Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Atruvia AG
Fiduciastraße 20
76227 Karlsruhe

für den Sicherheitsbereich

RZ R

die Erfüllung aller Anforderungen für hohen Schutzbedarf des Trusted Site Infrastructure Kriterienkatalogs

TSI.STANDARD V4.3
Level 3 (erweitert)

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 5 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Infra-structure 2021 TÜVIT® Trusted Site

Certificate ID: 66778.21

© TÜViT – TÜV NORD GROUP – www.tuvit.de

Zertifikatsgültigkeit:
15.12.2021 – 31.12.2023

Essen, 15.12.2021

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen
www.tuvit.de

ZUM ZERTIFIKAT

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), RZ R“, Version 1.0 vom 09.12.2021, TÜV Informationstechnik GmbH

Prüfanforderungen

- „TSI.STANDARD Kriterienkatalog, TSI.STANDARD V4.3“ vom 01.04.2021, TÜV Informationstechnik GmbH

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt. Hierbei sind die für den Prüfgegenstand nicht anwendbaren Prüfanforderungen ausgegraut.

Prüfgegenstand

Gegenstand der Prüfung ist der Sicherheitsbereich „RZ R“ der Atruvia AG. Dieser wird im Prüfbericht detailliert beschrieben.

Prüfergebnis

Das Prüfergebnis lautet „Level 3 (erweitert)“. Hierbei werden in den Bewertungsaspekten CON, FIR, CAB und ORG alle Anforderungen des nächst höheren Levels erreicht.

Zusammenfassung der Prüfanforderungen

Prüfanforderungen für Trusted Site Infrastructure, TSI.STANDARD V4.3:

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 Sicherheitssysteme 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 Rechenzentrumsverbund (DDC – Dual Site Data Center)

Der Rechenzentrumsverbund besteht aus zwei TSI geprüften Rechenzentren, die einzeln mindestens die Levelstufe unterhalb des Dual Site Levels erreicht haben. Die Rechenzentren befinden sich in getrennten Gebäuden mit getrennter Versorgung, haben eine redundante Datennetzverbindung und unterscheiden sich in der Größe um max. 30%. Bei Dual Site Level 4 haben die Rechenzentren einen Mindestabstand von mehreren Kilometern, abhängig von der Risikobetrachtung.

L 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)
Dual Site Level 2-4	Beide Rechenzentren erreichen einzeln mindestens die Levelstufe unterhalb des Dual Site Levels.