Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Deutsche Rentenversicherung - Rechenzentrum Würzburg GmbH
Berner Straße 1
97084 Würzburg

für den Sicherheitsbereich

Rechenzentrum Würzburg (RZW)

die Erfüllung aller Anforderungen

EN 50600
Verfügbarkeitsklasse 3

unter Verwendung des Trusted Site Infrastructure Kriterienkatalogs TSI.STANDARD V4.2 der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.
Die Anlage ist Bestandteil des Zertifikats und besteht aus 7 Seiten.
Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Infra-structure
TÜViT®
2021 Trusted Site

Certificate ID: 66680.21

Zertifikatsgültigkeit
30.03.2021 - 31.07.2023

Essen, 30.03.2021

Joachim Faulhaber
stellv. Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Prüfbericht

- „Prüfbericht – Trusted Site Infrastructure (TSI.STANDARD), Rechenzentrum Würzburg (RZW)“, Version 1.0 vom 17.03.2021, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind definiert in den Normen:

- DIN EN 50600-1, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 1: Allgemeine Konzepte; Deutsche Fassung EN 50600-1:2012

- DIN EN 50600-2-1, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-1: Gebäudekonstruktion; Deutsche Fassung EN 50600-2-1:2014

- DIN EN 50600-2-2, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-2: Stromversorgung; Deutsche Fassung EN 50600-2-2:2014

- DIN EN 50600-2-3, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-3: Regelung der Umgebungsbedingungen; Deutsche Fassung EN 50600-2-3:2014

- DIN EN 50600-2-4, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-4: Infrastruktur der Telekommunikationsverkabelung; Deutsche Fassung EN 50600-2-4:2015

- DIN EN 50600-2-5, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-5: Sicherungssysteme; Deutsche Fassung EN 50600-2-5:2016

- DIN EN 50600-3-1, Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 3-1: Informationen für das Management und den Betrieb; Deutsche Fassung EN 50600-3-1:2016

und wurden überprüft unter Verwendung der Prüfanforderungen:

- „TSI.STANDARD Kriterienkatalog, TSI.STANDARD V4.2“ vom 01.01.2019, TÜV Informationstechnik GmbH

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist der Sicherheitsbereich „Rechenzentrum Würzburg (RZW)“ der Deutsche Rentenversicherung - Rechenzentrum Würzburg GmbH. Dieser wird im Prüfbericht detailliert beschrieben.

Prüfergebnis

Das Ergebnis lautet „EN 50600 Verfügbarkeitsklasse 3“.

Zusammenfassung der Prüfanforderungen

Prüfanforderungen gemäß TSI.STANDARD V4.2, welche die Anforderungen der DIN EN 50600 enthalten:

1 Umfeld (ENV – Environment)

Gefährdungspotenziale aus dem Umfeld sind gemieden. Die Standortentscheidung des Objekts ist unter Berücksichtigung der Risiken u. a. von Wasser-, Explosions-, Trümmer-, Erschütterungs- und Schadstoffgefährdung erfolgt.

2 Bauliche Gegebenheiten (CON – Construction)

Die Gebäudekonstruktion sowie Fenster und Türen bieten einen Zutritts-, Brand- und Trümmerschutz. Das Gebäude ist gegen Blitzeinschlag geschützt. Der Sicherheitsbereich liegt abseits öffentlicher Zugänge und gefährlicher Produktionsprozesse und bildet einen eigenen Brandabschnitt. Eine Trennung zwischen Grob- und Feintechnik ist erfolgt. Es besteht ein baulicher Brand- und Wasserschutz.

3 Brandmelde- und Löschtechnik (FIR – Fire Alarm & Extinguishing Systems)

Eine Brandmeldeanlage ist im gesamten Sicherheitsbereich installiert und zu einer Alarmempfangsstelle aufgeschaltet. Benachbarte Räume, doppelter Fußboden, abgehängte Decken und Luftkanäle sind in die Brandüberwachung einbezogen. Neben der Alarmierung werden Abschaltfunktionen und Schadensbegrenzungsmaßnahmen ausgelöst, z. B. durch eine Gaslöschanlage. Eine zusätzliche Versorgung mit geeigneten Handfeuerlöschern ist gegeben.

4 Sicherheitssysteme (SEC – Security Systems & Organization)

Es existiert eine Zugangskontrollanlage (ZKA). Ein Einbruchschutz ist mehrstufig gegeben, dabei werden alle sicherheitskritischen Bereiche mittels einer Einbruchmeldeanlage (EMA) überwacht. Die Anlage wird von einer Haupt- und einer Zusatzenergiequelle gespeist. Die Alarme werden an eine ständig besetzte Sicherheitszentrale übertragen.

5 Verkabelung (CAB – Cabling)

Kommunikations- und Datenkabel sind gemäß DIN EN 50174-2 mit dem nötigen Abstand zu einander und zu Stromkabeln auf getrennten Kabelführungen verlegt. Datenkabel werden nicht durch Bereiche mit Gefährdung geführt oder sind speziell geschützt. WAN-Trassen verlaufen kreuzungsfrei, und ein Anschluss an mindestens 2 Provider (ab Level 3) ist realisiert.

6 Energieversorgung (POW – Power Supply)

Der Nachweis einer nach einschlägigen DIN-Normen und VDE-Vorschriften erfolgten Elektroinstallation ist erbracht. Es existieren angepasste Aufteilungen und Absicherungen der Stromkreise. Sie sind gegen Überspannung geschützt. Ausfälle sind durch eine redundante Auslegung abgefangen. Eine Notstrom- und USV-Versorgung der IT- wie auch der Sicherheitszentrale ist gegeben. Tests zur Inbetriebsetzung sind erfolgt.

7 Raumlufttechnische Anlagen (ACV – Air Conditioning & Ventilation)

Die Abwärme der IT-Geräte wie auch der Infrastrukturkomponenten wird durch Kühlung hinreichend abgefangen. Es ist sichergestellt, dass Lufttemperatur, Luftfeuchte und Staubbelastung entsprechende Grenzen einhalten. Feuer- und Rauchklappen sind gemäß Brandschutzkonzept eingebaut. Die Einhaltung der Klimavorgaben wird fernüberwacht. Ausfälle sind durch eine redundante Auslegung abgefangen. Tests zur Inbetriebsetzung sind erfolgt.

8 Organisation (ORG – Organization)

Alle Sicherheitseinrichtungen werden einem regelmäßigen Funktionstest unterzogen. Regelmäßige Wartungen an Verschleißteilen der Infrastrukturkomponenten bzw. IT-Hardware sind in einem Wartungsplan festgelegt. Die Datensicherungsmedien werden brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt.

9 Dokumentation (DOC – Documentation)

Es existiert eine Dokumentation der Infrastrukturmaßnahmen (DIM) bzw. ein Sicherheitskonzept. Ebenso gibt es Regelungen für das Zugangskontrollsystem, das Zutrittsberechtigte definiert und die Verfahren zur Ausgabe der Schlüssel, Codekarten etc. beschreibt. Lagepläne für das Gebäude und alle Infrastrukturkomponenten sowie Schemata und Datenblätter liegen vor. Ein Brandschutzkonzept ist vorhanden. Ein Notfallkonzept bzw. Alarmplan liegen vor.

10 EN 50600

Die ergänzenden Anforderungen zur ganzheitlichen Abdeckung der DIN EN 50600 sind umgesetzt.

Drei aufsteigende Granularitätsniveaus legen den Umfang der Messungen zur Ermittlung der Energieeffizienz fest.

Die folgende Tabelle zeigt den zu Grunde gelegten Zusammenhang zwischen der DIN EN 50600 (Teile 2-2, 2-3, 2-4: Verfügbarkeitsklassen und Granularitätsniveaus) und den TSI Leveln in den Bereichen POW, ACV und CAB:

DIN EN 50600-2-2/-3/-4 Verfügbarkeitsklasse	1	2	3	4
DIN EN 50600-2-2 Granularitätsniveau	-	2	2	2
DIN EN 50600-2-3 Granularitätsniveau	-	-	2	2
DIN EN 50600-2-4 Granularitätsniveau	-	-	-	-
TSI Level für POW, ACV und CAB	1	2	3	4

Zur Erreichung der Verfügbarkeitsklasse X müssen alle Anforderungen in den Bereichen POW, ACV und CAB mindestens im korrespondierenden TSI Level X erreicht werden.

L TSI Level

Level 1	Mittlerer Schutzbedarf (entspricht den Infrastrukturanforderungen der BSI-Grundschutzkataloge im Baustein Serverraum)
Level 2	Erweiterter Schutzbedarf (Redundanzen kritischer Versorgungssysteme, mit ergänzenden Anforderungen bei o. g. Bewertungsaspekten)
Level 3	Hoher Schutzbedarf (vollständige Redundanzen kritischer Versorgungssysteme – No Single Point of Failures bei wichtigen zentralen Systemen)
Level 4	Sehr hoher Schutzbedarf (zusätzlich ausgeprägte Zutrittssicherung, keine benachbarten Gefährdungspotenziale, bei Alarmmeldungen minimale Interventionszeiten)