Sec-IT

Mehr Sicherheit.
Mehr Wert.

Anforderungskatalog

zur Bewertung und Zertifizierung von Betriebsrechenzentren

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®

TÜV SÜD Sec-IT GmbH
Ridlerstraße 65
80339 München
Deutschland

Sec-IT

Inhalt

Sec-IT

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.

1.7 Ständige Verbesserung

Das Ergebnis der Bewertung von internen Prozessen 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 und Datum oder Revision des Dokuments / der Aufzeichnung hervorgehen.

1.9 Notfall- und Störungsmanagement

Um Störungen und Notfälle zu beherrschen gibt es unter anderem Eskalationspläne, die auch die Kundenkommunikation abdecken. Die Eskalationspläne werden regelmäßig getestet, Auftretende Störungen und Notfälle sowie die daraufhin eingeleiteten Maßnahmen werden aufgezeichnet.

1.10 Risikomanagement

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

Sec-IT

1.11 Dokumentation

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

a) Betriebshandbücher oder adäquate Beschreibungen, die die grundlegenden Prozesse und Verfahren zum Betrieb des Rechenzentrums beschreiben.
b) Service-Level-Agreements mit Lieferanten
c) Service-Level-Agreements mit Kunden
d) Ein Verfahren zur geregelten Durchführung von Änderungen an Infrastruktur und Anlagen („Changemanagement“)

1.12 Erreichbarkeit

Betriebspersonal des Rechenzentrums ist während festgelegter Zeiten entsprechend den betrieblichen Erfordernissen 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 Verfahren ab.

2 Personelle Anforderungen

2.1 Rollen- bzw. Stellenbeschreibungen

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

2.2 Schulung

Notwendige Schulungen werden durchgeführt und die Teilnahme daran dokumentiert.

2.3 Eintritt, Änderung und Austritt von Mitarbeitern

Es existiert ein definiertes Verfahren für Eintritt, Änderung und Austritt von Mitarbeitern. Darin ist eine geregelte Einschulung und Vergabe von Benutzerrechten berücksichtigt. Zur Nutzung überlassene Unternehmenswerte werden dokumentiert.

2.4 Betriebsfremde Personen

Der Aufenthalt von Kunden, Technikern, Fremdpersonal und Besuchern ist nachvollziehbar und erkennbar dokumentiert. Betriebsfremde Personen werden vor Betreten über notwendige Verhaltensregeln belehrt. Techniker und Fremdpersonal erhalten Berechtigungen nur zeitlich befristet und nur soweit zur Erfüllung der Aufgaben notwendig. Besucher werden dauerhaft von einem Mitarbeiter oder einer berechtigten Person begleitet.

Sec-IT

3 Anforderungen an das Gebäude

3.1 Standort

Geographische Risiken und nachbarliche Risiken (z.B. Risiken durch Hochwasser, Erdbeben, Flugverkehr, Explosionsgefährdungen, politische Risiken etc.) werden betrachtet.

3.2 Gebäudestruktur, Bauweise

Die Gebäudestruktur ist dem Zweck angemessen, es existiert eine Sicherheitskonzeption für das Gebäude. Es bietet einen grundlegenden EMV-Schutz (Faradayscher Käfig).

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.

3.3 Zutritt

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

Das Rechenzentrum verfügt über einen angemessenen Zutrittsschutz.

3.4 Wartung, Dokumentation

Gebäudestruktur, Raumaufteilung und Gebäudetechnik sind auf aktuellem Stand dokumentiert. Die gebäudetechnischen Einrichtungen werden regelmäßig getestet. 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. Wesentliche Anlagen sind n+1-redundant ausgelegt. Risiken nicht redundanter Anlagenteile sind in der Risikobewertung berücksichtigt.

5 Stromversorgung

5.1 Auslegung, Planung, Ausführung

Ein Stromversorgungskonzept mit Ziel- und Zweckdefinition muss vorhanden sein, das für Netzanbindung, 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

Die Anbindung an das öffentliche Energienetz ist angemessen ausgelegt. Anschlussleitungen in das Gebäude sind unterirdisch verlegt.

Klima- und lüftungstechnische Anlagen werden n+1-redundant versorgt. IT-Racks werden redundant versorgt.

5.3 Notfallversorgung: USV, NEA

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

Eine inselbetriebsfähige NEA nach IS 8528 mit n+1-Redundanz ist vorhanden. Die Redundanz kann z.B. durch 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 sind aktuelle Kennzahlen ablesbar (Auslastung, USV-Kapazität, Phasenverteilung etc.)

Sec-IT

5.5 Test und Wartung

Die Anlagen zur Sicherung der Energieversorgung werden ja 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.

6 Klima und Lüftung

6.1 Auslegung

Das Klimatisierungssystem ist in den wesentlichen Komponenten n+1-redundant ausgelegt. Redundanz kann auch durch Anschlussmöglichkeit für mobile Kälte hergestellt werden. Anlagen und Leitungsnetz sind mit Leckageerkennungssystemen und Kondenswasserführungen ausgestattet.

6.2 Planung, Ausführung

Ein Klimatisierungskonzept mit Ziel- und Zweckdefinition muss vorhanden sein, das für Kälte- und Lüftungsanlagen mindestens beinhaltet: Planungsunterlagen, 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

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 und einstellbar (Luftfeuchtigkeit und Temperatur). Bei Über-/Unterschreitung von Vorgabewerten erfolgt eine Alarmierung.

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

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 B.

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 an eine ständig besetzte Stelle.

Sec-IT

7.2 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