Sichere Infrastrukturen für IT-Systeme

TÜV NORD GROUP

Trusted Site Infrastructure

Infra-structure 2017 Trusted Site

Certificate ID: 00000.17

Inhalt

1 Einleitung

Informations- und Kommunikationssysteme bilden die Grundlage für eine Vielzahl von unternehmerischen Entscheidungen und Aktivitäten. Ihre Verfügbarkeit hat eine elementare Bedeutung für das Unternehmen. Ausfälle können heutzutage schnell existenzbedrohend werden.

Zeitkritische Zugriffe, Just-in-time Abläufe, ein hoher Vernetzungsgrad und Online-Geschäfte steigern erheblich den Verfügbarkeitsanspruch wie auch die Anforderungen an die Leistungsfähigkeit der Systeme, der Datenhaltung und der unterstützenden Infrastruktur. Dabei ist in den letzten Jahren eine Tendenz zur Zentralisierung der geschäftskritischen Produktiv-Hardware zu verzeichnen. Um die Wahrscheinlichkeit von Systemausfällen und Datenverlusten in derart konzentrierten Umgebungen zu verringern, bedarf es ausgereifter Schutzkonzepte und verlässlicher sicherheitstechnischer Bewertungen.

Diese Bewertungen sind je nach Branche auch dort sinnvoll, wo eine methodische Risikoeinschätzung belastbare Aussagen gegenüber Dritten liefern soll oder wo Grundlagen für eigene Einschätzungen gesucht werden, z. B. bei Versicherungspolicen.

1.1 Gefährdungspotenziale

Das Gefährdungspotenzial im Bereich physischer Sicherheit ist vielfältig und in seinen Auswirkungen gravierend. Laut den IT-Grundschutz-Katalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden die folgenden vier Gefährdungskategorien angenommen:

- **Höhere Gewalt**, wie zum Beispiel Blitz, Feuer oder Wasser.
- **Organisatorische Mängel**, etwa fehlende oder unzureichende Regelungen oder unbefugter Zutritt zu schutzbedürftigen Räumen.
- **Technisches Versagen**, zum Beispiel der Ausfall von Stromversorgung, internen Versorgungsnetzen und vorhandenen Sicherungseinrichtungen.
- **Vorsätzliche Handlungen**, wie unbefugtes Eindringen, Diebstahl, Vandalismus und Anschläge.

1.2 Physische Sicherheit

Die Funktionssicherheit von IT-Systemen kann nur durch ein ganzheitliches Schutzkonzept optimiert werden. Die Sicherheitsaspekte auf dem Gebiet der Infrastruktur, sprich die physische Sicherheit, sind ebenso wichtig wie die organisatorische und die informationstechnische Sicherheit (IT-Systeme und ihre Anwendungen). Für die beiden letztgenannten Sicherheitsaspekte gibt es zunehmend Verfahren und Lösungen (siehe Kapitel 6), wogegen die physische Sicherheit lange Zeit kaum systematisch untersucht wurde. Dies hat sich mit dem Erscheinen der EN 50600 Norm geändert. Hiermit steht erstmals ein umfänglicher, europäisch abgestimmter Leitfaden zur Verfügung.

Der Kriterienkatalog der TÜV Informationstechnik GmbH hilft seit 14 Jahren, gezielt und vollständig die physischen Gegebenheiten zu erfassen, zu beurteilen und zu bewerten. Die Katalogversion TSI V4.0 deckt die Anforderungen der DIN EN 50600 Norm ab und empfiehlt sich als standardisierte Prüfmethodik für die DIN EN 50600 Konformitätsbewertung.

1.3 Ziele

Die objektive Identifikation und angemessene Behebung von Sicherheitsrisiken der IT-Infrastruktur sind ein unmittelbares Anliegen eines IT-Betreibers. Es geht darum, Präventivmaßnahmen zum physischen Schutz der IT- und Kommunikationssysteme durchzuführen und eine Infrastruktur sicherzustellen, die den Anforderungen auf Basis von vorhandenen Normen und ihren Grenzwerten genügt. Ziel ist dabei, eine möglichst hohe System- und Datenverfügbarkeit und eine nahezu hundertprozentige Funktionssicherheit zu garantieren.

2 Trusted Site Infrastructure (TSI)

Die TÜV Informationstechnik GmbH (TÜViT) hat durch Erfahrungen bei der Abnahme von Trust Center für elektronische Signaturen ein standardisiertes Verfahren zur Prüfung von sicheren Infrastrukturen für IT-Systeme entwickelt und die dabei als sachgerecht anerkannten Maßnahmen berücksichtigt. Das Verfahren ist in das TÜViT-Zertifizierungsprogramm „Trusted Site“ als

Trusted Site Infrastructure (TSI)

aufgenommen. Der zugrunde liegende Prüfkatalog im derzeitigen Versionsstand orientiert sich an den Maßnahmenempfehlungen der Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI), berücksichtigt die einschlägigen EN- und DIN-Normen, insbesondere der DIN EN 50600: Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren, VDE-Vorschriften und VdS-Publikationen und trägt den Erkenntnissen aus dem Praxisalltag im Sinne von „Best Practices“ Rechnung.

Das Verfahren erlaubt die Untersuchung der einer IT-Installation zugrunde liegenden Infrastruktur in angemessener Weise unter besonderer Berücksichtigung der individuellen Umgebung und der häufig anzutreffenden Komplexität solcher Installationen.

TSI ist im Jahr 2002 eingeführt worden und ist heute im Markt als Bewertungsschema für die physische Sicherheit akzeptiert. Dazu beigetragen haben die stete Weiterentwicklung des Programms und die Zusammensetzung des Auditorenteams mit Sachverständigen aus den unterschiedlichen Disziplinen. Die Basis für eine nachvollziehbare und transparente Bewertung von Rechenzentren ist der TSI-Kriterienkatalog. Der kompakte, leicht verständliche und übersichtliche Kriterienkatalog wird mittlerweile häufig in Ausschreibungen für neue Rechenzentrums-projekte als verbindliche Umsetzungsanforderung zitiert und dient als Maßstab für Rechenzentren nach dem Stand der Technik.

Es gibt eine Vielzahl von Möglichkeiten, ein sicheres Rechenzentrum zu realisieren, dabei ist die Kombination der Möglichkeiten schier unendlich.

Comply or Explain

Das hohe Maß an Expertise unserer Auditoren ermöglicht ein Vorgehen nach dem Prinzip „Comply or Explain“ und bietet eine deutlich größere Flexibilität als reine Checklisten. Dies bedeutet, dass ein Rechenzentrum nicht immer genau eine „typische“, allgemein anerkannte oder „geforderte“ Lösung bietet, sondern dass ein Betreiber für ein spezielles Rechenzentrum mit alternativen Lösungen mitunter genauso gut aufgestellt ist oder eine besondere Herausforderung sogar besser löst. „Comply or Explain“ bedeutet in diesem Fall, dass auch Sonderlösungen positiv bewertet werden können, wenn sie genauso wirksam und zuverlässig sind.

Wer sind unsere Kunden?

TSI-zertifizierte Rechenzentren finden sich in unterschiedlichen Branchen, wie z. B. Banken, Energieversorgungsunternehmen, Co-Locationanbietern, in der chemischen Industrie, Automobilindustrie, Flughäfen, mittelständische Produktionsbetriebe, etc.

Der Anwendungsbereich von Trusted Site Infrastructure (TSI) ist aber nicht auf IT- und Kommunikationssysteme beschränkt. Auch andere zu schützende Werte in Sicherheitslagern oder Archiven benötigen Infrastrukturmaßnahmen, um sie vor Zugriffen zu schützen oder um Anforderungen an Umgebungsbedingungen zu erfüllen. Die zu berücksichtigenden Bewertungsaspekte (siehe Kapitel 3) treffen in aller Regel auch auf die zuletzt genannten Anwendungsbereiche zu.

Was bringt Ihnen eine Zertifizierung?

Eine Zertifizierung demonstriert die Funktionssicherung unter den geforderten Schutzzielen gegenüber Dritten und erzeugt Vertrauen auf der Grundlage einer „Third Party Inspection“. Hieraus ergeben sich Vorteile, wie z. B.:

- Sicherheit bei der Planungsvergabe eines neuen Rechenzentrums, wenn die Zertifizierung zum Ausschreibungsbestandteil wird
- Vertrauensnachweis für die Marktpositionierung, da mit der Erteilung eines Zertifikats die besonderen Anstrengungen hinsichtlich der Sicherheitsmaßnahmen dokumentiert werden und ein Wettbewerbsvorteil herausgestellt werden kann
- Qualitätssicherung und auch -verbesserung bei eigener Projektsteuerung sowie Standortbestimmung für interne Entscheidungsprozesse
- Vertrauenssicherung gegenüber überwachenden Institutionen
- Nachweis für die Innenrevision
- Bei regelmäßiger Überprüfung die Gewissheit, das Rechenzentrum auf dem Stand der Technik zu haben, da die TSI-Anforderungen weiterentwickelt werden

Unsere Auditoren erstellen einen detaillierten Prüfbericht für Ihr Rechenzentrum. Mit diesem dokumentieren Sie gegenüber Dritten die Qualität Ihrer Installationen und Ihre Zuverlässigkeit als Betreiber oder Dienstleister. Behörden, Kunden und Versicherer können sich anhand des Prüfberichts davon überzeugen, dass Ihr Rechenzentrum konsequent auf Verfügbarkeit und Sicherheit ausgerichtet ist. Ein TSI-Prüfbericht kann den Zeitaufwand für Audits zu übergeordneten Zertifizierungen (z. B. für Ihre gesamte Firma) drastisch reduzieren.

Von diesen Vorteilen profitieren prinzipiell alle Rechenzentrumsbetreiber. Einige Aspekte treffen aber in besonderem Maße auf ASPs, ISPs, Colocationanbieter und Industriezweige zu, die in ausgeprägten Verfügbarkeits- oder Sicherheitsverpflichtungen als Dienstleister stehen.

3 Bewertungsaspekte

Für die TSI-Zertifizierung stellt TÜViT auf der Basis von erfüllten Mindestanforderungen das von einer IT-Infrastruktur erreichte Sicherheitsniveau fest. Dabei wird eine Reihe von Bewertungsaspekten in die Untersuchung einbezogen (siehe Abbildung 1):

- Umfeld (**ENV**: Environment)
- Baukonstruktion (**CON**: Construction)
- Brandschutz, Melde- & Löschtechnik (**FIR**: Fire Protection, Alarm & Extinguishing Systems)
- Sicherheitssysteme & -organisation (**SEC**: Security System & Organization)
- Struktur der Verkabelung (**CAB**: Cabling)
- Energieversorgung (**POW**: Power Supply)
- Raumlufttechnische Anlagen (**ACV**: Air Conditioning & Ventilation)
- Organisation (**ORG**: Organization)
- Dokumentation (**DOC**: Documentation)
- Rechenzentrumsverbund (**DDC**: Dual Site Data Center)

Abbildung 1: Bewertungsaspekte der TSI-Zertifizierung

Für jeden der in Kapitel 0 benannten Bewertungsaspekte gibt es eine Reihe von definierten Kriterien, die bei der TSI-Zertifizierung angewendet werden. Die damit verbundenen Anforderungen sind in Kapitel 10 in Listen zusammengestellt und in den folgenden Abschnitten kurz erläutert.

3.1 Umfeld

Das Gebäude umgibt die aufgestellte Informationstechnik und bietet einen äußeren Schutz. Die Lage des Gebäudes spielt hinsichtlich der umliegenden Gefahrenpotenziale ebenso eine Rolle wie die Lage des Sicherheitsbereichs im Gebäude, um gegebenen potenziellen Gefahrenquellen a priori auszuweichen. Umgebungsgefährdungen, hervorgerufen durch Wasser, Explosionen, Trümmer, Erschütterungen oder Schadstoffe werden gemieden. Ebenso werden Verkehrswege mit Gefahrguttransporten gemieden, um sich direkten wie indirekten Auswirkungen wie z. B. Absperrungen zu entziehen.

3.2 Baukonstruktion

Das Mauerwerk, Fenster und Türen bieten einen Zugriffs- (DIN V EN 1627), Brand- und Rauchschutz (DIN 18095). Ebenso ist sichergestellt, dass wassergefährdete Gebäudeabschnitte (VdS 2007), EM/RF-Störfelder (EN 50147 Teil 1) und gefährliche Produktionsprozesse in angrenzenden Räumen gemieden werden. Das Gebäude verfügt über einen äußeren Blitzschutz (EN 62305-1) und mindestens der Sicherheitsbereich stellt einen eigenen Brandabschnitt dar (DIN 4102). Die Versorgungsleitungen sind in Schutz gebenden Konstruktionen verlegt. Der Funktionserhalt der IT-Systeme und der Datenträger ist bei Umgebungsbränden in Nachbarräumen sichergestellt (EN 1047-2).

3.3 Brandschutz, Melde- und Löschtechnik

Die Risikofaktoren Feuer und Rauchgase lassen sich über Brandmeldeanlagen (DIN EN 54), Brandfrühesterkennung (DIN EN 54-20), Brandschutzklappen und Gaslöschtechnik beherrschen. Die Brandmeldesensorik (DIN EN 54) berücksichtigt alle Sicherheitsbereiche und ist an den richtigen Stellen angebracht. Ein Brandschutzkonzept ist mit der örtlichen Feuerwehr abgestimmt.

Die Brandmeldeanlage ((DIN EN 54, VdS 2095, DIN 14675, DIN VDE 833-2) überwacht den gesamten Sicherheitsbereich und ist über eine sichere Verbindung bei einer ständig besetzten Stelle aufgeschaltet.

Nebenräume, doppelter Fußboden, abgehängte Decken und Luftkanäle sind in die Brandüberwachung einbezogen worden. Wichtig ist, dass neben der Alarmierung Schadensbegrenzungsmaßnahmen ausgelöst werden, etwa durch eine Gaslöschanlage im Sicherheitsbereich (VdS 2380, VdS 2093) oder durch andere geeignete Maßnahmen.

3.4 Sicherheitssysteme und -organisation

Die Sicherheitssysteme bieten einen Schutz vor vorsätzlichen Handlungen. Hierzu zählen ein Zugangskontrollsystem und eine Einbruchmeldeanlage, um Diebstahl (Hardware wie Daten), Sabotage und Vandalismus frühzeitig zu entdecken, Akteure abzuschrecken und rechtzeitig Gegenmaßnahmen einzuleiten.

Ein Zugangskontrollsystem inklusive entsprechender Zugangsregelung ist sowohl für den Sicherheitsbereich wie auch für alle Infrastrukturkomponenten (z. B. Verteiler) vorhanden (EN 60389-11). Der Einbruchschutz ist mehrstufig ausgelegt und alle sicherheitskritischen Bereiche sind mittels einer Einbruchmeldeanlage überwacht (EN 50131). Dabei sind die Anlagen ebenfalls mit Notstrom versorgt und über einen gesicherten Übertragungsweg (EN50136 und EN 50518) zu einer ständig besetzten Sicherheitszentrale durchgeschaltet.

3.5 Telekommunikationsverkabelung

Die Kommunikationsverkabelung stellt die Verbindung des Rechenzentrums zur Außenwelt dar. Die innere Verkabelung wird je nach Anspruch auf einfachen Wegen bis hin zu redundanten Wegeführung unter Nutzung redundanter aktiver Komponenten ausgeführt. Kommunikations- und (Kupfer basierte) Datenkabel sind gemäß EN 50174-2 mit dem nötigen Abstand zueinander auf getrennten Kabelführungen verlegt. Die Verkabelung erfolgt über Haupt, Bereichs- und Lokalverteiler und erlaubt einen leichten Um- und Ausbau ohne Betriebsunterbrechung. Punkt-zu-Punkt-Verkabelung wird vermieden. Datenkabel werden nicht durch Bereiche mit Gefährdung verlegt oder sind speziell geschützt. WAN-Trassen verlaufen kreuzungsfrei und es ist ein Anschluss an mind. 2 Provider realisiert.

3.6 Energieversorgung

Die Energieversorgung ist für die IT-Systeme essentiell. Sie bedient unterschiedlichste Leistungsabnehmer und unterliegt steter Veränderung. Die Elektroinstallation ist auf der Basis der einschlägigen nationalen Normen und Vorschriften (insbesondere in Deutschland DIN VDE 0100) ausgeführt und gegen Überspannung geschützt. Angepasste Aufteilungen und Absicherungen der Stromkreise sind vorgesehen und Vorkehrungen für Erweiterungen getroffen. Die IT-Systeme werden unterbrechungsfrei mit Strom versorgt (EN 62040 bzw. EN 88528-11). Alle kritischen Infrastrukturen (IT-, Telekommunikations-, Sicherheits- und Klimasysteme) sind an eine Notstromversorgung angeschlossen.

Bei der Einspeisung sind Ausweichmöglichkeiten gegeben, wie etwa ein Ringanschluss. Die Elektroinstallation ist im gesamten Gebäude als TN-S-Netz ausgelegt, ansonsten sind besondere Vorkehrungen hinsichtlich der Elektroverteilung zu treffen. Grundsätzlich werden IT-Geräte getrennt von anderen Verbrauchern versorgt. Der Überspannungsschutz ist mindestens in zwei Stufen ausgeführt (VdS 2833), ein Potenzialausgleich (DIN EN 50310) ist sichergestellt und eine Differenzstromüberwachung (DIN EN 62020) in wichtigen Segmenten ist gegeben.

3.7 Raumlufttechnische Anlagen

IT-Systeme wie auch Archive und Komponenten der Stromversorgung (USV, Batterien) sind auf bestimmte Umgebungsbedingungen angewiesen. Lufttemperatur, relative Luftfeuchte und Staubanteil werden innerhalb vorgegebener Grenzwerte gehalten. Eine Kontamination der Außenluft wird erkannt und ein automatischer Verschluss der Außenluft sichergestellt.

Die Grenzwertüberwachung in den IT-Räumen erfolgt redundant. Außenanlagen sind in das Blitzschutzkonzept eingebunden und sind gegen unbefugten Zutritt geschützt. Eine redundant ausgelegte Klimatisierung erhöht die Verfügbarkeit und ermöglicht Wartungen ohne Betriebsunterbrechung. Die Anlagenteile sind in das Brandschutzkonzept eingebunden. Der Ausfall von Mess-, Steuer- und Regeltechnik ist fehlertolerant ausgelegt. Maßnahmen gegen und zur Detektion von Leckagen sind getroffen. Trassen sind gegen Gefährdungen geschützt. Die Anlagen sind in der Lage, die Wärmeabgabe der IT auch bei hohen Außentemperaturen sicher abzuführen. Der Betrieb der Anlagen wird über eine Gebäudeleittechnik überwacht.

3.8 Organisation

IT-Infrastrukturkomponenten können auch versagen. Die Komponenten werden daher regelmäßigen Überprüfungen des Zustandes und der Eigenschaften unterzogen, um die ständige Wirksamkeit und Verfügbarkeit der Infrastrukturkomponenten im Sinne der Sicherheitsanforderungen belegen zu können. Verantwortlichkeiten sind klar definiert. Genauso sind Regelungen notwendig, die Zutrittsberechtigungen definieren, bei Erweiterungen an Infrastrukturkomponenten die Prüfung von Seiteneffekten veranlassen und die Schulung der Mitarbeiter sicherstellen. Auch die regelmäßige Sicherung oder Spiegelung der Daten zu einer zweiten Lokation wird als essenziell angesehen.

Verfahrensanweisungen regeln die Prüfung der Auslegung der Elektroinstallation und der raumlufttechnischen Anlagen bei Erweiterungen. Alle Sicherheitseinrichtungen werden regelmäßigen Funktionstests unterzogen. Ein jährlicher Wartungsplan definiert Art und Intervall der Wartung an Verschleißteilen der Infrastrukturkomponenten. Unverzichtbar ist, die Kommunikation nach draußen auch beim Ausfall der TK-Anlage sicher zu stellen. Die Datensicherungsmedien müssen brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt und gemäß EN 1047 ausreichend geschützt werden.

Ein Lifecyclemanagement wie auch ein Kundenmanagement (soweit die Konstellation zutrifft) ist eingeführt. Wichtige Schlüsselindikatoren zum sicheren und nachhaltigen wie auch energieeffizienten Betrieb des Rechenzentrums werden erfasst, ausgewertet und zur Verbesserung genutzt.

3.9 Dokumentation

Die Überprüfung der Maßnahmen und der installierten Infrastruktur kann nachhaltig nur im Kontext einer dokumentierten Risikoanalyse bzw. eines Sicherheitskonzepts erfolgen. Daraus leiten sich Art und Umfang der Präventivmaßnahmen ab. Die gewonnenen Erkenntnisse dienen dazu, das Gefährdungspotenzial für das Unternehmen bei Ausfall der IT-Systeme abzuschätzen und transparent zu machen.

Die Infrastrukturinstallation wird ihrem Verfügbarkeitsanspruch letztendlich nur dann gerecht, wenn im Schadensfall Verhaltensregeln vorliegen und auf aktuelle Pläne und Dokumentationen zurückgegriffen werden kann, um schnelle, sachgerechte und sichere Reaktionen zu gewährleisten.

Die Dokumentation sollte sich deshalb nicht nur auf die Beschreibung von Maßnahmen (DIM) beschränken sondern zu einem umfassenden Sicherheitskonzept (Siko) ausgebaut werden.

Im Sicherheitskonzept werden Schwachstellen und Gefährdungen identifiziert, resultierende Risiken bewertet, Kompensationsmaßnahmen daraus abgeleitet und ihre Umsetzung beschrieben. Regelungen werden schriftlich dargelegt und sind im Unternehmen den Betroffenen bekannt. Wartungspläne sind ggf. durch entsprechende Verträge abgesichert. Je nach angestrebtem Bewertungslevel (siehe Kapitel 4.1) wird für eine erfolgreiche Prüfung entweder eine „Dokumentation der Infrastrukturmaßnahmen“ (DIM) oder ein vollständiges Sicherheitskonzept bereitgestellt.

4 TSI-Zertifizierungsprojekt

4.1 Bewertungslevel

Der Prüfkatalog ermöglicht TÜViT, den Zustand der Infrastruktur zu beurteilen und erlaubt, daraus Verfügbarkeitsaussagen für die IT-Installation abzuleiten. So erhält der Betreiber bei der Abnahme der installierten Infrastrukturkomponenten die Sicherheit, alle notwendigen Vorkehrungen getroffen und für ein funktionierendes Zusammenwirken aller Komponenten gesorgt zu haben.

Zertifiziert werden können vier Sicherheitsstufen, die aufeinander aufbauen: Level 1 bis Level 4 oder anders ausgedrückt: grundsolide bis high-end:

- **Level 1** – Mittlerer Schutzbedarf

Die Anforderungen im Level 1 entsprechen denen der BSI Grundschutz-Kataloge in der Schicht Infrastruktur bzgl. der Bausteine Serverraum, Gebäude, elektrotechnische Verkabelung, Datenträgerarchiv und Raum für technische Infrastruktur. Abhängig von der Schutzbedarfserhebung können die BSI-Vorgaben bzgl. Brandisolierung (DIN EN 1047-2) und Netzersatzaggregat zur Anwendung kommen, was in den höheren TSI Level berücksichtigt wird.

- **Level 2 – Erweiterter Schutzbedarf**

Diese Sicherheitsstufe definiert ergänzende Anforderungen bei allen Bewertungsaspekten. Insbesondere wird die Standortwahl bewertet und an Hand eines Sicherheitskonzepts eine detaillierte Analyse vorgenommen. Die Anforderungen an die Wirksamkeit der Maßnahmen sind erhöht. Redundanzen in der Energieversorgung und die Sicherstellung einer sekundären Energieversorgung sind obligatorisch.

- **Level 3 – Hoher Schutzbedarf**

Die Möglichkeit, Wartungen ohne Unterbrechung des Betriebs durchzuführen, die Beherrschung von Komponentenfehlern, Trassen- oder Raumverluste in der Elektro-versorgung zeichnen Level 3 aus. Des Weiteren gibt es ergänzende Anforderungen in der Klimatisierungstechnik, erhöhte Anforderungen an die Einbruchhemmung und zusätzliche Zutrittsrestriktionen. Ggf. vorhandene Standortrisiken werden kompensiert.

- **Level 4 – Sehr hoher Schutzbedarf**

Ein dediziertes Gebäude für den alleinigen RZ-Betrieb, vollständige Pfadredundanzen der Versorgungssysteme und darüber hinaus ausgeprägte Zutrittssicherung über Perimeterschutz und Vereinzelungsanlagen kennzeichnen Level 4. Die Nachbarschaft muss gefährdungsfrei sein und auf Alarmmeldungen muss innerhalb minimaler Interventionszeiten reagiert werden können.

- **Erweitert**

Der ausgewiesene Level im Zertifikat ist der minimal erreichte Level über alle Bewertungsaspekte. Sind alle Anforderungen eines Bewertungsaspekts (ENV, CON, FIR, SEC, CAB, POW, ACV) im nächst höheren Level erfüllt, werden diese Aspekte mit dem Attribut „erweitert“ im Zertifikat ausgezeichnet.

4.2 Workshop

TÜViT vertieft die in diesem Dokument dargelegten Bewertungsaspekte auf Wunsch in Form eines Workshops beim Interessenten. Dieser Workshop dient sowohl der Entscheidungsfindung als auch der Vorbereitung auf eine Zertifizierung. Gleichzeitig erfolgt eine erste Planungsbegutachtung oder aber bei einer vorhandenen Installation eine Einschätzung der Prüffähigkeit. TÜViT weist den Interessenten dabei auf offensichtliche Abweichungen hin. Weitere Inhalte des eintägigen Workshops sind:

- Darstellung der Prüfabläufe,
- Detaildarstellung und Diskussion der Bewertungsaspekte,
- Zuordnung der Anforderungen zu den Level,
- Hinweise zum Aufbau eines Sicherheitskonzepts,
- Begehung des Rechenzentrums bzw. Einsichtnahme in die Pläne bei einem Neubau, sowie
- Diskussion des weiteren Vorgehens.

4.3 Projektablauf

Nach dem Workshop entscheidet der Interessent, ob er in die Evaluierung einsteigen möchte. Ist dies der Fall, muss eine Dokumentation der Infrastrukturmaßnahmen (DIM für Level 1) oder ein Sicherheitskonzept mit den entsprechenden Plänen zur detaillierten Prüfung eingereicht werden.

Anhand der Dokumentation überprüft und kommentiert TÜViT den Umfang, die Wirkung und die widerspruchsfreie Anwendung der Maßnahmen. Es wird dem Kunden die Möglichkeit gegeben, das Dokument zu überarbeiten und erkannte Schwachstellen zu bereinigen. Ist die Überarbeitung erfolgt, gilt die Dokumentation als Grundlage für den weiteren Bewertungsprozess. Im anschließenden Vorort-Audit (Umsetzungsprüfung) prüft TÜViT, ob die Maßnahmen und Komponenten wie beschrieben umgesetzt bzw. eingesetzt werden.

Anschließend erstellt TÜViT einen Prüfbericht für den Kunden. Vorausgesetzt, dass alle Kriterien erfüllt sind, erhält der Kunde ein Zertifikat, das zur Nutzung eines entsprechenden Prüfzeichens berechtigt.

4.4 Zertifikat und Prüfzeichen

Auf der Basis der Bewertungskriterien für Trusted Site Infrastructure wird bei Erfüllung aller Teilaspekte für den untersuchten Sicherheitsbereich ein Zertifikat erteilt (**Abbildung 2**).

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

<Firma>
<Straße>
<Ort>

für den Sicherheitsbereich

<Rechenzentrum>

die Erfüllung aller Anforderungen des Regelwerks

<Trusted Site Infrastructure TSI V4.0 Level 4>

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

Die Anlage ist Bestandteil des Zertifikats und besteht aus <X> Seite(n).

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht, Version 0.0 vom <Datum>.

Dieses Zertifikat ist bis zum <Datum> gültig.

Infra-structure 2017 Trusted Site

Certificate ID: 00000.17

Essen, <Datum> gez. Dr. Sutter
Zertifizierungsstelle

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

Abbildung 2: Musterzertifikat Trusted Site Infrastructure

Das Zertifikat berechtigt zur Nutzung des Prüfzeichens „Trusted Site Infrastructure“ (siehe Deckblatt). Die Bewertungsaspekte aus Kapitel 3 sind im Anhang zum Zertifikat abgedruckt. Das Zertifikat ist zwei Jahre gültig und kann danach verlängert werden.

Das Prüfzeichen steht sowohl für die Website als auch für Broschüren des Betreibers zur Verfügung und kann entsprechend werbewirksam eingesetzt werden. Ebenso wird – kein Widerspruch vorausgesetzt – das Zertifikat unter www.tuvit.de veröffentlicht.

4.5 Re-Zertifizierung

Das Zertifikat ist zwei Jahre gültig und kann durch eine Re-Zertifizierung um weitere zwei Jahre verlängert werden. Das Audit bzw. die Begehung des Rechenzentrums erfolgt ca. sechs Monate vor Ablauf des Zertifikats, um dem Betreiber für den Fall von Abweichungen Gelegenheit zu geben, diese bis zum Ablauf des Erstzertifikats zu korrigieren. Das Folgezertifikat beginnt mit dem Ablaufdatum des Erstzertifikats. Voraussetzung ist, dass es keine Abweichungen zum Zeitpunkt des Zertifikatswechsels gibt. Hierdurch ist ein kontinuierlicher, unterbrechungsfreier Nachweis der Güte des Rechenzentrums gegenüber Dritten möglich. Die Planung der Überprüfungszeiträume sowohl auf Betreiber- wie auch auf der Prüferseite kann ohne Aufwand vorgenommen werden. Jährliche Überwachungsaudits – wie bei Managementaudits üblich – entfallen und reduzieren so Ihren Aufwand.

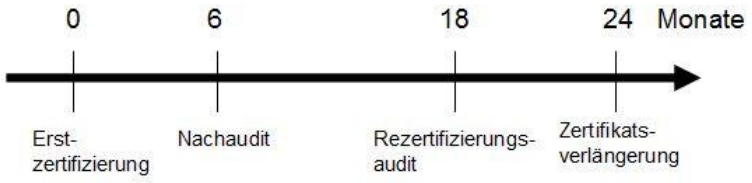

Abbildung 3: Zeitablauf Re-Zertifizierung

5 Dual Site Zertifizierungsanforderungen

Bei der Konzeption von Rechenzentren sind zwei Trends feststellbar: zum einen ist eine Konsolidierung von Rechenzentren zu verzeichnen, die zur Aufgabe vieler kleiner Serverräume zugunsten einiger weniger größerer Installationen führt. Zum anderen wird konsequent eine Risikoverteilung auf mindestens zwei Standorte verfolgt, wobei die Aufwände für die Versorgungstechnik ausgewogen und auf diesen Fall angepasst sind. Diesem Trend trägt TSI mit einer Dual Site Zertifizierung Rechnung. Hier werden zwei Rechenzentren im Verbund bewertet. Der erreichte Zertifizierungs-Level des Dual Site Zertifikats hängt von den erreichtem Level jedes einzelnen Rechenzentrums ab.

Voraussetzung für ein Dual Site Zertifikat ist, dass

- sich die IT-Flächen der beiden Rechenzentren in der Größe um maximal 1/3 unterscheiden.
- für beide Rechenzentren eine erfolgreiche TSI-Prüfung durchgeführt wurde.
- die beiden Rechenzentren durch eine redundante Datennetz-verbindung verbunden sind.
- Umgebungsgefährdungen sich nie gleichzeitig auf beide Rechen-zentren auswirken können.
- sich die Rechenzentren in getrennten Gebäuden befinden und getrennte Versorgungsinfrastrukturen aufweisen.

Je nach Zertifizierungslevel sind für ein Dual Site Zertifikat weitere Forderungen zu erfüllen:

- **Dual Site Level 2**

Die beiden Rechenzentren sind Level 1 geprüft mit Erweiterungen in einigen Bewertungsaspekten (CON, SEC, ORG, DOC). Des Weiteren ist eines der Rechenzentren mit einem Netzersatzgerät ausgestattet.

- **Dual Site Level 3**

Die beiden Rechenzentren sind Level 2 geprüft mit Erweiterungen in einigen Bewertungsaspekten (CON, SEC, DOC).

- **Dual Site Level 4**

Die beiden Rechenzentren sind Level 3 geprüft mit Erweiterungen in einigen Bewertungsaspekten (SEC, DOC). Des Weiteren haben die beiden Rechenzentren einen Abstand von mehreren Kilometern. Eine ständig besetzte Sicherheitszentrale befindet sich an einen der Standorte.

Das Dual Site Zertifikat gilt unter der Bedingung, dass IT-Komponenten redundant in beiden Rechenzentren aufgestellt werden.

6 Weitere TSI-Dienstleistungen

Mit der Anerkennung des TSI-Katalogs im Markt wächst die Nachfrage an TSI-bezogenen Dienstleistungen der TÜViT. Aktuell erstreckt sich das Portfolio neben den Prüf- und Zertifizierungstätigkeiten auf:

- **Bewertungen von Entwurfsplanungen**

Die Planung neuer Rechenzentren wird häufig unter Berücksichtigung der TSI-Kriterien vorgenommen und die Zertifizierung nach einem bestimmten Zertifizierungslevel in Rechenzentrumsausschreibungen vorgegeben. Hat die Planung das Entwurfsstadium erreicht, kann sie von TÜViT auf eine spätere Zertifizierungsfähigkeit hin bewertet werden und dem Planungsbüro wie auch dem Bauherren Planungssicherheit geben.

- **Standortbewertungen**

Der TSI-Katalog enthält u. a. Anforderungen an den Standort. Das erreichbare Sicherheitsniveau hängt letztendlich auch von dem Standort und der Beherrschung möglicher Umgebungsgefährdungen ab. In diesem Zusammenhang bietet TÜViT Standortbewertungen an, um eine optimale Ausgangsposition für das zu planende Rechenzentrum zu garantieren.

- **Schwachstellen-/Gap-Analysen**

Zur Einschätzung der Verfügbarkeitsqualitäten bestehender Rechenzentren und zur Aufdeckung von Schwachstellen bietet TÜViT eine Gap-Analyse an, in der Abweichungen zu den TSI-Anforderungen identifiziert und Verbesserungspotenzial aufgezeigt werden. Diese Hilfestellungen können mittels Planungshäusern zu konkreten Maßnahmen ausgearbeitet und umgesetzt werden, um ein zertifizierungsfähiges Rechenzentrum zu erhalten.

- **Qualitätssicherung bei der Inbetriebnahme**

Eine qualifiziert begleitete Inbetriebnahme leistet zusätzlich einen wichtigen Beitrag für eine spätere Zertifizierung. Entscheidend bei den Inbetriebnahmetests ist, dass alle zu unterstellenden Szenarien berücksichtigt werden, die Durchführung sachgerecht erfolgt und die Ergebnisse korrekt dokumentiert und interpretiert werden. Dies wird einer Prüfung unterzogen und die Ergebnisse in einem aussagekräftigen Bewertungsbericht dargelegt.

- **TSI Training**

Mit der Verbreitung der TSI-Zertifizierung werden immer häufiger Kenntnisse zu Inhalten des TSI Katalogs und zur Vorgehensweise bei einer Zertifizierung verlangt. Dies hat TÜViT aufgegriffen und bietet hierzu eine zweitägige Schulung an. Im internationalen Umfeld ist diese Schulung eine Voraussetzung, um eine TSI Professional Auszeichnung als Qualifizierungsnachweis zu erlangen.

Hiermit werden nicht nur Planungshäuser und Ingenieurbüros adressiert sondern auch Betreiber von Rechenzentren, die sich intensiv mit dem Kriterienkatalog auseinandersetzen wollen.

7 Zertifizierung von Rechenzentren

Wie bereits eingangs erläutert, kann man von einem sicheren Rechenzentrum nur dann sprechen, wenn angemessene Sicherheitsmaßnahmen unter physischen, informationstechnischen und organisatorischen Gesichtspunkten getroffen wurden. Neben dem Prüfprogramm zur physischen Sicherheit, deckt TÜViT durch weitere Prüfprogramme auch die anderen Aspekte inkl. organisatorischer Qualitätsbewertungen ab, so dass in diesem modularen TÜViT-Schema eine umfassende Sicherheits- und Qualitätsaussage zu einem Rechenzentrumsbetrieb dargestellt werden kann.

Trusted Site Security analysiert die Netzsicherheit und die Güte der Systemhärtung, um die informationstechnischen Sicherheitsaspekte abzudecken. Durch **Trusted Site ITSM** wird die Betrachtung um die Sicht auf die Prozesse des IT Service Managements erweitert und der Nachweis erbracht, dass bei der Gestaltung der IT Service Prozesse die Kundenanforderungen berücksichtigt wurden. Die Prüfprogramme ergänzen sich durch ihren unterschiedlichen Fokus. Ihre Kombination führt zu einer ganzheitlichen Betrachtung und gibt dem Betreiber einen universellen Sicherheits- und Qualitätsnachweis in Form von drei Zertifikaten, die dokumentieren, dass alle Facetten berücksichtigt wurden und Sicherheitsmaßnahmen durchgängig auf hohem Niveau für alle drei Sicherheitseckpfeiler umgesetzt wurden.

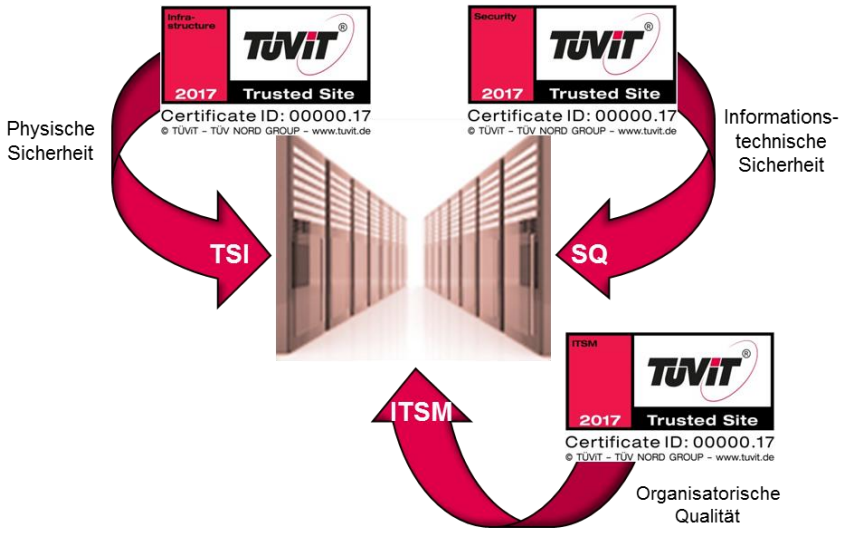

Abbildung 4: Zertifizierung von Rechenzentren

8 Trusted Site Zertifizierungs-Familie (Auszug)

Die TÜV Informationstechnik GmbH vergibt Trusted Site Prüfzeichen, die die Erfüllung von Sicherheits- und Qualitätseigenschaften für IT-Systeme bestätigen.

Trusted Site — *Security*

untersucht im Rahmen einer **S**icherheits-technischen **Q**ualifizierung die IT-Sicherheit von (typischerweise vernetzten) IT-Installationen und bestätigt die Erfüllung von geeigneten Sicherheitszielen.

Trusted Site — *ITSM*

untersucht die IT Service Management-Prozesse des ITIL-Referenzmodells in Bezug auf die Qualität, Vollständigkeit und Implementierungstiefe in Bezug auf die in der ISO 20000 dargelegten Vorgaben für die Organisation.

Trusted Site — *Privacy*

untersucht Organisationen, Teilbereiche von Organisationen oder Businessprozesse in Bezug auf die Erfüllung von Datenschutzanforderungen und deren sicherheitstechnische Umsetzung.

Trusted Site — *PK-DML*

untersucht die technischen und organisatorischen Maßnahmen von Dokumentenmanagement-Lösungen sowie die Sicherheitsvorkehrungen für eine revisionssichere Archivierung.

Die TÜViT-Prüfzeichen können bei übereinstimmender Laufzeit und gleichem Untersuchungsbereich im Unternehmen auch als Kombinationsprüfzeichen vergeben werden.

9 Änderungen von TSI V3.2 nach V4.0

- Die Anforderungen der „DIN EN 50600 - Einrichtungen und Infrastrukturen von Rechenzentren“ wurden in den TSI-Katalog übertragen.
- Es kommen wahlweise die bekannten und weiterentwickelten TSI Kriterien zur Anwendung oder mit Ergänzung weiterer 18 Kriterien (siehe orange Kennzeichnung) eine Vollprüfung auf Konformität mit der DIN EN 50600.
- Diverse Anforderungen wurden präzisiert, um Planern und Rechenzentrumsbetreibern ein hohes Maß an Planungssicherheit zu geben.
- Die Logik bei der Anwendung der Forderungsklassen B und C wurde verbessert. Alle Grundanforderungen stehen nun als Erläuterung unter dem Kriterium, die Beschreibung zu einer Forderungsklasse beinhaltet nur noch die Ergänzung.
- Einige Kriterien sind zu anderen Gewerken verschoben worden, um die Prüfung effizienter zu gestalten.
- Mit „Struktur der Verkabelung“ wird ein neues Kapitel in den Katalog integriert.

10 TSI Katalog V4.0

Umfeld

Nr.	Kriterium / Subkriterium
ENV01.01	Meidung von Hochwasser- und Überschwemmungsgebieten
ENV02.01	Meidung von explosionsgefährdeten Produktions- und Lagerstätten bzw. Leitungen
ENV03.01	Meidung von Betrieben oder Lagerstätten mit Schadstoff-ausstoß oder Schadstofffreisetzung
ENV04.01	Meidung von elektromagnetischen Störquellen
ENV05.01	Meidung von Erschütterungsquellen
ENV06.01	Meidung von Verkehrswegen mit erhöhtem Gefahrgutaufkommen
ENV07.01	Meidung von anschlagsgefährdeten Objekten in der Nachbarschaft
ENV08.01	Meidung von Orten in der Nähe von Großveranstaltungen und Zuwegen dorthin
ENV09.01	Außerhalb von Trümmerkegelbereichen höherer Bauwerke
ENV10.01	Außerhalb von Staudammabfluss- und Lawinengebieten

Baukonstruktion

Nr.	Kriterium / Subkriterium
CON01.01	Unauffällige, nicht exponierte Lage des Sicherheitsbereiches
CON01.02	Meidung von Gebäudebereichen mit Gefährdungspotenzial
CON01.03	Zusammenhängender Sicherheitsbereich
CON01.04	Sinnvolle funktionale Raumaufteilung mit brandschutztechnischer Trennung
CON01.05	Ausreichende Dimensionierung bzgl. Fläche, Höhe, Statik und Wegeführung
CON01.06	Physische Trennung der Zuständigkeitsbereiche des Technik- und IT-Personals
CON01.07	Baukörper zur alleinigen RZ-Nutzung
CON01.08	Perimeter- bzw. Vorfeldabsicherung
CON01.09	Keine Parkmöglichkeit an Außenwänden von IT-Räumen
CON01.10 EN50600	Zugangswege und gesicherte Anlieferung
CON02.01	Vermietungsrecht und Gebäudenutzung
CON03.01	Äußerer Blitzschutz
CON04.01	Schutzgebende Bauweise unter Nutzung geeigneter Baumaterialien
CON04.02	Einbruchhemmende Sicherheitsgrenze für die IT-Zone
CON04.03	Absicherung der Technik-Zone
CON04.04	Meidung von Fenstern im Sicherheitsbereich
CON04.05	Sabotage- und Durchstiegssicherung von Kanälen, Steigschächten & Außenöffnungen
CON04.06	Schutz für Übergabepunkte von Versorgungsnetzen und Außeninstallationen
CON04.07 EN50600	Umsetzung eines Schutzzonen-Schalenmodells
CON05.01	Meidung brennbarer Ausbaustoffe und Einrichtungsgegenstände
CON05.02	Absicherung von Türen, Fenstern und Abschlüssen gegen Brand und Rauch gemäß EN 1634
CON05.03	Ordnungsgemäße Ausführung von Brandschotts

Nr.	Kriterium / Subkriterium
CON05.04	Einhaltung von Temperatur- und Luftfeuchtegrenzwerten bei Umgebungsbränden
CON06.01	Konstruktiver Wasserschutz
CON06.02	Meidung flüssigkeitsführender Leitungen in Räumen der Energieversorgung und in IT-Räumen
CON08.01	Notbeleuchtung und ausgeschilderte Fluchtwege

Brandschutz, Melde- und Löschtechnik

Nr.	Kriterium / Subkriterium
FIR01.01	Einsatz einer geeigneten Brandmeldeanlage nach Stand der Technik
FIR01.02	Überwachung von IT- und Technikbereichen
FIR01.03	Überwachung angrenzender Räume
FIR01.04	Ausreichende Melderdichte
FIR01.05	Raumnutzungsbezogene Meldertypen
FIR01.06	Einsatz von Brandfrühesterkennungssystemen
FIR01.07	CO_2-Handfeuerlöscher
FIR01.08	Vorbeugender Brandschutz in elektrischen Schalträumen
FIR02.01	Automatische Lösch- bzw. Brandvermeidungsanlage oder Ersatzlösung
FIR02.02	Überwachung der Löschbatterien bzw. der Brandvermeidungsanlage
FIR02.03	Löschbatterien bzw. Brandvermeidungsanlage in einem eigenen, zutrittsgeschützten Raum
FIR02.04	Brandschutzklappen über BMA-Signal angesteuert
FIR03.01	ORG: Wartung von BMA, BLA und brandschutztechnischen Abschlüssen

Sicherheitssysteme und -organisation

Nr.	Kriterium / Subkriterium
SEC01.01	ZKA: Einsatz einer geeigneten Zutrittskontrollanlage nach Stand der Technik
SEC01.02	ZKA: Schutz der Zentrale
SEC01.03	ZKA: Sabotagegeschützte Verlegung und Überwachung der Leitungen
SEC01.04	ZKA: Komponenten mit Notstrom-Versorgung
SEC01.05	ZKA: Einsatz geeigneter Leser
SEC01.06	ZKA: Sicherheit des Identifikationsmerkmalträgers (IMT)
SEC01.07	ZKA: Protokollierung der Zutritte
SEC01.08	ZKA: Identifizierung des Benutzers über zweites Merkmal
SEC01.09	ZKA: Realisierung von Zonenkonzepten
SEC01.10	ZKA: Türoffenzeitüberwachung
SEC02.01	EMA: Einsatz einer geeigneten Einbruchmeldeanlage nach Stand der Technik
SEC02.03	EMA: Einsatz von Bewegungsmeldern auf den IT-Flächen
SEC02.04	EMA: Überwachung von Technikräumen
SEC02.05	EMA: Überwachung von IT-Räumen
SEC02.06 EN50600	EMA: Sichere Alarmübertragung
SEC03.01	Videoüberwachungsanlage
SEC04.01	Perimeter- bzw. Vorfeldüberwachung
SEC05.01	Personenvereinzelung
SEC06.01	ORG: Regelmäßige Wartung und Inspektion
SEC06.02	ORG: Absicherung des Arbeitsplatzes für IMT-Administration
SEC06.03	ORG: Sicherheitsdienstleister
SEC06.04	ORG: Sicherheitsdienstleister vor Ort

Verkabelung

Nr.	Kriterium / Subkriterium
CAB01.01	Gesicherte, separierte und redundante WAN-Trassen
CAB01.02 EN50600	Struktur der Kommunikationsverkabelung
CAB01.03 EN50600	Redundante, separierte Telekommunikationskabelführung
CAB01.04	Geordnete Verlegung von Kabeln
CAB01.05	Rackeinspeisung über eine gegen zufälliges Lösen gesicherte Verbindung
CAB01.06 EN50600	Ausführung von Kreuzungspunkten
CAB01.07 EN50600	Schutz der Datenleitungen vor Störquellen
CAB02.01 EN50600	Ausführung von Schränken und Gestellen
CAB03.01 EN50600	ORG: WAN-Versorgung über mindestens 2 Provider

Energieversorgung

Nr.	Kriterium / Subkriterium
POW01.01	Netzform TN-S
POW01.02	Die Stromversorgung erfolgt über Primär- und Sekundärversorgungen
POW01.03	Die Primärversorgung erfolgt über 2 getrennte Wege
POW01.04	Sekundärstromversorgung
POW01.05	Sekundärversorgung Redundanzen
POW01.06	A/B-Versorgung für die IT-Verbraucher
POW02.02	Versorgungstrassen mit Schutz gegen äußere Beeinflussungen
POW02.03	IT-Verteiler besitzen eigene Zuleitung ohne Abzweig
POW02.04	IT-Verteiler im Sicherheitsbereich ausschließlich zur Versorgung der IT
POW05.01	Überspannungsschutz für die Elektroversorgung
POW05.02	Überspannungsschutz für Kommunikations- und Signalleitungen
POW06.01	Absicherung der Steuerung für Leistungsschalter
POW07.01	Erdung aller metallischen Gegenstände auf möglichst kurzem Wege
POW08.01	Überwachung sinnvoller Segmente auf Ableitströme
POW08.02	Vermeidung zentraler Fehlerstromschutzeinrichtungen
POW08.03	Netzüberwachung und -messung
POW09.01	USV: Zentrale USV
POW09.02	USV: Externer Bypass
POW09.03	USV: Redundanzen

Nr.	Kriterium / Subkriterium
POW09.04	USV: Aufstellung von USV und Batterien in brandschutztechnisch getrennten Räumen
POW09.07	USV: Batterien
POW09.08	USV: Auslegung einer USV-Anlage mit Leistungsreserven
POW09.09	USV: Dimensionierung des Energiespeichers für vollständigen Shutdown der IT
POW10.03	NEA: Vorbereitung und vertragliche Absicherung für mobile Netzersatzanlage
POW10.04	NEA: Auslegung der NEA mit Leistungsreserven
POW10.05	NEA: Tankreserve für mindestens 48 h
POW10.06	NEA: Tankanlage
POW10.07	NEA: Regelmäßige Funktionskontrolle
POW10.08	NEA: Sichere Aufstellung der Umschalteinrichtung
POW11.01	ORG: Selektivitätsberechnung
POW11.02	ORG: Überwachung der Betriebszustände
POW11.03	ORG: Störmeldungen an eine ständig besetzte Stelle
POW11.04	ORG: Regelmäßige Wartung der elektrischen Anlagen
POW11.05	ORG: Tests bei Erstinbetriebnahme und Austausch

Raumlufttechnische Anlagen

Nr.	Kriterium / Subkriterium
ACV01.01	Einhaltung von betriebssicheren Umgebungsbedingungen in Rechenzentrumsbereichen
ACV01.02	Ausreichende Belüftung von technischen Komponenten und Rechenzentrumsbereichen
ACV02.01	Gefährdungsfreie und luftströmungsoptimale Geräteaufstellung
ACV03.01	Leckagesicherung und -überwachung in IT- und elektrischen Betriebsräumen
ACV04.01	Redundante Auslegung aktiver Anlageteile (erzeuger-, verteilerseitig)
ACV04.02	Ausführung von Verrohrung und passiven Komponenten
ACV04.03	Auslegung für Wartungen ohne Betriebsunterbrechung
ACV04.04	Geschützte Trassen gegen Fremdbeeinflussung und Brand
ACV04.05	Ausführung und Redundanz der Klimatisierung (verbraucherseitig)
ACV05.01	Raumluftfilterung
ACV05.02	Verhinderung des Eindringens von Rauch und Staub in IT-Räume
ACV05.03	Absicherung der Außenluftzuführung
ACV06.01	Örtliche Trennung der Komponenten in der Kältezentrale
ACV07.01	Sabotagesicherung der Rückkühlwerke
ACV07.02	Ausreichende Dimensionierung und betriebssichere Aufstellung der Rückkühlwerke
ACV08.01	Plankonforme Auslegung und wartungsfreundliche Aufstellung der Kälteanlagen
ACV09.01	Sichere elektrische Versorgung der Komponenten der Klimatisierung
ACV09.02	Sichere Wasserversorgung von Rückkühlwerken mit Wasserbesprühung
ACV09.03	Sichere Steuerung und Regelung
ACV10.01	Überwachung der Betriebszustände

Nr.	Kriterium / Subkriterium
ACV10.02	Unabhängige Überwachung von Temperatur und Feuchte
ACV10.03 EN50600	Befähigung zur Energieeffizienz
ACV11.01	ORG: Nachweis zu Prüfungen von Dichtheit, Korrosionsschutz und Dämmung
ACV11.02	ORG: Regelmäßige Wartung der Komponenten der Klimatisierung
ACV11.03	ORG: Störmeldungen an eine ständig besetzte Stelle
ACV11.04	ORG: Tests bei Erstinbetriebnahme und Austausch

Organisation

Nr.	Kriterium / Subkriterium
ORG01.01	Trennung von IT-Produktion und -Archivierung / -Sicherung
ORG02.01	Ausschilderung des Rauchverbots
ORG03.01	Regelmäßige Anlagenbegehungen
ORG04.01	Ordnungsgemäßer Betrieb
ORG05.01	Realisierung eines Sicherheitsmanagements für physische Belange
ORG05.02 EN50600	Realisierung eines Lifecyclemanagements
ORG05.03 EN50600	Realisierung eines Kundenmanagements
ORG05.04 EN50600	Erfassung wichtiger Schlüsselindikatoren (KPI, Key Performance Indicators)
ORG06.01	Abstimmungsverfahren zwischen IT-Betrieb, Lifecycle-management und Facilitymanagement
ORG07.01	Angepasste Wartungsverträge für die einzelnen Gewerke
ORG08.01	Regelungen für Wartungs- und Reparaturarbeiten
ORG09.01	Sicherheitsunterweisung des Personals
ORG09.02	Vertrauenswürdige und zur Vertraulichkeit verpflichtete Mitarbeiter und Dienstleister
ORG10.01	Vertretungsregelungen
ORG11.01	WAN-Versorgung über mindestens 2 Provider
ORG12.01	Meidung von Lagehinweisen auf das Rechenzentrum

Dokumentation

Nr.	Kriterium / Subkriterium
DOC01.01	Sicherheitskonzept / Dokumentation von Infrastrukturmaßnahmen
DOC01.02	Risikoanalyse Umfeld
DOC01.03	Alarmplan / Notfallkonzept
DOC01.04	Brandschutzkonzept
DOC01.05 EN50600	Standortgutachten bei Neubauprojekten
DOC02.01	Gelände- und Gebäudepläne
DOC02.02	Raumgrundrisspläne zum IT-Bereich und Technikbereich
DOC03.01	Trassenpläne der Hauptversorgungswege
DOC03.02 EN50600	Dokumentation der Telekommunikationsverkabelung
DOC04.01	Strangschema Elektroversorgung
DOC04.02	Rohr- und Instrumentierungsplan Kälte
DOC04.03	Übersichten Brandmeldelinien und -melder
DOC04.04	Übersicht Lösch- und Brandvermeidungseinrichtungen
DOC04.05	Pläne zu Sicherheitseinrichtungen EMA/ZKA/Video
DOC04.06 EN50600	Leistungsbedarfsrechnung und Auslegungsvorgaben
DOC04.07 EN50600	Klimatisierungskonzept
DOC05.01	Wartungspläne
DOC06.01	Betriebsanweisungen
DOC06.02 EN50600	Regelungen für Rechenzentrumskunden bei Fremdvermietung
DOC07.01	Raumliste
DOC07.02	Datenblätter
DOC08.01	Nachweis über die Durchführung von Leistungs- und Funktionstests bei Inbetriebnahme

Rechenzentrumsverbund

Nr.	Kriterium / Subkriterium
DDC01.01	Die Größe der RZ2 IT-Fläche ist mind. 2/3 der RZ1 IT-Fläche.
DDC02.01	Die Rechenzentren befinden sich in getrennten Gebäuden und werden getrennt mit WAN-Anbindung, Strom und Kälte versorgt.
DDC02.02	Ausreichender, risikoorientierter Abstand zwischen RZ1 und RZ2.
DDC03.01	RZ1 und RZ2 sind untereinander über eine redundante Datenverbindung vernetzt.
DDC04.01	Die ENV-Einzelanforderungen sind wahlweise beim RZ1- oder RZ2-Standort erfüllt.

11 Über TÜViT

Die **TÜV Informationstechnik GmbH** - kurz **TÜViT** - mit Sitz in Essen ist einer der führenden Prüfdienstleister für IT-Sicherheit und IT-Qualität. Wir unterstützen Hersteller, Betreiber und Anwender von IT-Systemen, IT-Produkten sowie IT-Infrastrukturen durch Prüfung und Zertifizierung, ihre Unternehmenswerte zu bewahren.

Unsere Experten im Bereich der IT-Sicherheit konzentrieren sich auf Themen wie Common Criteria Evaluationen, Cyber Security, Mobile Security, Industrial Security, Penetrationstests, Bewertung von Informationssicherheits-Managementsystemen nach ISO/IEC 27001 sowie Datenschutz-Audits. Ein weiterer Aspekt ist die Prüfung und Zertifizierung von Rechenzentren hinsichtlich ihrer physischen Sicherheit und Hochverfügbarkeit.

Im Bereich der IT-Qualität koordiniert TÜViT anhand anerkannter Standards das Projekt-, Qualitäts- und Risikomanagement, um unsere Kunden beim Erreichen wichtiger Unternehmensziele zu unterstützen.

Unsere Dienstleistungen werden stets nach dem Stand der Technik ausgeführt und erfüllen höchste Sicherheits- und Qualitätsansprüche.

Zahlreiche Akkreditierungen und Zertifizierungen durch nationale und internationale Organisationen und Behörden weisen unsere Kompetenzen auf dem Gebiet der IT-Sicherheit und IT-Qualität nach.

Bundesamt für Sicherheit in der Informationstechnik

- Anerkennung nach DIN EN ISO/IEC 17025:2005 für Prüfungen nach ITSEC/ITSEM/CC/CEM sowie BSI-TR 03121-1, BSI-TR 03121-3, BSI-TR 03132, BSI TR-03104 und BSI TR-03105 Teil 3 und Teil 5
- IT-Sicherheitsdienstleister für den festgelegten Anwendungsbereich IS-Revision und IS-Beratung und Penetrationstests
- Lizenzierte Auditoren für IT-Grundschutz und ISO/IEC 27001
- Lizenzierte Auditoren für De-Mail

Deutsche Akkreditierungsstelle

- Prüflabor für IT-Qualität: Kompetenz für Prüfungen in den Bereichen IT-Ergonomie und IT-Sicherheit, akkreditiert nach DIN EN ISO/IEC 17025:2005
  - Prüfstelle IT-Sicherheit: Akkreditierung für Prüfungen nach ITSEC/ITSEM/CC/ISO 15408/CEM
  - Prüfstelle IT-Ergonomie: Akkreditierung für Evaluationen nach DIN EN ISO 9241-110, DIN EN ISO 9241-11, ISO/IEC 25051, DIN EN ISO 13407 und ISO 9241-210
- Zertifizierungsstelle: Kompetenz für Zertifizierungen von Produkten, Prozessen und Dienstleistungen in den Bereichen IT-Sicherheit und Sicherheitstechnik (ITSEC, Common Criteria, ETSI EN 319 401 / 319 411-1 / 319 411-2 / 319 421, ETSI TS 101 456 / 102 042 / 102 023, DIN EN 50518-1:2014 / -2:2014 / -3:2014) nach DIN EN ISO/IEC 17065:2013
- Zertifizierungsstelle: Kompetenz für Zertifizierungen von Produkten, Prozessen und Dienstleistungen nach DIN EN ISO/IEC 17065:2013 und ETSI EN 319 403 V2.2.2 im Bereich qualifizierte Vertrauens-diensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste im Anwendungsbereich der VERORDNUNG (EU) Nr. 910/2014 (eIDAS)

Bundesnetzagentur

- Bestätigungsstelle nach SigG/SigV für die Bestätigung von Produkten für qualifizierte elektronische Signaturen
- Bestätigungsstelle nach SigG/SigV für die Bestätigung der Umsetzung von Sicherheitskonzepten für Zertifizierungsdiensteanbieter

Die Deutsche Kreditwirtschaft

- Gelistete Prüfstelle für elektronischen Zahlungsverkehr

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

- Sachverständige Prüfstelle für IT-Produkte (rechtlich/technisch)
- EuroPriSe Gutachter (rechtlich/technisch)

Information-technology Promotion Agency, Japan

- Prüfstelle IT-Sicherheit: Akkreditierung für Prüfungen nach CC/CEM

National Institute of Technology and Evaluation, Japan

- Prüfstelle IT-Sicherheit: Akkreditierung nach DIN EN ISO/IEC 17025 in dem Bereich der IT / Common Criteria Evaluationen (Lab Code: ASNITE0019T)

National Institute of Standards and Technology
National Voluntary Laboratory Accreditation Program, USA

- Prüfstelle IT-Sicherheit (NVLAP Lab Code: 200636-0) für Cryptographic Module Testing (Scopes 17BCS, 17CAV/01, 17CMH1/01, 17CMH1/02, 17CMH2/01, 17CMH2/02, 17CMS1/01, 17CMS1/02, 17CMS2/01, 17CMS2/02) und Biometrics Testing

Europay, MasterCard and Visa, USA/Großbritannien/Japan

- Full Service Laboratory für Prüfungen von ICs und Chipkarten nach EMVCo Sicherheitsrichtlinien
- Modular Label Auditor

Visa, USA

- Test House zur Durchführung von Visa Chip Product Sicherheitsevaluationen

MasterCard, Großbritannien

- Akkreditiert zur Durchführung von CAST (Compliance Assessment and Security Testing) Evaluationen

Betaalvereniging Nederland, Niederlande

- Evaluation Laboratory

In nationalen und internationalen Forschungsprojekten und Gremien gestaltet TÜViT den Stand der Technik aktiv mit.

TÜViT betreibt selbst ein wirksames Qualitätsmanagementsystem und Umweltmanagement, welche nach ISO 9001:2008 bzw. ISO 14001:2004 zertifiziert sind und erfüllt somit die hohen Ansprüche und Erwartungen ihrer Kunden.

TÜViT gehört zur **TÜV NORD GROUP** mit Hauptsitz in Hannover. TÜV NORD beschäftigt über 10.000 Mitarbeiter weltweit und ist neben dem nationalen Markt in 70 Staaten Europas, Asiens und Amerikas vertreten. Während der 140-jährigen TÜV-Tradition hat TÜV NORD technische Tests und Prüfungen in zahlreichen Bereichen durchgeführt und entwickelt. Die TÜV NORD GROUP ist nach ihren Grundsätzen verpflichtet, ihre Dienstleistungen unabhängig sowie neutral anzubieten und durchzuführen.

12 Ansprechpartner

Dipl.-Inform. Joachim Faulhaber

Produktmanager Data Center

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen

Tel.: +49 201 8999-584
Fax: +49 201 8999-555
j.faulhaber@tuvit.de
www.tuvit.de

Dipl.-Ing. Mario Lukas, MBA

Global Account Manager Data Center

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen

Tel.: +49 201 8999-567
Fax: +49 201 8999-555
m.lukas@tuvit.de
www.tuvit.de