

Checkliste:

Kriterien für die Auswahl eines sicheren Rechenzentrums

Wenn die eigene IT-Abteilung nicht über die technischen oder personellen Ressourcen verfügt, um ein Rechenzentrum unternehmensintern zu betreiben, bieten die Services eines externen Rechenzentrums eine attraktive Möglichkeit, die eigene IT zu entlasten.

Die Entscheidung, diese Aspekte der Unternehmens-IT auszulagern, bietet auch zahlreiche Vorteile: Zum einen bieten Rechenzentrums-Dienstleister meist ein höheres Know-how und vertraglich garantierten Service, auf der anderen Seite verfügen sie über höhere Sicherheitsvorkehrungen, die von der internen IT in den meisten Fällen nicht selbst umgesetzt werden könnten.

Jedoch gibt es auch zwischen Rechenzentrums-Dienstleistern Qualitätsunterschiede, insbesondere im Hinblick auf die Sicherheit und Performance. Um Ihnen bei dem Entscheidungsprozess für ein sicheres Rechenzentrum zu helfen, finden Sie hier eine detaillierte Checkliste mit Kriterien, die bei der Auswahl berücksichtigt werden sollten:

1. Serverstandort des Rechenzentrums

- **Sichere geografische Lage** im Hinblick auf Naturkatastrophen wie Überschwemmungen, Erdbeben oder Waldbrände.
- **Abstand zu Orten mit besonderer Gefährdung** wie Tankstellen, Atomkraftwerken, Bergwerken, Flughäfen oder chemischen Produktionen.
- **Neutrales, nicht auffälliges Gebäude** in einem Gewerbegebiet.
- **Sitz in Deutschland**, um dem Bundesdatenschutzgesetz und damit den strengen Regeln für die Verarbeitung und Speicherung personenbezogener Daten zu unterliegen.

2. Brandschutzvorkehrungen

- **Brandschutz** durch moderne Brandmelde- und Löschsysteme (z. B. Inertgaslösungen).
- **Trennung von Büroräumen** zum Betriebsbereich des Rechenzentrums mit separaten Brandschutzzonen für die elektrischen Betriebsräume.
- **Vernetzung der Brandmelde-systeme** mit Feuerwehr- oder Polizeidienststellen.

3. Physische Sicherheit

- **Zutrittskontrolle** nach Zuständigkeit mit mehrstufiger Authentifizierung, biometrischen Scannern und Sicherheitspersonal.
- **Überwachung rund um die Uhr** mit Videokameras.

4. Stromversorgung

- **Mehrfache Stromzufuhr** von Versorgern und unterbrechungsfreie Stromversorgung (USV-System).
- **Notstromversorgung** mit Dieselgeneratoren oder anderen Notstromaggregaten für den Betrieb bei Stromausfall.

5. Zertifizierungen und Compliance

- **ISO 27001** Zertifizierung für Informationssicherheits-Managementsysteme.
- **DIN EN 50600** Zertifizierung für den Bau des Rechenzentrums.
- **SOC 1, SOC 2, SOC 3** zur Sicherstellung der nötigen Compliance-Standards.
- **Andere branchenspezifische Zertifizierungen** je nach Anforderungen (z. B. PCI-DSS für Zahlungsdaten, HIPAA für Gesundheitsdaten).

6. Netzwerkinfrastruktur

- **Redundante Internetverbindungen** von mehreren Internet Service Providern zur Sicherstellung der Konnektivität.
- **Hohe Bandbreite und geringe Latenz** für schnelles und zuverlässiges Netzwerk.
- **Eigenes Breitbandnetz**, um eine lückenlose Verschlüsselung des gesamten Datenverkehrs zu gewährleisten.

7. Skalierbarkeit und Flexibilität

- **Erweiterungsmöglichkeit** der Kapazität nach Bedarf.
- **Flexibilität der Vertragsbedingungen** und Entsprechung mit den Geschäftsanforderungen.

8. Kühlung

- **Effiziente Kühltechnologien** und Redundanz in der Kühlung.
- **Gebäudeleittechnik** für die Umweltüberwachung von Temperatur und Luftfeuchtigkeit.

9. Daten- und Netzwerksicherheit

- **Netzwerk-Sicherheitsmaßnahmen** mittels Firewalls und Intrusion Detection Systems (IDS).
- **Sicherheitssystem** zum Schutz vor DDoS-Angriffen.
- **Verschlüsselung** von Daten im Ruhezustand und bei Übertragung.

10. Kundensupport

- **Support-Level** mit hoher Verfügbarkeit und Qualität.
- **Garantie** für Serviceverfügbarkeit und Reaktionszeiten.
- **Kostenstruktur**, die transparent und nachvollziehbar ist.