GOPAS Solutions

HOST Hamburg

WILLKOMMEN IM RECHENZENTRUM HOST-HAMBURG

Rechenzentrum HOST-Hamburg

Wendenstraße 375-379
20537 Hamburg
Tel.: 040/303 79 59 20
Fax: 040/303 79 59 59
E-Mail: info@hosthamburg.de

BESSERE PERFORMANCE... DURCH ERSTKLASSIGEN SERVICE

- Konzentrieren Sie sich ganz auf Ihre Kernaufgaben, statt auf Aspekte wie Hosting, Infrastruktur und Konnektivitätsprobleme
- Verschaffen Sie sich Business Continuity durch hochverfügbare Datenanbindungen und redundante Systeme
- Netzwerküberwachung und Serververfügbarkeit rund um die Uhr
- Nutzen Sie unsere skalierbaren Lösungen für den schnellen und effizienten Ausbau Ihrer Geschäftsaktivitäten
- Gewinnen Sie wertvolle Bandbreite zum Beispiel durch Auslagerung Ihrer Web-Applikationen

HOUSING UND COLOCATION SERVICES

Im Rechenzentrum HOST-Hamburg der GOPAS Solutions GmbH bieten wir Colocation und Server-Housing für sichere und zuverlässige Services.

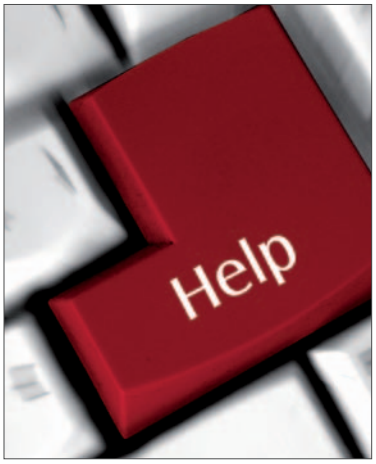
Mit unseren flexiblen Leistungen, vom Housing einzelner Höheneinheiten und kompletter Serverracks bis hin zu der Bereitstellung mehreren Racks in verschiedenen Brandschutzabschnitten, bieten wir ein skalierbares Umfeld für uneingeschränktes Wachstum der IT-Infrastruktur gemäß ihrer Geschäftsentwicklung.

MANAGED HOUSING SERVICES

Im Mittelpunkt einer Managed-Hosting-Lösung steht ein Server oder ein Serversystem mit dem HOST-Hamburg-Support-Paket.

HOST-Hamburg bietet Ihnen passend zu Ihrem Ser-vern, Managed Services für individuelle Systemerweiterungen und den Aufbau professioneller Geschäftslösungen. Ob Sie mehr Sicherheit durch eine Firewall benötigen oder ein komplexes Serversystem aufbauen möchten: Managed Services eröffnen Ihnen vielfältige Möglichkeiten für eine perfekte Systemabstimmung auf Ihr spezifisches Anforderungsprofil. Darüber hinaus stehen Ihnen je nach Bedarf unterschiedlich dimensionierte Backup- und Monitoring-Services zur Verfügung.

RECHENZENTRUM



IT-Verantwortliche müssen die Sicherheit ihrer IT-Anwendungen immer aus verschiedenen Perspektiven betrachten. Dazu gehören die physikalische Sicherheit der IT-Systeme, der Schutz vor Übergriffen (logische Sicherheit) und die technische Sicherheit, die für hohe Verfügbarkeit sorgt.

Sollten diese Aspekte der IT-Sicherheit nicht gewährleistet sein, drohen hohe wirtschaftliche Verluste. Bei der Abwehr möglicher Schäden durch Sicherheitslecks sehen sich die Verantwortlichen mit einer Vielzahl rechtlicher, betriebswirtschaftlicher und organisatorischer Anforderungen konfrontiert. Die Investitionen in IT-Sicherheit sind in den letzten Jahren erheblich gestiegen.

PHYSIKALISCHE / TECHNISCHE SICHERHEIT

Die physikalische Sicherheit eines Rechenzentrums ist definiert über die architektonischen Gegebenheiten, die Sicherung der Außenanlage, Brand- und Wasserschutz, Raucherkennung, eventuell umliegende Gefahrstoffproduktion, das Wachpersonal, die notwendigen technischen, geistigen und biometrischen Identifikationsmerkmale sowie die zugangsrelevanten Prozesse.

Die technische Sicherheit befasst sich mit den Fragen der Energieversorgung, der Klimatisierung und der Netzwerkanbindung.

LOGISCHE SICHERHEIT

Aufbauend auf diesen Aspekten der physikalischen/technischen Sicherheit bezieht sich logische Sicherheit im Rechenzentrum auf den Schutz vor unbefugtem Zugriff auf Daten und Applikationen sowie deren Schutz vor Viren, Trojanern und anderen Schadprogrammen.

Des Weiteren gehören zur logischen Sicherheit neben einem proaktiven und kontinuierlichen Performance-, Verfügbarkeits- und Patchmanagement die mehrfach redundante, also funktional doppelt vorhandenen, Bereitstellung der Systemarchitekturen im Stand-by-Modus.

Alle IT-Komponenten, Leistungsparameter und Vorgänge werden rund um die Uhr durch das 24x7 Operation Center überwacht. Ebenso sind die Datensicherung und die -archivierung Bestandteil der logischen Sicherheit. Tägliche inkrementelle und regelmäßige komplette Backups gewähren einen optimalen Schutz vor Datenverlusten. Um die Wiederherstellbarkeit der Kundendaten sicherzustellen, werden die Backup-Medien separat gelagert.

RISIKOFAKTOR FEUER

Ein großes Risiko für ein Rechenzentrum stellen Brände dar. Ein Brand bedeutet nicht nur den Verlust von Daten und Werten, sondern auch lange Wiederherstellungszeiten und damit eine Nichtverfügbarkeit von geschäftskritischen Applikationen.

Im Rechenzentrum HOST-Hamburg hat die Brandprävention daher einen hohen Stellenwert. Moderne Feuerkontroll- und Überwachungssysteme reagieren bei ersten Anzeichen von Brandgefahr, alarmieren den 24/7-Sicherheitsdienst und leiten automatisch Löschvorgänge mit INERGEN® ein. Löschsysteme, die CO_2 oder Argon als Löschmittel verwenden, bergen das Risiko, Menschen erheblich zu schädigen; bis hin zum Tod.

INERGEN® (ein Gemisch aus Stickstoff, Argon und Kohlenstoffdioxyd) hingegen beschleunigt unter Sauerstoffmangel die Atmung, so dass im Raum befindliche Personen keinen Schaden erleiden. Für Kunden mit einem hohen Sicherheitsbedarf stellen wir Racks in getrennten Brandschutzabschnitten zur Verfügung.

STROMVERSORGUNG

Alle Systeme, die zur Sicherheit oder als Services im Rechenzentrum betrieben werden, sind abhängig von einer stabilen und gleichmäßigen Stromversorgung. Die Stromversorgung des Rechenzentrums ist daher völlig autark. Das dreistufige System von Trafostation, batteriegestützter Notstromanlage (USV) und generatorgestütztem Netzersatzsystem ermöglicht einen zuverlässigen Schutz gegen Spannungsschwankungen (Doppelwandlertechnologie der USV) und Ausfall des Netzstroms.

Unter Volllast kann das Rechenzentrum über 48 Stunden mittels der Notstromeinrichtungen versorgt werden. Regelmäßige Ausfall- und Belastungstest dieser Einrichtungen garantieren die Zuverlässigkeit im Ernstfall. Die Racks werden über separate Phasen (A+B Feed) redundant versorgt.

KLIMATISIERUNG

Bei Einsatz von Hochleistungskomponenten im Server- und Netzwerkbereich entsteht eine unterschiedlich große Hitzeentwicklung. Zu hohe Temperaturen können sich negativ auf die Stabilität und Lebensdauer auswirken und den Energiebedarf steigern. Aus diesem Grund sind im Rechenzentrum HOST-Hamburg redundante Präzisionsklimageräte installiert worden. Durch den Klimaboden werden die Komponenten immer optimal gekühlt (Kaltgang-Warmgang Prinzip). Die Belastungsgrenzwerte der eingesetzten Systeme werden dadurch nie erreicht, so dass alle Komponenten unter optimalen Betriebs- und Umfeldbedingungen laufen.

RISIKOFAKTOR ZUGANG

Eine Absicherung des Rechenzentrums gegen Elementargefahren ist jedoch nicht ausreichend. Gefahr droht auch durch mutwillige Sabotage, Einbruch- und Diebstahl und unbefugtes Betreten des Rechenzentrums und sicherheitsrelevanter Bereiche insbesondre. Deshalb ist der Zugang zum Rechenzentrum nur für einen befugten Personenkreis möglich. Über personengebundene RFID-Transponder und PIN-Codes gelangt autorisiertes Personal unser Kunden in den Sicherheitsbereich. Alle Aktivitäten werden über die engmaschige Videoüberwachung dokumentiert.

SYSTEMMONITORING

Die Überwachung vitaler Netzwerkkomponenten, Server und Dienste wird im zentralen Monitoringsystem von erfahrenen Systemtechnikern sichergestellt. Dabei wird nicht nur auf Ausfälle oder Probleme rechtzeitig reagiert, sondern auch im Rahmen von proaktivem Monitoring (vorbeugende Wartung) diejenigen Werte überwacht, die auf ein kommendes Problem hindeuten. Das Monitoring läuft 24/7 und ist mit einem Eskalationsplan und Notfallplänen gekoppelt, bei dem auch außerhalb der regulären Arbeitszeit Warnungen und Fehlermeldungen an die verantwortlichen Spezialisten gemeldet werden.

KONNEKTIVITÄT

Neben den Sicherheitsaspekten ist eine sichere, schnelle und hochverfügbare Internetanbindung von entscheidender Bedeutung für die Leistungsfähigkeit eines Rechenzentrums.
Das Backbone vom Rechenzentrum HOST-Hamburg ist daher über mehrere Borderrouter mit Lichtwellenleitern an verschiedene, große Provider redundant angebunden. Durch die professionelle und vorausschauende Netzplanung ist es möglich, die Bandbreiten den jeweiligen Anforderungen des Kunden anzupassen.

Die leistungsstarken Anbindungen ermöglichen geringe Latenzzeiten für kritische Applikationen. Latenzzeiten zum DE-CIX und zu anderen Internet-Austauschknoten liegen im Durchschnitt bei 2 ms. Jeder Kunde erhält einen eigenen IP-Adressbereich.

Optional stellen wir Ihnen auch eine redundante Switchinginfrastruktur bzw. Ports von verschiedenen Switches zur Verfügung. Durch den komplett redundanten Aufbau gibt es keinen „Single Point of Failure“ in Ihrer Anbindung.

TECHNISCHER ÜBERBLICK

- Stellflächen in autonomen Brandabschnittbereichen
- Redundantes Klimasystem (N + 1)
- Physikalisch getrennte Zufuhrstrassen
- Performanter und redundanter Backbone
- 24/7-Videoüberwachung mit Aufzeichnung
- 24/7-Zutrittskontrolle
- 24/7-Sicherheitsdienst
- Doppelboden für Versorgung und Klimatisierung
- Brandmeldeanlage mit Rauch- und Handmeldern
- Automatisches INERGEN®-Löschsystem
- Unterbrechungsfreie Stromversorgung USV von MGE UPS®
- Netzersatzanlage (Diesel-Notstromgenerator) von KNURZ®
- Physikalisch getrennte Zufuhrstraßen zu den Brandabschnittbereichen

GOPAS Solutions GmbH
Heimfelder Straße 110
D-21075 Hamburg

Tel.: +49 (0)40/3 03 79 59-0
Fax: +49 (0)40/3 03 79 59-59
www.gopas.de

Amtsgericht Hamburg
HRB 67326
GF: Sebastian Gerber