

hyperspace Applikationshosting bietet umfassende Sicherheitsfunktionen, um eine Gefährdung Ihrer Kundendaten auszuschließen. Das Streben nach Sicherheit hat unsere höchste Priorität. Durch ständige Weiterentwicklung unserer Sicherheitsinfrastruktur bieten wir unseren Kunden ein Höchstmaß an Sicherheit und Datenschutz auf dem aktuellen Stand der Technik. Zu den Sicherheitsmaßnahmen des hyperspace Applikationshostings gehören unter anderem:

- Ein Team erfahrener Techniker und Sicherheitsexperten im Rechenzentrum Hannover, die kontinuierlich für den Schutz der Daten und Systeme sorgen.
- Kontinuierlicher Einsatz bewährter und aktueller Firewalls, SSL- Verschlüsselungstechniken und anderer Sicherheitstechnologien, einschließlich solcher, die wir selbst exklusiv für unsere Applikationen entwickelt haben.
- Fortlaufende Bewertung neuer Entwicklungen und Bedrohungen im Bereich der Sicherheit.

Sicherheitsdetails Unsere ausgereifte Sicherheitsinfrastruktur wurde von professionellen Experten konfiguriert und vor Inbetriebnahme rigorosen Tests unterzogen. Sie umfasst bewährte, aktuelle Firewall- und Eindringerrfassungssysteme, SSL Verschlüsselungstechniken und weitere Sicherheitstechnologien.

Physische Sicherheit. Unser Produktionssystem befindet sich in einer Anlage, in der die physische Sicherheit durch folgende Maßnahmen rund um die Uhr gewährleistet ist: Identifikation aller im Rechenzentrum tätigen Personen, ausfallsichere Stromversorgung, Temperaturregulierung im Datencenter, Brandschutzeinrichtungen und weitere Sicherungsfunktionen, die für einen sicheren Betrieb der Server sorgen und mit deren Hilfe Sicherheitsrisiken auf vorausschauende Weise erkannt werden. Eine tägliche Datensicherung sorgt dafür, dass Ihre Daten selbst im Falle von Störungen oder Systemausfällen nicht verloren sind.

Datenverschlüsselung. hyperspace setzt die leistungsstärksten Verschlüsselungsprodukte (SSL) namhafter Anbieter zum Schutz der Kundendaten und Kundenkommunikation ein. Das Schloss-Symbol im Browser zeigt an, dass die Daten während der Übertragung vollständig vor unautorisiertem Zugriff geschützt sind.

Benutzerauthentifizierung. Benutzer können nur mit einer gültigen Kombination aus Benutzername und Kennwort auf hyperspace Anwendungen zugreifen. Diese Angaben können zudem bei der Übertragung mit SSL verschlüsselt werden. Die Wahl von Kennwörtern, die sich leicht erraten lassen, wird verhindert. Jeder Benutzer wird über eine verschlüsselte Sitzungs-ID eindeutig identifiziert. Um die Sicherheit zusätzlich zu erhöhen, ist die Sitzungsdauer zeitlich begrenzt und wird nach einer gewissen Zeit der Inaktivität automatisch beendet

Anwendungssicherheit. Das robuste Anwendungssicherheitsmodell verhindert, dass ein hyperspace-Kunde auf die Daten eines anderen Kunden zugreifen kann. Das Sicherheitsmodell wird bei jeder Anforderung neu angewendet und während der gesamten Benutzersitzung durchgesetzt.

Interne Systemsicherheit. Innerhalb der Netzwerk-Firewalls werden die Systeme durch Übersetzung der Netzwerkadresse, Anschlussumleitung, IP-Maskierung, nicht routingfähige IP-Adressenschemas und andere Maßnahmen geschützt. Die genauen Details dieser Funktionen sind herstellerspezifisch und geschützt. Alle Sicherheitseinrichtungen werden von professionellen Experten laufend aktualisiert und gewartet. Dabei wird ausschließlich von den jeweiligen Herstellern ausgebildetes und entsprechend zertifiziertes Personal eingesetzt.

Betriebssystemeicherheit. hyperspace gewährleistet eine hohe Sicherheit auf Betriebssystemebene, da für die Produktionsserver nur ein Minimum an Zugriffspunkten verwendet werden. Alle Betriebssystemkonten werden durch wirksame Kennwörter geschützt. Für alle Betriebssysteme werden regelmäßig die vom jeweiligen Hersteller empfohlenen Sicherheits-Patches installiert. Außerdem werden alle nicht erforderlichen Benutzer, Protokolle und Prozesse deaktiviert und/oder entfernt, um die Betriebssysteme noch weiter zu immunisieren.

Servermanagement-Sicherheit. Alle Daten, die von einem Kunden in die hyperspace-Anwendung eingegeben werden, sind Eigentum dieses Kunden. Die Mitarbeiter und Entwickler von hyperspace haben keinen direkten Zugriff auf die Produktionsgeräte von hyperspace, es sei denn, dies ist für die

Verwaltung, Wartung und Überwachung des Systems oder für Sicherungen erforderlich. Das Systems Engineering-Team von hyperspace erledigt alle Aufgaben im Zusammenhang mit Sicherungen und der Verwaltung, Wartung und Überwachung des Systems. Alle Wartungsarbeiten sind nur von ausgewählten Arbeitsplätzen aus möglich, die zudem besonders geschützt sind. Die Kommunikation zwischen Wartungsarbeitsplatz und Server erfolgt ebenfalls verschlüsselt.

Entwicklungs-Sicherheit. Die Entwicklung aller hyperspace Applikationen erfolgt nach dem Fusebox-Standard innerhalb eines vordefinierten Prozessablaufs mit 6 Phasen. Durch den extrem modularen Aufbau, die exakte Definition aller Schnittstellen vor Beginn der Programmierung und die hohe Wiederverwendungsrate der einzelnen Module werden nicht nur Fehlerquellen minimiert, sondern auch der Aufwand bei späteren Änderungen und Ergänzungen reduziert. Die zugehörige Entwicklungsdokumentation erstellen wir nach dem XML-basierten Fusedoc 2.0-Standard. Für Qualitätssicherung und Qualitätskontrolle werden Testprogramme und Tools zur Komplexitätsprüfung und Risikobewertung von Quelltexten anhand der Methode "Zyklomatische Komplexität nach McCabe" eingesetzt, die sich sehr gut für die Beurteilung von Fusebox-Entwicklungsprojekten eignet. Alle Änderungen an Softwaremodulen werden mithilfe einer serverbasierten Versionskontroll-Software verfolgt und dokumentiert. Externe Entwickler erhalten keinerlei Zugang zu Produktionssystemen, Kundenpassworten oder Kundendaten und sind verpflichtet, für alle von Ihnen erstellten Programme und Programmteile entsprechende Testmodule zu erstellen, mit denen wir bei hyperspace die Programme auf modularer Ebene testen können.

Das mehrschichtige Sicherheitskonzept von hyScore Applikationen:

Durch die Architektur der Anwendung bedingt und durch entsprechende Sicherheitseinrichtungen auf der Seite des Providers gewährleistet hyperspace einen optimalen Schutz Ihrer Daten auf dem aktuellen Stand der Technik:

- Standig gewartete Firewalls schützen den Server vor unbefugtem Zugriff.
- SSL-Verschlüsselungstechniken von führenden Anbietern schützen die übertragenen Daten vor Ausspähung.
- Ein ausgefeiltes Berechtigungskonzept innerhalb der Anwendung und die Anmeldung mit Benutzername und Kennwort regelt den Zugriff auf alle Informationen innerhalb der Applikation.
- Die mehrschichtige Anwendungsarchitektur von hyScore-Applikationen bietet durch das Isolieren von Anwendungen und Prozessen und das Auslagern der Datenbanken und Dateien zusätzlichen Schutz vor unbefugten Zugriffen.