Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

LVM Versicherung
Kolde-Ring 21
48126 Münster

für den Sicherheitsbereich

Rechenzentrum DC2, Münster

die Erfüllung aller Anforderungen für hohen Schutzbedarf des Prüfkatalogs

Trusted Site Infrastructure TSI V3.2 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 zugehörigen Prüfbericht bis zum 31.12.2017.

Infra-structure TSI66286.15 2015 TÜViT® Trusted Site

Voluntary Validation

© TÜViT - Member of TÜV NORD GROUP

Zertifikat-Registrier-Nr.:
TUVIT-TSI66286.15

Essen, 02.12.2015

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

Zertifizierungssystem

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

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.0 vom 24.08.2015, TÜV Informationstechnik GmbH

Prüfbericht

- „Prüfbericht – Trusted Site Infrastructure (TSI), Rechenzentrum DC2, Münster“, Version 1.0 vom 24.11.2015, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Trusted Site Infrastructure – TSI Kriterienkatalog“, Version 3.2 vom 01.10.2014, TÜV Informationstechnik GmbH

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

Prüfgegenstand

Gegenstand der Prüfung ist der Sicherheitsbereich „Rechenzentrum DC2, Münster“ der LVM Versicherung. Dieser wird im Prüfbericht detailliert beschrieben.

Prüfergebnis

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

Zusammenfassung der Prüfanforderungen

Prüfanforderungen für Trusted Site Infrastructure (TSI), Version 3.2:

1 Umfeld (ENV – Environment)

Gefährdungspotenziale aus dem Umfeld sind zu meiden. Die Standortentscheidung des Objekts ist u. a. unter den Gesichtspunkten Wasser-, Explosions-, Trümmer-, Erschütterungs- und Schadstoffgefährdung zu treffen.

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. Die Trassenverläufe im Gebäude sind abgesichert. Eine Trennung zwischen Grob- und Feintechnik ist erfolgt.

3 Brandmelde- und Löschtechnik (FIR – Fire Prot. / Alarm / Extinguishing Systems)

Eine Brandmeldeanlage ist im gesamten Sicherheitsbereich installiert und bei der Feuerwehr 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)

Es existiert eine Zugangskontrollanlage (ZKA). Ein Einbruchschutz ist mehrstufig gegeben, dabei werden alle sicherheitskritischen Bereiche mittels einer Einbruchmeldeanlage überwacht. Die Anlage ist notstromversorgt und durchgeschaltet zu einer ständig besetzten Sicherheitszentrale.

5 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. Eine Notstromversorgung der IT- wie auch der Sicherheitssysteme ist gegeben.

6 Raumlufttechnische Anlagen (ACV – Air Conditioning and Ventilation)

Die Abwärme der IT-Geräte wie auch der Infrastrukturkomponenten wird durch Kühlung hinreichend abgefangen. Ein Staubschutz und die Einhaltung von Luftfeuchtwerten sind gegeben. Feuer- und Rauchklappen sind gemäß Brandschutzkonzept eingebaut. Die Einhaltung der Klimavorgaben wird fernüberwacht. Ausfälle sind durch eine redundante Auslegung abgefangen.

7 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 Kommunikation nach draußen ist auch beim Ausfall der TK-

Anlage sichergestellt. Die Datensicherungsmedien werden brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt.

8 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 liegen vor. Ein mit der Feuerwehr abgestimmtes Brandschutzkonzept ist vorhanden. Ein Notfallkonzept bzw. Alarmplan liegen vor.

9 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 5 km.

L Level

Level 1	Mittlerer Schutzbedarf (entspricht den Infrastrukturanforderungen der BSI Grundschutzkataloge)
Level 2	Erweiterter Schutzbedarf (mit ergänzenden Anforderungen bei o. g. Bewertungsaspekten)
Level 3	Hoher Schutzbedarf (vollständige Redundanzen kritischer Versorgungssysteme – No Single Point of Failure, klimatische Grenzwerteinhaltung gem. EN 1047-2)
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.