist.

SERVERLOSES BACKUP

Das serverlose Backup erfolgt durch einen (zeitgesteuerten) Anstoß des Servers. Hierbei werden die Daten direkt vom Netzwerk-Speicher des Servers in einen zweiten Speichertopf (z. B. über performante Fibre-Channel-Verbindungen) kopiert. Hierdurch sind sowohl die Sicherung wie auch Rücksicherung sehr performant, aber auch mit hohen Investitionskosten verbunden.

SICHERUNGSKONZEPT

Um eine effiziente Datensicherung zu realisieren, ist es notwendig, die Datenbestände zu analysieren (Schutzbedarfsfeststellung), einem regelmäßigen Review (Neubewertung) zu unterziehen, ein Datenspeicherungskonzept zu erarbeiten und dies alles zu dokumentieren. Als Ergebnis können sich durchaus hybride Formen der Sicherung von Daten ergeben, zum Beispiel Spiegelung tagsüber, nächtliches inkrementelles Backup und am Wochenende Full-Backup und Zweit-Backup in der Cloud.

3-2-1-REGEL

Es sollte die 3-2-1-Regel berücksichtigt werden: 3 Sicherungen jeder Datei auf 2 verschiedenen Medien, davon 1 an einem anderen Standort. So kann die Wahrscheinlichkeit eines Datenverlustes weitestgehend minimiert werden.

RECOVERY/RÜCKSPIELUNG

Unter Recovery wird das Rücksichern einer Datensicherung auf das Ursprungssystem oder ein Ersatzsystem verstanden. Ein Recovery sollte nie vom Originalmedium erfolgen. Durch die Nutzung einer 1-zu-1-Kopie - die gegebenenfalls mit einem autarken System erstellt wurde - kann verhindert werden, dass z. B. Ransomware das Originalbackup-Medium manipuliert.

RECOVERY-TEST

Ein Test der Wiederherstellung der Sicherungen sollte mindestens jährlich erfolgen. Hierzu wird die erstellte Sicherung auf ein Testsystem zurückgesichert und anschließend die Funktionsfähigkeit der Rücksicherung überprüft.

DISASTER-RECOVERY

Im Falle eines Disaster-Recoverys sollen die Auswirkungen eines großmaßstäbigen Datenverlustes behoben werden. Je nach Datenvolumen, technischer Kapazitäten und Investment können die hierdurch bedingten Ausfallzeiten von wenigen Minuten bis hin zu Tagen und gar Wochen liegen.

ROLLBACK-OPTION

Von einem Rollback wird gesprochen, wenn es bei oder nach einer Veränderung des Systems, beispielsweise nach Hotfix, Patch, Update, und so weiter, zu Fehlern kommt und der Ursprungszustand wiederhergestellt werden muss. In der Regel werden hier Snapshots wiederhergestellt.

RECHTLICHE ASPEKTE DER DATENSICHERUNG

Die Daten sind das Vermögen in der Informationsgesellschaft und müssen entsprechend geschützt werden. Eines der größten Haftungsrisiken für IT-Verantwortliche stellt ein fehlendes bzw. fehlerbehaftetes Backup dar. Funktionsuntüchtige Datensicherungen und der damit verbundene Datenverlust können dienstrechtliche bzw. arbeitsrechtliche Sanktionen sowie Schadensersatzanforderungen (§ 823 BGB i.V.m. § 251 Abs. 2 Satz 1 BGB; analog BGH Urteil vom 9.12.2008 - VI ZR 173/07, BGH Urteil vom 02.07.1996 - X ZR 64/94, OLG Karlsruhe Urteil vom 20.12.1995 - 10 U 123/95) nach sich ziehen.

DATENSCHUTZ

Die Backupmedien sind analog der darauf befindlichen Daten zu klassifizieren. Das gilt insbesondere für personenbezogene Daten (DSGVO). Entsprechend dieser Einstufungen sind die Backupmedien zu verwahren.

§ AUFTRAGSDATENVERARBEITUNG

Die Speicherung von Sicherungsdaten bei Dienstleistern in einer Cloud stellt eine Auftragsdatenverarbeitung i.S.v. Art. 28 DSGVO dar und ist daher vertraglich zu regeln.

§ ZUVERLÄSSIGKEIT

Sicherungsmedien unterliegen einem Alterungsprozess; Magnetbänder nutzen ab und Festplatten haben eine beschränkte Nutzungsdauer.

§ SICHERES LÖSCHEN/VERNICHTEN VON DATENSICHERUNGEN

Sicherungsmedien können personenbezogene Daten enthalten. Sie müssen daher sicher und datenschutzkonform durch zertifizierte Betriebe unter Beachtung der DIN 66399 vernichtet werden.

§ DOKUMENTATIONSPFLICHT

Sämtliche Vorgänge im Umgang mit Sicherungsmedien sind aufzuzeichnen. Die Dokumentationspflicht erstreckt sich auch auf Sicherungskonzept und Recovery-Tests.

! LOG-DATEIEN

Auf die Log-Dateien der Datensicherung sollte geachtet werden. Es empfiehlt sich, diese ebenfalls zu sichern.

§ ARCHIVIERUNGSANFORDERUNGEN

Datensicherungen erfüllen nicht die an Archivierungssysteme gestellten rechtlichen und technischen Anforderungen. Eine Datensicherung darf daher nicht als Archivierung angesehen werden.

? KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911/215 49 - 523 für Sie erreichbar.