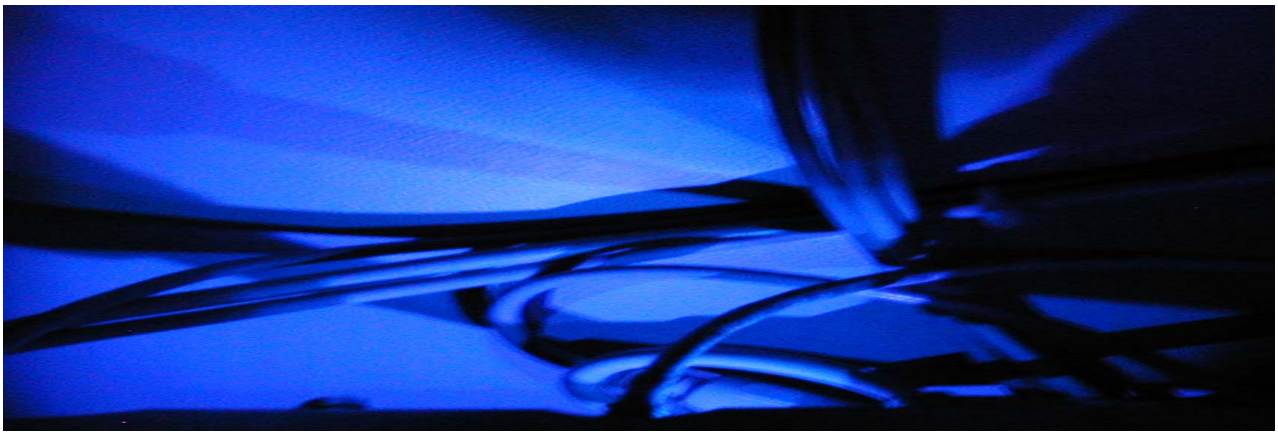

Das mehrschichtige Sicherheitskonzept von hyperspace Applikationen

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

- Standig gewartete Firewalls schützen die hyperspace 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 hyperspace-Applikationen bietet durch das Isolieren von Anwendungen und Prozessen und das Auslagern der Datenbanken und Dateien zusätzlichen Schutz vor unbefugten Zugriffen.

Das Streben nach Datensicherheit hat unsere höchste Priorität. hyperspace Applikationshosting bietet deshalb in allen Bereichen umfassende Sicherheitsfunktionen, um eine Gefährdung Ihrer Kundendaten auszuschließen:

Physische Sicherheit

Unsere Produktionsserver befinden sich im Hostway-Rechenzentrum in Hannover. Die physische Sicherheit unserer Server und Ihrer Daten wird u.a. durch folgende Maßnahmen rund um die Uhr gewährleistet: Identifikation aller im Rechenzentrum tätigen Personen, Zugang nur für berechtigte Personen nach vorheriger Anmeldung, ausfallsichere Stromversorgung, Temperaturregulierung im Datencenter, Brandschutzeinrichtungen sowie weitere Sicherungsfunktionen, die für einen sicheren Betrieb der Server sorgen und mit deren Hilfe Sicherheitsrisiken auf vorausschauende Weise erkannt werden.

Datenverschlüsselung

hyperspace setzt leistungsstarke Verschlüsselungsprodukte (SSL) namhafter Anbieter (z.B. VeriSign, Thawte) 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. 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.

Backup

Eine tägliche, ausgelagerte Datensicherung sorgt dafür, dass Ihre Daten selbst im Falle von Störungen oder Systemausfällen nicht verloren sind.

Interne Systemsicherheit

Der Zugriff auf die Server wird durch Firewalls des Rechenzentrums und zusätzliche Firewall-Software auf den Hosting-Servern nach dem aktuellen Stand der Technik geschützt. Grundsätzlich sind auf unseren Servern nur solche Portadressen freigeschaltet, die für den Produktionsbetrieb unbedingt notwendig sind.

Betriebssystem

hyperspace gewährleistet eine hohe Sicherheit auf Betriebssystemebene, da für die Produktionsserver nur ein Minimum an Zugriffspunkten verwendet wird. 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 oder entfernt, um die Betriebssysteme noch weiter zu immunisieren.

Datensicherheit und Servermanagement

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 unbedingt erforderlich. hyperspace Mitarbeiter und Vertragspartner sowie die Mitarbeiter des Rechenzentrums sind selbstverständlich auf das Datengeheimnis verpflichtet. Wartungsarbeiten an den Servern sind nur von ausgewählten hyperspace-Arbeitsplätzen aus möglich, die zudem besonders geschützt sind. Die Kommunikation zwischen Wartungsarbeitsplatz und Server wird verschlüsselt. Mitarbeiter des Rechenzentrums haben keinen Zugriff auf die Anwendungen der Kunden von hyperspace.

Entwicklungssicherheit

Alle Entwicklerarbeitsplätze werden von Virenschutz-Software und anderen Schutzprogrammen nach aktuellem Stand der Technik geschützt. 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.