Datenschutz auf höchstem Niveau

hyperspace beachtet die Datenschutzbestimmungen der Bundesrepublik Deutschland und der EU-Datenschutzgrundverordnung. Wir behandeln personengebundene Daten streng vertraulich und geben diese nicht zu Werbezwecken an Dritte weiter.

Der Betrieb unserer Server erfolgt in Deutschland, die Daten werden innerhalb Deutschlands verarbeitet, es gilt deutsches Recht.

Gemeinsam mit unserem Rechenzentrumsbetreiber Hostway in Hannover treffen wir umfassende Maßnahmen auf dem aktuellen Stand der Technik für den Schutz der Daten, die Sie uns anvertraut haben.

hyperspace Dimensions und hyperspace Franchise Manager sind mit dem Siegel „Software Hosted in Germany" des Bundesverband IT-Mittelstand e.V. zertifiziert.

Hostway Deutschland GmbH ist durch das Bundesamt für Sicherheit in der Informationstechnik nach ISO 27001 „IT-Grundschutz" zertifiziert (Zertifikats-Nr.: BSI-IGZ-0230-2016).

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.

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 und Anwendungssoftware

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 Betriebssysteme und Anwendungssoftware 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.

Applikationsserver

Der Applikationsserver wird gemäß den Herstellerempfehlungen gegen unautorisierte Zugriffe abgesichert. Sicherheitspatches und Updates werden regelmäßig installiert. Die Sicherheitsfeatures werden wöchentlich durch einen externen Dienstleister überprüft.

Datenverschlüsselung

hyperspace setzt leistungsstarke Verschlüsselungsprodukte (SSL/TLS) 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 müssen sich für den Zugang in hyperspace Dimensions in der Regel (siehe Ausnahmen, unten) mit Benutzername und Passwort authentifizieren. 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.

Ausnahmen

Bei der Nutzung von Single Sign On-Schnittstellen zu externen Systemen z.B. über AD-Sync mit Kerberos oder SAML erfolgt die Authentifizierung auf andere Weise. Beim automatischen Login über einen Email-Link erfolgt die Authentifizierung über ein verschlüsseltes Token mit zeitlicher Begrenzung.

Single Sign On

Für den Betrieb von hyperspace im eigenen Kundennetzwerk empfehlen wir eine zentrale Single Sign On Lösung, z.B. mittels Active Directory Integration und Kerberos.

Bei gehosteten Lösungen ist Single Sign On nur via SAML 2.0 oder VPN möglich.

Passwortsicherheit

Das Passwort wird nicht in der Datenbank gespeichert, sondern nur der Hashwert des Passwortes, der zuvor zusätzlich mit einem SALT-String verfälscht wurde. Der SALT-String ist pro Userkonto unterschiedlich und wird mittels Triple-DES (DESede) erzeugt. Das Hashverfahren ist SHA-256.

Passwortlänge und -Komplexität

Wenn ein User ein neues Passwort vergibt, wird durch einen farbigen Balken die Sicherheit des Passwortes visualisiert. Dabei werden Länge und Komplexität der eingegebenen Zeichenkette berücksichtigt. Passworte in hyperspace müssen mindestens 10 Stellen lang sein und bestehen aus Buchstaben, Sonderzeichen und Zahlen Erlaubte Sonderzeichen sind: !$§%&*_-?/\(){}[]+

Groß-/Kleinschreibung wird unterschieden, ist aber mit Rücksicht auf die Benutzer von mobilen Endgeräten nicht gefordert.

Die Mindestlänge der Passworte kann bei den Mandanteneinstellungen auf einen Wert von mindestens 10 und höchstens 32 Stellen festgelegt werden.

Zeitliche Begrenzung von Passworten

Passworte laufen nach einer einstellbaren Frist von mindestens 1 bis maximal 180 Tagen automatisch ab. Passworte die älter sind, müssen beim nächsten Login geändert werden

Passwortänderungen

- Administratoren können die Passworte aller Benutzer ihres Mandanten zurücksetzen.
- Administratoren können für neue Benutzer ein initiales Passwort vergeben.
- Falls ein neues Passwort vergeben oder das Passwort von einem Admin zurückgesetzt wurde, wird dem Benutzer beim nächsten Login eine entsprechende Hinweismeldung angezeigt und der Benutzer muss sich ein neues Passwort vergeben.
- Benutzer können ihr eigenes Passwort jederzeit beim Benutzerprofil ändern.
- Benutzer können ein neues Passwort auf dem Login-Bildschirm anfordern. Die Anforderung eines neuen Passwortes erfolgt in 2 Stufen: 1.) Eingabe von Login-Name und dazu passender Emailadresse, wenn diese Daten zu einem vorhandenen Benutzerkonto passen, das nicht gesperrt ist, wird eine Email mit einem Link zur Passwortanforderung an diese Mailadresse gesendet. Der Link ist 20 Minuten lang gültig. 2) Durch Klick auf den Link in der Email öffnet sich ein Dialog, mit dem ein neues Passwort vergeben werden kann. Dabei werden die Mindestanforderungen an die Komplexität überprüft. Wichtig: Der Link funktioniert nur mit dem gleichen Endgerät und im gleichen Browser, mit dem auch schon den ersten Schritt ausgelöst wurde.
- Wir speichern die Hashwerte der letzten 10 Passworte und vergleichen sie bei einer Passwortänderung mit dem aktuellen Passwortwunsch. Sind die Hashwerte identisch, kann das gewünschte neue Passwort nicht verwendet werden.

Bulk-Änderungen

Administratoren können alle wesentlichen Einstellungen für Benutzer mittels Import einer CSV-Datei ändern. Dabei kann auch das Passwort des Benutzers zurückgesetzt werden. Auch neue Benutzer lassen sich mittels CSV-Import anlegen. Neue Benutzer erhalten dabei ein automatisch erzeugtes, sicheres Passwort, das beim ersten Login geändert werden muss.

Außerdem gibt es ein spezielles Wartungsprogramm für Administratoren, mit denen die Passworte aller Benutzer auf einmal zurückgesetzt werden können.

Protokollierung und Sperrung erfolgloser Loginversuche

Die maximale Anzahl erfolgloser Versuche ist systemintern auf 3 Versuche festgelegt. Beim 4. Versuch wird das Konto des Benutzers gesperrt.

Die Dauer der Sperrung kann für jeden Benutzertyp (Administrator, Bearbeiter, Partner/Erfasser, Leser) individuell bei den Mandanteneinstellungen festgelegt werden. (1 – 999 Minuten).

Die Sperrung eines Benutzerkontos kann manuell durch einen Administrator aufgehoben werden.

Backup

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

Schutz gegen Angriffe

Cross-Site Scripting

Alle eingegebenen Benutzereingaben und URL-Parameter werden durch eine spezielle Prüfroutine auf Scripting-Angriffe geprüft und verdächtige Bestandteile vor der weiteren Verarbeitung entfernt.

SQL-Injection

Eine Typprüfung der Variablen, die an SQL-Abfragen übergeben werden, verhindert wirkungsvoll SQL-Injection-Angriffe auf die Datenbank. Beim Login-Formular findet zusätzlich noch eine mehrfach gestaffelte Abfrage der Benutzerdaten statt.

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 erfolgen von Arbeitsplätzen, die 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. Alle Änderungen an Softwaremodulen werden mithilfe einer serverbasierten Versionskontroll-Software verfolgt und dokumentiert. Alle Änderungen werden in speziellen Entwicklungssystemen vorgenommen und dann zuerst in Testsystemen geprüft, bevor sie in den Produktionssystemen implementiert werden.

Auftragsdatenverarbeitung

Wir bieten Ihnen auf unserer Website einen Mustervertrag zur Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz und EU Datenschutz-Grundverordnung kostenlos zum Download an: http://www.hyperspace.de/global/de/agb.html

Datenschutzbeauftragter

Als externer Datenschutzbeauftragter für hyperspace gemäß § 4f Absatz 1 Bundesdatenschutzgesetz ist seit dem 01.07.2017 die ER Secure GmbH, In der Knackenau 4, 82031 Grünwald bestellt.