Technisches Konzept: Datensicherungsrichtlinien

1. Projekttitel und Zweck

Projekttitel: Automatisierte Datensicherungsrichtlinien

Zweck: Sicherstellung der regelmäßigen, automatisierten Datensicherung, der feuerfesten Speicherung an zwei verschiedenen Standorten sowie der Unterstützung von Bare Metal Recovery.

2. Ausgangssituation und Problemstellung

In der aktuellen IT-Umgebung besteht die Notwendigkeit, die Datenintegrität zu gewährleisten und gleichzeitig die Wiederherstellbarkeit im Falle von Hardwareausfällen, Datenverlust oder Katastrophen sicherzustellen. Die Herausforderung ist es, eine robuste Strategie zu implementieren, die sowohl die Automatisierung der Sicherungsprozesse als auch die Sicherheit der gespeicherten Daten berücksichtigt.

3. Lösungsansatz

Implementierung eines automatisierten Datensicherungssystems, das regelmäßig Sicherungen erstellt, diese an zwei feuerfesten Standorten speichert und Bare Metal Recovery unterstützt. Dies umfasst die Verwendung von redundanten Speicherlösungen sowie die Erstellung von vollständigen Systemabbildern zur Wiederherstellung der IT-Infrastruktur.

4. Technische Umsetzung

4.1 Komponenten

- **Backup-Software:** Softwarelösung zur Automatisierung der Datensicherungsprozesse.
- **Storage-Lösungen:** Einsatz von feuerfesten externen Speichermedien (z. B. NAS, Cloud-Speicher).
- **Bare Metal Recovery Tool:** Spezielle Software zur Erstellung von Systemabbildern und Wiederherstellung auf neuer Hardware.

4.2 Datenfluss

1. Planung der Datensicherungsintervalle (z. B. tägliche, wöchentliche Sicherungen).
2. Automatisierte Erstellung der Datensicherung durch die Backup-Software.
3. Speicherung der Daten an zwei separaten, feuerfesten Standorten:
    - **Standort A:** Lokale, feuerfeste Sicherungsgeräte.
    - **Standort B:** Cloud-Backup bei einem zertifizierten Anbieter.
4. Periodische Tests der Wiederherstellungsfähigkeit mittels Bare Metal Recovery-Tests.

4.3 Speicherung und Zugriff

- **Backup-Typen:**
    - Vollständige Sicherungen: Wöchentliche Sicherungen eines vollständigen Systemabbildes.
    - Inkrementelle Sicherungen: Tägliche Sicherungen, die nur die seit der letzten Vollsicherung geänderten Daten enthalten.
- **Zugriffsrechte:** Strikte Zugriffssteuerung auf die Backup-Daten, um unbefugten Zugriff zu verhindern.

5. Datenschutz und Sicherheitskonzept

- **Verschlüsselung:** Alle Sicherungen werden während der Übertragung und Speicherung verschlüsselt.
- **Physische Sicherheit:** Lagerung der Speichermedien in feuerfesten Sicherheitsbehältern an beiden Standorten.
- **Zugriffskontrollen:** Nur autorisierte Personen haben Zugriff auf die Backup-Software und -Daten.

6. Implementierungsplan

1. Auswahl und Implementierung der Backup-Software.
2. Einrichtung der feuerfesten Speichersysteme an zwei Standorten.
3. Definition der Datensicherungsrichtlinien (Häufigkeit und Art der Sicherungen).
4. Durchführung von Testläufen für Bare Metal Recovery.
5. Schulung der Mitarbeiter im Umgang mit dem Backup-System.

7. Betrieb und Wartung

- **Regelmäßige Überprüfungen:** Monatliche Prüfungen der Backup-Protokolle zur Sicherstellung der Relevanz und Integrität der gesicherten Daten.
- **Wartungsintervalle:** Jährliche Tests der Bare Metal Recovery-Funktionalität sowie regelmäßige Updates der Backup-Software.
- **Notfallplan:** Erstellung eines Notfallplans zur schnellen Wiederherstellung der Dienste im Falle eines unerwarteten Datenverlusts.