

Hosting und Datenschutz

Wir arbeiten mit einem externen Datenschutzbeauftragten der Firma audatis - Datenschutz und Informationssicherheit zusammen. Diese Firma führt regelmäßige Datenschutz Audits unserer Firma durch.

Hosting (falls von Just Software gehostet)

Alle Server werden in deutschen Rechenzentren nach deutschem Datenschutz gehostet.

Mit unseren Hostern haben wir einen Vertrag zur Auftragsdatenverarbeitung abgeschlossen.

Protokolle

Wir verwenden http/https (mit entsprechendem Zertifikat), smtp, ssh (für Wartungszugänge) sowie FTP für die Übertragung von verschlüsselten Backups.

IP-Adressen und Serverlogs

IP-Adressen werden nur eine befristete Zeit gespeichert. Die genaue Zeit hängt von der Log-Rotation ab (max 60 Tage). Insgesamt werden in den Logs folgende Informationen gespeichert:

- IP-Adresse des/der Nutzers/Nutzerin
- Betriebssystem und Browsertyp
- Datum und Uhrzeit des Zugriffs
- Zugriffsmethoden, angeforderte Funktionen, übertragene Datenmenge
- Zugriffsstatus des Plattformservers
- ggf. Name der angeforderten Datei
- ggf. URL, von der aus die Daten angefordert wurde

Chat Nachrichten

Chat-Nachrichten werden in der Datenbank gespeichert. Der Chat speichert keine Statusänderungen (Online/offline).

Löschen von Daten / Schattentabellen

In JUST sind die Schattentabellen immer aktiv. Das bedeutet alle Informationen die von der Plattform gelöscht werden, werden 1 zu 1 in die Schattentabellen verschoben. Damit sind die Informationen für den normalen User in JUST nicht mehr sichtbar. Für den Administrator ist es aber möglich die Informationen aus den Schattentabellen wiederherzustellen. Dadurch erlangen wir eine Revisionssicherheit, da keine Informationen gelöscht werden.

Pflichtangaben von Usern

Die Pflichtangaben sind: Name, Vorname, E-Mail Adresse. Alle weiteren Angaben sind optional.

Cookies

Cookies sind sitzungsbezogen und werden nach Beendigung der Session wieder gelöscht. Diese Cookies beinhalten keine personenbezogenen Daten. Wenn die Option „Angemeldet bleiben“ ausgewählt wird, wird ein weiterer Cookie erzeugt, der die Anmeldedaten verschlüsselt speichert

und bei einem folgenden Abmeldevorgang gelöscht wird.

Authentisierung/Autorisierung

Jede Benutzerinteraktion in JUST unterliegt einer Authentisierung und Autorisierungsprüfung. Im Standardfall erfolgt die Authentisierung über Nutzernamen und Passwort. Sollte Kerberos konfiguriert sein, erfolgt diese Prüfung über ein Kerberos Ticket, das mit dem Active Directory des Kunden abgeglichen wird.

Backup (bei Hosting durch Just Software)

Mindestens einmal pro Tag werden die Daten von JUST gesichert und verschlüsselt auf einem Backup-Space abgelegt.

Cross-Site Scripting

Cross-Site Scripting wird durch den Einsatz unseres GWT Frameworks sowie im WYSIWYG-Editor über Antisamy verhindert.

SQL-Injection

Das Einfügen von SQL-Abfragen wird durch unseren Einsatz von Prepared Statements mittels mybatis verhindert, das für die Datenbankzugriffe verwendet wird.

Firewall

In unseren Standardprozessen zur Installation von JUST ist vorgesehen, einen Paketfilter entsprechend einzurichten, so dass ein Zugriff von außen nur auf die entsprechenden Services möglich ist, und zwar i.d.R. über SSH (22) und HTTP/HTTPS (80/443).

HTTPS Verschlüsselung

JUST bietet die Möglichkeit, eine sichere Ende-zu-Ende-Verschlüsselung mittels HTTPS (TLS) herzustellen. Der verwendete Algorithmus hängt vom TLS-Schlüssel ab. In der Regel ist dies AES mit 256 Bit Schlüssellänge.

Monitoring

Um den reibungslosen Betrieb von JUST zu gewährleisten, wird der Status der verwendeten Services und Ressourcen durch Nagios überwacht. Bei Überschreiten von Schwellenwerten werden automatisch Benachrichtigungs-E-mails versendet. Überwacht werden beispielsweise JUST Status (Heartbeat), Backup Status, Festplattenbelegung, CPU-Auslastung und Speicherbelegung (RAM).

Wartungszugriffe

Alle Wartungszugriffe werden protokolliert und sind nur mittels personalisiertem SSH Key möglich

Passwort-Anforderungen

Die Mindestanforderungen der von den Nutzern zu vergebenen Passwörtern beträgt: Mindestens 8 Zeichen, mindestens 1 Buchstabe, Groß- und Kleinschreibung oder eine Zahl oder ein Sonderzeichen.

Passwort-Verschlüsselung

User-Passwörter werden stets mittels eines Hash-Algorithmus (MD5) und einem geheimen Salt gesichert und in der Datenbank gespeichert. Eine Entschlüsselung ist somit nicht möglich. Die Passwörter für die E-Mail-Anbindung werden mittels AES verschlüsselt in der Datenbank abgelegt.

Sicherheits-Updates

Auf von Just Software gehosteten System werden regelmäßig Sicherheitsupdates eingespielt.

Timeout

Die Länge des Timeout bei Nutzerinaktivität kann plattformweit eingestellt werden. Die Standardeinstellung liegt derzeit bei 2h.

Folgende Cookies werden eingesetzt

jsChatTabCount: Ermöglichen das Chatten über mehrere Tabs/Fenster. Session Cookie (wird z.B. beim Schließen des Browsers gelöscht).

jc_locale: Speichert die Spracheinstellung des Nutzers. Langlebiger Cookie..

ll (Last Login): Hier wird ein Hash gespeichert. Bei erneutem Aufruf der Seite als nicht eingeloggter Benutzer wird dieser Hash mit der Datenbank abgeglichen, die über ein entsprechendes Mapping zur E-Mail-Adresse (oder Benutzername) verfügt. Dadurch wird der Wert der E-Mail-Adresse (Benutzername) in der Anmeldebox entsprechend vorbelegt. Langlebiger Cookie.

JUST_SESSION: Loggt den Nutzer in machen Apps von Just Social ein. Session Cookie (wird z.B. beim Schließen des Browsers gelöscht).

jwt: Loggt den Nutzer in machen Apps von Just Social ein. Session Cookie (wird z.B. beim Schließen des Browsers gelöscht).

loadproxy: Bei Cluster-Systemen wird dieser gesetzt, damit man immer auf demselben App-Server landet. (Gültigkeit 1 Tag)

Optional: Durch die Einbindung von Trackingtools wie z.B. Piwik oder Google Analytics können weitere Cookies angelegt werden.

Local Storage der Browser

Durch das Just interne Tracking von Seitenaufrufen in Page wird eine zufällig generierte ID für den Nutzer gespeichert, die nicht auf das Profil des Nutzers in Just Social zurückführbar ist.



Optional: Durch die Einbindung des durch Just angepassten Piwik Tracking Codes wird eine zufällig generierte ID für den Nutzer gespeichert, die nicht auf das Profil des Nutzers in Just Social zurückführbar ist.