united planet

TECHNISCHE DOKUMENTATION

Datenschutz in Intrexx

Inhalt

1.1. Vorwort

Intrexx ist eine Low-Code-Entwicklungsplattform und bietet die Möglichkeit datenbankgestützte Webapplikationen in beliebiger Form zu erstellen.
Mit der Entwicklungsumgebung werden in der Regel hochgradig kundenindividuelle Applikationen erstellt die sich dem Einflussbereich des Herstellers komplett entziehen. Diese Applikationen werden von folgenden Nutzerkreisen erstellt: Kunde, Partnerunternehmen oder die Mitarbeiter des United Planet Consulting.
Bei derartig erstellten Applikationen können personenbezogene Daten in beliebigen Datensätzen hinterlegt werden, wenn dies der jeweilige Anwendungsentwickler so vorsieht.
Die Plattform selbst bietet jedoch die Möglichkeit beliebige Sichten zu erstellen, die alle Informationen zu einem Benutzer darstellen könnten, wie auch die Möglichkeit, Daten zu anonymisieren oder komplett aus dem System zu entfernen. Die Erstellung dieser Prozesse und Sichten sind über individuelle Anpassungen an den bestehenden Applikationen in der Regel sehr einfach umsetzbar.

United Planet GmbH nimmt den Schutz Ihrer Daten sehr ernst. Wir haben in unserer Software Intrexx etliche Möglichkeiten integriert, um Ihre Daten vor unautorisiertem Zugriff zu schützen. Diese sollten nicht als alleinige Schutzmechanismen eingesetzt werden, sondern sind durch weitere Sicherheitsvorkehrungen zu ergänzen.
Auch ist nicht jeder dieser Schutzmechanismen nur in Intrexx einzustellen. Manches davon muss ebenfalls in der entsprechenden Software des Drittanbieters angepasst werden. Wie das zu tun ist, entnehmen Sie bitte der Dokumentation des Herstellers.

1.2. Schutzmechanismen in Intrexx

1.2.1. Speicherung von Daten in Intrexx

Die Speicherung der Applikationsdaten in Intrexx erfolgt in Datenbanken von Drittherstellern. Sie werden weder von United Planet entwickelt oder zur Verfügung gestellt. Diese Datenbanksysteme sind verantwortlich für die Art und Weise, wie sie Daten vor unautorisiertem Zugriff schützen.

Intrexx unterstützt für alle Datenbanksysteme eine verschlüsselte Übertragung. Das entsprechende Zertifikat muss manuell von einem Portaladministrator in den Zertifikatsspeicher von Intrexx aufgenommen werden. Nicht hinterlegten Zertifikaten wird nicht vertraut.

Neben den Applikationsdaten fallen auch systembedingte Daten und Protokolle an, welche im lokalen Dateisystem gespeichert werden:

- Von einem Intrexxportal versandte E-Mails können in einem lokalen Dateiordner abgelegt werden um z.B. Compliance Richtlinien zu erfüllen. Dies ist standardmäßig deaktiviert.

- Das Protokollieren von Benutzer-Logins ist ebenfalls per default ausgeschaltet. Allerdings werden fehlerhafte Loginversuche festgehalten (kein Passwort). Diese stehen jedoch nur in den Protokolldateien des Intrexxservers und sind so nur für Serveradministratoren einsehbar.

- Push-Nachrichten (Intrexx Share) werden auf dem Server ebenfalls im Standard nicht gespeichert. Dies ist von einem Portaladministrator jedoch portalweit aktivierbar.

1.2.2. Portal- und Applikationsexporte

Intrexx bietet über den Portalmanager die Möglichkeit Applikationen und Portale zu exportieren. In den Portalexporten befinden sich alle Daten aller Applikationen sowie die Benutzerdatenbank. Die Exporte sind mit Sorgfalt zu behandeln und sicher, gegen Zugriffe dritter abzulegen. In Applikationsexporten ist steuerbar, ob Daten exportiert werden sollen oder nicht. Enthält eine Applikation personenbezogene Informationen muss für die Exportdateien der Zugriff von dritten verhindert werden. Sofern nicht zwingend notwendig, sollten Applikationen stets ohne Daten exportiert werden.

1.2.3. Datenübertragung

Intrexx überträgt Daten an Drittsysteme. Im Detail sind das:

- Bei einem Webserver-Zugriff auf das Portal werden Webseiten mit Daten an den aufrufenden Client gesendet. Welche Daten der Benutzer zu sehen bekommt, hängt von seinen Zugriffsrechten ab. Der auf dem Intrexxserver installierte Webserver übernimmt die Aufgabe des Datenaustausches mit dem Client. Standardmäßig wird unverschlüsselt über das http Protokoll übertragen, was jedoch bei jedem Webserver von einem Serveradministrator auf eine verschlüsselte Übertragung (https) geändert werden kann. In zukünftigen Versionen von Intrexx werden neue Portale in den Standardeinstellungen mit https konfiguriert.

- Alle sogenannte Connectoren/Adapter von Intrexx haben die Möglichkeit implementiert, über verschlüsselte Verbindungen auf die entsprechenden Drittsysteme zuzugreifen. Ausnahmen sind der Connector für Abacus (Nutzung einer JDBC-Verbindung) und Lotus Notes. Dies muss in der Software aktiv geschaltet und die Connectoren entsprechend konfiguriert sein.

- Mobile App: Hier werden Daten von einem Portal an das Smartphone eines Benutzers übertragen. Dies sind Benachrichtigungen der Applikation Share über neue Beiträge, Kommentare oder Likes. Die Übertragungswege vom Portal zum United Planet Push-Gateway sowie von dort zum Anbieter des Smartphone-Betriebssystems (Apple, Google) sind verschlüsselt. Der Kommunikationsweg dieser Anbieter zum Smartphone des Benutzers ist in deren Händen. Derzeit sind die Verbindungen ebenfalls verschlüsselt und es nicht davon auszugehen, dass sich das ändern wird. Die Nachrichten werden auf den Servern bis zur Weiterleitung zwischengespeichert.

- Von Intrexx generierte E-Mails werden auf dem von Portaladministratoren konfigurierten Übertragungsweg weitergereicht. Verschlüsselte Protokolle werden auch hier unterstützt.

- Bei der Verwendung einer sogenannten NFR-Lizenz, werden Daten des Portals verschlüsselt an United Planet GmbH übermittelt. Es sind keine personenbezogenen Daten enthalten. Im Detail sind das Meta-Informationen über die Anzahl der User, die Anzahl der Applikationen, die Namen der Applikationen, die Anzahl Datengruppen und die Anzahl von Seiten einer Applikation.

- Bei anderen Lizenzen findet außer beim Onlineupdate keine Datenübertragung an United Planet GmbH statt. Das Onlineupdate sendet die Versionsnummer der Intrexxinstallation.

1.2.4. Applikations- und Benutzerrechte in einem Portal

Das Rechtesystem in Intrexx erlaubt sehr viele Einstellmöglichkeiten. Dies gilt sowohl für die administrativen Tätigkeiten am Portal wie auch die Zugriffrechte an den einzelnen Applikationen.

Die Administrationsrechte können portalweise eingestellt werden. Hier gibt es diese Möglichkeiten, Portalbenutzern Rechte an den einzelnen Komponenten zu geben.

Der Zugriff auf die Applikationen durch die Benutzer kann sehr genau eingestellt werden. Sowohl Benutzer wie auch Gruppen sind selektierbar.

Bei einer neu erstellten Applikation, werden keine Zugriffsrechte außer für die Gruppe der Administratoren gesetzt. Benutzer/Gruppen müssen erst explizit die Rechte bekommen. So ist ein versehentlicher Zugriff auf Daten durch nicht autorisierte Benutzer nicht möglich.
Eine Auflistung, welche Rechte im Detail einstellbar sind, finden Sie im Anhang.

Benutzerkonten können durch einen Prozess anhand von Benutzereigenschaften (z.B. Verfalldatum) gesperrt werden. Dies verhindert, dass bei zeitlich befristete Zugänge wie z.B. Praktikanten nicht vergessen wird, diese zu deaktivieren.

Beim Löschen eines Portal-Benutzers wird auch dessen Share-Profil gelöscht bzw. anonymisiert. Die Beiträge des Users bleiben bestehen, da es sonst zu inkonsistenten Datenstrukturen führen kann.

Es ist möglich, die Authentifizierung der Portal-Benutzer gegenüber einem Verzeichnisdienst durchzuführen.
Alternativ können auch Benutzer in Intrexx angelegt werden. Hierbei ist es möglich,

Komplexitätsanforderungen für Passwörter vorzugeben, welche den Passwortrichtlinien des Unternehmens entsprechen.

1.3.Cookies

Intrexx erzeugt bei der Nutzung diverse Cookies. Das sind kleine Textdateien auf dem zugreifenden System, welche Informationen zu dem Nutzer o.ä. speichern können.

Intrexx speichert grundlegend keine personenbezogenen Informationen in seine Cookies ab. Die Art und den Inhalt der Intrexx Cookies zeigen wir nachfolgend auf.

Cookies können unterschiedliche Funktionen und Eigenschaften besitzen. Ein Cookie kann bis zu 4093 Byte groß werden.

1.3.1.Allgemeine Cookies

Session-Cookies oder persistentes Cookies

Ein Session-Cookie existiert nur solange der Browser nicht geschlossen wird. D.h. das Cookie wird vom Browser nicht persistent gespeichert.

Ein persistentes Cookie wird bis zu einem vom Anbieter vorgegebenen Datum auf der Festplatte / Browser des Benutzers gespeichert.

Session Cookies sollten von Typ HTTP-only sein, damit diese nur vom erzeugenden Server und nicht per JavaScript ausgelesen werden können. Webseiten bzw. Portale sollten generell nur Verschlüsselt betrieben werden – in diesem Fall sollten auch die Cookies mit dem secure Flag versehen werden, damit diese nur über die verschlüsselte Verbindung gesendet werden.

First-Party oder Third-Party-Cookie

Ein First-Party-Cookie wird von der besuchten Seite gesetzt und vom Browser bei jeder Anfrage an die besuchte Seite zurückgesandt.

Third-Party-Cookies werden von einer anderen als der besuchten Seite im Hintergrund erzeugt und vom Browser bei Anfragen an beliebige Seiten, welche den Erzeuger verwenden. Typisch für diese Art von Cookies sind Tracker.

Funktionscookies

Um die Usability einer Webseite zu erhöhen, werden sogenannte Funktionscookies eingesetzt. Hier werden z.B. Einstellungen gespeichert, die bei einem erneuten Besuch der Webseite voreingestellt werden sollen. Das können z.B. Sortiereinstellungen von Tabellen, die eingestellte Sprache oder Währung sein. Auch Warenkörbe werden häufig in Cookies gespeichert, um diesen bei Verlassen des Shops und erneutem Laden wiederherzustellen. Funktionscookies haben in der Regel eine längere Lebensdauer.

1.3.2. Intrexx Cookies

Das Session Cookie (co_SId)

Um die Sitzung eines Benutzers (Gast oder Authentifiziert) eindeutig zu identifizieren, wird eine Session-ID vergeben. Diese wird Serverseitig per Zufall erzeugt und dort für die Dauer der Sitzung geführt. Damit diese Sitzung auch dem Client (Browser) zugeordnet werden kann, wird die Session-ID in einem Cookie gespeichert.

Achtung: Damit die Session-ID nicht in der URL geführt wird, müssen Cookies aus Sicherheitsgründen verwendet werden. Intrexx verwendet bei den Session Cookies das httpOnly Flag, um ein Auslesen per JavaScript zu verhindern. Zusätzlich wird das secure Flag verwendet, damit Cookies nur über verschlüsselte Verbindungen gesendet werden.

Das Cookie enthält nur die Session-ID und keine weiteren personenbezogenen Informationen. Die Gültigkeitsdauer des Cookies ist auf die Sitzungsdauer begrenzt, wird also nicht persistent gespeichert. Das Cookie wird zudem nur an die besuchte Intrexx-Seite zurückgesendet.

Das Layout Cookie (co_Layout)

Das Layout Cookie speichert das eingestellte Layout des Benutzers zum jeweiligen Portal und ist vom Typ „first party". Im Wert des Cookies steht der Portalbetreiber, aber keine personenbezogenen Daten des Benutzers. Die dem Cookie-Namen angehängte GUID dient zur Identifikation des Layouts (jedes Layout in Intrexx besitzt eine eindeutige Kennung in Form einer GUID)

Das Sprach-Cookie (co_Lang)

Die vom Benutzer im Portal eingestellte Sprache, wird im Sprach-Cookie gespeichert. Als Wert wird der ISO-Schlüssel der gewählten Sprache gespeichert (de, en, fr, …). Das vom Typ „first party" Cookie enthält keine benutzerbezogenen Informationen.

Das Locale-Cookie (co_Locale)

Kann der Benutzer ein Länderschema auswählen, wird dieses im Locale Cookie gespeichert. Als Wert wird der ISO-Schlüssel (z.B. EN-en, DE-de) gespeichert. Auch dieses Cookie vom Typ „first party" enthält keine benutzerbezogenen Informationen.

1.3.3.Mögliche „fremderzeugte" Cookies in Intrexx-Portalen

Cookies können durch zusätzliche Programmierung in Intrexx via JavaScript erzeugt werden. Dies erfolgt jedoch durch spezielle Anpassungen im Rahmen der Applikations-Entwicklung, welche in den Händen der Kunden liegt. Grundsätzlich sollten nach aktueller Rechtslage solche Anpassungen generell dokumentiert werden, damit kundenspezifische Cookie-Erzeugungen bekannt sind.

Häufig werden Cookies auch durch in Intrexx-Portalen eingebundene Komponenten wie Tracker (GoogleAnalytics, eTracker, …) erzeugt. Dabei werden in der Regel alle Daten, die über den Request ermittelbar sind (darunter auch die vollständige IP-Adresse), gespeichert und extern an den Tracking-Dienstleister übertragen.

Auch Aufrufe von externen Webseiten über ein Intrexx-Portal kann zu Cookies im Portal-Kontext führen. D.h. die Cookie-Liste im Browser des Benutzers kann viele Cookies auflisten, welche nicht durch Intrexx bzw. das Portal selbst erzeugt wurden.

1.4. Anhang

1.4.1. Konfigurierbare Portalrechte

- Eigenschaften des Portals
- Module
  - Design
  - Applikationen
  - Beziehungen
  - Prozesse
  - Benutzer
- Veröffentlichung von Scripten
- Externe Anbindungen (Datenbank, Webservices, OData-Services, Dokumentenintegration, SAP-Gateway, Lotus Notes, Microsoft Exchange, SAP BO, Abacus, M-Files)
- Zugriff auf Werkzeuge
  - System-Monitor
  - Aufgabenplanung
  - Variablen
  - E-Mail-Service

1.4.2. Konfigurierbare Applikationsrechte

- Applikation
  - Vollzugriff
  - Benutzen
  - Verwalten
- Seiten
  Rechte sind für jede einzelnen Seite einstellbar
  - Benutzung
- Datengruppen (Datenbank-Tabellen)
  Rechte sind für jede einzelnen Datengruppe einstellbar
  - Vollzugriff
  - Datensätze lesen (alle)
  - Datensätze lesen (nur eigene)
  - Datensätze hinzufügen
  - Datensätze ändern (alle)
  - Datensätze ändern (nur eigene)
  - Datensätze löschen (alle)
  - Datensätze löschen (nur eigene)
- Dateien
  Rechte sind analog zu den Datengruppen einstellbar

1.4.3. Liste der Schutzmechanismen

- E-Mail-Service deaktiviert (Default)
- Verschlüsselte Übermittlung an
  - Microsoft Exchange
  - Datenbanksystem
  - SAP
  - M-Files
  - OData
  - Microsoft Office 365

    - Lotus Notes
    - Abacus
- Verschlüsselter Zugriff (https) der Clients auf Portal möglich
- Push-Nachrichten deaktiviert (Default)
- Verschlüsselte Übertragung von Push-Nachrichten zum Smartphone des Benutzers (Default)
- Nicht hinterlegten Zertifikaten wird nicht vertraut
- Protokollieren von Benutzer-Logins deaktiviert (Default). Ausnahme: Fehlerhafter Login
- Bei NFR-Lizenz: Übertragen Daten enthalten keine personenbezogenen Daten
- Portal-Administrationsrechte individuell einstellbar. Default: Benutzer haben keine Rechte
- Applikations-Nutzungsrechte individuell einstellbar. Default: Benutzer haben keine Rechte
- Prozess zur automatisierten Deaktivierung von Benutzerzugängen möglich
- Löschen eines Benutzers: Löschen oder Anonymisieren der personenbezogenen Daten
- Möglichkeit die Authentifizierung der Benutzer von einem externen Verzeichnisdienst übernehmen zu lassen
- Passwort-Komplexitätsvoraussetzungen einstellbar