

Highest Security Level
von osite network GmbH

Rechenzentrum „Wo liegen meine Daten“

Ihre Daten werden in einem deutschen Rechenzentrum mit höchsten Sicherheitsstandards verarbeitet und gespeichert.

Der physikalische Zugang zum Rechenzentrum in Düsseldorf ist nur für autorisierte Personen möglich. Mittels RFID-Lesegeräten und einem biometrischen Handscanner wird die Identität geprüft und nur berechtigten Personen der Zugang zum Rechenzentrum gewährt.

Das Rechenzentrum verfügt über Außen- und Innenwände in Massivbauweise und ist mit selbstschließenden Türen ausgestattet. Die Colocation-Flächen sind mit einem Doppelboden ausgestattet (600-mm- Rechteckplatten, bei einer Höhe von bis zu 500 mm). Der Zugang zum Rechenzentrum erfolgt ebenerdig, sodass ein problemloses Transportieren des Equipments möglich ist.

Das gesamte Rechenzentrum wird rund um die Uhr kameraüberwacht. Die Kameras befinden sich sowohl an allen Zugängen (zum Rechenzentrum), wie auch in den Colocation-Flächen selbst. Sämtliche Aufnahmen werden gespeichert und über einen vordefinierten Zeitraum langzeitarchiviert. Das Rechenzentrum ist mit einer Alarmanlage ausgestattet. Hiermit werden insbesondere sämtliche Eingangsbereiche, sowie besonders kritische Zonen vor unbefugtem Zutritt abgesichert. Weiterhin verfügt das gesamte Rechenzentrum über ein modernes Brandfrüherkennungssystem, welches sowohl oberhalb, wie auch unterhalb des Doppelbodens einen möglichen Brand frühzeitig erkennt und die entsprechenden Maßnahmen einleitet. Beide Systeme sind mit einem örtlichen Sicherheitsdienst verbunden und werden Fernüberwacht.

Highest Security Level

Zur Sicherstellung einer dauerhaften Stromversorgung wurde insbesondere – auch bei der Energieversorgung – Wert auf ein hohes Maß an Verfügbarkeit und Redundanz gelegt. Der Strom wird dauerhaft durch redundante USV-Anlagen gepuffert, wodurch nicht nur vollständige Stromausfälle, sondern auch Stromschwankungen im Netz des Energieversorgers ausgeglichen werden.

Für längere Stromausfälle steht ein Notstromgenerator zur Verfügung und liefert bei Bedarf bis zu 100% des Stroms. Passende Kontrollmechanismen stellen bei Komponenten mit hohen Anlaufströmen, wie etwa Motorlasten und Gleichrichter sicher, dass diese nacheinander gestartet werden. Der Generator hat eine Anlaufzeit von etwa 30 Sekunden. Er wird einmal monatlich auf seine Funktionsfähigkeit überprüft und getestet. Der Kraftstoffvorrat ist für einen dauerhaften Betrieb des Notstromgenerators ausgelegt. Weiterhin ist eine Betankung im laufenden Betrieb möglich, um auch längere Ausfallzeiten überbrücken zu können.

Die Klimatisierung erfolgt über den Doppelboden. Die eingesetzten Klimaanlage sind speziell für den Einsatz in Rechenzentren ausgelegt und sorgen neben einer optimalen Kühlung auch für ein minimales Kondensierungsrisiko. Die Eingangsklimatisierung beträgt $21\text{ °C} \pm 2\text{ °C}$, $50\% \text{ RH} \pm 20$ und unterliegt einer ständigen Überwachung. Die Kühlleistung der einzelnen Klimaanlage beträgt ca. 50 kW.

Backup-Sicherheit

Die Datensicherung Ihres Servers erfolgt nach folgendem Datensicherungskonzept:

Intervall: täglich, ab 23 Uhr

Medium: Komplettsicherung Ihrer Daten auf separater Festplatte, 1 Tag später auf Bandsicherung

Eine zusätzliche Sicherung dieser Daten erfolgt im wöchentlichen Intervall.

osite network GmbH setzt auch in der Backup Strategie auf mehrere Lösungen. So werden z. B. viele Daten in verschiedenen Szenarien und mehrfach am Tag oder in der Woche gesichert. Hier wird darauf geachtet, welche Daten schnellstmöglich bei einem Notfall wiederhergestellt werden müssen.

Sämtliche Daten unserer Kunden werden in den täglichen Backups auf unterschiedlichen Storage-Systemen gespeichert und gesichert. Für Kunden mit speziellen Anforderungen bietet osite network GmbH individuelle Konfigurationsmöglichkeiten an, z. B. monatliche oder jährliche Backups auf Band zu speichern und auslagern zu lassen.

Unser Sicherheitskonzept berücksichtigt dabei die individuellen Wünsche der Kunden, z.B. die VPN Anbindung ganzer Standorte an unser Rechenzentrum. Zusätzlich haben wir Anti-Virus, Spam Filter und Web-Virus Filter im Einsatz, welche das Spektrum potentieller Angriffsmöglichkeiten abbildet und verhindert.

Die Hard-Facts der Sicherheitsfaktoren gelistet:

- ✓ Sehr hoher Verfügbarkeitsstandard (Tier-3) mit Ausfallsicherheit auf allen Ebenen
- ✓ Rechenzentrum in Deutschland nach BDSG
- ✓ DIN ISO 9001:2015 und DIN EN 27001:2013 zertifiziert
- ✓ Überwachung durch Sicherheitsdienst
- ✓ Redundante Gebäudeführung
- ✓ Mehrfache redundante Carrier-Anbindungen
- ✓ Diverse Glasfaser-Leitungen zu Übergabepunkten der wichtigsten Carrier im Connecta Parc
- ✓ 24 Stunden / 7 Tage Videoüberwachung
- ✓ Zutrittskontrolle mittels RFID-Chip und biometrischem Handscanner
- ✓ Antistatischer Doppelboden
- ✓ Brandfrüherkennungsanlage
- ✓ 100 % Ökostrom aus Wasserkraft