Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

is4 IT-Services GmbH & Co. KG
Marienstraße 88
32425 Minden

für den Sicherheitsbereich

Rechenzentrum 2

die Erfüllung aller Anforderungen für hohen Schutzbedarf des Prüfkatalogs

Trusted Site Infrastructure TSI V1.3 Level 2

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

Die Anlage ist Bestandteil des Zertifikats und besteht aus 3 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht 6632_6642_BD, V 1.0 vom 10.11.2006.

Dieses Zertifikat ist bis zum 31.10.2009 gültig.

Infra-structure TSI6642.07 TÜViT® 2007 Trusted Site

Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-TSI6642.07

Essen, 29.10.2007 **gez. Dr. Sutter**
Zertifizierungsstelle

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

Prüfbericht

TÜV®

Prüfbericht – Trusted Site Infrastructure zu den Rechenzentren 1 und 2 der is4 IT-Services GmbH & Co. KG, Version 1.0 vom 10.11.2006, TÜV Informationstechnik GmbH

Prüfanforderungen

Zusammenfassung der Anforderungen für Trusted Site Infrastructure (TSI), Version 1.3

1 Dokumentation

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 und ein Wiederanlaufplan liegen vor.

2 Bauliche Gegebenheiten

Das Gebäude ist unauffällig und liegt in keinem unmittelbaren Gefahrenbereich. Das Mauerwerk bzw. die umgebende Konstruktion sowie Fenster und Türen bieten einen Zugriffs-, Brand- und Trümmerschutz. Das Gebäude ist gegen Blitzeinschlag geschützt. Der Sicherheitsbereich liegt abseits öffentlicher Zugänge, gefährlicher Produktionsprozesse, EM/RF-Störpotentiale und wassergefährdender Gebäudeabschnitte. Der Sicherheitsbereich befindet sich in einem eigenen Brandabschnitt.

3 Sicherheitssysteme

Es existiert ein Zugangskontrollanlage (ZKA) für den Sicherheitsbereich und allen Infrastrukturkomponenten (z. B. Verteiler der Versorgungsnetze). 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.

4 Energieversorgung

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. Notstromversorgung der IT- wie auch der Sicherheitssysteme ist gegeben. Eine redundante Einspeisung der Elektroversorgung über das öffentliche Netz ist vorhanden.

5 Brandmelde- und Löschtechnik

Eine Brandmeldeanlage ist in 2-Linienausführung im gesamten Sicherheitsbereich installiert und bei der Feuerwehr aufgeschaltet. Nebenräume, doppelter Fußboden, abgehängte Decken und Luftkanäle sind in die Brandüberwachung einbezogen. Neben der Alarmierung werden Schadensbegrenzungsmaßnahmen ausgelöst. Eine Versorgung mit geeigneten Handfeuerlöschern ist gegeben.

6 Raumlufttechnische Anlagen

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

Alle Sicherheitseinrichtungen werden einem regelmäßigen Funktionstest unterzogen. Regelmäßige Wartungen an Verschleißteilen der Infrastrukturkomponenten bzw. IT-Hardware sind in einem Einsatzplan festgelegt. Die Kommunikation nach draußen ist auch beim Ausfall der TK-Anlage sichergestellt. Die Datensicherungsmedien werden brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt.

L Level 2 und Level 3 Aspekte

Bei Level 2 wird ein Sicherheitskonzept zur Verfügung gestellt. Bei Level 3 sind folgende Zusatzkriterien erfüllt: Risikoanalyse Umfeld; Temperatur- & Luftfeuchtegrenzwerte gem. EN 1047; Erhöhte Widerstandsfestigkeit von Fenstern & Türen; ZKA mit Identifizierung, Bewegungsmelder; Schutz der Versorgungsleitungen; TN-S Netz, Netzersatzanlage; redundante USV; Brandfrühesterkennung; Rauchdichtigkeit; Überwachung Frischluft, Regelungen Systemerweiterung, redundante Datennetzanbindung; angepasste Wartungsverträge.