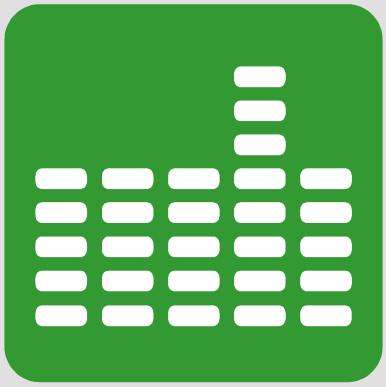


managedhosting.de
Whitepaper

managedhosting.de

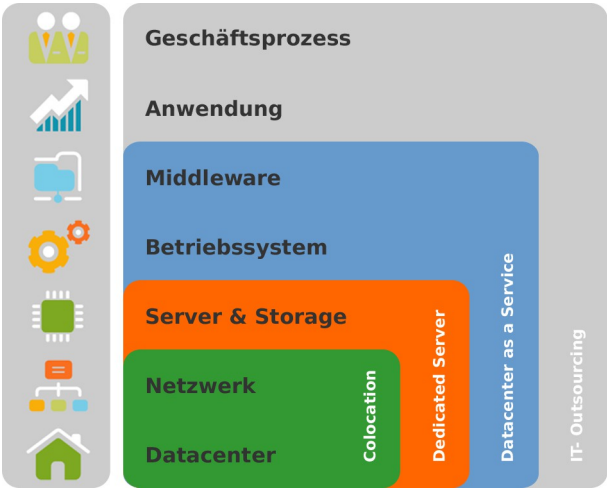
Whitepaper

Datacenter und IT- Sicherheit

Version 1.3

Hochverfügbarkeit

Die ständige Verfügbarkeit einer Applikation ist ungleich schwieriger zu realisieren, als die einer technischen Ressource, wie z. Bsp. eines Servers.



Die Verfügbarkeit einer Applikation hängt letztendlich vom reibungslosen Zusammenspiel etlicher Komponenten ab:

- Stromversorgung und Klimatisierung,
- Netzwerkinfrastruktur & Internetanbindung,
- Server und Storagesysteme,
- Betriebssystem,
- und Middleware wie Datenbanken, Webserver

Fällt nur ein einziger Baustein durch Überlastung oder Defekt aus, führt das sofort auch zum Ausfall der Applikation.

managedhosting.de hat sich dieser Herausforderung gestellt und bietet Hochverfügbarkeitslösungen zu einem bisher nicht erreichbaren Preis- Leistungsverhältnis an. Möglich wird dies durch den konsequenten Einsatz moderner Virtualisierungstechnologien in Verbindung mit einer Enterprise IT- Infrastruktur.

Grundlage jeder IT- Infrastruktur ist ein Datacenter welches die heutigen Anforderungen erfüllen kann.

Bei managedhosting.de setzen wir dabei auf den höchstmöglichen Standard: Alle Server befinden sich in Tier III und Tier IV[1] - zertifizierten Rechenzentren namhafter Betreiber.

- Vollständig redundante Stromversorgung
- Brandfrüherkennung (VESDA) & Gaslöschung
- Redundante Kabelführungen aller Medien
- Alle Server und Komponenten sind mit redundanten Netzteilen ausgestattet oder mehrfach im Parallebetrieb vorhanden.
- Alle Steckdosen sind fernschalt-, mess- und überwachbar

Die garantierte mittlere Verfügbarkeit der Datacenter-Infrastruktur beträgt 99,982% - 99,995% pro Jahr. Es sind jedoch über einen Zeitraum von mehr als 2 Jahren keine Ausfälle durch Störungen oder Wartungsarbeiten zu verzeichnen gewesen.

IT- Sicherheit

IT- Sicherheit ist ein immer aktuelles, komplexes und dynamisches Thema mit vielen Spezialbereichen, die alle IT- Komponenten betreffen. Sich laufend verändernde Rahmenbedingungen verlangen zusätzlich eine kontinuierliche Anpassung und Optimierung. Hinzu kommen juristische Fragestellungen und zu berücksichtigende Standards.

Gerade kleine und mittelständische Unternehmen fühlen sich aufgrund objektiv beschränkter Ressourcen in Sachen IT- Sicherheit oft überfordert. Die Nutzung der Datacenter- Ressourcen von managedhosting.de ist der richtige Weg, diese Lücke zu schliessen.

Nur ganzheitliche, präventive Sicherheitslösungen verbunden mit einer nach innen und aussen gerichteten, hochperformanten Netzwerkinfrastruktur führen zu optimaler IT- Funktionssicherheit und decken sowohl logische als auch physikalische Aspekte ab. So verfügen unsere Datacenter über eine Vielzahl technischer Vorkehrungen und fest etablierter Prozesse, um Ausfällen oder Einschränkungen auf Server-, System- und Netzwerkebenen wirksam vorzubeugen.

Betrieb

Neben einem proaktiven und kontinuierlichen Performance-, Verfügbarkeits- und Patchmanagement gehört die mehrfach redundante, also funktional doppelt vorhandene, Bereitstellung der Systemarchitekturen zum Standard. Alle IT- Komponenten, Leistungsparameter und Vorgänge werden rund um die Uhr überwacht und protokolliert.

Aus diesen Daten werden zusätzlich Prognosen und Trends ermittelt und die Ergebnisse individuell zur Verfügung gestellt.

Täglich inkrementelle und wöchentlich komplette Backups gewährleisten darüber hinaus einen optimalen Schutz vor Datenverlusten.

Um die Wiederherstellbarkeit der Daten auch im Katastrophenfall sicherzustellen, werden die gesicherten Daten dabei auf Kundenwunsch auch redundant an mehreren getrennten Standorten aufbewahrt.

Alle Details um die Aspekte der logischen Sicherheit und kundenindividuellen Spezifikationen werden in den entsprechenden Leistungsbeschreibungen und Service Level Agreements umfassend dargestellt.

Datacenter

Zu den besonders wichtigen Bestandteilen einer effektiven Sicherheitsstrategie gehört auch die gesamte Gebäudetechnik in ihren unterschiedlichen Ausführungen.

Hierzu gehören Sicherheitsvorkehrungen gegen Elementarrisiken, unauthorisierten Zutritt oder sonstige Notfallsituationen.

Unsere Datacenter sind konsequent gegen alle potenziellen äusseren Einflussfaktoren und Gefahrenquellen abgeschirmt. Eine lückenlose Aussenhaut- und Innenraumüberwachung registriert jeden ungewöhnlichen Vorfall, alarmiert und leitet automatisch wirkungsvolle Gegenmassnahmen ein.

Brandfrüherkennung / Brandschutz

Eine grosse Bedrohung für ein Rechenzentrum entsteht durch ein mögliches Feuer. Dabei ist ein sich ausbreitendes Feuer, das im Notfall durch ein System von Gaslöschanlagen unmittelbar und automatisch bekämpft wird, nicht die grösste Gefahr.

1 http://en.wikipedia.org/wiki/Data_center

Klimatisierung

Bereits die übermässige Erwärmung der vorhandenen elektronischen Bauteile kann grossen Schaden anrichten. Die betroffenen Komponenten fallen dann nicht sofort aus, sondern altern überproportional schnell und sind schwieriger zu kontrollieren. Redundante Klimaanlagen sorgen deshalb für eine jederzeit konstante Temperatur und Luftfeuchtigkeit.

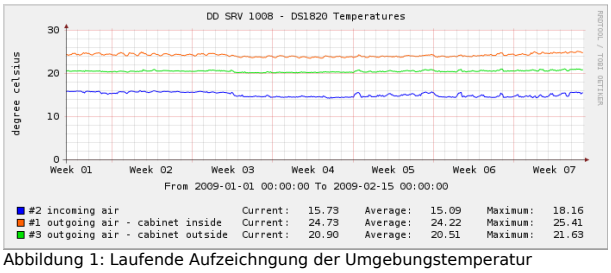


Abbildung 1: Laufende Aufzeichngung der Umgebungstemperatur

Die technischen Grenzwerte der eingesetzten Systeme werden dabei weit unterschritten, so dass alle IT- Systeme unter optimalen Betriebsbedingungen eingesetzt werden können.

Wasser

Wasser stellt im Zusammenhang mit der IT ein besonderes Risikopotential dar. So können z. Bsp. kleine Lecks in der Klimaanlage irreparable Folgeschäden großer Teile der Infrastruktur auslösen. Sie werden oft nicht direkt bemerkt und können schwer lokalisiert und bekämpft werden.

Wasserdetektoren mit Sensoren auch im Doppelboden identifizieren eventuelle Lecks sofort und vermeiden so eine mögliche Beschädigung.

Zutrittskontrolle

Eine Absicherung des Datacenters gegen Brände, Hitze und Wasser ist aber noch nicht ausreichend. Gefahr geht auch von mutwilliger Sabotage, Einbruch und Diebstahl oder von unbeabsichtigter Beschädigung der IT- Infrastruktur durch unbefugte Personen aus.

Der Zugang zum Datacenter und zu sämtlichen sensiblen Bereichen ist ausschliesslich auf autorisiertes Fachpersonal beschränkt. Befugte werden sowohl vom Sicherheitspersonal als auch durch mehrere separate Kontrollsysteme eindeutig identifiziert.

Der Zutritt zu operativen Bereichen führt über Vereinzelungszellen mit speziellen Kartenlesern und Bewegungs-, Infrarot- und Lichtsensoren. Ein unbefugter Zutritt wird dadurch praktisch unmöglich.

Stromversorgung

Alle Systeme, die zur Sicherheit oder als Dienstleistung in Rechenzentren betrieben werden, sind abhängig von einer stabilen und gleichmäßigen Stromversorgung. Die Stromversorgung des Datacenters ist daher völlig autark. Ein dreistufiges System aus direkter Anbindung zur Trafostation, batteriegestützten Notstromanlagen und Dieselgeneratoren ermöglicht einen zuverlässigen Schutz gegen Spannungsschwankungen und Stromausfälle.

Alarmierung

Auch mit einer durchdachten Sicherheitsstrategie kann man den Notfall nicht ausschliessen. Im Falle eines Falles müssen die Prozesse dann perfekt aufeinander abgestimmt sein.

Alle ansässigen Feuerwehr- und Sicherheitskräfte werden in kontinuierlichen Abständen in das Datacenter eingewiesen. So ist ein schnellstmöglicher Eingriff bei einem Alarm garantiert und Notfallprozesse sind bereits im Vorfeld abgestimmt und koordiniert.

Internetanbindung

Die Anbindung eines Datacenters muss äusserst hohen Ansprüchen hinsichtlich Geschwindigkeit, Transfervolumen und Sicherheit gerecht werden.

Deshalb realisieren wir die Verbindungen zum Internet und zu den Hochgeschwindigkeitsnetzen weiterer Carrier und Peering- Partner redundant direkt im Datacenter. Als Mitglied des RIPE-NCC verfügen wir über einen eigenen IP-Adressbereich und betreiben mehrere Autonome Systeme mit direkten Anbindungen an Carrier wie Eu-Networks, Level3, BT oder envia TEL. Als Mitglied des BCIX unterhalten wir zusätzlich direkte Netzkopplungen mit mehr als 40 Anbietern.

Selbstverständlich sind auch im Netzwerkbereich alle Komponenten mehrfach redundant ausgelegt.

Personal

Die Anforderungen an das Personal in einem Rechenzentrum sind beachtlich. Neben einer hohen technischen Qualifikation zur Aufrechterhaltung der Einsatzbereitschaft aller operativen Systeme, erfordert die Aufgabe besondere Zuverlässigkeit, Sorgfalt und Genauigkeit im täglichen Arbeitsablauf.

In unserem Datacenter besteht die Personalstruktur aus einem System aus Leitstand, mobilem Kontrolldienst, Alarmverfolgung und einer Notrufzentrale.

Ein eventueller Alarm wird sofort der örtlichen Polizei und einem Alarmverfolger gemeldet, der unverzüglich die notwendigen Maßnahmen einleitet. Störungen werden rund im die Uhr an die Notrufzentrale weitergeleitet.

Datenschutz und Datensicherheit

Die managedhosting.de GmbH hat ihre Rechenzentrumsdienstleistungen gemäß ISO / IEC 27001 vom TÜV InterCert Saar vollständig zertifizieren lassen. Damit sind wir einer der ersten VMware vCloud Powered Service Provider in Deutschland, der diese Zertifizierung für seine VMware basierte Cloud-Infrastruktur erhalten hat.

TÜV InterCert SAAR
ISO 27001:2005
Certificate No.:13-I-0000002-TIC

Unseren Kunden garantiert die Zertifizierung größtmögliche Sicherheitsvorkehrungen und höchste technische Standards. Gleichzeitig ermöglicht unsere Zertifizierung nach ISO/IEC 27001 unseren Kunden eine kostengünstigere Umsetzung der gesetzlich vorgeschriebenen Mindestanforderungen an das Risikomanagement für den eigenen IT-Betrieb.

Fragen?
Rufen Sie an! Wir beraten Sie gern.

Hotline: 0800 6737877 (kostenfrei)
E-Mail: sales@managedhosting.de
Internet: www.managedhosting.de