Sec-IT

Mehr Sicherheit.
Mehr Wert.

Anforderungskatalog

zur Bewertung und Zertifizierung von Hochverfügbarkeitsrechenzentren

Version 1.1
Stand: 15.05.2014

Autor: Marko Hoffmann

Sitz: München
Amtsgericht München HRB 197 698
USt-IdNr. DE282283450
Informationen gemäß § 2 Abs. 1 DL-InfoV unter www.tuev-sued.de/impressum

Geschäftsführer:
Herbert Huß

Telefon: +49 89 5791-3894
Telefax: +49 89 5155-1097
www.tuev-sued.de

TÜV SÜD Sec-IT GmbH
Ridlerstraße 65
80339 München
Deutschland

Sec-IT

Inhalt

Sec-IT

1 Organisatorische Anforderungen

1.1 Verpflichtung auf die Anforderungen

Die für das Rechenzentrum und die dazugehörigen Geschäftsprozesse verantwortlichen Mitarbeiter verpflichten sich, alle Anforderungen aus diesem Katalog und alle relevanten gesetzlichen Bestimmungen zu erfüllen. Sie weisen die Übernahme dieser Verantwortung durch geeignete Maßnahmen nach.

1.2 Vermittlung der Anforderungen

Die in diesem Katalog aufgeführten Anforderungen werden in der Organisation allen davon betroffenen Mitarbeitern in angemessener Art und Weise vermittelt.

1.3 Festlegung von Verantwortlichkeiten

Zur Erfüllung aller Anforderungen sind Verantwortlichkeiten und Befugnisse in der Organisation vollständig und eindeutig festgelegt. Es existiert eine angemessene Stellvertreterregelung. Der Aufbau der Organisation ist dokumentiert.

1.4 Einsatz wirksamer Verfahren

Es sind Verfahren wirksam, die geeignet sind, die Anforderungen in der Organisation umzusetzen.

1.5 Bereitstellung der erforderlichen Mittel

Die notwendigen und geeigneten Mittel zur Erfüllung der Anforderungen werden bereitgestellt (z.B. geschultes Personal, erforderliche Infrastruktur).

1.6 Bewertung der Konformität

Die Organisation bewertet regelmäßig ihre Konformität bzgl. der Anforderungen, um deren Einhaltung nachhaltig sicherzustellen. Die Durchführung dieser Bewertung erfolgt geplant, die Ergebnisse werden dokumentiert.

1.7 Ständige Verbesserung

Das Ergebnis der Bewertung von Kundenzufriedenheit und Konformität zu diesem Anforderungskatalog wird zur ständigen Verbesserung der Organisation verwendet

1.8 Lenkung von Dokumenten

Das Unternehmen verwendet eine Dokumentenlenkung für betriebswichtige Dokumente und Aufzeichnungen, aus der zumindest Ersteller/Freigebender und Datum oder Revision des Dokuments / der Aufzeichnung hervorgehen.

1.9 Notfall- und Störungsmanagement

Um Schäden aus Störungen und Notfällen zu minimieren gibt es ein Konzept zum Umgang mit Störungen und Notfällen. Es enthält unter anderem Eskalationspläne, die auch die Kundenkommunikation abdecken. Notfallpläne und Eskalationspläne werden regelmäßig getestet, Auftretende Störungen und Notfälle sowie die daraufhin eingeleiteten Maßnahmen werden aufgezeichnet.

Zur Vermeidung von Störungen und Notfällen wird für das RZ eine regelmäßig aktualisierte und dokumentierte Analyse bezüglich sogenannter single points of failure durchgeführt, darin erkannte Probleme werden anhand angemessener Maßnahmen behoben.

Sec-IT

1.10 Risikomanagement

Die Organisation führt regelmäßig eine umfassende Risikoanalyse durch, in der die Risiken für den Betrieb des Rechenzentrums sowie sich aus der Verwendung externer Dienstleister ergebende Risiken beschrieben sind und entsprechende Maßnahmen zur Beherrschung der Risiken zugeordnet werden. Das Restrisiko ist von der Leitung der Organisation zu freizugeben.

1.11 Dokumentation

Der Betrieb des Rechenzentrums wird dokumentiert. Dabei sind unter anderem folgende Dokumente zu führen:

a) Betriebshandbücher oder adäquate Beschreibungen, die die Prozesse und Verfahren zum Betrieb des Rechenzentrums beschreiben.
b) Weiterführende Dokumentation für Prozesse und Verfahren.
c) Service-Level-Agreements mit Lieferanten
d) Service-Level-Agreements mit Kunden
e) Ein Verfahren zur geregelten Durchführung von Änderungen an Infrastruktur und Anlagen („Changemanagement“)
f) Ein präventives und reaktives Incidentmanagement, das Sicherheitsvorfälle sowie Betriebsstörungen und Notfälle aufzeichnet und deren Behebung dokumentiert.
g) Ein Kennzahlensystem mit Monitoring der SLA-Vorgaben aufgrund definierter Schwellwerte wird verwendet. Wesentliche Kennzahlen werden regelmäßig ausgewertet und an verantwortliche Stellen berichtet.
h) Durch das RZ bereitgestellte Leistungen sind detailliert festgelegt und werden Interessierten Parteien zur Verfügung gestellt.

1.12 Erreichbarkeit

Betriebspersonal des Rechenzentrums ist rund um die Uhr („24/7“) bei definierten, angemessenen Reaktionszeiten erreichbar. Dies kann durch ständig besetzte Stellen oder durch Bereitschaftsdienste umgesetzt werden.

1.13 Geplante Serviceunterbrechungen

Notwendige Serviceunterbrechungen („Downtime“) werden geplant und internen Stellen sowie Kunden mit angemessener Vorlaufzeit mitgeteilt. Entsprechende Vorgaben sind definiert und dokumentiert.

1.14 Löschung und Vernichtung von Daten

Die Löschung und Vernichtung von Daten auf Papier oder Datenträgern läuft nach einem definierten und dokumentierten Verfahren ab.

2 Personelle Anforderungen

2.1 Rollen- bzw. Stellenbeschreibungen

Die Verantwortung, Rechte und Pflichten sowie Vertretungsregelungen der Stelleninhaber müssen in entsprechenden Rollen- bzw. Stellenbeschreibungen klar definiert sein. Bei Entscheidungsträgern sind darüber hinaus auch die Befugnisse zu definieren.

2.2 Schulung

Der Schulungsbedarf der Mitarbeiter wird regelmäßig und systematisch festgestellt. Notwendige Schulungen werden durchgeführt und die Teilnahme daran dokumentiert. Schulungsinhalte werden regelmäßig aktualisiert und aufgefrischt.

Außerdem wird der Erfolg von Schulungsmaßnahmen bewertet.

2.3 Recruiting, Eintritt, Änderung und Austritt von Mitarbeitern

Für auszuschreibende Stellen existieren Anforderungsprofile. Bewerber werden hinsichtlich Ihrer Eignung für einen Einsatz in sicherheitskritischen Bereichen überprüft.

Es existiert ein definiertes Verfahren für Eintritt, Änderung und Austritt von Mitarbeitern. Darin ist eine geregelte Einschulung und Vergabe von Benutzerrechten berücksichtigt.

Vergabe und Entzug von Rechten sowie zur Nutzung überlassene Unternehmenswerte und deren Rückgabe werden dokumentiert. Die Verpflichtung auf das Datenschutzgeheimnis sowie weitere Sicherheits- und Vertraulichkeitsrichtlinien wird dokumentiert.

2.4 Betriebsfremde Personen

Der Aufenthalt aller Personen im Sicherheitsbereich ist nachvollziehbar und erkennbar dokumentiert. Alle Personen werden vor Betreten über notwendige Verhaltensregeln belehrt und vor dem Betreten von Sicherheitsbereichen angemessen überprüft.

Techniker und Fremdpersonal erhalten Berechtigungen nur zeitlich befristet und nur soweit zur Erfüllung der Aufgaben notwendig. Die Freigabe der Berechtigungen ist zu dokumentieren.

Besucher erhalten Zutritt nur mit Freigabe eines dazu berechtigten Mitarbeiters des Rechenzentrums und werden dauerhaft von einem Mitarbeiter oder einer berechtigten Person begleitet.

Mitgeführte Gegenstände (Werkzeuge, Geräte, Speichermedien etc.) müssen angemeldet und überprüft werden. Nicht zugelassene Gegenstände werden außerhalb des Sicherheitsbereichs verwahrt.

3 Anforderungen an das Gebäude

3.1 Standort

In der Risikobewertung (siehe 1.10) müssen geographische Risiken und nachbarliche Risiken enthalten sein (z.B. Risiken durch Hochwasser, Erdbeben, Flugverkehr, Explosionsgefährdungen, politische Risiken etc.) und durch angemessene Maßnahmen auf ein akzeptables Maß reduziert sein.

3.2 Gebäudestruktur, Bauweise

Die Gebäudestruktur ist dem Zweck angemessen, unterschiedliche Funktions- und Sicherheitsbereiche sind räumlich getrennt, für Sicherheitszonen existiert ein angemessenes risikominimierendes Konzept. Das Gebäude bietet einen grundlegenden EMV-Schutz (Faradayscher Käfig). Es gibt redundante Gebäudezugänge und zugehörige Sicherheitskontrollen.

Die Außenwände der IT-Fläche sind fensterlos. Bereiche unterschiedlicher Kunden sind durch geeignete Maßnahmen voneinander zugriffssicher getrennt.

Für die Aufstellung von USV/Batteriesystem, Netzersatzanlage und IT-Racks gibt es entsprechende Eigungsnachweise bezüglich der Gebäudestatik.

Es gibt keine äußerlichen Hinweise (Schilder etc.) auf das RZ, das Gebäude ist äußerlich soweit baulich möglich unauffällig.

3.3 Zutritt

Die Verantwortung für Vergabe und Entzug von Zutrittsrechten ist definiert.

Das Rechenzentrum verfügt über einen Zutrittsschutz, der in die Gebäudetechnik integriert ist und der Zutritte / verweigerte Zutritte, Verlassen / verweigertes Verlassen zu einzelnen Sicherheitsbereichen protokolliert.

Der Zutritt ist so zu regeln, dass nur einzelne Personen die Sicherheitsbereiche betreten können und hierbei identifiziert und dokumentiert werden.

Der Zutritt zur IT-Fläche ist nur über die Authentisierung mit zwei unabhängigen Merkmalen möglich. (Zum Verlassen der IT-Fläche muss mindestens eines der Merkmale verwendet werden.)

Für den Notfall existieren zugängliche Parkplätze für Betriebspersonal bzw. Notdienst.

3.4 Alarmsystem

Das Rechenzentrum verfügt über eine an die Gebäudetechnik angeschlossene Einbruchmeldeanlage mit Alarmierung einer 24/7 erreichbare Sicherheitszentrale, in der Verfahren für den Alarmierungsfall definiert sind.

Der Außenbereich des Rechenzentrums wird dauerhaft überwacht.

3.5 Gebäudetechnik

Die Einrichtungen der Gebäudetechnik sind an die unterbrechungsfreie Stromversorgung angeschlossen, wesentliche Einrichtungen sind redundant ausgeführt.

Die gebäudetechnischen Einrichtungen werden regelmäßig getestet.

3.6 Wartung, Dokumentation

Gebäudestruktur, Raumaufteilung und Gebäudetechnik sind auf aktuellem Stand dokumentiert. Alle Anlagen und Einrichtungen der Gebäudetechnik werden regelmäßig und geplant gewartet.

4 Kommunikation

Die Kommunikationseinrichtungen des Rechenzentrums werden über die USV-Anlage notgespeist. Zueinander redundante Bereitstellungsanlagen werden redundant mit Energie versorgt. Die Anbindung an öffentliche Netze findet an mindestens zwei getrennten POPs statt. Eingangsleitungen in das Gebäude sind räumlich getrennt. Beliebige Einfachfehler im Datennetz des Rechenzentrums führen nicht zum Ausfall der WAN-Anbindung.

Sec-IT

5 Stromversorgung

5.1 Auslegung, Planung, Ausführung

Ein Stromversorgungskonzept mit Ziel- und Zweckdefinition muss vorhanden sein, das für USV und NEA mindestens beinhaltet: Planungsunterlagen mit Redundanznachweisen, Prüfnachweise der geplanten Anlagen (Typ- und Stückprüfprotokolle), Schutzselektivitätsbetrachtungen für redundante Systeme. Energieverteiler und Leitungsführungen sind fachgerecht ausgeführt, wartungsfreundlich und gut erreichbar und bieten Reserven für Erweiterungen

5.2 Netzeinspeisung, interne Versorgung

An das öffentliche Stromnetz ist das Rechenzentrum mit mindestens 2 getrennten Leitungen an unterschiedliche Umspannwerke/Mittelspannungsverteilungen angebunden.

Versorgungsleitungen sind räumlich getrennt unterirdisch verlegt.

Interne Versorgungsleitungen und Verteiler sind 2N-redundant ausgelegt, klima- und lüftungstechnische Anlagen werden 2N-redundant versorgt. Alle redundanten Systeme werden räumlich getrennt installiert. IT-Racks werden redundant versorgt.

5.3 Notfallversorgung: USV, NEA

Eine USV mit 2N(n+1)-Redundanz ist vorhanden. Die USV ist nach EN 62040, das Batteriesystem nach EN 50272-2 ausgelegt.

Eine inselbetriebsfähige NEA nach ISO 8528 mit n+2-Redundanz ist vorhanden. Die Redundanz kann z.B. durch n+1 und zusätzliche Anschlussmöglichkeit für eine mobile NEA erreicht werden.

5.4 Monitoring und Dokumentation

Die Anlagen der Stromversorgung sind dokumentiert, die Dokumentation ist auf aktuellem Stand und beinhaltet unter anderem Zuleitung, Beschriftung, Kabelführung, Kennzeichnungen von Anlagen und Geräten.

An den Anlagen vor Ort und an zentraler Stelle sind aktuelle Kennzahlen ablesbar (Auslastung, USV-Kapazität, Phasenverteilung etc.)

5.5 Test und Wartung

Die Anlagen zur Sicherung der Energieversorgung werden je nach technischen Anforderungen regelmäßig getestet, die Testergebnisse sind zu dokumentieren und zu bewerten. Dabei erfolgt eine NEA Funktionsprobe monatlich, Tests von Umschalteinrichtungen halbjährlich, sowie ein Black-Building-Test jährlich Wartungen der Stromversorgung finden geplant und regelmäßig statt.

Sec-IT

6 Klima und Lüftung

6.1 Auslegung

Das Klimatisierungssystem ist insgesamt so ausgelegt, dass eine 2N-Redundanz oder gleichwertig erreicht wird. Wesentliche Systeme sind zusätzlich n+2-redundant auszuführen, dies kann z.B. auch durch n+1 und zusätzliche Anschlussmöglichkeit für mobile Kälte erreicht werden. Redundante Systeme sind räumlich getrennt.

Anlagen und Leitungsnetz sind mit Leckageerkennungssystemen und Kondenswasserführungen ausgestattet, das Rohrleitungssystem ggf. räumlich getrennt.

6.2 Planung, Ausführung

Ein Klimatisierungskonzept mit Ziel- und Zweckdefinition muss vorhanden sein, das für Kälte- und Lüftungsanlagen mindestens beinhaltet: Planungsunterlagen mit Redundanznachweisen, Prüfnachweise der geplanten Anlagen (Typ- und Stückprüfprotokolle) Anlagen und Leitungsführungen sind fachgerecht ausgeführt, wartungsfreundlich und gut erreichbar und bieten Reserven für Erweiterungen

6.3 Ausfallsicherheit

Bei Ausfall der Gebäudeleittechnik muss nachweisbar ein Weiterbetrieb des Rechenzentrums erfolgen. Die Anlagen zu Kälte- und Lüftungsversorgung können auch ohne Gebäudetechnik manuell gesteuert werden. Steuerungsanlagen sind per redundanter USV abgesichert.

6.4 Monitoring und Dokumentation

Die Anlagen der Klimatisierung sind dokumentiert, die Dokumentation ist auf aktuellem Stand und beinhaltet unter anderem Zuleitung, Beschriftung, Kabelführung, Kennzeichnungen von Anlagen und Geräten.

An den Anlagen vor Ort sind aktuelle Kennzahlen und Anlagenbetriebszustände ablesbar. An zentraler Stelle sind alle wichtigen Anlagenbetriebszustände und Vorgabewerte überwacht und aufgezeichnet, hierbei kommen mehrere angemessen positionierte Meßstellen zum Einsatz. Die Regelung von Temperatur und Luftfeuchtigkeit nach Werkskalibrierung ist vor Ort auch bei Ausfall der Gebäudetechnik möglich. Bei Über-/Unterschreitung von Vorgabewerten wird eine ständig erreichbare Stelle alarmiert.

6.5 Test und Wartung

Die Anlagen zur Klimatisierung werden regelmäßig je nach technischer Anforderung getestet, die Testergebnisse sind zu dokumentieren und zu bewerten. Dabei wird die Umschaltung der Kälteanlagen halbjährlich getestet. Hinsichtlich Laufzeiten der Anlagen werden Hygieneverordnungen beachtet und ein Betriebsstundenmanagement eingesetzt. Wartungen der Klimatechnik finden geplant und regelmäßig statt

Sec-IT

7 Brandschutz

Sämtliche gesetzlichen, behördlichen und versicherungstechnischen Brandschutzvorgaben werden eingehalten. Die Brandschutzausstattung des Gebäudes erfüllt die Empfehlungen des Bitkom-Leitfadens „Betriebssichere Rechenzentren“, Kapitel 6.2.3, Kategorie D.

7.1 Branderkennung und -meldung

Eine Brandmeldeanlage nach DIN 14675 ist in Betrieb. Die Erkennung erfolgt mit Sensoren zur Brandfrühesterkennung, dabei ist eine Zweimelder-Abhängigkeit umgesetzt. Die Alarmierung erfolgt über die Gebäudetechnik an eine ständig besetzte Sicherheitszentrale.

7.2 Brandbekämpfung

Eine Brandlöschanlage mit geeignetem Löschmittel ist vorhanden. Alternativ kann durch eine Brandvermeidungsanlage / Sauerstoffreduzierungsanlage das Schutzziel erreicht werden.

Im Brandfall ist ein Erstangriff durch geschultes eigenes Personal vor Ort möglich.

7.3 Test, Wartung und Dokumentation

Die Brandschutzanlagen sind dokumentiert, die Dokumentation ist auf aktuellem Stand. Wartungen der Brandschutztechnik finden geplant und regelmäßig statt. Die Anlagen zum Brandschutz werden regelmäßig entsprechend bauaufsichtlichen Vorgaben getestet, die Testergebnisse sind zu dokumentieren und zu bewerten.

8 Blitzschutz/Potentialausgleich

Ein Blitzschutzkonzept ist vorhanden, das auch einen EMV-Schutz berücksichtigt. Hierbei werden die verschiedenen Blitzschutzzonen im Rechenzentrum unterschieden.

Ein Blitzschutzsystem nach EN 62305 Teil 1 bis 4 ist vorhanden, es beinhaltet außerdem einen EMV-gerechten Potentialausgleich. Der Potentialausgleich für die IT-Anlagen erfolgt gemäß EN 50310