

Zwei Standorte für doppelte Sicherheit

Unsere Server stehen in zwei professionellen, nach höchstem Sicherheitsstandard konzipierten Rechenzentren. Beide Rechenzentren sind nach ISO/IEC 27001 zertifiziert.

Die Standorte laufen im so genannten Aktiv-aktiv-Betrieb, d.h. jeweils ein Teil unserer Services (Instanzen) läuft in einem der Rechenzentren, um eine optimale Lastverteilung zu erreichen. Gleichzeitig dient jeder der beiden Standorte für den jeweils anderen als Standby-Rechenzentrum. Aufgrund einer identischen Infrastruktur und Hardware sowie vollständig gespiegelter Daten kann das jeweilige Standby-Rechenzentrum innerhalb weniger Minuten die Aufgaben des anderen Standorts mit übernehmen. Somit ist selbst in einem Worst-Case-Szenario, wie dem physikalischen Verlust eines der Rechenzentren, ein fortlaufender Betrieb gewährleistet.

Beide Standorte sind durch mehrstufige Zutrittskontrollen geschützt und werden rund um die Uhr überwacht. Außerdem sorgen Feuerschutztüren, Feuermelde- und Brandlöscheinrichtungen sowie USV-Systeme (zur unterbrechungsfreien Stromversorgung) dafür, dass die Daten unserer Kunden absolut sicher sind.

- **Performante Internet-Anbindung durch hohe Bandbreiten**
- **Mehrfache Carrier-Redundanz**
- **Hochverfügbare Stromversorgung durch redundante Anbindung an das Versorgungsnetz**
- **Notstrom über USV und Dieselgeneratoren bzw. Brennstoffzellen-Kraftwerk**
- **Drei verschiedene Brandmeldesysteme**
- **Brandschutzwände und -türen**
- **Sicherheitspersonal 365 Tage im Jahr rund um die Uhr vor Ort**
- **Permanente Videoüberwachung**
- **7-stufiges Zugangskontrollsystem**
- **Kontinuierliche Kontrolle von Temperatur und Luftfeuchtigkeit**
- **Einsatz von Präzisionsklimageräten**
- **2-stufige Luftfilterung**



Verfügbarkeit, Vertraulichkeit und Integrität aller Kundendaten haben für uns höchsten Stellenwert.

Hochmodernes Equipment und lückenloser Service

Bei der Auswahl unserer Vertragspartner im Bereich Infrastruktur und Hardware setzen wir ausschließlich auf führende Anbieter markterprobter Lösungen. Im Bereich Network & Security vertrauen wir auf Cisco, im Bereich Storage auf EMC². Unsere Server-Hardware liefert Fujitsu Technology Solutions.¹

Das gesamte System wird rund um die Uhr durch Monitoring-Programme überwacht. Diese prüfen sowohl einzelne Parameter innerhalb der Plattform als auch die Erreichbarkeit von außen. Je nach kritischer Einstufung der auf diese Weise identifizierten Ereignisse wird ein vorab definierter Alarmplan in Gang gesetzt. Um Störungen auch außerhalb der normalen Geschäftszeiten so schnell wie möglich beheben zu können, stehen unsere technischen Mitarbeiter in 24-Stunden-Rufbereitschaft.

Schutz vor Angriffen Dritter

Mehrstufiges Sicherheitssystem

Unsere Serverfarm ist für höchste Performance und Sicherheit ausgelegt. Wir setzen die neueste Sicherheitssoftware ein und haben unsere Plattform so aufgebaut, dass sie optimal gegen Angriffe Dritter geschützt ist, z. B.:

- durch doppelte Firewall-Systeme, vergleichbar mit einer doppelten, dicken Mauer
- durch die Trennung von Frontend und Backend, d. h. es gibt nur eine einzige „Sicherheitstür“, über die ein Zugriff von außen möglich ist. Der dahinter liegende Bereich ist komplett abgeschottet
- durch die physische Trennung von Applikations- und Daten-Servern, d. h. die Anwendungen laufen auf einem System, während die Daten auf einem anderen gespeichert sind.

¹ Alle genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen Eigentümer.

Maßnahmen zum Schutz gegen unerlaubten Zugriff

Passwortgeschützter Zugang

Nur Projektmitglieder, die persönlich von unserem Auftraggeber oder seinem Vertreter (z. B. Projektadministrator) eingeladen worden sind, besitzen Zugriff auf ein Projekt. Die Kennwörter der Projektmitglieder werden bei uns nicht gespeichert, sondern lediglich ein „digitaler Fingerabdruck“ dieser. Auf diese Weise ist es praktisch unmöglich, Rückschlüsse auf das Original zu ziehen. Somit sind diese Kennwörter auch nicht unseren Mitarbeitern bekannt. Selbstverständlich sollte jeder Benutzer sein Kennwort sicher verwahren, damit kein Unbefugter davon Kenntnis erlangt.

Optionale Beschränkung des Zugriffsortes (IP-Restriction)

Grundsätzlich kann unser System von überall her genutzt werden, wo ein Internetzugang zur Verfügung steht. Soll die Nutzung jedoch so eingeschränkt werden, dass ein Zugriff nur noch von einem bestimmten Standort aus (z. B. Bürogebäude) möglich ist, können wir dies ebenfalls einrichten.

Optionale Zwei-Faktor-Authentifizierung (RSA SecurID Login)

Für diesen doppelten Zugangsschutz greifen wir auf eine Lösung von RSA Security zurück, ein weltweit führender Anbieter im Bereich der Authentifikationstechnologie. Dabei wird ein so genannter Token eingesetzt, der alle 60 Sekunden automatisch eine neue, sechsstellige Zahlenkombination generiert und anzeigt. Der Nutzer muss zuerst eine vierstellige PIN-Nummer eingeben und im Anschluss daran den sechsstelligen Passcode, den ihm sein Token gerade anzeigt. Erst dann erhält er Zugang zu seinem Benutzerkonto (Account).

Maßnahmen zum Schutz gegen Computerviren

Anti-Viren-Software

Viren und Computerwürmer gehören heute leider zum Alltag. Wir setzen eine zuverlässige Anti-Viren-Software ein, die sich täglich automatisch aktualisiert. So werden auch neue Formen und Abarten von Computerviren sofort erkannt. Die Bearbeitung und Verbreitung einer virenbehafteten Datei innerhalb von think project! ist damit so gut wie ausgeschlossen.



Absicherung gegen Datenverlust

Zusätzliche Hardware und Hardwarekomponenten

Für alle Server – Hochleistungscomputer, die für unterschiedliche Aufgaben speziell konfiguriert wurden – stehen identische Ersatzserver bereit. Darüber hinaus sind sowohl an den Betriebs- als auch an den Ersatzservern alle essenziellen Hardwarekomponenten (Netzteil, Netzwerkkarten, Festplatten und Prozessoren) doppelt vorhanden.

Doppeltes Speichernetzwerk (SAN – Storage Area Network)

Unser Speichernetzwerk besteht aus einem System von Festplatten, die über Glasfaserkabel miteinander verbunden sind (fibre channel to disc). Auf diesem Festplattensystem können etwa 50 Terabyte unkomprimierter Daten gespeichert werden. Dieses System ist in unseren beiden Rechenzentren identisch vorhanden. Um die Sicherheit nochmals zu erhöhen, werden alle Daten in das jeweils andere Rechenzentrum gespiegelt, d. h. alle Kundendaten werden dort ein zweites Mal gespeichert.

Externe Datensicherung (Back-up)

Zusätzlich zur Datensicherung in unserem doppelten Speichernetzwerk sichern wir täglich alle Daten auf externen Datenträgern. Einmal pro Woche werden die gesammelten Datenträger an einen dritten Standort (Bankschließfach) verbracht.

Sichere Datenübertragung

Verschlüsselte Kommunikation

Ohne besondere Maßnahmen werden im Internet im Prinzip alle Daten in Klartext übertragen. Das bedeutet, auf ihrem Weg von einem Rechner zum anderen könnten diese Daten von Dritten verhältnismäßig einfach mitgelesen, geändert oder sogar gelöscht werden. Um dies zu verhindern, setzen wir Verschlüsselungsverfahren (Transport Layer Security TLS) ein, die eine sichere Übertragung der Daten ermöglichen. Ein Ausspähen der Daten ist damit praktisch ausgeschlossen.

Zwei unabhängige
Rechenzentren für doppelte
Sicherheit

Hochverfügbare
Internetanbindung und
Stromversorgung

Monitoring rund um die Uhr

Verschlüsselte
Datenübertragung

5-fache Datenspeicherung
an drei Standorten

Die internetbasierte Projektplattform think project! wird in 40 Ländern von namhaften Bauherren, Investoren, Projektentwicklern, Projektsteuerern, Bauunternehmen sowie Architektur- und Ingenieurbüros eingesetzt – bis heute in über 5.000 Projekten mit mehr als 90.000 Benutzern.

think project! vereinfacht die Zusammenarbeit in Projekten, sorgt für eine lückenlose Dokumentation und kann direkt über das Internet genutzt werden. think project! unterstützt ein effizientes Projekt-, Informations- und Risikomanagement und hilft so Zeit und Kosten zu sparen.

Ansprechpartner weltweit

www.thinkproject.com/network