Rittal – Das System.

Schneller – besser – überall.

Whitepaper
Physische Sicherheit in der IT- und Rechenzentrums-Technologie

Bernd Hanstein

Inhaltsverzeichnis

Executive Summary 4
Einführung 5
Testverfahren und Prüfinstitute 7
Detailbetrachtung der physischen Bedrohungen 8
Feuer 8
Korrosive Gase und Rauch 9
Trümmerlasten 10
IP-Schutzarten: Schutz vor Staub, Wasser und festen Partikeln 11
Schutz vor Fremdzugriff 13
EMV-Schutz 14
Modulare Sicherheitsräume und Safe-Lösungen 17
Micro Data Center 17
Sicherheitsräume 19
Literatur 24
Abkürzungsverzeichnis 25

Autor: Bernd Hanstein

Nach Abschluss des Diplomstudiengangs der Physik an der Justus-Liebig-Universität in Gießen im Jahr 1987 hat Bernd Hanstein in der Zentralen Forschung der Siemens AG auf dem Gebiet der Testverfahren für hochintegrierte Schaltungen gearbeitet. Anschließend war er in verschiedenen Positionen innerhalb der Siemens AG im Unternehmensbereich Öffentliche Netze für die Implementierung großer ITK-Projekte zuständig. Nach dem Wechsel zu Siemens VDO Automotive im Jahre 2002 war Bernd Hanstein als Hauptabteilungsleiter für den weltweiten Systemtest der Multimediageräte für Kraftfahrzeuge verantwortlich. Seit 2007 hat er die Leitung des IT-Produktmanagements bei Rittal in Herborn inne. Seine Schwerpunkte: IT-Komponenten, RiMatrix-Systemlösungen und Rechenzentrumstechnologie.

Abbildungsverzeichnis

Abbildung 1: Darstellung der physischen Infrastruktur eines Rechenzentrums 5
Abbildung 2: Rittal ECB•S-Zertifikat 7
Abbildung 3: IP-Schutzartprüfung 12
Abbildung 4: EMV-Prüfung 15
Abbildung 5: Produktportfolio Micro Data Center Level E, Level B, Level A 17
Abbildung 6: Rittal IT-Sicherheitsraum 20

Tabellenverzeichnis

Tabelle 1: IP-Systematik – Schutz vor Staub und Festkörpern 11
Tabelle 2: IP-Systematik – Schutz vor Wasser 12
Tabelle 3: RC-Systematik – Schutz vor Fremdzugriff 14
Tabelle 4: EMV Produkt-, Produktfamilien- und Fachgrundnormen 14
Tabelle 5: EMV Prüfnormen (für Raumschirmung) 15
Tabelle 6: Übersicht der MDC Eigenschaften 19
Tabelle 7: Produktportfolio der Rittal Sicherheitsräume 21
Tabelle 8: Übersicht der Sicherheitsraum-Eigenschaften von Rittal 22

Executive Summary

Rechenzentren stellen eine Schlüsseltechnologie in der zunehmend digitalisierten Welt dar. Sie beherbergen die Server und Storage-Systeme mit den zugehörigen Netzwerkkomponenten, so dass Applikationen zu den vereinbarten Verfügbarkeiten und mit der geforderten Leistung zur Verfügung stehen. Ebenso wichtig ist die physische Infrastruktur, die für diese Komponenten die Stromversorgung und Kühlung aber auch die Überwachung aller Betriebsparameter bereitstellt.

Immer größere Bedeutung gewinnen dabei alle Aspekte rund um das Thema Sicherheit. Diese beginnt mit den bekannten Lösungen der Virenabwehr und Firewall-Systemen, doch auch der Schutz gegen physische Bedrohungen erfordert eine zunehmende Beachtung. Dazu gehört die Abwehr ganz konkreter Bedrohungen wie Einbruch und Diebstahl, aber auch das Vermeiden eines ungewollten Abhören über EMV-Ausstrahlung der IT-Geräte, sowie die „traditionellen“ Gefahrenpotentiale durch Feuer, Rauch, Wasser und Staub, um nur einige zu nennen.

Das vorliegende Whitepaper beleuchtet die einzelnen Bedrohungsszenarien und zeigt auf, mit welchen Maßnahmen physischen Gefahren begegnet werden kann.

Einführung

Computertechnik ist einer der Grundbausteine der modernen Gesellschaft. Es gibt keinen Bereich, in denen Computer und vernetzte Kommunikation nicht bereits Einzug gehalten. Diese Dienste, egal ob sie bewusst wahrgenommen werden oder still im Hintergrund arbeiten, benötigen Rechenleistung und Netzwerk-infrastruktur. Diese muss auch physisch durch Hard- und Software in einer geeigneten Umgebung aus Klimatisierung, Stromversorgung und Netzanbindung in Rechenzentren bereitgestellt werden – trotz aller Virtualisierung. Rechenzentren sollen zudem vor physischen Gefahren wie Feuer, Wasserschäden, Einbruch und Diebstahl schützen. Dieser Schutz wird durch die stetig fortschreitende Digitalisierung immer wichtiger.

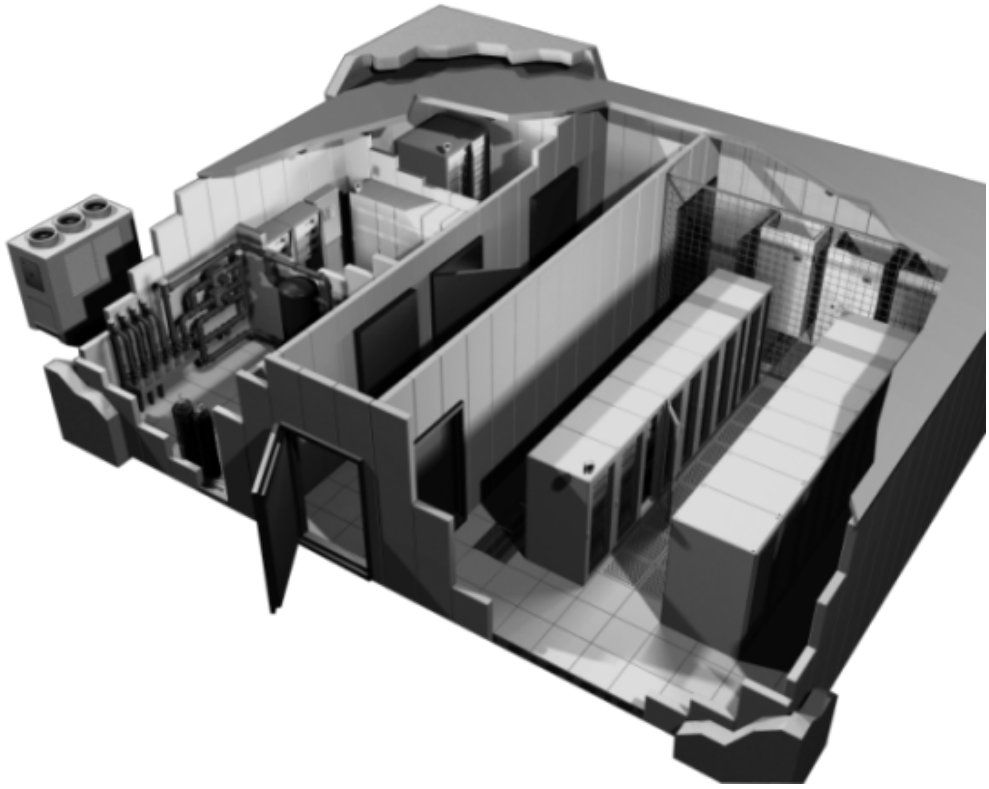

Abbildung 1: Darstellung der physischen Infrastruktur eines Rechenzentrums

Die Schutzwirkung des Rechenzentrums vor physischen Gefahren muss auf mehreren Ebenen ansetzen, denn die Bedrohungen wirken über unterschiedliche Vektoren. Die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) listen 27 Gefährdungen für Rechenzentren auf [Ref. 1], von höherer Gewalt über organisatorische Mängel, technisches Versagen bis hin zum vorsätzlichen Handeln.

Dagegen helfen bewährte Konzepte aus der IT-Sicherheit, die auf die jeweiligen Gefährdungen zugeschnitten sind. Gegen Feuer schützen beispielsweise

Brandschutzmauern, deren eventuell vorhandene Kabeldurchführungen ebenfalls in der Lage sind, dem Brand ausreichend lange zu trotzen. Ein noch größeres Problem stellt Wasserdampf dar, den Beton aufgrund seiner kristallinen Restfeuchte bei hohen Temperaturen abgibt. Hier sind Dampfsperren und Hitzeschutzbeschläge erforderlich. Damit ein Rechenzentrum seinen Inhalt zuverlässig schützen kann, sind also zahlreiche Aspekte bei Planung, Ausstattung und Aufbau zu beachten. Das gilt selbstverständlich nicht nur für den gemauerten Raum, sondern für modulare Versionen von Rechenzentren, wie sie auch Rittal mit Grundschutzraum, Hochverfügbarkeitsraum und der Safe-Lösung Micro Data Center anbietet.

Waren früher einige Tage Ausfallzeit pro Jahr durchaus akzeptabel, hat die immer größere Abhängigkeit der Wirtschaft von digitalen Systemen zu erheblich stringenteren Anforderungen geführt. Mit gutem Grund: Ausfälle der IT kommen die deutsche Wirtschaft teuer zu stehen. Allein mittelständischen Unternehmen entstanden durch den Ausfall geschäftskritischer IT-Systeme Kosten von bis zu 380.000 Euro pro Jahr. Das geht aus einer Studie hervor, für die das Marktforschungsunternehmen Techconsult [Ref. 2] im Jahr 2013 300 Unternehmen mit 200 bis 4.999 Mitarbeitern befragt hat. Eine Umfrage von EMC [Ref. 3] ermittelte entweder Datenverluste oder Ausfallzeiten in den letzten zwölf Monaten bei 56 Prozent der Unternehmen in Deutschland.

wenn es um den Schutz komplexer Systeme geht, ist eine ganzheitliche Betrachtung erforderlich. Ein Rechenzentrum besteht aus zahlreichen Gewerken. Klimatisierung, Stromversorgung und -verteilung, Netzwerkanbindung, Zugriffskontrolle und nicht zuletzt die bauliche Hülle, ausgeführt als konventionell gebauter Raum oder als modulares „Raum-in-Raum“-System. Dabei kommt es nicht in erster Linie darauf an, dass die Einzelkomponenten feuerfest und wasserbeständig sind, sondern vielmehr das gesamte System diese Kriterien erfüllen. Hier sind Anwender aufgefordert, Zertifizierungen und Prüfsiegel genau zu hinterfragen. Nur so lässt sich herausfinden, ob die Schutzwirkung in ihrer Gesamtheit besteht – und nicht nur für einzelne Elemente. Darum hat eine erfolgreich absolvierte Systemprüfung immer die größere Aussagekraft bezüglich der Schutzwirkung als eine Reihe von Einzelprüfungen.

Klimatisierung, Stromversorgung, Datenanbindung – all diese Komponenten sollten optimal in das Rechenzentrumskonzept integriert und deren Verwaltung mit dem RZ-Management gekoppelt sein. Rittal bietet zu vielen dieser Bereiche – wie Klimatisierung, 19“-Schranktechnik und Rechenzentrumsmanagement – gesonderte Whitepaper an, die diese Themen umfassend beleuchten.

Testverfahren und Prüfinstitute

Auch wenn es Komplettangebote zur Zertifizierung von Rechenzentren gibt, kommt es letztlich auf die Prüfung der einzelnen Gewerke an. Brandschutz, Schutz vor Wasserschäden oder vor Staub und Rauch müssen bei einem Rechenzentrum durch Einzelnachweise belegt werden. Dafür sind viele internationale Standards verantwortlich, darunter das Deutsche Institut für Normung (DIN), europäische Normen (EN), die European Certification Body GmbH (ECB) und die International Organization for Standardization (ISO).

Der Vorteil der einzelvertraglich vereinbarten Verbindlichkeit von Normen liegt darin, dass sich Rechtsstreitigkeiten von vornherein vermeiden lassen, da es sich bei den Normen um eindeutige Festlegungen handelt. Wenn es im Kauf- und Werkvertragsrecht um Sachmängel geht, spricht der Beweis des ersten Anscheins für den Anwender der Norm in dem Sinne, dass er die im Verkehr erforderliche Sorgfalt beachtet hat. Damit kann er auch dem Vorwurf der Fahrlässigkeit begegnen.

Auch die Hersteller selbst können, wenn sie dafür akkreditiert sind, Prüfungen durchführen, beispielsweise die Schutzartprüfung.

Besonders die European Certification Body GmbH (ECB) wird heute von vielen Anwendern als die maßgebliche Zertifizierung für Rechenzentren angesehen. Sie ist eine neutrale, akkreditierte Zertifizierungsstelle nach ISO/IEC 17065 [Ref. 4]. Sie erteilt die ECB•S-Zertifikate für Erzeugnisse der Sicherheitsbranche. Die ECB•S-Zertifizierung der European Security Systems Association (ESSA) e.V. basiert ausschließlich auf den Anforderungen der europäischen Normung und ist international anerkannt. Jedes Produkt wird einzeln registriert und kann jederzeit einer produktionstechnisch unangemeldeten Güteüberwachung unterliegen. Für die Versicherungswirtschaft ist die Zertifizierung eine verlässliche und objektive Grundlage für die Risikokalkulation und der damit verbundenen sicherheitstechnischen Einstufung. Der Rittal Hochverfügbarkeitsraum verfügt beispielsweise über eine ECB•S-Zertifizierung.


CERTIFICATE

ECB·S

Rittal GmbH & Co. KG

Certificate Number

This certificate will expire on

29 November 2015

ECB·S

Abbildung 2: Rittal ECB•S-Zertifikat

Die größten physischen Gefahren für ein Rechenzentrum sind Feuer, Wasser, Staub und Rauchgase, Trümmerlasten, EMV-Strahlung (elektromagnetische Verträglichkeit) und Fremdzugriff. Für jeden dieser Gefahrenvektoren gibt es einen oder mehrere relevante Normen, die es einzuhalten gilt. So wird oft verlangt, dass eine Wand einen bestimmten Feuerwiderstand hat, beispielsweise F 90 oder F 120 nach DIN 4102 bzw. EI 90 oder EI 120 gemäß der EN 1363 [Ref. 8] aufweist. Eine solche Wand erfüllt ihre Funktion bei einem Brand 90 beziehungsweise 120 Minuten lang. Ziel dieser Klassifizierung ist der Schutz von Menschenleben, nicht der des Rechenzentrums. Wenn die IT im Fokus des Schutzes stehen soll, kommt es darauf an, dass nicht nur eine Wand, sondern das Rechenzentrum als Ganzes dem Feuer standhält.

Das BSI fordert ebenfalls die systemweite Prüfung für IT-relevante Räume. So wird in Maßnahme 1.6 „Einhaltung von Brandschutzvorschriften“ [Ref. 5] zwar nur gefordert, dass die bestehenden Brandschutzvorschriften wie die DIN 4102 „Brandverhalten von Baustoffen und Bauteilen“ [Ref. 6] und Verordnungen der MBO, LBO, MLAR sowie die Auflagen der Bauaufsichtsbehörden unbedingt einzuhalten sind. Für Räume, in denen wichtige IT-Geräte und Datenträger (Server, Datensicherung etc.) untergebracht sind, sollten allerdings zudem die Regelungen der Norm EN 1047 Teil 2 [Ref. 7] Beachtung finden.

Detailbetrachtung der physischen Bedrohungen

Feuer

Feuer ist wahrscheinlich die von Administratoren am meisten gefürchtetste Bedrohung für Rechenzentren und Serverräume. Schon kleine Brände können durch die entstehenden aggressiven Gase große Schäden an IT-Equipment und Infrastruktur anrichten. Entsprechend fällt die Prüfung auf Feuerwiderstand sehr intensiv aus. Schon für die Bauteilprüfung F 90/ EI 90 nach DIN 4102/ EN1363 [Ref. 6, Ref. 8] werden die Einzelbauteile wie Wände, Türen oder Baustoffe, nach einer Einheitstemperaturkurve beflammt. Die Prüfzeit beträgt 90 Minuten bei mehr als 1.100° C. Dabei darf die Temperatur auf der brandabgewandten Seite, lediglich um bis zu 140 Kelvin (K) ansteigen (punktuell bis 180 K). Die relative Luftfeuchte wird bei diesem Test nicht gemessen. Sie kann darum, je nach Baustoff, schon nach kurzer Zeit auf 100 % ansteigen und wäre für die Server und Infrastruktur im Inneren des Rechenzentrums gefährlich.

Zertifizierten Schutz gewährleistet nur eine Systemprüfung, bei der das komplette Rechenzentrum mit allen Komponenten, einschließlich Türen und Schotts für Kabel

und Rohre unter dem Ernstfall ähnlichen Bedingungen getestet wird. Eine Systemprüfung gemäß der EN 1047-2 [Ref. 7] verlangt beispielsweise eine Beflammungszeit von 60 Minuten. Daran schließt sich eine 24-stündige Abkühlungsperiode im geschlossenen Brandofen an. Diese Zeit wird auch als Nachheizperiode bezeichnet. Das Prüfobjekt bleibt so lange im Brandraum, bis nach einigen Stunden die höchste Innentemperatur im Prüfling erreicht ist. Das besondere Augenmerk ist auf bauliche Schwachstellen wie Türen, Türzargen und Kabel- und Rohreinführungssystemen gerichtet. Um die Prüfung zu bestehen, darf die Temperatur im Inneren nicht mehr als 50 K über die Ausgangstemperatur steigen und – ebenso wichtig – die relative Luftfeuchtigkeit darf 85 % nicht überschreiten. Produkte, die diesen und die weiteren Tests der EN 1047-2 Anforderung erfolgreich absolviert haben, werden in der ECB•S Datenbank registriert. Auch wenn in DIN 4102 [Ref. 6] und EN 1363 [Ref. 8] in der Regel Bauteilprüfungen beschrieben werden, können komplette Systemlösungen wie Safes und Sicherheitsräume gemäß diesen Normen geprüft werden.

Korrosive Gase und Rauch

Gas- und Rauchdichtigkeit ist eine zentrale Anforderung, die Rechenzentren und Serverräume erfüllen müssen. Der Faktor Dichtigkeit ist elementar, wenn der Rauch eines Feuers im Serverraum gehalten werden muss, damit er sich nicht auf andere Gebäudeteile ausdehnt. Brände in IT-Umgebungen werden nicht mit Wasser, sondern z. B. mit inerten Gasen oder durch Sauerstoffentzug gelöscht. Das funktioniert aber nur zuverlässig, wenn die Gase auch innerhalb des Raumes bleiben und nicht durch undichte Stellen in den Rest des Gebäudes entweichen. Ebenso muss eine Brandvermeidung durch Sauerstoffentzug scheitern, wenn durch Türen, Fenster oder bauliche Mängel Frischluft in den Raum gesaugt wird. Brennt es außerhalb des Rechenzentrums, kommt der Abdichtung eine ebenso große Rolle zu. Dann müssen die IT-Komponenten im Rechenzentrum vor aggressiven Gasen geschützt werden, da die Leiterplatten in den Servern, Switchen und anderer Hardware korrodieren könnten.

Relevante Normen für die Zertifizierung sind die DIN 18095 [Ref. 9] und die EN 1634 [Ref. 10]. Teil 3 der EN 1634 legt ein Prüfverfahren und die dazu gehörenden Prüfbedingungen zur Ermittlung der Leckage von kaltem und warmem Rauch von einer Seite eines Abschlusses zur anderen fest. Gemessen wird die sogenannte Leckrate für jede untersuchte Prüfbedingung. Im Zusammenhang mit Rechenzentren werden in der Regel Türen und Druckentlastungsklappen getestet, weil sie normalerweise die einzigen beweglichen Öffnungen in den Raum hinein darstellen. Durch das Feuer baut sich auf der dem Rauch ausgesetzten Seite ein Druck von bis zu 50 Pascal (Pa) auf, der Druckunterschied zwischen den beiden Seiten treibt den Rauch durch alle vorhandenen Spalten und Öffnungen. Eine Tür, die ihre Aufgabe als Teil des Brandsicherheitssystems erfüllt, muss den Durchstrom von Rauch verhindern, um sicherzustellen, dass die Bedingungen auf der anderen Seite der Tür nicht unerträglich werden.

Der Test erfolgt in einer Prüfkammer, in deren Vorderseite das Prüfobjekt eingebaut wird. Für den nötigen Druck sorgt ein Gebläsesystem. Eine Heizung erzeugt Temperaturen von etwa 200° C, um die Rauchtemperatur nachzubilden. Systembedingte Spalte, beispielsweise an Schwellen oder zwischen Türflügeln, werden ausgemessen und aufgezeichnet. Auch automatische Schließmechanismen werden vor der Prüfung getestet und einige Male benutzt. Dieser kurze Test ersetzt jedoch keine Dauerprüfungen der Mechanismen. Er soll nur sicherstellen, dass die Tür ordnungsgemäß schließen lässt.

Die eigentliche Prüfung auf Rauchdichtigkeit wird mit unterschiedlichen Druckstufen bis zu 50 Pa und bei 20°C und 200°C Raumtemperatur durchgeführt. Erfolgreich getestete Prüflinge dürfen eine in der Norm definierte Luftwechselrate zwischen Innenraum und Außenbereich nicht überschreiten. Wichtig ist auch, während des Tests festzuhalten, ob und wenn ja welche Elemente der Tür durch die Hitze verformt werden und ob die Tür nach Abschluss des Tests noch geöffnet werden kann.

Trümmerlasten

Ebenso sind Gefahren zu betrachten, die durch herabstürzende Trümmer verursachen. Die dabei frei werdenden Kräfte können große Zerstörungen bei der Hardware und Infrastruktur anrichten. Zusätzlich zu den Brandprüfungen der Sicherheitsräume und der Safe-Lösungen definieren die Normen Stoß- und Sturzprüfungen.

Die EN 1047-2 [Ref 7.] beschreibt eine Stoßprüfung für Hochverfügbarkeitsräume. Diese Prüfung wird durchgeführt, nachdem der Raum bereits 45 Minuten beflammt wurde. Auch die DIN 4102 beschreibt eine Stoßprüfung. Dabei muss eine als Brandwand genutzte Wand nach der Beflammung (Feuerwiderstandstest nach DIN 4102 ETK [Ref. 6]) einer definierten Schlagbelastung standhalten. Soll die Wand eine tragende Funktion haben, entsteht dabei für das Prüfobjekt zusätzliche Druckbelastung.

Diese Schlagfestigkeit wird in einer eigenständigen Norm EN 50 102 [Ref. 11] geregelt. Sie wird im IK-Code spezifiziert und macht eine Aussage über den äußeren mechanischen Schutz. Wie der Test durchgeführt wird, ist in der entsprechenden Produktnorm geregelt. Pro Fläche werden fünf Beanspruchungen durchgeführt (gleichmäßig verteilt, Pendel oder Freifall). Der Prüfling muss dabei auf einem starren Rahmen montiert sein und darf nicht nachgeben. Auch exponierte Stellen wie Scharniere oder Verschlüsse. Nach der Prüfung muss der Prüfling voll funktionsfähig sein und darf insbesondere keine Beeinträchtigungen der Schutzart aufweisen.

IP-Schutzarten: Schutz vor Staub, Wasser und festen Partikeln

Staub wird selten als physische Gefahr gesehen und in einer typischen Büroumgebung in Deutschland führt Staub praktisch nie zu IT-Problemen. Anders sieht es in Produktionshallen aus, wo Staub in großen Mengen vorherrscht und nicht vollständig durch Absaugungen entfernt werden kann. Auch hier müssen IT-Systeme arbeiten und dürfen dem Staub nicht ungeschützt ausgesetzt sein. Wasser hingegen ist eine ganz offensichtliche Gefahr für IT-Anlagen, die jeder sofort als solche erkennt. Beim Outdoor-Einsatz darf IT-Equipment weder nass oder auch nur feucht werden. Wasserschäden durch Rohrbrüche oder ähnliches gilt es unbeschadet zu überstehen. Je nach Einsatzzweck und Objekt ist der Schutz gestaffelt und wird durch die sogenannten IP-Schutzarten nach EN 60 529 [Ref. 12] definiert. Prüfungen nach EN 60 529 klassifizieren den Schutz von elektrischen Betriebsmitteln bis zu einer Nennspannung von 72,5 kV durch Gehäuse, Abdeckungen und ähnliches.

Die IP-Schutzarten (IP = International Protection) geben durch eine einfache Zahlenkombination an, wogegen das Gehäuse seinen Inhalt schützt. Generell sollen Personen vor Zugang zu gefährlichen Teilen innerhalb des Gehäuses geschützt werden. Ebenso muss das Betriebsmittel innerhalb des Gehäuses gegen das Eindringen von festen Fremdkörpern und von Wasser gesichert sein. Gefährlich sind in diesem Sinne aktive Teile, die einen elektrischen Schlag erzeugen können und mechanische Teile, deren Berührung gefährlich ist.

Die Schutzart wird in der Form IP XY angegeben. Die Zahlen der ersten Kennziffer reichen von 0 bis 6, die nächsthöhere Zahl beinhaltet jeweils alle niedrigeren. Sie definieren den Schutz vor festen Gegenständen und Staub.

Code	**Schutzeigenschaft**
IP 1x	geschützt gegen feste Fremdkörper Ø 50 mm und größer
IP 2x	geschützt gegen feste Fremdkörper, Ø 12,5 mm und größer
IP 3x	geschützt gegen feste Fremdkörper, Ø 2,5 mm und größer
IP 4x	geschützt gegen feste Fremdkörper, Ø 1,0 mm und größer
IP 5x	staubgeschützt
IP 6x	staubdicht

Tabelle 1: IP-Systematik – Schutz vor Staub und Festkörpern

Die Zahlen der zweiten Kennziffer kennzeichnen den Schutz vor Wasser. Sie reichen von 0 bis 8, bis 6 gilt der gleiche Beinhaltungsmechanismus wie bei der ersten Ziffer.

Code	**Schutzeigenschaft**
IP x1	senkrecht fallendes Tropfwasser

IP x2	senkrecht fallendes Tropfwasser, Gehäuse 15° geneigt
IP x3	Sprühwasser im Winkel von 60° zur Senkrechten
IP x4	Spritzwasser aus jeder Richtung
IP x5	Strahlwasser aus jeder Richtung
IP x6	starkes Strahlwasser aus jeder Richtung
IP x7	zeitweiliges Untertauchen in Wasser unter genormten Druck- und Zeitbedingungen
IP x8	dauerndes Untertauchen in Wasser

Tabelle 2: IP-Systematik – Schutz vor Wasser

In Deutschland führen die Prüfungen zu einem großen Teil von TÜV und VDE durch. Darüber hinaus sind Prüflaboratorien von Herstellern entsprechender Produkte mit Schutzartprüfungen befasst. So ist das Rittal QM-Prüflabor durch den DAKKS und durch UL unter anderem auch für Schutzarten akkreditiert. Neben den IP-Prüfungen gemäß EN finden bei Rittal Schutzartprüfungen gemäß UL- und NEMA-Vorschriften statt, die für den amerikanischen Markt von großer Bedeutung sind.

Abbildung 3: IP-Schutzartprüfung

Geprüft wird kurzzeitig und ohne Dauerbeanspruchung, wie sie etwa bei stunden- oder tagelangen Regenfällen auftreten kann. Daher ist eine hohe Schutzart nicht gleichbedeutend mit der Eignung für die Aufstellung im Freien. Für die Tests auf das Eindringen von Fremdkörpern und Staub wird zunächst mit Objekten mit definierten Größen versucht, in den Prüfling vorzudringen. Für die Tests ab IP 5x kommt eine Staubkammer mit oder ohne Möglichkeit zur Erzeugung von Unterdruck zum Einsatz. Als eingebrachtes Testmittel wird Talkumpuder verwendet, das sich gut auf Flächen nachweisen lässt. Bei IP 5x darf Staub nur in einer solchen Menge eindringen, dass das zufriedenstellende Arbeiten des Gerätes oder die Sicherheit nicht beeinträchtigt

werden. Der Höchstwert gemäß DIN EN 62208 [Ref. 13] beträgt ein Gramm Staub pro Quadratmeter Bodenfläche. Bei IP 6x darf überhaupt kein Staub eindringen.

Die Tests mit Flüssigkeiten werden über Tropfgeräte, Schwenkrohre und Brausen mit unterschiedlichen Düsendurchmessern durchgeführt. Ab IP x7 kommen Tauchbecken zum Einsatz. Alle Test haben das gleiche Ziel: Das Wasser darf keine schädliche Wirkung haben.

Schutz vor Fremdzugriff

Normalerweise sollten die Rechenzentren im Inneren von Gebäuden vor Eindringlingen gut geschützt sein, weil diese erst alle anderen Hindernisse wie Tore, Rezeption, Kameras und aufmerksame Mitarbeiter überwinden müssen. Nichtsdestotrotz ist es wichtig, dass ein Raum, der teure Hardware und wichtige Daten beherbergt, auch einem Einbruchsversuch widersteht. Wie gut er das kann, gibt die Resistance Class (RC) an. Die Norm RC wird in DIN V ENV 16 27 ff [Ref. 14] definiert. Der Werkzeugangriff erfolgt analog zu DIN EN 1630/ 2011-09 [Ref. 15] und nutzt ein sechsstufiges Klassifizierungssystem.

Unterschieden wird nach den Fähigkeiten des Täters und seiner Ausstattung mit Hilfsmitteln. Die Bandbreite reicht von einem unerfahrenen Täter/Vandalismus ohne Werkzeug bis zu einem erfahrenen, sehr motivierten Täter, dem eine ganze Reihe leistungsfähiger Elektrowerkzeugen zur Verfügung stehen. Dazu gibt es jeweils Zeitvorgaben, in denen der Prüfling dem Angriff standhalten muss, um den Test zu bestehen.

Für die Kategorie RC 1 weisen die Bauteile einen begrenzten bis geringen Grundschutz gegen Aufbruchsversuche mit körperlicher Gewalt wie Gegentreten, Gegenspringen, Schulterwurf, Hochschieben und Herausreißen auf. Zudem wird ein maximal drei Minuten langer zerstörungsfreier Manipulationstest mit Kleinwerkzeugen zur Demontage von außen abschraubbarer Komponenten durchgeführt. Die Dauer des Angriffs gilt pro Angriffspunkt. Wird beispielsweise ein kompletter Sicherheitssafe geprüft, gibt es mehrere Angriffspunkte wie Scharnierseite Tür, Bandseite Tür und Kabeleinführung. Die Gesamtzeit ergibt sich aus der Summe aller Angriffspunkte. Die übrigen Kategorien führt die nachfolgende tabellarische Übersicht auf.

Code	Dauer	Erfahrung	Beschreibung / Hilfsmittel
RC 2	3 min	Gelegenheits-täter	einfache Werkzeuge: Schraubendreher, Zange und Keil
RC 3	5 min	gewohnt vorgehender Täter	zusätzlich: zweiter Schraubendreher und einem Stemmeisen
RC 4	10 min	erfahrener Täter	zusätzlich: Säge- und Schlagwerkzeugen, z. B. Schlagaxt, Stemmeisen, Hammer und Meißel, sowie einer Akku-Bohrmaschine
RC 5/ RC6	10 min	erfahrener Täter	zusätzlich: weiteres Werkzeug an der Hand, bis hin zu Bohrmaschine, Stich- oder Säbelsäge und Winkelschleifer mit einem max. Scheibendurchmesser von 250 mm.

Tabelle 3: RC-Systematik – Schutz vor Fremdzugriff

EMV-Schutz

Elektromagnetische Felder sind eine unvermeidliche Folge von fließendem Strom. Die abgestrahlte Energie, EMV (elektromagnetische Verträglichkeit)-Strahlung genannt, ist unerwünscht, wenn nicht sogar schädlich. Starke Felder können sich negativ auf andere elektronische Geräte auswirken und Informationen für unerwünschte Mithörer empfangbar machen.

IT-Sicherheitsräume schützen – wenn sie korrekt geplant und umgesetzt sind – Hardware und Informationen vor den negativen Folgen von EMV-Strahlung. Die EMV beschreibt, wie Geräte vor Störstrahlungen aus anderen Quellen geschützt werden können. Hierzu sind spezielle Maßnahmen erforderlich.

Ein Sicherheitsraum bietet im Grundzustand noch keinen durchgängig definierten Schutz. Es geht bei EMV aber auch darum, Abstrahlungen zu verhindern, aus denen Unbefugte wertvolle und sensible Informationen abgreifen können. Die IT-Sicherheitsräume von Rittal enthalten bereits ab Werk einen EMV-Grundschutz, der durch weitere konstruktive Maßnahmen noch erhöht werden kann. Die nachfolgende Tabelle gibt einen Überblick über die relevanten Normen:

Anwendungsbereich	Störaussendung	Störfestigkeit
Informationstechnische Einrichtungen	EN 55022 (P)	EN 55024 (P)
Wohnbereich	EN 61000-6-3 (FG)	EN 61000-6-1 (FG)
Industrieanlagen	EN 61000-6-4 (FG)	EN 61000-6-2 (FG)
Signalübertragung auf Niederspannungsnetzen	EN 50065-1 (P)	EN 61000-6-2 (FG)
Beleuchtungseinrichtungen	EN 55015 (P)	EN 61000-6-2 (FG)

Tabelle 4: EMV Produkt-, Produktfamilien- und Fachgrundnormen

Die Normung zur EMV legt für Produkte und Umgebungsbereiche Grenzwerte der Störaussendung in definierten Frequenz – und Feldstärkebereichen fest, zum Beispiel in DIN EN 55022 (VDE 0878-22):2011-12 [Ref. 16].

Das System aus diesen Grenzwerten und den in DIN EN 55024 (VDE 0878-24):2011-09 [Ref. 17] beschriebenen abgestuften Anforderungen zur Störfestigkeit von Informationstechnischen Einrichtungen stellt im alltäglichen Betrieb die elektromagnetische Verträglichkeit zwischen Geräten aller Arten und den IT Einrichtungen sicher.

Anwendungsbereich / Prüfung	**Norm**
Absorberräume, Teil 1: Schirm-dämpfungsmessung	EN 50147-1 : 1996
IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures	IEEE Std 299-1997

Tabelle 5: EMV Prüfnormen (für Raumschirmung)

Die EMV-Eigenschaften von IT-Sicherheitsräumen müssen zwei Aufgaben erfüllen. Sie sollen zum einen verhindern, dass IT-Einrichtungen gewollt oder ungewollt durch eingestrahlte elektromagnetischer Felder behindert werden, zum anderen müssen sie die Abstrahlung sicherheitsrelevanter Informationen aus der IT-Einrichtung vermindern. Die Schirmwirkung der Gerätegehäuse und der Schränke, in denen die Geräte untergebracht sind, kann durch zusätzliche Raumschirmung noch wesentlich erhöht werden. Normative Vorgaben gibt es dazu allerdings keine.

Abbildung 4: EMV-Prüfung

Auch hier wäre der Idealfall eine schlitzfreie, elektrisch leitende Hülle, die weder Signale hinein noch heraus lässt. Das ist in der Praxis allerdings unmöglich. Denn IT-Sicherheitsräume und Safe-Lösungen sind aus Wandsegmenten aus Stahlblech zusammengesetzt, die über flächige, leitende Verbindungen eine schlitzfreie, leitende Grundhülle ermöglichen. Öffnungen oder Fugen müssen mit geeigneten Mitteln geschirmt werden, was insbesondere bei Zugangstüren einen erheblichen konstruktiven Aufwand bedingt. Wie gut die Schirmung ausfällt, bestimmen die Größen der notwendigen Öffnungen und die Güte der dort eingesetzten Schirmungselemente sowie deren Verbindung zur Grundhülle. Dabei lautet ein Grundsatz: Je größer (rechteckige Öffnungen/Fugen: längste Seite; runde Öffnung: Durchmesser) die schlecht geschirmte Öffnung, umso eher fällt die Schirmwirkung im betrachteten Frequenzbereich zu niedrigeren Werten ab.

Je höher die Frequenz des auftreffenden elektromagnetischen Felds ist, desto negativer wirken sich Öffnungen in der Hülle aus. Daher sind einige Punkte, wie die Verwendung spezieller Dichtungen und Kabeldurchführungen, oder der Einsatz von Filter-Steckverbindern zu beachten. Grundsätzlich bestimmt dabei die konstruktive Ausführung des Dichtungssystems weitgehend die Schirmdämpfung. Je mehr Befestigungspunkte für Wände und Scharnier- und Verschlussdruckpunkte für Türen vorhanden sind und je gleichmäßiger damit der Anpressdruck und der Kontakt (niedrige Impedanz) von Hülle und Tür/Deckel entlang den Dichtungen sind, umso näher ist das Ideal. Leitende Spezialdichtungen aus Metallgewebe auf Schaumstoffkörper als Kombinationsdichtungen für EMV und IP-Schutzart erreichen hohe Schirmdämpfungswerte im Frequenzbereich bis 1 GHz oder darüber hinaus. Sie verbinden die metallisch blanken Innenflächen von Türen und abnehmbaren Wänden, Dach- und Bodenblechen mit den metallisch blanken Dichtkanten des Gehäusekörpers oder -gerüsts

Mit vertretbaren Maßnahmen können für Sicherheitsräume Schirmdämpfungswerte von bis zu 60 dB im Frequenzbereich von 30 MHz bis 3 (10) GHz realisiert werden. Schirmdämpfungswerte oberhalb 60 dB erfordern im relevanten Frequenzbereich einen außerordentlichen konstruktiven Aufwand. Derart hohe Schirmwirkungen sind in der Regel nur bei IT-Sicherheitsräumen für Behörden (Militär, Polizei, Nachrichtendienste, Ministerien etc.) zu finden. Die Sicherheitsräume von Rittal erfüllen die Basisanforderungen der EMV und lassen sich mit vertretbarem Aufwand auf einen erhöhten EMV-Schutz aufwerten.

Weitergehende Informationen zu der EMV-Thematik finden sich in einem separaten Whitepaper des Systemanbieters für IT-Infrastrukturen [Ref. 18].

Modulare Sicherheitsräume und Safe-Lösungen

Im Prinzip kann jeder Raum als Serverraum genutzt oder zum Rechenzentrum umgebaut werden. Dabei sind unterschiedliche Aspekte der IT-Infrastruktur zu beachten. Ohne Kühlung kommt zum Beispiel die Wärmeabfuhr der IT-Geräte im Sommer schnell an ihre Grenzen, der Zutritt kann häufig nicht kontrolliert werden und nicht selten stehen die Geräte auf dem Boden, wo sie bei einem Wasserschaden beschädigt werden. Falls kein geeigneter Raum zur Verfügung steht, sind modulare IT-Sicherheitsräume oder IT-Sicherheits-Safes eine sinnvolle Alternative. Ein Sicherheitsraum wird in einen bestehenden Raum eingebaut und rüstet alle Aspekte nach, die ein zuverlässiges Rechenzentrum ausmachen. Er schützt vor physischen Gefahren und bietet systemgeprüften Schutz für die IT.

Micro Data Center

Eine Nummer kleiner aber nicht minder professionell schützen IT-Sicherheits-Safes vor physischen Gefahren. Das sind voll ausgestattete Kompaktrechenzentren, die an ihrem Standort lediglich mit den entsprechenden Versorgungsleitungen verbunden werden müssen. Rittal hat neben dem Micro Data Center (MDC), Level A für Grundschutzanforderungen auch den Micro Data Center Level B und den Micro Data Center Level E im Angebot.

Abbildung 5: Produktportfolio Micro Data Center Level E, Level B, Level A

Das MDC Level A ist ein Komplettsystem mit eingebauter Kühlung und einem Zwei-Türen-System für einfache Installation und Verwaltung. Es ist als Kleinst-rechenzentrum für den Mittelstand zum Schutz für Server- und Storage-Anwendungen sowie für geschäftskritische Daten konzipiert und bringt im Inneren bis zu 15 19“ Höheneinheiten unter.

Das MDC Level B ist bereits standardmäßig mit dem Rittal TS IT Rahmengestell inklusive vorderer und hinterer 19“-Ebene ausgestattet und in zwei unterschiedlichen Höhen (42 oder 47 Höheneinheiten) sowie mit zwei unterschiedlichen Innentiefen (1.000 mm und 1.200 mm) erhältlich. Der Safe bietet Brandschutz über 90 Minuten und wurde gemäß der EN 1363 getestet. Er bietet Einbruchschutz RC 2, Schutzart IP 56 und wurde durch die Materialprüfanstalt für Bauwesen (MPA) in Braunschweig auf Rauchdichtigkeit in Anlehnung an die EN 1634 getestet.

Als Safe für hohe Sicherheitsanforderungen bietet der MDC Level E Brandschutz über 90 Minuten nach DIN 4102 (Einhaltung der Grenzwerte der EN 1047-2, ΛT 50 K, rel. Luftfeuchte < 85% über 30 Minuten), die Schutzart IP 56, Widerstandsklasse RC2, optional RC 3 oder WK 4 und schützt zuverlässig vor Rauchgasen.

Eigenschaft MDC	**Level E**	**Level B**	**Level A**
Nutzbare HE	42/47	42/47	15
Nutzbare Innentiefe mm	1.000/1.200	1.000/1.200	1.000
Brandschutz	Feuerwiderstandsklasse F 90 (DIN 4102 Teil 2) Einhaltung der Grenzwerte ΔT < 50 K, rel. Luftfeuchte < 85 % über 30 Minuten	Feuerwiderstandsklasse EI 90/ F 90 (DIN EN 1363-1: 1999/ in Anlehnung an DIN 4102-2:1997	Feuerwiderstandsklasse F 90 (DIN 4102 Teil 2), Einhaltung der Grenzwerte ΔT < 50 K, rel. Luftfeuchte < 85 % über 10 Minuten
Einbruchschutz	RC 2, optional RC 3 Werkzeugangriff analog DIN EN 1630/2011-09/RC 2 optional WK IV Werkzeugangriff analog DIN V ENV 1630/1999-04	RC 2 Werkzeugangriff analog DIN EN 1630/ 2011-09/RC 2	WK II Werkzeugangriff analog DIN V ENV 1630/1999-04/WK II
Schutzart	IP 56 gemäß EN 60529	IP 56 gemäß EN 60529	IP 55 gemäß EN 60 529
Rauchschutz	in Anlehnung an DIN 18095-2: 1991-034)	in Anlehnung an DIN EN 1634-3: 2005-01	
Modularität	ja	ja	nein
Umhausung bei laufendem Betrieb	ja	nein	nein
Erweiterbarkeit	ja	nein	nein

Tabelle 6: Übersicht der MDC Eigenschaften

Durch modulare und erweiterbar aufgebaute Ausstattungskomponenten lassen sich die Micro Data Center zum voll ausgestatteten Kompaktrechenzentrum komplettieren. Dazu gehören aus dem Rittal Produktportfolio das Überwachungssystem Computer Multi Control III (CMC III), die Brandmelde- und Löschanlage DET-AC III, intelligente Stromverteilung durch die Power Distribution Unit (PDU) bzw. das Stromverteilungssystem Power System Modul (PSM) sowie ein Kühlgerät.

Sicherheitsräume

Ein modularer IT-Sicherheitsraum kann sowohl in einen neuen als auch nachträglich in einen bestehenden Raum eingebaut werden. Er lässt sich praktisch ohne Staub- und Lärmerzeugung montieren, einfach erweitern und sogar an einer anderen Stelle wieder aufbauen. Dabei bietet er häufig besseren Schutz vor Bränden, Wasserschäden und EMV-Strahlung als ein gewöhnlicher Raum. In Abhängigkeit zur benötigten Verfügbarkeit stehen Raumsysteme für den Grundschutz als auch für

Hochverfügbarkeitsansprüche zur Auswahl. Der Hochverfügbarkeitsraum von Rittal bietet höchste physische Sicherheit für Rechenzentren und IT-Systemstandorte. Das System wurde durch die ECB nach ECB•S Regeln zertifiziert und erfüllt die Forderungen der EN 1047-2 uneingeschränkt.

Abbildung 6: Rittal IT-Sicherheitsraum

IT-Sicherheitsräume werden in der Regel mit Sicherheitstürsystemen ausgestattet. Je nach Anforderung können diese in ihrer Ausführung stark variieren. Um gegen Vandalismus und Einbruchsversuche gerüstet zu sein, sollte das Sicherheitstürsystem ein hoch feuerbeständiges, mehrwandiges Stahltürblatt mit umlaufender Türzarge und umlaufendem Feuer- und Dichtungsfalz aufweisen. Im Türfalzbereich sind unter anderem Hohlkörper-Gummidichtungen und expandierende Hochtemperaturdichtungen angebracht. Einen wesentlichen Bestandteil stellt die Verschlusstechnik dar. Sie soll zum einen zuverlässig vor fremdem Zugriff schützen, und zum anderen bei Notfällen eingeschlossene Personen schnell aus dem Gefahrenbereich ins Freie entlassen. Dazu sind Schlösser mit einem Hochsicherheitsriegelwerk, Riegelbolzen und Panikentriegelung ausgestattet. Das Hochsicherheitsriegelwerk verfügt über eine Aufnahme der Schlosseinheiten. Personen, die sich im Alarmfall (bei geschlossener Tür) noch im Raum befinden, können diesen durch die standardisierte Panikentriegelung jederzeit verlassen. Automatiken um die Tür zu schließen, sollten sich variabel in ihrer Verzögerung einstellen lassen.

Grundschutzraum GSR	Grundschutzraum Plus GSR Plus	Hochverfügbarkeitsraum HVR
		
Grundschutz Räume für IT-Infrastrukturen, Schaltzentralen	**Erweiterter Grundschutz** Rechenzentren mit mittlerem Sicherheitsbedarf, Backup-Rechenzentren	**Hochverfügbarkeitsschutz** Haupt-Rechenzentren mit hohen Sicherheits-anforderungen, Hochverfügbarkeitslösung

Tabelle 7: Produktportfolio der Rittal Sicherheitsräume

Fast immer ist es notwendig, den Türstatus des Eingangs zu überwachen. Professionelle Sicherheitsräume stellen dafür ein Türüberwachungssystem zur Verfügung, das potenzialfreie Kontakte über einen VdS-konformen Schnittstellenverteiler herausführt. So kann der Türstatus mit dem zentralen Gebäudemanagement gekoppelt werden. Geht es nur darum, den Zustand der Tür abzufragen, reicht ein Türmeldekontakt. Auch die Riegel selbst können bei professionellen Sicherheitsräumen überwacht werden, beispielsweise um sie auf eine Einbruchmeldeanlage oder Sicherheitszentrale aufzuschalten. Türen in einem systemgeprüften Sicherheitsraum gewährleisten optimalen Schutz gegen Feuer, Wasser, Einbruch und andere physische Gefahren.

Ideal wäre ein Schutzraum, wenn er keine Öffnungen bräuchte. Das ist allerdings aufgrund der Tür nicht möglich. Doch auch die IT-Infrastruktur in Sicherheitsraum und Sicherheits-Safe muss mit Kühlung, Strom und Netzwerk verbunden werden. Dafür sind Kabelschottsysteme zuständig, deren Eigenschaften die Schutzwirkung des Gesamtsystems nicht schwächen dürfen.

Es gibt sie in zahlreichen Ausführungen: als Hartschottsysteme, die im Bereich der Kabeleinführung eine höhere Manipulationssicherheit bieten, und als ein mit flexiblem Dichtungsmaterial gefülltes Weichschottsystem, das meist als Standard mit den Sicherheitsräumen ausgeliefert wird. Ein abweichender Formfaktor sind mit Dichtungsmodulen gefüllte Rundschotts, die besonders für bauseitig vorhandene Kabel, Rohre und Kabeltrassen geeignet sind. Für den korrekten Abschluss des gefüllten Schotts sollten immer vom Hersteller autorisierte Spezialisten herangezogen werden. Nur so ist die volle Schutzwirkung des Sicherheitsraums garantiert.

Kriterium	Norm	GSR	HVR
Systemprüfung	Prüfung der nachfolgenden Wertigkeiten als Gesamtsystem bzw. -konstruktion	Ja	Ja
Brandschutz	ECB·S Zertifizierung gem. EN 1047-2, 50 K Temperaturanstieg und 85 % rel. Luftfeuchtigkeit bis zu 24 Stunden (Nachheizperiode), Beflammungszeit 60 Minuten	Nein	Ja
	50 K Temperaturanstieg und 85 % rel. Luftfeuchtigkeit ohne Nachheizperiode, Beflammungszeit 30 Minuten	Optional	-
	F 120 nach DIN 4102	Nein	Ja
	F 90 nach DIN 4102	Ja	-
Korrosive Brandgase	Rauchgasdichtigkeit in Anlehnung an DIN 18 095	Ja	Ja
Trümmerlasten	Stoßprüfung zu 200 kg	Ja	Ja
Wasser	IP x6 nach EN 60 529	Ja	Ja
	Schutz gegen stehendes Wasser	-	Ja
Staub	IP 5x nach EN 60 529	Ja	Ja
Fremdzugriff	WK IV nach DIN V ENV 1630, nur Türsystem	-	Ja
	WK III nach DIN V ENV 1630, oder DIN V 18 103 (ET2)	Optional	Ja
	WK II nach DIN V ENV 1630	Ja	-
EMV	Schutz gegen hochfrequente Ein- und Ausstrahlungen	Optional	Optional

Tabelle 8: Übersicht der Sicherheitsraum-Eigenschaften von Rittal

IT-Equipment im Sicherheitsraum braucht Kühlung. Dafür sind verschiedene Verfahren verfügbar, einige verlangen die Zufuhr von Frischluft durch eine oder mehrere entsprechende Öffnungen im Raum. Brennt es in der Umgebung des Sicherheitsraumes, muss eine solche Öffnung verschlossen werden, damit kein Rauch von außen in den Sicherheitsraum gelangen kann. Das passiert, indem die Öffnung(en) durch Klappen oder Schieber aus hochfeuerbeständigen Materialien das Rauchgas blockieren.

Der Antrieb solcher Klimaschieber oder Brandschutzklappen muss im Brandfall unabhängig von der Stromversorgung sein. Je nach Größe, Lage und Form der Öffnung sind verschiedene Antriebsarten realisierbar. So kann für einen Klimaschieber im Normalfall für die Be- und Entlüftung ein elektrisches Antriebsystem genutzt werden. Im Brandfall muss die Klappe die Öffnung durch ein

rein mechanisches Konzept, beispielsweise eine Feder oder einen Magneten, verschließen.

Ein verwandtes Bauelement ist der Überdruckschieber. Wird eine Löschanlage mit Inertgas oder einem chemischen Löschmittel aktiviert, muss der entstehende Überdruck abgeleitet werden. Das erledigt ein entsprechender, hochfeuerfester Schieber mit elektropneumatischem Antrieb. Im Alarmfall erfolgt die Druckableitung durch kurzzeitiges Öffnen des Schiebers. Gerade bei rein mechanischen Verschlüssen müssen die Dichtungen optimal auf den Einsatzfall angepasst und hoch effektiv sein. Das erfordert sehr flexible und dicht schließende Dichtungsbänder mit extremen Temperaturfestigkeiten.

Für die Sicherheit im Rechenzentrum und damit auch in Sicherheitsräumen sowie in Sicherheitssafes ist eine technisch hochwertige Brandfrühesterkennung in Verbindung mit hochwertiger Löschtechnik unverzichtbar. Um möglichst schnell eingreifen zu können, ist eine Brandfrüherkennungsanlage notwendig, die schon geringste Rauchentwicklungen erkennt. Dabei werden hauptsächlich Streulicht-Detektoren eingesetzt. Das Maß für die Rauchdichte ist die Streuung des Lichtstrahls an den vorhandenen Rauchpartikeln. Streulicht-Detektoren funktionieren sowohl als punktförmige Melder an der Decke als auch in hochsensiblen Rauchansaugsystemen.

Aufgrund der gezielten Luftführung in einem Rechenzentrum gelangt entstehender Rauch erst sehr spät oder gar nicht bis zu den Meldern, die an der Decke platziert sind. Um eine frühzeitige Erkennung sicher zu stellen, ist daher ein aktives Rauchansaugsystem unumgänglich.

Die Ansteuerung einer Aktivlöschung geschieht in der Regel über eine Zweimelder- oder Zweigruppenabhängigkeit, so dass Fehlauslösungen möglichst verhindert werden. Für die Löschung werden zumeist Inertgase oder ein chemisches Löschgas eingesetzt. Löschschaum und Pulverlöschsysteme können dagegen nicht verwendet werden, weil sie die IT-Systeme und deren Netzteile beschädigen würden. Eine Brandvermeidung kann durch den Einsatz einer Sauerstoffreduktionsanlage erzielt werden. Sie reduziert den Sauerstoff im Rechenzentrum dabei so weit, dass die Entstehung eines Brandes nicht möglich ist.

Literatur

Ref. 1 BSI Grundschutzkatalog, Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Ref. 2 Studie „Kritische IT-Systeme im Mittelstand“, Techconsult im Auftrag von HP Deutschland, 2013, Link: http://www.softexpress.de/Media/seite_hardware/ProactiveCare/HP_Ergebnispr%C3%A4sentation_Kritische_IT_Mittelstand_Handout_2013.pdf

Ref. 3 EMC-Studie, 2014, Link: http://germany.emc.com/about/news/press/2014/20141209-01.htm

Ref. 4 ISO/IEC 17065, Link: http://www.iso.org/iso/catalogue_detail.htm?csnumber=46568

Ref. 5 BSI Maßnahme 1.6 „Einhaltung von Brandschutzvorschriften“, Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01006.html

Ref. 6 DIN 4102 „Brandverhalten von Baustoffen und Bauteilen“

Ref. 7 EN 1047-2, Link: http://www.beuth.de/langanzeige/DIN+EN+1047-2/113261910.html

Ref. 8 EN 1363 „Feuerwiderstandsprüfungen – Teil 1: Allgemeine Anforderungen“

Ref. 9 DIN 18095 „Türen; Rauchschutztüren; Begriffe und Anforderungen“

Ref. 10 EN1634 „Prüfungen zum Feuerwiderstand und zur Rauchdichte für Feuer- und Rauchschutzabschlüsse, Fenster und Beschläge“

Ref. 11 EN 50102 „Schutzarten durch Gehäuse für elektrische Betriebsmittel (Ausrüstung) gegen äußere mechanische Beanspruchungen (IK-Code)“

Ref. 12 EN 60529 „Schutzarten durch Gehäuse (IP-Code)“

Ref. 13 DIN EN 62208 „Leergehäuse für Niederspannungs-Schaltgerätekombinationen - Allgemeine Anforderungen„

Ref. 14 DIN EN 1627 „Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung“

Ref. 15 DIN EN 1630 „Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit gegen manuelle Einbruchversuche“

Ref. 16 DIN EN 55022 „Einrichtungen der Informationstechnik - Funkstöreigenschaften - Grenzwerte und Messverfahren“

Ref. 17 DIN EN 55024 „Einrichtungen der Informationstechnik - Störfestigkeitseigenschaften - Grenzwerte und Prüfverfahren“

Ref. 18 Rittal – „Whitepaper – EMV-Schutz bei Sicherheitsräumen“

Abkürzungsverzeichnis

BSI	Bundesamtes für Sicherheit in der Informationstechnik
CMC	Computer Multi Control (Rittal Monitoringsystem für die IT Infrastruktur)
DAKKS	Deutsche Akkreditierungsstelle
DETA-AC	Rittal Brandmelde- und Löschanlage
DIN	Deutsches Institut für Normung
ECB	European Certification Body GmbH
EMV	elektromagnetische Verträglichkeit
EN	Europäische Norm
ESSA	European Security Systems Association (ESSA) e.V.
GSR	Grundschutzraum
HE	Höheneinheit = 44,45 mm
HVR	Hochverfügbarkeitsraum
IEC	International Electrotechnical Commission
IK-Code	Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)
IP-Code	Schutzarten durch Gehäuse
ISO	International Organization for Standardization
IT	Informationstechnik
LBO	Landesbauordnung
MDC	Micro Data Center

MBO	Musterbauordnung
MLAR	Muster-Leitungsanlagen-Richtlinie über brandschutztechnische Anforderungen an Leitungsanlagen
NEMA	National Electrical Manufacturers Association
NOAEL	NOAEL-Wert (No Observed Adverse Effect Level)
PDU	Rittal Power Distribution Unit
PSM	Rittal Power System Modul (modulare PDU)
RC	Resistance Class
RZ	Rechenzentrum
TÜV	Technischer Überwachungsverein
UL	Underwriters Laboratories Inc., Zertifizierung in den USA
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VDMA	Verband Deutscher Maschinen- und Anlagenbau
VdS	VdS Schadenverhütung GmbH, http://vds.de
WK	Widerstandsklasse (ersetzt durch RC-Code)

Rittal – Das System.

Schneller – besser – überall.

- Schaltschränke
- Stromverteilung
- Klimatisierung
- IT-Infrastruktur
- Software & Service

RITTAL GmbH & Co. KG
Auf dem Stützelberg · D-35726 Herborn
Phone + 49(0)2772 505-0 · Fax + 49(0)2772 505-2319
E-Mail: info@rittal.de · www.rittal.de · www.rimatrix5.de