



# Kurzprofil - Anforderungen an ein geprüftes Rechenzentrum

## Stufe 2 tekPlus – Hochverfügbarkeit

### Kurzprofil „Rechenzentrum“ Stufe 2 tekPlus Hochverfügbarkeit

der tekit Consult Bonn GmbH

TÜV Saarland Gruppe

Version 1.1

Stand 13.05.2015

# 1 Grundlagen – Rechenzentrumssicherheit

## 1.1 Allgemein – „Geprüftes Rechenzentrum Stufe 2 tekPlus Hochverfügbar“

Gewerbliche und industrielle Betriebe sowie Öffentliche Verwaltungen sind in hohem Maße von der ordnungsgemäßen Funktion ihrer Informationstechnologie abhängig. Von besonderer Bedeutung neben der Vertraulichkeit und Integrität der Daten ist die Verfügbarkeit der IT-Systeme, Anwendungen und Komponenten im Rechenzentrum. Die zentrale IT im Rechenzentrum nimmt eine Schlüsselfunktion für die nachfolgenden Produktions- und Verwaltungsprozesse ein. Ausfälle des Rechenzentrums können daher eine ernste Bedrohung für Unternehmen, Verwaltungen und deren Kunden darstellen.

Anforderungen an ein „Geprüftes Rechenzentrum“ gehen über gesetzliche Anforderungen aus dem Baurecht und Arbeitsschutz hinaus. Spezifische Gesetzgebungen, Standards und Normen sind zusätzlich zu beachten. Die Ausfallsicherheit eines Rechenzentrums bzw. Rechenzentrumsverbundes ergibt sich aus der Konzeption des Rechenzentrums und der Nachhaltigkeit des Betriebes durch motivierte und gut ausgebildete Mitarbeiter.

Ein vom TÜV-Saarland durch die tekit Consult Bonn zertifiziertes „**Geprüftes Rechenzentrum – Stufe 2 tekPlus Hochverfügbar**“ erfüllt hohe Anforderungen der Funktionssicherheit an Verfügbarkeit und Informationssicherheit nach weltweiten Standards zur Rechenzentrumssicherheit, nach BSI IT Grundsicherheit, BITKOM, TIA - 942 und ISO 27001. Es ist auf einen weitgehend unterbrechungsfreien Betrieb ausgelegt. Wartungen können zu betriebsfreien Zeiten vorgenommen werden.

Durch die redundante Auslegung in vielen Infrastrukturkomponenten wird eine hohe Verfügbarkeit erreicht. Die Konzeption des Rechenzentrums und die definierten Betriebsprozesse sorgen für eine hohe Absicherung gegen Betriebsausfälle. Qualifiziertes, qualitäts- und sicherheitsbewusst handelndes Personal sichert den Rechenzentrumsbetrieb zusätzlich ab.

Notfall- und Wiederanlaufpläne stellen sicher, dass nach etwaigen Ausfällen der Betrieb so schnell wie möglich wiederhergestellt wird.

## 1.2 Normen, Anforderungen und Standards zum Anforderungskatalog

Das Rechenzentrum soll auf Sicherheitsaspekte geprüft und anschließend TÜV zertifiziert werden. Die Prüfungen werden in Anlehnung an BSI IT Grundschatz, BITKOM, TIA -942 und ISO 27001 auf Basis des vorliegenden TÜV Saarland Anforderungskataloges durchgeführt.

Es finden folgende Normen und Grundsätze ganz oder teilweise Eingang in den Anforderungskatalog:

- BSI IT Grundschatz,
- ISO 27001 und ISO 27002
- BITKOM Leitfaden und Planungshilfe betriebssicheres Rechenzentrum
- VDE Normen und VdS-Veröffentlichungen
- Tier Classification
- TIA 942
- Grundsätzen der ordnungsgemäßen Buchführung
- DIN 4102 Brandverhalten von Baustoffen
- EN 1047 (Teil 1 und 2) / ECB S Belastbarkeit von Datenträgern und Hardware
- EN 60529 International Protection Classes (Schutzarten)
- DIN 1627 Einbruchsschutz
- DIN 18095 Rauchschutztüren
- DIN 14096 Teil B (Brandschutzordnung)
- VDI 2054 Raumluftechnisch Anlagen für Datenverarbeitung
- des Bundesdatenschutzgesetz (BDSG)
- GmbHG bzw. AktG und KonTraG

## **Inhalte mit dem Bezug zum Anforderungskatalog**

### **2 Anforderungen an das Informationssicherheitsmanagement**

- 2.1 Beauftragter für Informationssicherheit
- 2.2 Richtlinien und Konzepte zur Informationssicherheit
- 2.3 Organisation der Informationssicherheit
- 2.4 Meldung von Sicherheitsereignissen und Verstößen

### **3 Bauliche Anforderungen**

- 3.1 Risiken im und im Umfeld des Rechenzentrums
- 3.2 Bauliche Ausführung

### **4 Technische Anforderungen**

- 4.1 Stromversorgung und Verteilung
- 4.2 Unterbrechungsfreie Stromversorgung
- 4.3 Netzersatzanlage
- 4.4 Klimatisierung
- 4.5 Einbruchmeldeanlage / Zutrittskontrolle
- 4.6 Brandschutz
- 4.7 Verkabelung von Datenleitungen

### **5 Anforderungen an Redundanzen**

- 5.1 Ausweichrechenzentrum
- 5.2 Stromversorgung und Verteilung
- 5.3 Klimatisierung
- 5.4 Netzzugang
- 5.5 Netzwerk

### **6 Anforderungen an Dokumentation und Betriebsführung**

- 6.1 Einleitung, Abgrenzung, Ziele und Ausgangssituation
- 6.2 Gefahrenlage
- 6.3 Risikoanalyse

- 6.4 Sicherheitsanforderungen
- 6.5 Betriebspersonal vor Ort, Bereitschaftsdienste und entferntes Management
- 6.6 Lenkung der Dokumente
- 6.7 Lenkung der Aufzeichnungen
- 6.8 Konzept Zutrittsregelungen
- 6.9 Alarmmeldung und Alarmorganisation
- 6.10 Kommunikationskonzept
- 6.11 Externe Dienstleister und Lieferanten
- 6.12 Kontinuierlicher Geschäftsbetrieb
- 6.13 Dokumentation der baulichen Ausführung
- 6.14 Dokumentation der Stromversorgung und Verteilung
- 6.15 Dokumentation der Klimatisierung bzw. Raumluftechnik
- 6.16 Dokumentation des Brandschutzes
- 6.17 IT-Betriebsprozesse / Arbeiten
- 6.18 Wartungsarbeiten
- 6.19 Regelmäßige Überprüfung
- 7 Organisatorische Anforderungen**
- 7.1 Allgemeine Anforderungen
- 7.2 Zutrittsregelungen
- 7.3 Arbeiten Dritter im Rechenzentrum
- 7.4 Datensicherung und Archivierung
- 7.5 Wartung**
- 7.6 Funktionsprüfungen
- 7.7 Anforderungen an das Personal
- 7.8 Notfall Management
- 7.9 Sicherheitsbewusstsein