# Stellungnahme

## „Zertifizierung der Serverräume IT Compact“

| | |
|---|---|
| **Sachverständiger:** | Andreas Ebbersmeyer |
| **Auftraggeber:** | Conect GmbH<br>Herr Karl-Heinrich Spiering<br>Königstraße 6a<br>23847 Rethwisch |
| **Auftrag:** | Stellungnahme zur möglichen Zertifizierung der Conect-Serverräume „IT Compact“ im produktiven Einsatz nach ULD Gütesiegel und BSI Grundschutz. |
| **Datum der Auftragserteilung:** | 2014-03-24 |
| **Datum der Stellungnahme:** | 2014-04-02 |

**Ausfertigung Nr. 1**

Diese Stellungnahme besteht aus insgesamt 35 Seiten inklusive Deckblatt.

Zwei Ausfertigungen wurden erstellt, davon eine für unsere Unterlagen.

# Inhaltsverzeichnis

# I. Allgemeines

## 1. Aufgabenstellung

Die Firma Conect GmbH möchte eine Sachverständigen-Stellungnahme zu möglichen ULD- oder BSI-Grundschutz-Zertifizierungen ihrer Serverräume „IT Compact“.

## 2. Vorliegende Unterlagen des Auftraggebers

Es liegen folgende Unterlagen bei uns vor:

- Energieeffizienz-Gutachten „Baumuster Domino IT Compact Server Center“ der Firma IT-Backbone GmbH, Hamburg
- IT Compact Info Heft 01
- Broschüre „Wie fit ist Ihr Server-Center“
- IT Compact Musterzelle PUE / EUE Ermittlung (Messstellenaufbau PUE Kategorie 3
- Ansicht PS40 Musterzelle
- Ansicht „Automatische Netzumschaltung“ PS40 Musterzelle
- Schaltplan (Klemmenbelegungsplan) PS40 Musterzelle
- Wiring-Diagramm Umschaltfeld Musterzelle
- Grundrisszeichnungen IT Compact Musterzelle

Weiterhin erfolgte eine Vor-Ort-Besichtigung am 2014-03-14

## 3. Rechtliche Grundlagen

Für die ULD-Gütesiegel-Zertifizierung gilt der „Anforderungskatalog für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH“.

Für die BSI-Grundschutzzertifizierungen gelten die „IT-Grundschutz-Kataloge“.

# II. ULD Gütesiegel

## 1. Einleitung

Durch das Gütesiegel des Unabhängigen Landeszentrums für Datenschutz (ULD) wird bescheinigt, dass die Vereinbarkeit eines Produktes mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde. Um dieses Gütesiegel zu erhalten, muss ein zweistufiges Verfahren durchlaufen werden. In der ersten Stufe wählt der Hersteller oder Vertreiber eines Produktes einen oder mehrere Sachverständige aus, die das Produkt sowohl aus rechtlicher als auch technischer Sicht begutachten müssen. Hierbei muss es sich um Sachverständige handeln, die vom ULD als solche anerkannt wurden. Diese müssen hierzu neben ihrer Unabhängigkeit und Zuverlässigkeit insbesondere ihre Fachkunde nachweisen.

In der zweiten Stufe reicht der Hersteller Gutachten und Antrag beim ULD ein, welches dann die Gutachten und das Produkt prüft. Sind schließlich alle Fragen aus Sicht der Zertifizierungsstelle geklärt, so erhält der Hersteller das Gütesiegel für sein Produkt.

## 2. Anforderungskatalog für die Begutachtung von IT-Produkten

Der Anforderungskatalog stellt beispielhaft Datenschutz- und Datensicherheits-anforderungen sowie in ihrem Zusammenhang zu berücksichtigende Fragestellungen nach wichtigen Rechtsnormen dar und ist in vier Komplexe aufgeteilt.

Die Texte im Komplex 1 stellen zunächst Anforderungen an die Technikgestaltung dar. Dies betrifft insbesondere die Anforderungen der Datenvermeidung und der Transparenz.

Komplex 2 zählt die einschlägigen Datenschutzbestimmungen auf, um die Zulässigkeit der angestrebten Datenverarbeitung überprüfen zu können.

In Komplex 3 wird untersucht, welche technisch-organisatorischen Maßnahmen zum Schutz der Betroffen das Produkt unterstützt. Diese Maßnahmen leiten sich in erster Linie aus der Datenschutzverordnung (DSVO) ab.

Komplex 4 stellt Kriterien vor, um die Umsetzungen der Rechte der Betroffenen (z.B. Benachrichtigung, Auskunft, Transparenzgebote) beurteilen zu können.

Alle Komplexe müssen gleichermaßen bei der Prüfung des IT-Produktes berücksichtigt werden.

## 3. Stellungnahme

Die meisten der zu prüfenden Katalogpunkte stehen in Bezug zu der tatsächlichen Verarbeitung personenbezogener Daten. Diese gibt es bei einem Serverraum ohne die eigentlichen Rechner nicht.

In Betracht kommen somit lediglich folgende Punkte des ULD-Anforderungskataloges:

### 3.1 Katalogpunkt 1.3: Transparenz und Produktbeschreibung

Durch die konsequent beibehaltene grafische Oberfläche der Sicherungsbelegung und der Netzumschaltung mit deren Kurzbeschreibungen direkt auf den Serverschrankwänden wird für eine zusätzliche Produktbeschreibung gesorgt, welche stets präsent ist und nicht verlegt werden kann.

### 3.2 Katalogpunkt 3. 1.1.4 Weitere technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen finden sich im § 9 BDSG und der entsprechenden Anlage:

***§ 9 Technische und organisatorische Maßnahmen***

*Öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.*

***Anlage zu § 9***

*Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,*

*1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),*

*2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),*

*3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),*

*4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),*

*5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),*

*6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),*

*7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),*

*8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

Durch die abschließbaren Serverschrank-Elemente wird für eine zusätzliche Zutrittskontrolle gesorgt.

Gleichzeitig verhindern diese Türen eine ungewollte Nutzung der Sicherungselemente und stellen so eine Verfügbarkeitskontrolle dar.

Durch das Drei-Wege-Benachrichtigungssystem per E-Mail, SMS und Anzeige am Serverschrank können Ausfallzeiten durch schnellstmögliche Benachrichtigung verringert werden.

Ebenso verringern die grafische Oberfläche der Sicherungsbelegung und der Netzumschaltungen mit deren Kurzbeschreibungen direkt auf den Serverraumwänden die Ausfallzeiten, da keinerlei Dokumentationen mehr in Ordnern gesucht werden müssen.

# III. BSI-Grundschutz-Kataloge

## 1. Einleitung

Der BSI-IT-Grundschutz bietet eine effektive Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie z. B. die BSI-Standards zum Informationssicherheitsmanagement und die IT-Grundschutz-Kataloge. Dazu gehört auch die ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, die sowohl eine Prüfung des Informationssicherheitsmanagements als auch der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz umfasst.

Die IT-Grundschutz-Kataloge beinhalten die Baustein-, Maßnahmen- und Gefährdungskataloge. Die Vorgehensweise nach IT-Grundschutz, Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse findet man unter den BSI-Standards.

## 2. Beschreibung nach BSI

*Der Serverraum dient in erster Linie zur Unterbringung von Servern, z. B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage. Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang oder weitere Hardware (Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein.*

*In einem Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum.*

## 3. Gefährdungen

Für den IT-Grundschutz eines Serverraumes werden im Bausteinkatalog B 2.4 folgende typische Gefährdungen angenommen:

Höhere Gewalt: Feuer (G 1.4), Wasser (G 1.5), Unzulässige Temperatur und Luftfeuchte (G 1.7), Ausfall von Patchfeldern durch Brand (G1.16).

Organisatorische Mängel: Fehlende oder unzureichende Regelungen (G 2.1), Unbefugter Zutritt zu schutzbedürftigen Räumen (G 2.6).

Technisches Versagen: Ausfall der Stromversorgung (G 4.1), Ausfall interner Versorgungsnetze (G 4.2), Spannungsschwankungen (G 4.6).

Vorsätzliche Handlungen: Manipulation oder Zerstörung von Geräten oder Zubehör (G 5.1), Manipulation an Informationen oder Software (G 5.2), Unbefugtes Eindringen in ein Gebäude (G 5.3), Diebstahl (G 5.4), Vandalismus (G 5.5).

### 3.1 Gefährdungskatalog 1.4: Feuer

*Neben direkten durch das Feuer verursachten Schäden an einem Gebäude oder dessen Einrichtung lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.*

*Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.*

### 3.2 Gefährdungskatalog 1.5: Wasser

*Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.*

### 3.3 Gefährdungskatalog 1.7: Unzulässige Temperatur und Luftfeuchte

*Jedes Gerät hat einen Temperaturbereich, innerhalb dessen seine ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Raumtemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Betriebsstörungen und zu Geräteausfällen kommen.*

*So wird z. B. in einem Serverraum durch die darin befindlichen Geräte elektrische Energie in Wärme umgesetzt und daher der Raum aufgeheizt. Bei unzureichender Lüftung kann die zulässige Betriebstemperatur der Geräte überschritten werden. Bei Sonneneinstrahlung in den Raum sind Temperaturen über 50°C nicht unwahrscheinlich.*

*Zu Lüftungszwecken werden oft die Fenster des Serverraumes geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.*

*Bei der Lagerung von digitalen Langzeitspeichermedien können zu große Temperaturschwankungen oder zu große Luftfeuchtigkeit zu Datenfehlern und reduzierter Speicherdauer führen. Einige Hersteller geben die optimalen Lagerbedingungen für Langzeitspeichermedien mit Temperaturen von 20 bis 22°C und einer Luftfeuchtigkeit von 40% an. Auch analoge Speichermedien wie Papier oder Mikrofilme benötigen bestimmte Lagerbedingungen. Wird Papier beispielsweise zu feucht gelagert, kann es schimmeln oder sich auflösen.*

### 3.4 Gefährdungskatalog 1.16: Ausfall von Patchfeldern durch Brand

*Patchfelder und Leitungsverteiler, auf die die internen Leitungen des Hausnetzes und die externen des öffentlichen Netzes auflaufen, können durch einen Brand so stark beschädigt werden, dass eine reibungslose Datenübertragung darüber nicht mehr möglich ist. Der Schaden wird dabei nicht ausschließlich durch die Hitze des Feuers verursacht. Allein schon der Brandrauch kann die empfindliche Anschlusstechnik massiv beschädigen. Der Einsatz von Löschmitteln (Wasser, Pulver, Schaum) führt zu weiteren Schäden.*

*Nach einem solchen Schadensereignis ist es dann in der Regel nicht mehr möglich, bereitstehende Ersatz-Hardware einfach an derart beschädigte Patchfelder bzw. Leitungsverteiler anzuschließen, um so zumindest einen Notbetrieb rasch wieder aufnehmen zu können.*

*Im Allgemeinen sind sehr umfangreiche, kosten- und zeitintensive Reparaturarbeiten erforderlich, die mit einem längeren Ausfall der IT einhergehen.*

### 3.5 Gefährdungskatalog 2.1: Fehlende oder unzureichende Regelungen

*Die Bedeutung übergreifender organisatorischer Regelungen und Vorgaben für das Ziel Informationssicherheit nimmt mit dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.*

*Von der Frage der Zuständigkeiten angefangen bis hin zur Verteilung von Kontrollaufgaben kann das Spektrum der Regelungen sehr umfangreich sein. Auswirkungen von fehlenden oder unzureichenden Regelungen werden beispielhaft in den anderen Gefährdungen des Gefährdungskatalogs G2 beschrieben.*

*Vielfach werden nach Veränderungen technischer, organisatorischer oder personeller Art, die wesentlichen Einfluss auf die Informationssicherheit haben, bestehende Regelungen nicht angepasst. Veraltete Regelungen können einem störungsfreien Betrieb entgegen stehen. Probleme können auch dadurch entstehen, dass Regelungen unverständlich oder zusammenhanglos formuliert sind und dadurch missverstanden werden.*

### 3.6 Gefährdungskatalog 2.6: Unbefugter Zutritt zu schutzbedürftigen Räumen

*Alle Räume, in denen schutzbedürftige Informationen aufbewahrt bzw. weiterverarbeitet oder in denen schutzbedürftige Geräte betrieben werden, werden dadurch zu schutzbedürftigen Räumen. Beispiele hierfür sind Büroräume, aber auch Archive, in denen Datenträger und Akten zentral aufbewahrt werden. Ebenso hierzu zählen Technik-Verteilräume mit zentralen Komponenten wie Stromverteiler, Netzkoppelelemente und Server.*

*Unbefugte Personen können in solchen Räumen durch vorsätzliche Handlungen (z. B. Manipulationen oder Vandalismus), aber auch durch unbeabsichtigtes Fehlverhalten (z. B. aufgrund mangelnder Fachkenntnisse) Schäden verursachen. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann der Betriebsablauf schon dadurch gestört werden, falls untersucht werden muss, wie ein solcher Vorfall möglich war oder ob Schäden aufgetreten sind oder Manipulationen vorgenommen wurden.*

*Eindringlinge könnten beispielsweise Passwörter zurückgesetzt, direkt auf die Server zugegriffen oder aktive Netzkomponenten manipuliert haben. Außerdem könnten sie sensible Informationen auf Papier oder Datenträgern entwendet oder verändert haben.*

*Nicht nur Räume auf dem Betriebsgelände müssen vor unbefugtem Zutritt geschützt werden, sondern auch dienstlich genutzte Räume im häuslichen Umfeld. Einbruchsicherungen (z. B. abschließbare Fenstergriffe, Sicherheitsschlösser und Sicherheitsverriegelung und -verglasung an Haustüren) werden im privaten Umfeld für häusliche Arbeitsplätze oft aus Kostengründen nicht realisiert. Dadurch ist beispielsweise bei Telearbeitsplätzen der Schutz vor Einbrüchen niedriger als innerhalb eines Unternehmens oder einer Behörde.*

### 3.7 Gefährdungskatalog 4.1: Ausfall der Stromversorgung

*Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Bei einer Messung mit circa 60 Messstellen wurden 1983 in Deutschland rund 100 solcher Netzeinbrüche registriert. Davon dauerten fünf Ausfälle bis zu einer Stunde und einer länger als eine Stunde. Diese Unterbrechungen beruhten einzig auf Störungen im Versorgungsnetz. Dazu kommen Unterbrechungen durch Abschaltungen bei nicht angekündigten Arbeiten oder durch Kabelbeschädigungen bei Tiefbauarbeiten.*

*Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Rohrpostanlagen, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen, Sprinkleranlagen, Telefonnebenstellenanlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druckerzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig.*

*Die Liberalisierung des Strommarktes führte in einigen Industrieländern zu einer Verschlechterung des Versorgungsniveaus. Auch in Deutschland könnte daher die Gefahr wachsen, dass Probleme durch Ausfälle der Stromversorgung oder durch Schaltvorgänge an nationalen Versorgungsübergängen entstehen.*

### 3.8 Gefährdungskatalog 4.2: Ausfall interner Versorgungsnetze

*Es gibt in einem Gebäude eine Vielzahl von Netzen, die der Ver- und Entsorgung und somit als Basis für alle Geschäftsprozesse einer Institution einschließlich der IT dienen. Der Ausfall von Versorgungsnetzen wie:*

- *Strom,*
- *Telefon und*
- *Kühlung*

*kann eine Vielzahl von Aufgaben beeinträchtigen. Ein solcher Ausfall kann aber auch zu einer sofortigen Störung des IT-Betriebs führen. Demgegenüber kann es bei Ausfall in den Bereichen:*

- *Heizung bzw. Lüftung,*
- *Wasser,*
- *Löschwasserspeisungen,*
- *Abwasser,*
- *Rohrpost,*
- *Gas,*
- *Melde- und Steueranlagen (Einbruch, Brand, Hausleittechnik) und*
- *Sprechanlagen*

*unter Umständen zu zeitverzögerten Störungen kommen.*

*Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.*

### 3.9 Gefährdungskatalog 4.6: Spannungsschwankungen

*Durch Schwankungen der Versorgungsspannung kann es zu Funktionsstörungen und Beschädigungen der IT kommen. Die Schwankungen reichen von extrem kurzen und kleinen Ereignissen, die sich kaum oder gar nicht auf die IT auswirken, bis zu*

*Totalausfällen oder zerstörerischen Überspannungen. Die Ursache dafür kann in allen Bereichen des Stromversorgungsnetzes entstehen, vom Netz des Energieversorgungsunternehmens bis zum Stromkreis, an dem die jeweiligen Geräte angeschlossen sind.*

*Außerhalb des Energieversorgungsnetzes ist auch auf allen anderen elektrisch leitenden Netzen (wie Telefonanbindung, Gebäudeleittechnik, Wasser- oder Gasleitungen etc.) mit Einkopplungen von Überspannungen zu rechnen.*

### 3.10 Gefährdungskatalog 5.1: Manipulation oder Zerstörung

*Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, Geräte, Zubehör, Schriftstücke und andere Datenträger (z. B. DVDs, USB-Sticks) oder ähnliches zu manipulieren oder zu zerstören. Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tiefgreifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen, die erhebliche Ausfallzeiten nach sich ziehen können.*

### 3.11 Gefährdungskatalog 5.2: Manipulation an Informationen oder Software

*Informationen oder Software können auf vielfältige Weise manipuliert werden: durch falsches Erfassen von Daten, Änderungen von Zugriffsrechten, inhaltliche Änderung von Abrechnungsdaten oder von Schriftverkehr, Änderungen in der Betriebssystem-Software und vieles mehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen und Software-Komponenten manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.*

*Manipulationen an Informationen oder Software können unter anderem aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden.*

### 3.12 Gefährdungskatalog 5.3: Unbefugtes Eindringen in ein Gebäude

*Wenn Unbefugte in ein Gebäude oder einzelne Räumlichkeiten eindringen, kann dies verschiedene andere Sicherheitsgefährdungen nach sich ziehen. Dazu gehören beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen. Maßnahmen, die dagegen gerichtet sind, wirken dadurch auch gegen die entsprechenden Folgegefährdungen. Bei qualifizierten Angriffen versierter Täter ist die Zeitdauer entscheidend, in der die Täter ungestört ihr Ziel verfolgen können. Ziel eines Einbruchs kann der Diebstahl von IT-Komponenten oder anderer leicht veräußerbarer Ware sein, aber auch das Kopieren oder die Manipulation von Daten oder IT-Systemen. Dabei können nicht offensichtliche Manipulationen weit höhere Schäden als direkte Zerstörungsakte verursachen.*

*Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.*

### 3.13 Gefährdungskatalog 5.4: Diebstahl

*Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und daraus resultierenden Konsequenzen entstehen.*

*Von Diebstählen sind neben teuren IT-Systemen wie Servern auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig betroffen.*

### 3.14 Gefährdungskatalog 5.5: Vandalismus

*Durch Vandalismus wird fremdes Eigentum zerstört oder beschädigt. Die Auswirkungen sind mit denen eines Anschlags sehr verwandt, nur dass Vandalismus nicht wie dieser gezielt geplant und umgesetzt wird, sondern meist Ausdruck spontaner, blinder Zerstörungswut ist.*

*Sowohl Außentäter (z. B. enttäuschte Einbrecher, außer Kontrolle geratene Demonstranten) als auch Innentäter (z. B. frustrierte oder psychisch labile Mitarbeiter) kommen als Verursacher in Betracht. Die tatsächliche Gefährdung durch Vandalismus ist schwerer abschätzbar als die eines Anschlages, da ihm in der Regel keine zielgerichtete*

*Motivation zugrunde liegt. Mögliche Auslöser für Vandalismus können unter anderem Meinungsverschiedenheiten, persönliche Probleme, Mobbing oder ein schlechtes Betriebsklima sein.*

## 4. Maßnahmenkataloge

In den Maßnahmenkatalogen der BSI-Grundschutz-Kataloge werden für BSI- und/oder ISO 27001-Auditierungen erforderliche Bestimmungen beschrieben. Für Serverräume und deren Betrieb gehören hierzu:

### 4.1 Maßnahmenkatalog 1.1: Einhaltung einschlägiger Normen und Vorschriften

*Für nahezu alle Bereiche der Technik gibt es Richtlinien, Normen bzw. Vorschriften. Diese können von Standardisierungsorganisationen, Branchenvereinigungen, Anwendergruppen oder staatlichen Institutionen herausgegeben worden sein, z. B. DIN (Deutsches Institut für Normung), ISO (International Standards Organization), VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik), VDMA (Verband Deutscher Maschinen und Anlagenbau), VdS (Verband der Sachversicherer).*

*Diese Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für die Benutzer und Sicherheit für den Betrieb gewährleisten.*

*Bei der Planung und Errichtung von Gebäuden, bei deren Betrieb und Umbau sowie beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.*

*Die Beachtung von Normen ist für sich keine Sicherheitsmaßnahme. Sie bedeutet, dass Mindestanforderungen erfüllt werden und der aktuelle Stand der Technik und des Wissens beachtet wird.*

### 4.2 Maßnahmenkatalog 1.6: Einhaltung von Brandschutzvorschriften

*Die bestehenden Brandschutzvorschriften (z. B. nach der Norm DIN 4102 Brandverhalten von Baustoffen und Bauteilen) und die Auflagen der Bauaufsicht für Gebäude sind unbedingt einzuhalten. Die örtliche Feuerwehr sollte bei der Brandschutzplanung hinzugezogen werden.*

*Für Räume, in denen wichtige IT-Geräte und Datenträger (Server, Datensicherungen, etc.) untergebracht sind, sollten zudem die Regelungen der Norm EN 1047 Teil 2 beachtet werden. Ziel ist hier, durch besondere Maßnahmen wie dem Einbau von Türen mit Brand- und Rauchschutzqualität, der sorgfältigen Ausführung von Schottungen und eventuell sogar der Ertüchtigung von Wänden, die Wirkung eines Brandes auf die Inhalte solcher Räume möglichst gering zu halten.*

*Bei Besprechungs-, Schulungs- und Veranstaltungsräumen sind unter Umständen die entsprechenden Regelungen für den Brandschutz in Versammlungsstätten zu beachten. Da es hier je nach Nutzungsart unterschiedliche Zusatzforderungen wie beispielsweise hinsichtlich der Öffnungsart und -breite von Türen im Verlauf von Flucht- und Rettungswegen und Beschilderungen gibt, sollte auch hier bei der Planung die örtliche Feuerwehr befragt werden.*

*Es sollte eine Person benannt werden, die für die Einhaltung von Brandschutzvorschriften verantwortlich ist. Dies kann ein Brandschutzbeauftragter oder eine mit dem Aufgabengebiet betraute Person sein, die auch entsprechend geschult ist.*

*Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel in den Publikationen der VdS Schadenverhütung GmbH zu finden sind.*

*Besonders wichtig ist es, die Fluchtwege gut auszuschildern. Dafür sind die vorgeschriebenen Kennzeichen zu verwenden und die Vorschriften zu deren Anbringung einzuhalten. Die Fluchtwege müssen immer offen gehalten werden, das heißt insbesondere, dass sie nicht versperrt werden dürfen, z. B. durch im Flur abgestelltes Inventar oder indem die Fluchttüren abgeschlossen werden.*

*Damit die Feuerwehr im Brandfall schnell mit der Brandbekämpfung beginnen kann, ist es wichtig, dass die Brandmeldezentrale, das Brandmeldetableau und die Einspeisepunkte für Löschwasser durch Beschilderung schnell gefunden werden können.*

*Zur Verwirklichung eines effizienten Brandschutzes ist die Zusammenarbeit aller zuständigen Verfahrensbeteiligten notwendig. Hierunter fallen die Funktionen*

- *des Brandschutzbeauftragten (Arbeitgeber ist für die Einhaltung der Brandschutzvorschriften verantwortlich),*

- *der Fachkraft für Arbeitssicherheit (in Deutschland erforderlich nach §§ 5, 6 Arbeitssicherheitsgesetz, diese ist zuständig für die Ausgestaltung des betrieblichen Brandschutzes) und*

- *des Sicherheitsbeauftragten (in Deutschland erforderlich nach § 22 SGB VII, dieser hat ausführende Tätigkeiten, z. B. zur Verhütung von Arbeitsunfällen und Berufskrankheiten, und arbeitet der Fachkraft für Arbeitssicherheit zu).*

### 4.3 Maßnahmenkatalog 1.10: Sichere Türen und Fenster

*Wenn Türen und Fenster einen Übergang zwischen Sicherheitszonen bilden, müssen sie angemessenen Schutz bieten. Eine Außentür muss z. B. vor Einbrüchen schützen, ebenso müssen die erreichbaren Fenster gesichert werden. Im Innenbereich müssen Türen, die die Grenze eines Brandabschnitts bilden, selbst Brandschutzqualität haben, zudem können sie oder auch andere Innentüren eine zweite Linie des Einbruchschutzes bilden.*

*Sicherheitstüren und -fenster sind in Normen klassifiziert. Aus dem Schutzziel des zu sichernden Bereichs und dem Schutzbedarf der Institution lässt sich eine Auswahl der angemessenen Ausführung von Türen und Fenstern treffen:*

- *In der Norm DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, der Norm DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung – Anforderungen und Klassifizierung" sind die Bauelemente in Widerstandsklassen (RC, engl. Resistance Class) eingeordnet worden. Türen gemäß der Klassifizierungen RC1 bis RC4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Serverräumen, Räumen mit technische Infrastruktur sowie bei Keller- und Lieferanteneingängen). Die Widerstandsklassen RC5 und RC6 sind in der Regel nur bei sehr speziellen Erfordernissen angemessen und spielen daher bei IT-Grundschutzbetrachtungen keine Rolle.*

- *Als selbstschließende feuerhemmende und gegebenenfalls rauchdichte Tür (z. B. FH-Tür T30, nach DIN 18082 "Feuerschutzabschlüsse") verzögern sie die Ausbreitung eines Brandes.*

- *Sie schützen in der Ausführung als selbstschließende Rauchschutztür (DIN18095-1 "Türen; Rauchschutztüren; Begriffe und Anforderungen") die Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten hindurch kommt. Für die geringen Flughöhen*

*von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden.*

*Es können auch mehrere Schutzeigenschaften in einer Tür kombiniert werden, es gibt beispielsweise rauchdichte Brandschutztüren, die zudem Schutz gegen Einbruch bieten.*

*Die Sicherungsmaßnahmen aller raumumschließenden Bauelemente müssen gleichwertig sein:*

- *Bei Verwendung einbruchhemmender Türen ist im Fassadenbereich die Verwendung einbruchhemmender Fenster oder Fassadenelemente (siehe DIN EN1627-1630:2011 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung") zu erwägen.*

- *Weiterhin ist es z. B. nicht zweckmäßig, eine einbruchhemmende Tür der höchsten Widerstandsklasse in eine Gipskartonwand einzubauen.*

- *Beim Einbau einer feuerhemmenden oder rauchdichten Tür ist darauf zu achten, dass auch die umgebende Wand gleichwertig feuerhemmend und rauchdicht ist und nicht durch offene Oberlichter oder ungeschottete Kabeldurchführungen ein Bypass besteht.*

*Anforderungen zur Ausführung von Sicherheitstüren finden sich in den Maßnahmen M 1.47 Eigener Brandabschnitt und M 1.19 Einbruchsschutz.*

*Der Einsatz von Sicherheitstüren ist hinsichtlich der Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus (siehe M 1.6 Einhaltung von Brandschutzvorschriften) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches den Einbau von Sicherheitstüren und die Gefahrenmeldung und Alarmierung zur Prüfung und Intervention berücksichtigt. Denn hat ein potentieller Angreifer ein ganzes Wochenende Zeit für einen Einbruchsversuch, wird ihn auch eine hochwertige einbruchhemmende Tür nicht von seinem Ziel abhalten, Daten oder Einrichtung zu entwenden oder zu zerstören.*

*Für die Ausstattung von Rechenzentren sollte für die Türen inklusive deren Einbausituation die Widerstandsklasse RC3 gemäß DIN EN 1627-1630:2011 als Mindestwert angesetzt werden. Lediglich wenn für die Sicherheit ganz besonders günstige Bedingung vorliegen, insbesondere falls die Interventionszeit hilfeleistender*

*Kräfte kurz ist (maximal 2 Minuten), kann in Ausnahmefällen eine RC2-Tür ausreichen. Liegt die Interventionszeit hilfeleistender Kräfte hingegen bei 5 Minuten und höher, ist sogar eine RC3-Tür als unzureichend anzusehen und es empfiehlt sich der Einbau von RC4-Türen. Sinngemäß gelten die gleiche Überlegungen natürlich auch für alle anderen, die RZ-Hülle bildenden Bauelemente.*

*Hinweis: Ziel eines Einbruches könnte es auch sein, Daten oder IT-Systeme zu manipulieren. Daher sollten zentrale z. B.-Systeme nach Einbrüchen auf ihre Integrität überprüft werden (siehe dazu auch M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle).*

*Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.*

*Außerdem ist regelmäßig zu prüfen, dass die Sicherheitstüren und –fenster funktionstüchtig sind. Sie müssen in einem ordentlichen mechanischen Zustand sein, sicher öffnen und schließen und überwachende Installationen wie Schließkontakte müssen funktionieren.*

### 4.4 Maßnahmenkatalog 1.18: Gefahrenmeldeanlage

*Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen und die Anforderungen der DIN EN 50518 "Notruf- und Serviceleitstellen" zu beachten.*

*Es sollte ein Konzept für die Gefahrenerkennung, Weiterleitung und Alarmierung für die verschiedenen Gebäudebereiche erstellt werden. Dieses muss an Veränderungen bei der Nutzung angepasst werden. Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das dem Gebäude und dem Risiko entsprechend geplant und installiert werden muss. Planung, Installation und Wartung einer Gefahrenmeldeanlage sollte daher durch Experten durchgeführt werden. Falls diese nicht im eigenen Haus vorhanden sind, sollte auf externe Unterstützung zurückgegriffen werden. So gibt es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme, die entsprechend der Sicherheitsanforderungen und der Umgebung ausgewählt werden müssen. Zur Einbruchserkennung können z. B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras u. a. eingesetzt werden.*

*Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert sein müssen und möglichst wenig Änderungen an der Trassenbelegung vorgenommen werden sollten.*

*Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (siehe DIN VDE 0833 Teil 1-3 "Gefahrenmeldeanlagen für Brand, Einbruch und Überfall") vorzusehen.*

*Ist keine GMA vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (eventuell Telefonleitung) an anderer Stelle.*

*Für den Betrieb eines Rechenzentrums muss eine GMA zur Brand- und Einbruchdetektion installiert sein. Weitere Detektionsbereiche können nach Lage des Standorts und dessen Infrastruktur sinnvoll sein.*

*Es gibt Räume wie Serverraum, Datenträgerarchiv, die einen erhöhten Schutzbedarf haben. Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es*

*Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.*

*Vor der Planung einer GMA muss ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Bei der Planung von Gefahrenmeldeanlagen für private bzw. gewerbliche Objekte sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.*

### 4.5 Maßnahmenkatalog 1.19: Einbruchsschutz

*Erfahrungsgemäß wählen Einbrecher ihre Ziele danach aus, wie hoch das Risiko und Aufwand im Verhältnis zum erwarteten Gewinn sind. Daher sollten alle Maßnahmen zum Einbruchsschutz darauf zielen, die Erfolgsaussichten von Tätern zu minimieren. Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden. Dazu gehören:*

- *einbruchhemmende Türen und Fenster, beispielsweise mit der Widerstandsklasse RC2 (nach DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung*
- *Anforderungen und Klassifizierung") oder höherwertig, wenn die Gefährdungslage es erforderlich macht,*
- *Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenster,*
- *besondere Schließzylinder, Zusatzschlösser und Riegel,*
- *Sicherung von Kellerlichtschächten,*
- *Verschluss von nicht benutzten Nebeneingängen,*
- *einbruchgesicherte Notausgänge,*
- *Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.*

*Empfehlungen hierzu geben die örtlichen Beratungsstellen der Kriminalpolizei.*

*Alle Maßnahmen zum Einbruchsschutz sollten sinnvoller Weise eine durchgehend gleichwertige Hülle um den Bereich bilden, der gegen unbefugten Zutritt geschützt*

*werden soll. Türen sind in ausreichend feste Wände einzubauen. Lüftungsöffnungen sind in geeigneter Form zu vergittern. (maximale Gitterweite 10x20 cm). Auch in Doppelbodenbereichen und über abgehängten Decken sind Maßnahmen zum Zutrittsschutz umzusetzen. Die Gleichwertigkeit und Durchgängigkeit des Einbruchsschutzes sollte durch eine fachkundige Person während der Planung, bei der Umsetzung und später im Betrieb regelmäßig begutachtet werden.*

*Bei der Planung materieller Sicherungsmaßnahmen ist darauf zu achten, dass Bestimmungen des Brand- und Personenschutzes, z. B. die Nutzbarkeit von Fluchtwegen, nicht verletzt werden. Dies gilt insbesondere für Änderungen an Brandschutzelementen, die einer Typenfreigabe unterliegen.*

*Den Mitarbeitern ist bekanntzugeben, welche Regelungen und Maßnahmen zum Einbruchsschutz beachtet werden müssen, also beispielsweise dass Türen, Fenster oder Rollladensicherungen abends abgeschlossen werden müssen.*

*Auch innerhalb eines Gebäudes kann der Einbau von einbruchhemmenden Elementen sinnvoll sein. Die Absicherung ist zu erwägen bei besonderen zutrittskontrollierten Bereichen wie den Räumen der Geschäftsleitung, Serverräumen oder den Kerneinheiten eines Rechenzentrums.*

### 4.6 Maßnahmenkatalog 1.24: Vermeidung von wasserführenden Leitungen

*In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen wie z. B. Server befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes oder Bereiches, versehen werden.*

*Außerhalb der Heizperiode sind diese Ventile zu schließen.*

*Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen,*

*da so ein eventueller Leitungsschaden schnell entdeckt werden kann. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen. Durch Sichtprüfungen müssen die vorhandenen Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft werden.*

*Es ist zu erwägen, wasserführende Leitung durch Wassermelder zu überwachen. Dafür können besondere Meldekabel unterhalb von Leitungen verlegt werden. Werden diese an eine Wassermeldeanlage angeschlossen, ist darüber eine schnelle und recht genaue Lokalisierung*

*des Wasseraustritts möglich. Eine solche Anlage muss auf eine ständig besetzte Stelle aufgeschaltet werden, um in Verbindung mit entsprechenden Reaktionsplänen und einer aktuellen Dokumentation ein schnelles Eingreifen möglich zu machen. Optional können Wassermelder mit automatisch*

*arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.*

*Als zusätzliche oder alternative Maßnahme empfiehlt sich eine selbsttätige Entwässerung (siehe M 1.14 Selbsttätige Entwässerung).*

*Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass in Gebäudeteilen mit IT-Systemen mit hohen Verfügbarkeitsanforderungen wasserführende Leitungen problematisch sind und was zu beachten ist. Es sollten Reaktionspläne vorhanden sein, in denen*

*beschrieben ist, welche Maßnahmen bei Wasserleckagen zu ergreifen sind.*

## 4.7 Maßnahmenkatalog 1.47: Eigener Brandabschnitt

*Die Festlegung von Brandabschnitten ist für den Brandschutz eines Rechenzentrums von größter Wichtigkeit. Die Wirkung zuverlässiger Brand und Rauchabschnitte hat sich bei vielen Großbränden eindrucksvoll bestätigt.*

*Die an Brandwände bzw. an die Größe der Brandabschnitte von Rechenzentren gestellten Anforderungen sollten über die in einschlägigen Normen, wie z. B. den Landesbauordnungen bzw. der DIN 4102 "Brandverhalten von Baustoffen und Bauteilen", gestellten Forderungen hinaus gehen.*

*Schutzziel für die Brandwand bzw. den Brandabschnitt sollte nicht nur der Personen- und Gebäudeschutz, sondern auch der Schutz des Inventars und dessen Verfügbarkeit sein. Somit ist nicht nur die Brandausbreitung durch Flammenwirkung und heiße Rauchgase, sondern auch Wärmestrahlung und Ausbreitung von kaltem Rauch zu verhindern.*

*Die nach DIN 4102 noch zulässige Wärmestrahlung kann für die Gebäudeeinrichtung, insbesondere im wärmeempfindlichen IT-Bereich, bereits vernichtende Wirkung haben. Aus diesen Gründen sollten mehrere Brand- und Rauchabschnitte im Bauvorhaben realisiert werden, die so groß wie nötig und so klein wie möglich sind.*

*Für ein Rechenzentrum ist zu prüfen, inwieweit weitere interne Brandabschnitte geschaffen werden sollten. Sollte ein eigener Brandabschnitt für die Kerneinheiten (IT-Räume, Datenträgerarchiv) erforderlich sein, so müssen Wände, Türen und auch notwendige Wand- und Deckendurchbrüche den F90-Anforderungen genügen.*

*Neben der baurechtlich erforderlichen Berücksichtigung der Norm DIN 4102 sollte für Rechenzentren, Serverräume und Datenträgerarchive die Einhaltung von Grenzwerten der maximalen relativen Luftfeuchte (aus der Norm EN 1047-2, Abschnitt 4.1, Tabelle 1) beachtet werden.*

*Wenn der Brandabschnitt des Rechenzentrums z. B. Büroeinheiten beherbergt, die in direktem betrieblichen Zusammenhang mit dem Rechenzentrum stehen, so sind innerhalb des Brandabschnitts F30-Wände und T30-Türen zwischen diesen Büros und dem Rechenzentrum-Kernbereich hinreichend. Die Büros sind dann in die Brandmeldeanlage mit einzubeziehen. Büroeinheiten ohne betrieblichen Bezug zum Rechenzentrum sind in anderen Brandabschnitten anzuordnen.*

*Es ist in der Planung und auch im Betrieb sicherzustellen, dass in solchen Räumen, die im Brandabschnitt des Rechenzentrums liegen, keine besonderen Brandlasten vorhanden sind.*

### 4.8 Maßnahmenkatalog 1.52: Redundanz, Modularität und Skalierbarkeit

*Das bewährteste Mittel zur Sicherstellung der Verfügbarkeit technischer Einrichtungen ist die Redundanz. Redundanz bedeutet, von etwas mehr zu haben, als für die eigentliche Aufgabenstellung erforderlich ist (aus dem Lateinischen: "redundare", im Überfluss vorhanden sein"). Im Bereich der IT bedeutet Redundanz damit auch das Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems. Damit*

*wird sofort das Hauptproblem von Redundanz sichtbar: Um Redundanz zu haben, müssen Überkapazitäten geschaffen werden.*

*Die Modularität beschreibt, ob eine erforderliche technische Leistung durch eine große oder mehrere kleinere Einheiten zur Verfügung gestellt wird. Durch geschickte Nutzung der Modularität kann die erforderliche Überkapazität bei der Redundanz deutlich reduziert werden.*

*Keine noch so weitsichtige Planung kann so gut sein, dass es nicht nach einiger Zeit erforderlich ist, vorhandene technische Systeme einem geändertem, meist gestiegenem Leistungsbedarf anzupassen. Je einfacher ein System durch simples Hinzufügen zusätzlich Einheiten erweiterbar ist, desto besser ist es skalierbar. Auch bei der Skalierbarkeit kann sich die Modularität günstig auswirken.*

*Die einfachste Redundanz ist die (N+1)-Redundanz. Bei ihr wird der erforderlichen Zahl von Einheiten (N, typisch ist N=1) eine weitere hinzugestellt. Fällt dabei die ursprünglich erforderliche Einheit aus, übernimmt die zusätzliche deren Funktion. Diese Redundanz bietet ausreichenden Schutz gegen eine Betriebsstörung der technischen Einrichtung selbst. Die (N+1)-Redundanz wird daher auch "Betriebsredundanz" genannt.*

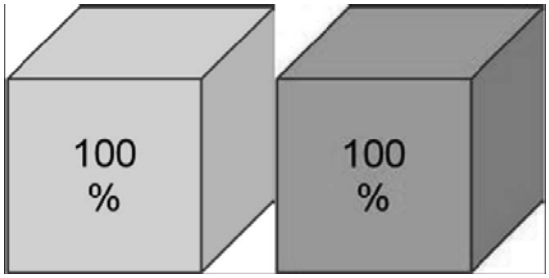


*Abbildung 1: (N+1)-Redundanz mit (N=1)*

*Befindet sich jedoch eine der beiden Einheiten in Wartung und ist damit nicht betriebsbereit, ist keine Redundanz mehr vorhanden. Zudem ist schon für diese einfache Betriebsredundanz bei diesem Modell eine Überkapazität von 100 % erforderlich.*

*Soll die Redundanz auch während einer Wartung gewährleistet sein, ist eine (N+2)-Redundanz aufzubauen. Dabei werden dem Wirksystem (N=1) zwei zusätzliche Systeme zur Seite gestellt.*

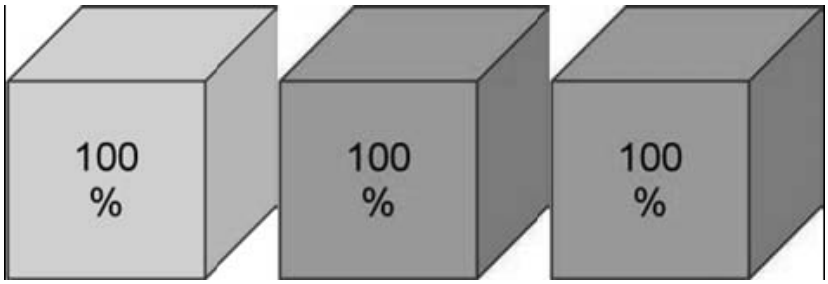


*Abbildung 2: (N+2)-Redundanz mit (N=1)*

*Zwar ist nun selbst bei wartungsbedingtem Ausfall eines der drei Systeme immer noch eine Redundanz gegeben. Dafür ist aber eine Überkapazität von 200 % erforderlich. Solche Lösungen stoßen daher rasch an räumliche und finanzielle Grenzen.*

*Hier schafft die Modularität sehr gut Abhilfe. Wird z. B. statt des Wertes 1 der Wert 2 für N gewählt, stellt sich der Aufbau einer (N+2)-Redundanz schon deutlich günstiger dar.*

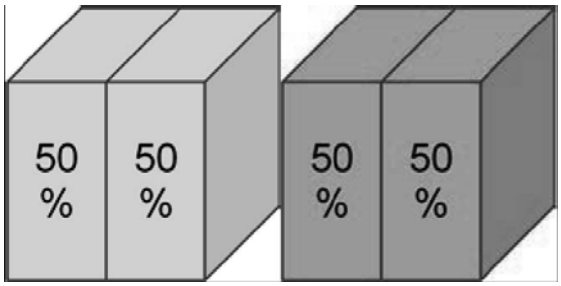


*Abbildung 3: (N+2)-Redundanz mit (N=2)*

*Bei gleicher Redundanzwirkung (Betriebs- und Wartungsredundanz) reduziert sich die Überkapazität von 200 % auf 100 %. Wird die Modularität z. B. auf (N=4) erweitert, sieht das Bild noch günstiger aus:*

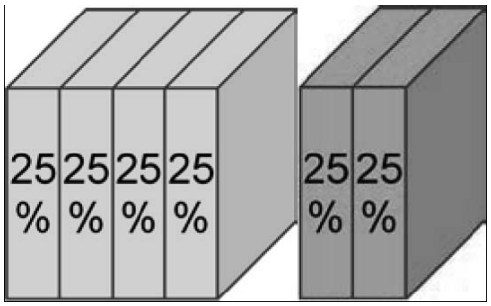


*Abbildung 4: (N+2)-Redundanz mit (N=4)*

*Zur Deckung der Grundlast stehen 4 Einheiten für jeweils 25 % der erforderlichen Leistung zur Verfügung. Weitere zwei 25 %-Einheiten bilden die Betriebs- und Wartungsredundanz. Die Überkapazität beträgt nur mehr 50 %.*

*Je höher der Wert für N getrieben wird, desto geringer wird die Überkapazität. Dass dieser Weg nicht endlos beschritten werden kann, ist klar. Zwar sinken durch die Modularität die Kosten für die Überkapazität. Gleichzeitig steigen aber die Kosten für die Unterbringung der Einheiten. Es ist erforderlich, alle Einheiten (im letzten Beispiel sind das schon 6) so unterzubringen und zu versorgen, dass durch ein externes Ereignis keinesfalls alle Einheiten zugleich betroffen sind.*

*Die Modularität enthält zugleich automatisch den Vorteil der Skalierbarkeit. Sobald der Leistungsbedarf steigt, kann den 4 Einheiten zu 25 % eine weitere kleine hinzugefügt werden. Bei der (N=1) Variante wäre eine Verdopplung des Erstsystems erforderlich, um das Redundanz-Prinzip aufrecht zu erhalten.*

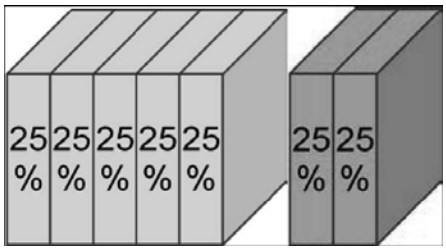


*Abbildung 5: Einfache Skalierbarkeit*

*Die Modularität hat als weiteren Vorteil, dass die Restkapazität beim Ausfall von mehr als 2 Einheiten größer ist.*

*Bei einer (N+2)-Redundanz ist gewährleistet, dass beim Ausfall von zwei Einheiten die Restkapazität mit 100 % ausreicht, um den Betrieb normal fortzuführen. Fällt bei (N+2) mit (N=1) tatsächlich eine dritte Einheit aus, ist die Restkapazität gleich Null. Wird N hingegen mit 4 festgelegt und fallen von den nun bei (N+2)-Redundanz vorhandenen 6 Einheiten tatsächlich 3 aus, steht immerhin noch eine Restkapazität von 75 % zur Verfügung. Bei entsprechendem Lastmanagement kann damit noch ein recht störungsfreier Betrieb aufrecht erhalten werden.*

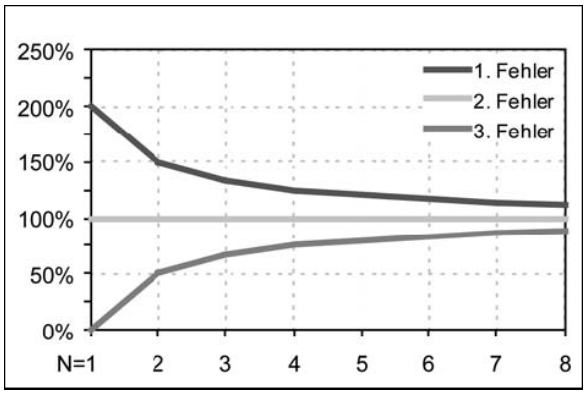


*Abbildung 6: Darstellung der Restkapazität bei (N+2)-Redundanz mit steigendem Wert für N*

*Da häufig die vorhandenen Ressourcen begrenzt sind, ist es nicht immer möglich, zur Erlangung einer Betriebs- und Wartungsredundanz tatsächlich 2 zusätzliche Einheiten zu installieren. Da Wartungsfälle in der Regel mit ausreichendem Vorlauf planbar sind, kann die zweite Einheit im Bedarfsfall auch als mobile Einheit temporär angeschlossen werden.*

*Eine solche mobile Einheit kann in der Institution selber vorrätig gehalten oder über einen externen Dienstleister angemietet werden. Hierzu sind entsprechende SLAs mit dem Dienstleister zu vereinbaren und es müssen die erforderlichen Anschlusspunkte vorbereitet sein.*

## 4.9 Maßnahmenkatalog 1.58: Technische und organisatorische Vorgaben

*Ein Serverraum sollte als geschlossener Sicherheitsbereich konzipiert sein. Dieser sollte möglichst gut zu sichernde Zugangstüren und Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen (siehe auch M 1.10 Sichere Türen und Fenster). Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei der Planung eines Serverraumes bzw. der Auswahl geeigneter Räumlichkeiten sollten potentielle Gefährdungen durch Umgebungseinflüsse möglichst minimiert werden. So ist Gefahrenpotentialen wie Wassereinbrüchen bei Flachdächern oder in Kellerräumen genauso zu begegnen wie EMV-Störquellen, z. B. Mobilfunk-Sendeeinrichtungen oder Drehstromaggregaten.*

*Bei der Planung sollte auch darauf geachtet werden, dass die Trassen der Versorgungsleitungen des Gebäudes, z. B. für Wasser oder Gas (siehe M 1.24 Vermeidung von wasserführenden Leitungen), nicht in unmittelbarer Nähe oder gar durch sensible Bereiche des Serverraums verlaufen.*

*Für die in Serverräumen betriebenen IT-Komponenten wird in vielen Fällen ein hohes Maß an Verfügbarkeit gefordert. Diesen Anforderungen kann durch redundante Auslegung der infrastrukturellen und technischen Einrichtungen Rechnung getragen werden (siehe Maßnahme M 1.52 Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur).*

*Ein Serverraum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und wichtiger noch für nur zeitweilig Beschäftigte, z. B. zu Wartungsarbeiten tätige, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.*

*IT-Systeme, die von Externen betreut werden, sollten in separaten Räumen aufgestellt werden. Es ist außerdem zu überlegen, IT-Systeme mit unterschiedlichem Schutzbedarf oder aus verschiedenen Bereichen in getrennten Serverräumen aufzustellen, um den Kreis der Zutrittsberechtigten klein zu halten.*

*In einem Serverraum sollten sich auf keinen Fall Geräte oder Ausrüstung befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, also z. B. Fax-Geräte oder Fotokopierer. Brennbare Materialen wie Druckerpapier sollten ebenfalls nicht in einem Serverraum gelagert werden.*

*Es sollte verboten werden, in einen Serverraum tragbare IT-Systeme, Mobiltelefone oder Kameras mitzubringen, wenn diese nicht unter der Kontrolle der jeweiligen Institution stehen. Generell sollte der Betrieb von Mobiltelefonen in Rechenzentren untersagt werden, da diese den Betrieb der IT-Systeme erheblich stören können. Ausnahmen hiervon müssen abgestimmt sein (siehe M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung).*

### 4.10 Maßnahmenkatalog 1.69: Verkabelung in Serverräumen

*Auch und gerade in Serverräumen und Rechenzentren müssen die Grundsätze der strukturierten Verkabelung nach EN 50173-1 "Informationstechnik - Anwendungsneutrale Kommunikationskabelanlagen - Teil 1: Allgemeine Anforderungen" beachtet werden. Eine speziell für Rechenzentren erarbeitete Erweiterung EN 50173-5 ist als Norm-Entwurf erschienen. Die Umsetzung der Anforderungen der Norm wird damit für den Anwender erleichtert.*

*Die Anforderungen aus dem vorhandenen oder geplanten Netzkonzept der Institution bilden die Grundlage für die Strukturierung der IT-Verkabelung in Serverräumen und Rechenzentren. Die Struktur legt fest, wie die Server vernetzt werden und wie sie an das LAN, an externe Netze und an Provider angebunden werden. In der Institution eingesetzte oder geplante betriebsunterstützende Systeme, wie z. B. Terminalserver, KVM-Switches und SAN/NAS (Storage Area Network, Network Attached Storage), sind vorausschauend zu berücksichtigen. Die Grundlagen für die Struktur der so genannten Access- und Konzentrationsbereiche der ITVerkabelung in Analogie zu den Gebäudestrukturen mit Etagenverteilern und Gebäudeverteilern sind damit festgelegt.*

*In größeren Installationen werden häufig Gruppen von Schränken, in denen Server aufgestellt sind, einem "Netzschrank" zugeordnet. Zwischen Netzschränken und den zugeordneten Serverschränken wird eine feste Verkabelung oder eine spezielle Systemverkabelung für Serverräume verlegt. Die Netzschränke wiederum sind untereinander nach Anforderung der Institution verbunden.*

*Um die Fläche des Serverraums bzw. Rechenzentrums bestmöglich zu nutzen, ist es erforderlich, ein auf die Anforderungen abgestimmtes Raumlayout zu entwickeln. In diesem Raumlayout sind die benötigten Flächen für die Schränke mit den Systemen, die die Institution betreibt (neben Servern auch Speichersysteme und aktive und passive Netzkomponenten), mit Reserven für die Zukunft zu gliedern. Es müssen dabei Sicherheitsaspekte wie die Anordnung der Fluchtwege, Betriebsaspekte wie die Anordnung der Transportwege und auch klimatechnische Gesichtspunkte berücksichtigt werden. Auf dieser Grundlage kann die Planung der elektrotechnischen Versorgung und der Trassenführung erfolgen.*

*Die Verwendung eines hochbelastbaren Doppelbodens ist für Serverräume und Rechenzentren zu empfehlen (siehe M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum). Wird der Doppelboden in die Luftführung der Schrankklimatisierung mit einbezogen, so sind die Trassensysteme zu berücksichtigen. Durch viele querende Trassen zwischen Frischluftzuführung in den Doppelböden und weiter entfernt davon stehenden Schränken, die eine hohe Wärmelast aufweisen, können "Wärmenester" entstehen. Obwohl die Klimaleistung für den Raum ausreichend bemessen ist, erhalten einige Schränke und die darin stationierten IT-Komponenten zu wenig gekühlte Luft. Das birgt die Gefahr von Ausfällen von Servern oder aktiven Netzkomponenten durch Überhitzung.*

*Zudem ist unbedingt auf eine nicht staubende Versiegelung des Estrichs bzw. Rohfussbodens zu achten.*

*Es ist zu empfehlen, so umfassend wie möglich fest zu verkabeln. Dies fördert eine fachgerechte Belegung der Trassensysteme im Doppelboden oder unter der Decke. Server sollten möglichst nicht mit Patchkabeln ohne zusätzliche Trassensysteme an zentral im Raum stationierte Server-Switches angeschlossen werden, auch wenn diese Verkabelungsart in der Praxis häufig angewandt wird. Eine solche "fliegende Verkabelung" ist besonders bei Nachverkabelungen gefährdet.*

*Auf die Anforderungen der Institution abgestimmte Schranksysteme, in denen Systeme zur Kabelführung und Überlängenablage vormontiert sind, erlauben eine übersichtliche und wartungsfreundliche Kabelführung im Schrank.*

*Auch wenn nur wenige Schränke vernetzt werden, ist es zweckmäßig, in den Schranksystemen Patchfelder für den Anschluss der Server und eine feste Verbindung dieser Patchfelder an den Netzknoten im Serverraum zu installieren. Wenn eine Neukonzeption ansteht, ist es zum Beispiel zu erwägen, pro Schrank ein Patchfeld für Kupferkabel der Kategorie 6 oder 7 (CAT-6 oder CAT-7, tauglich für 10 Gigabit-Anschluss) und gegebenenfalls zusätzlich ein LWL-Patchfeld vorzurüsten. Letzteres kann beispielsweise zum Anschluss der Server an Speichernetze dienen. Selbstverständlich ist die Vorrüstung von Schränken auf die Planungen der Institution abzustimmen.*

*Wenn keine baulichen Gründe dagegen sprechen, ist in vielen Fällen eine Kabelführung über Trassen, die unter der Decke des Serverraums verlaufen, der Kabelführung durch den Doppelboden vorzuziehen. Insbesondere wenn der Doppelboden der Klimatisierung dient, kann eine Doppelboden-Verkabelung die Führung der benötigten Kühlluft beeinträchtigen. Außerdem birgt die Verlegung der Kabel im Doppelboden erfahrungsgemäß die erhöhte Gefahr, dass nicht mehr benötigte Kabel nicht entfernt werden. Bei einer Verlegung der Kabel in gut zugänglichen Deckentrassen ist das Entfernen alter Kabel in der Regel deutlich einfacher.*

### 4.11 Weitere Maßnahmenkataloge

Für eine BSI- oder ISO 27001-Zertifizierung müssen selbstverständlich noch weitere Maßnahmenkataloge für die allgemeine Infrastruktur, die Betriebsorganisation, die allgemeinen Verkabelungen und die eingesetzten IT-Geräte sowie die genutzte Software beachtet werden.

## IV. Fazit

Bei angestrebten Zertifizierungen ist zu beachten, dass der Serverraum nur einen Teil einer IT-Landschaft abbildet.

Bei ISO 27001 und BSI-IT-Grundschutzzertifizierungen müssen die eingesetzten Server und Clients ebenso wie die genutzte Software dokumentiert und geprüft werden. Auch bedarf es der Dokumentation von allgemeiner und technischer Infrastruktur und Verfahrensabläufen.

Bei dem Gütesiegel des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein steht der Umgang personenbezogener Daten der einzelnen Verfahren im Vordergrund. Ob jedoch ein Verfahren rechtlich überhaupt zulässig ist, lässt sich nicht an den Serverschränken ausmachen. Hier muss zusätzlich geprüft werden, was das jeweilige Unternehmen oder die Behörde konkret mit den personenbezogenen Daten macht.

Bei unserem Vor-Ort-Test der Musterzelle hatte die Unterbrechung der primären Stromversorgung sofort das Notstromaggregat eingreifen lassen und den zuständigen Administrator per SMS benachrichtigt.

Die grafische Oberfläche der Sicherungsbelegung und der Netzumschaltung mit deren Kurzbeschreibungen direkt auf den IT Compact Serverschrankwänden sorgt für einen schnellen Überblick, ohne dass nach Belegungsplänen gesucht werden muss.

Die abschließbaren Serverschranktüren vermeiden ungewolltes und/oder unbefugtes Betätigen der Stromschaltelemente.

Nach Prüfung und Inaugenscheinnahme der Musterzelle des IT Compact Serverraumes gibt es keine Anhaltspunkte, die einer Zertifizierung dieses Produktes im produktiven Umfeld widersprechen.

## V. Literatur


- Bundesdatenschutzgesetz (BDSG)
- Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
- IT-Grundschutz-Kataloge, 13. Ergänzungslieferung 2013, Bundesamt für Sicherheit in der Informationstechnologie


Anhänge zu den Quellen liegen dieser Stellungnahme nicht bei, da sie frei verfügbar sind und kostenlos im Internet abgerufen werden können.

Zitate aus dem BDSG und den BSI-Grundschutzkatalogen sind kursiv gekennzeichnet.

Andreas Ebbersmeyer

Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich / technisch)

Diese Stellungnahme stellt keine verbindliche Rechtsauskunft dar.