WHITE PAPER

Informationssicherheit und Datenschutz bei Asana

So schützt Asana Ihre Daten

asana

Inhaltsübersicht

Letzte Aktualisierung: Februar 2020[1]

[1] Dieses White Paper beschreibt den derzeitigen Stand der Informationssicherheit bei Asana, der sich mit zukünftigen Funktions- und Produkteinführungen ändern kann.

Einleitung

Unternehmen auf der ganzen Welt setzen heutzutage neue Tools ein, um ihre Arbeit auf kollaborative und flexible Weise zu verwalten und zu organisieren – von täglichen Aufgaben bis hin zu strategischen Vorhaben. Diese Tools fallen unter eine neue Kategorie von Software, die als Arbeitsmanagement-Lösungen bekannt sind und Asana ist ein führender Anbieter in dieser Kategorie.

Asana hilft Teams wie Ihrem, ihre Arbeit zu planen, zu organisieren und durchzuführen, damit sie schneller geschäftliche Ergebnisse erzielen. Mehr als 75.000 zahlende Unternehmen und Millionen von Kunden in 190 Ländern nutzen Asana, um die Übersichtlichkeit und Einheitlichkeit in ihren Teams zu fördern. Sie erreichen dies, indem sie mithilfe von Asana dafür sorgen, dass alle Teammitglieder stets wissen, welche Arbeit zu erledigen ist, wer sie erledigt und wann diese Arbeiten fällig sind. Über 1 Milliarde Aufgaben wurden in Asana bereits erstellt.

Kunden vertrauen Asana ihre Daten an, damit sie sich auf solche Arbeiten konzentrieren können, die für ihr Unternehmen am wichtigsten sind. Deshalb konzentrieren wir uns nicht nur auf die Entwicklung einer einfach zu bedienenden kollaborativen Arbeitsmanagement-Lösung, sondern auch auf die Sicherheit der Daten unserer Kunden.

Bei Asana fördern wir das Sicherheitsbewusstsein aller Mitarbeiter durch unsere Unternehmenskultur. Unsere Kultur des Vertrauens und der Transparenz prägt die grundlegende Einstellung, das Bewusstsein und das Verständnis für die Wichtigkeit des Schutzes von Informationen unserer Kunden. Durch Richtlinien, Verhaltenskodizes und gemeinsame Leitbilder, die von unserem Führungsteam kommuniziert werden, wird dieses Bewusstsein in unseren Werten und Verhaltensstandards gestärkt. Unser Führungsteam ergreift außerdem alle nötigen Maßnahmen, um ein Umfeld zu schaffen, welches das Übernehmen und Überlassen der vollen Verantwortung fördert.

Bei der Gestaltung und Umsetzung unserer Sicherheitsstrategie und -praktiken lassen wir uns von den folgenden Grundsätze leiten:

- Physische und räumliche Sicherheit zum Schutz unserer Web- und mobilen Anwendungen vor unbefugtem Zugriff
- Gewährleistung der Verfügbarkeit unserer Anwendungen
- Vertraulichkeit zum Schutz von Kundendaten
- Integrität zur Aufrechterhaltung der Genauigkeit und Konsistenz der Daten während ihres gesamten Lebenszyklus

In diesem White Paper behandeln wir die Themen Informationssicherheit und Datenschutz unter den folgenden Aspekten: Infrastruktur, Produkt, operative Abläufe, Compliance und Zertifizierungen.

Auch wenn der größte Anteil dieses White Papers auf alle Asana-Pakete angewendet werden kann, bezieht es sich vor allem auf kostenpflichtige Asana-Pakete: Premium, Business und Enterprise.[2] Wenn über eine Funktion gesprochen wird, die nicht für alle Pakete verfügbar ist, wird entsprechend darauf hingewiesen.

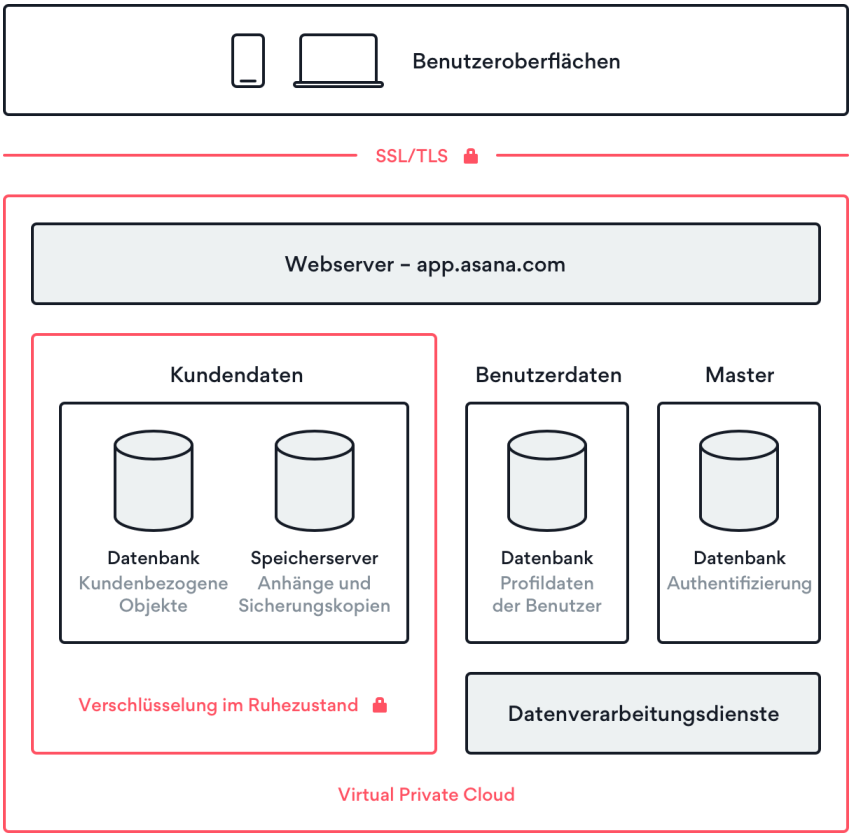
[2] Weitere Informationen über alle Asana-Pakete finden Sie unter asana.com/pricing.

Infrastruktur

Asana nutzt Angebote von Cloud Computing Services als Kernbausteine der Asana-Plattform, hauptsächlich von Amazon Web Services (AWS).

AWS verwaltet die Sicherheit und Compliance der Cloud-Computing-Infrastruktur, und Asana verwaltet die Sicherheit und Compliance der Software und sensibler Daten, die sich in der Cloud-Computing-Infrastruktur befinden. Bitte beachten Sie das Modell der geteilten Verantwortung (Shared Responsibility Model) von AWS.[3]

Asana verwendet die Virtual Private Cloud von Amazon und hat die Netzwerkarchitektur so konzipiert, dass sie sicher, skalierbar und einfach zu verwalten ist, indem sie die von AWS bereitgestellten Netzwerkdienste und Bausteine verwendet. *Elastic Compute Cloud* (EC2) Services von Amazon betreiben den Großteil der Asana-Plattform und bieten eine zuverlässige, skalierbare und sichere Möglichkeit zur Verarbeitung von Kundendaten. Im Folgenden wird eine vereinfachte Übersicht der Infrastruktur von Asana dargestellt.



[3] http://aws.amazon.com/compliance/shared-responsibility-model
* Verschlüsselung findet nur für Enterprise-Kunden statt.

Unsere Production-Infrastruktur ist so ausgelegt, dass nur unsere Load Balancer externen Webverkehr empfangen dürfen. Jedem Host ist eine Rolle zugeordnet und es werden Sicherheitsgruppen verwendet, um den erwarteten Datenverkehr zwischen diesen Rollen zu definieren.

Webserver

Das CloudFront Content Delivery Network (CDN) von Amazon wird verwendet, um die statischen Elemente von Asana skalierbar mit geringer Latenz und hohen Übertragungsgeschwindigkeiten bereitzustellen.

Datenbanken

Datenbanken laufen über den Relational Database Service (RDS) von Amazon, unter Verwendung einer Managed-MYSQL-Datenbank.

Master

Speichert verschlüsselte Passwörter (Hash und Salt per bcrypt) und Authentifizierungsinformationen für die verschiedenen Nutzer.

Kundendaten

Speichert alle Informationen, die von Kunden zu Asana hochgeladen wurden, einschließlich Teams, Projekte und Aufgaben.

Nutzerdaten

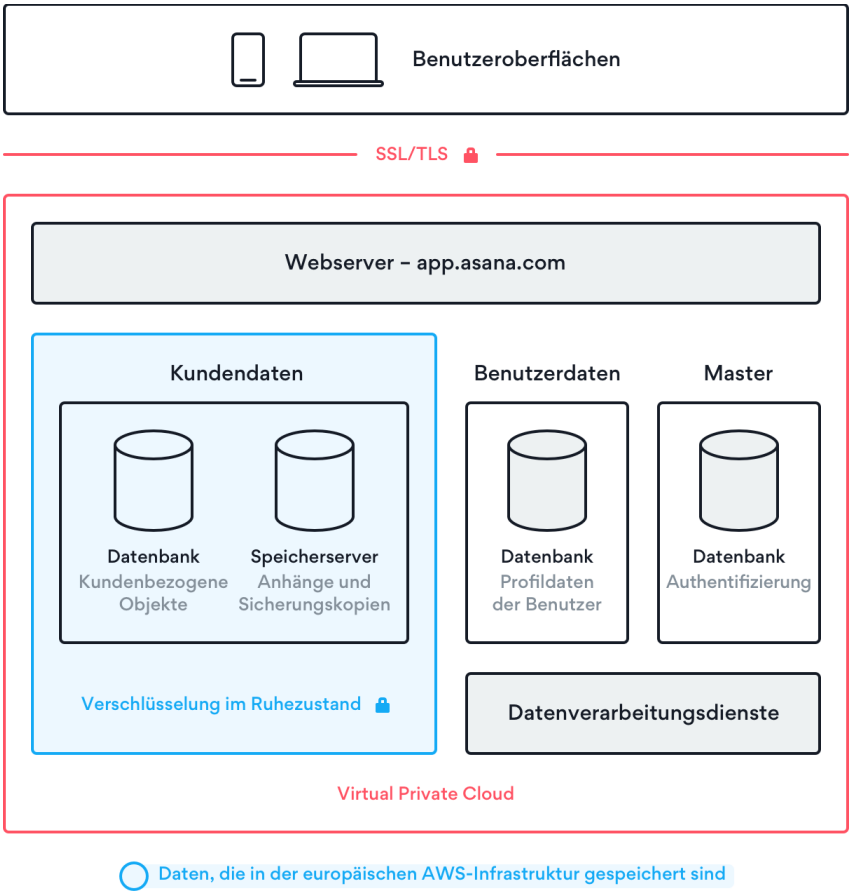
Speichert Informationen von Benutzerprofilen wie Name und E-Mail-Adresse.

Datenspeicherung

Server zur Datenspeicherung sind Simple Storage Service (S3) von Amazon. Sie speichern Anhänge und Datenbanksicherungskopien. Anhänge sind alle Dateien, die direkt von einem Computer zu Asana-Aufgaben hochgeladen werden. Anhänge, die von Cloud-gehosteten Kollaborationsplattformen für Inhalte stammen, werden als Links zu diesen Plattformen erstellt, aber nicht auf den Datenservern von Asana gespeichert.

Europäische Infrastruktur

Asana bietet seinen Enterprise-Kunden, die ihre Daten in Europa aufbewahren müssen, europäische Rechenzentren an. Die Kundendaten werden in der AWS-Region Frankfurt (Deutschland) gespeichert, wobei die Sicherungskopien in der AWS-Region Dublin (Irland) gespeichert werden. Die AWS-Einrichtungen werden sowohl für die US- als auch für die EU-Infrastruktur genutzt. Die Kundendaten des gesamten Unternehmens werden je nach Kundenwunsch entweder in den USA oder in der EU gespeichert. Die folgende Übersicht ist eine vereinfachte Darstellung der Infrastruktur von Asana für Kunden, die die europäische Infrastruktur nutzen.



Datensicherheit

Verschlüsselung während der Übertragung

Die Verbindungen zu app.asana.com sind mit einer 128-Bit-Verschlüsselung verschlüsselt und unterstützen TLS 1.2 und höher. Die Verbindungen werden mit AES_128_GCM verschlüsselt und authentifiziert und verwenden ECDHE_RSA als Austauschmechanismus für Keys. Asana unterstützt Forward Secrecy und AES-GCM und lässt keine unsicheren Verbindungen zu, die RC4 oder SSL 3.0 und darunter verwenden. Anmeldungen und sensible Datenübertragungen erfolgen ausschließlich über TLS/SSL.

Verschlüsselung im Ruhezustand

Für Enterprise-Kunden garantiert Asana die Verschlüsselung der Kundendaten im Ruhezustand mit AES 256 Bit geheimen Keys.

Multi-Tenancy

Die Infrastruktur wird von verschiedenen Kundeninstanzen gemeinsam genutzt, daher ist Asana eine mandantenfähige Webanwendung. Kontoauthentifizierung, logische Trennung von Datenbankfeldern und Funktionen zur Sitzungsverwaltung wurden implementiert, um den Kundenzugriff auf die mit dem jeweiligen Unternehmen verbundenen Daten zu beschränken.

Skalierung & Zuverlässigkeit

Asana verwendet Amazon Web Services, welche die Skalierbarkeit des Dienstes gewährleisten. Die Datenbank wird synchron repliziert, so dass wir diese nach einem Datenbankausfall schnell wiederherstellen können. Als zusätzliche Vorsichtsmaßnahme erstellen wir regelmäßig ein Abbild der Datenbank und verschieben dieses sicher in ein separates Rechenzentrum. Auf diese Weise können wir es bei Bedarf an anderer Stelle wiederherstellen, auch im Falle eines regionalen Amazon-Ausfalls.

Systemverfügbarkeit

Die Service-Verfügbarkeit ist für unsere Enterprise-Kunden zu 99,9 % gewährleistet.

Vertrauensseite

Vertrauen muss man sich verdienen, und wir glauben, dass es mit der transparenten Einsicht in den Status und die Leistung unseres Systems beginnt. Die Asana-Vertrauensseite zeigt die Verfügbarkeit der Web-App, mobilen App und API in den letzten 12 Stunden, 7 Tagen, 30 Tagen und im letzten Jahr an. Besuchen Sie trust.asana.com.

Backups

Es werden täglich Abbilder der Datenbank erstellt. Backups haben den gleichen Schutz wie „In-Production"-Datenbanken. Für Enterprise-Kunden garantieren wir die überregionale Speicherung von Backups.

Produktsicherheitsfunktionen

Asana bietet seinen Nutzern und Administratoren die notwendigen Funktionen zum Schutz ihrer Daten. Diese Funktionen bieten eine umfassende administrative Kontrolle und Einsicht in die Daten des Kunden. Die Verfügbarkeit der folgenden Funktionen variiert je nach Asana-Paket. Unsere Pakete finden Sie unter asana.com/pricing.

Administratoren

Administratoren können Teams verwalten, um Mitglieder und Gäste hinzuzufügen und zu entfernen, wenn diese dem Unternehmen oder einem Arbeitsbereich beitreten oder dieses/diesen wieder verlassen. Sie können auch unsere Admin-API verwenden, um Domain-Exporte, Konfigurationen, Berechtigungen, Anwendungen von Drittanbietern sowie Team- und Benutzereinstellungen zu verwalten.

Provisionierung und Deprovisionierung von Nutzern

Asana gibt seinen Nutzern und Administratoren die Kontrolle darüber, wer Zugriff auf ihre Daten hat.

- Nutzer und Administratoren können Mitglieder und Gäste (externe Mitglieder) zu ihren Unternehmen und Teams einladen.
- Administratoren können jeden dieser Nutzertypen mithilfe der Admin-Konsole entfernen.

Darüber hinaus können Enterprise-Kunden Asana mit ihrem Cloud-Identitätsanbieter über den SCIM-Standard (System for Cross-domain Identity Management) integrieren, um Nutzer zusammen mit anderen SaaS-Lösungen hinzuzufügen und zu entfernen.

Login-Sicherheit

Administratoren von Asana können entscheiden, mit welchem Mechanismus sich die Nutzer bei ihren Asana-Konten anmelden dürfen. Dafür gibt es drei verschiedene Möglichkeiten: persönliche Anmeldedaten für Asana, Google SSO oder Single Sign-On über SAML 2.0.

Passwortschutz

Wenn sich Nutzer mit ihren persönlichen Anmeldedaten in ihren Konten anmelden dürfen, können Administratoren angeben, welche Stärke ihre Passwörter aufweisen müssen. Wenn Sie „starke" Passwörter benötigen, müssen die Passwörter aus mindestens 8 Zeichen bestehen und drei der folgenden Zeichenarten enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.

Administratoren können auch das Zurücksetzen des Passworts für alle Nutzer im Unternehmen erzwingen.

Google SSO

Administratoren können von den Nutzern eines Unternehmens verlangen, dass sie sich mit ihrem Google G Suite-Konto bei Asana anmelden.

Single Sign-On per SAML

Unternehmensadministratoren können ihren Identitätsanbieter konfigurieren und die Nutzer auffordern, sich mit ihren Cloud IdP-Anmeldedaten bei Asana anzumelden. Dies wird über den SAML-Authentifizierungsstandard konfiguriert.

Zugriffsberechtigungen

Administratoren und Nutzer können andere Nutzer einladen und ihre Daten mit diesen teilen. Wenn Nutzer eingeladen werden, einem Unternehmen beizutreten, können sie verschiedene Berechtigungen für den Zugriff erhalten. Nutzer können auf Objektebene (Aufgabe, Projekt, Team oder Unternehmen) mit unterschiedlichen Zugriffsarten eingeladen werden. Berechtigungen werden für den Nutzer nicht auf Nutzerebene, sondern auf Objektebene definiert. Das bedeutet, dass ein einzelner Nutzer bestimmte Inhalte an einer Stelle vielleicht nur kommentieren kann, an anderer Stelle einige Inhalte vollständig vor ihm verborgen sind, einige Inhalte auf Anfrage bereitgestellt werden können und einige komplett zur Verfügung stehen. Weitere Details zu jedem Objekt und jeder Art von Berechtigungen finden Sie in unserem Asana-Handbuch: asana.com/de/guide.

Objekte bei Asana

Aufgaben

Aufgaben in Asana können privat oder sichtbar sein und sich in einem privaten oder in einem sichtbaren Projekt befinden.

Aufgabe:	**Zugänglich für:**
Private Aufgabe	Nur Aufgabenbeteiligte
Sichtbare Aufgabe	Alle Unternehmensmitglieder
Aufgabe in einem privaten Projekt	Aufgabenbeteiligte und Projektmitglieder
Aufgabe in einem sichtbaren Projekt	Aufgabenbeteiligte, Projekt- und Teammitglieder
Unteraufgaben	Aufgabenbeteiligte und diejenigen, die Zugriff auf die übergeordnete Aufgabe haben

Projekte

Projekte in Asana können privat oder sichtbar sein. Wenn eine Person Zugriff auf ein Projekt hat, kann sie ebenfalls auf alle Aufgaben und Diskussionen innerhalb dieses Projekts zugreifen. Wenn neue Nutzer einem Projekt hinzugefügt werden, erhalten sie entweder die Kommentar- oder die Bearbeitungsberechtigung.

Projekt:	Zugänglich für:
Privates Projekt	Projektmitglieder
Sichtbares Projekt	Team- und Projektmitglieder
Sichtbares Projekt in einem sichtbaren Team	Unternehmens-, Team- und Projektmitglieder

Teams

Teams in Asana können privat oder sichtbar sein oder die Mitgliedschaft per Anfrage zulassen. Wenn eine Person zu einem Team gehört, hat sie Zugriff auf alle Teamdiskussionen und sichtbaren Projekte innerhalb dieses Teams.

Team:	Zugänglich für:	Beitritt:
Verborgen	Teammitglieder	Nein
Sichtbar im Unternehmen	Team- und Unternehmensmitglieder	Ja
Mitgliedschaft auf Anfrage	Teammitglieder	Nach Bestätigung

Unternehmen

Ein Unternehmen ist in Asana das Objekt der höchsten Ebene und enthält Teams, Projekte und Aufgaben.

Nutzer

Die Nutzer in Asana erhalten individuelle Konten, die mit ihrer E-Mail-Adresse verknüpft sind. Wie oben erwähnt, kann ein Konto die Zugriffsberechtigung auf verschiedene Datenobjekte erhalten. Außerdem erhalten Nutzerkonten standardmäßig automatischen Zugriff auf ein Unternehmen, basierend auf ihrer jeweiligen E-Mail-Domain.

Vollmitglieder

Die Mitgliedschaft in einem Unternehmen basiert auf der Domain, die in Ihrer E-Mail-Adresse erscheint. Um Mitglied in einem Unternehmen zu werden, müssen Sie über eine E-Mail-Adresse in einer der zugelassenen E-Mail-Domains Ihres Unternehmens verfügen.

Unternehmensmitglieder können:

- Neue Teams erstellen
- Die vollständige Liste der Teams innerhalb des Unternehmens einsehen, denen sie eine Beitrittsanfrage senden können
- Namen und E-Mail-Adressen der anderen Mitglieder und Gäste im Unternehmen einsehen
- Auf Projekte und Aufgaben zugreifen, die innerhalb des Unternehmens sichtbar und zugänglich gemacht wurden

Gäste

Sie können auch mit Klienten, Auftragnehmern, Kunden oder anderen Personen zusammenarbeiten, die über keine E-Mail-Adresse in einer genehmigten E-Mail-Domain des Unternehmens verfügen. Diese Personen werden dann zu Unternehmensgästen. Gäste haben in Ihrem Unternehmen beschränkten Zugriff und können nur sehen, was explizit mit ihnen geteilt wird.

Ein Unternehmensgast kann nur dann einem Team beitreten, wenn er eingeladen wird. Gäste können keine Teams erstellen, einsehen oder Beitrittsanfragen an weitere Teams senden.

Mitglieder mit Zugriff auf spezifische Projekte

Jedes Team hat seine eigenen Mitglieder und Projekte. Nutzer, die nicht auf alle Projekte in einem Team zugreifen können, werden im Tab „Mitglieder" in den Teameinstellungen als Mitglieder mit Zugriff auf spezifische Projekte angezeigt.

Mitglieder mit Zugriff auf spezifische Projekte können Projekte und Aufgaben sehen, zu denen sie hinzugefügt wurden, aber keine Diskussionen oder andere Projekte des Teams.

Gästeverwaltung

Administratoren von Enterprise-Konten können entscheiden, wer externe Mitglieder (Gäste) einladen darf. Dafür stehen ihnen diese drei Optionen zur Verfügung:

- Nur Administratoren
- Administratoren und Unternehmensmitglieder
- Alle (dazu gehören sowohl die Mitglieder als auch die Gäste des Unternehmens)

Zulassung von Apps

Administratoren von Enterprise-Konten können entscheiden, welche Integrationen von Drittanbietern ihre Nutzer mit ihren Asana-Konten verwenden können und alle unerwünschten Integrationen blockieren. Unter asana.com/apps erfahren Sie, welche Anwendungen von Drittanbietern verfügbar sind.

Datenkontrolle

Kunden können ausgewählte Daten aus Asana bequem exportieren oder löschen und komplette Domain-Exporte über unsere API automatisieren.

Anwendungssicherheit

Asana ist eine webbasierte Software-as-a-Service-Anwendung. Nutzer können über einen Webbrowser, eine mobile Anwendung (Android und iOS) oder eine Schnittstelle zur Programmierung von Anwendungen (API) auf ihre Daten zugreifen.

Die in Asana enthaltenen Dienste und Komponenten sind hauptsächlich in JavaScript, TypeScript, Python und Scala geschrieben, basierend auf dem React Application Framework. Asana wird in Anlehnung an die von der OWASP Foundation definierten Best Practices in puncto Sicherheit entwickelt und verfolgt jederzeit einen Security by Design-Ansatz. Daher haben wir umfassende Mechanismen zur Vermeidung von Sicherheitsrisiken implementiert, einschließlich, aber nicht beschränkt auf die folgenden Themen:

- Injection
- Broken Authentication
- Gefährdung sensibler Daten
- XML Externe Entitäten (XXE)
- Broken Access Control
- Sicherheits-Fehlkonfiguration
- Cross-Site Scripting (XSS)
- Unsichere Deserialisierung
- Verwendung von Komponenten mit bekannten Schwachstellen
- Unzureichendes Logging und Monitoring
- Cross-Site Request Forgery (CSRF)
- Nicht validierte Um- und Weiterleitungen

Asana unterzieht sich für die 10 wichtigsten von der OWASP genannten Probleme einem jährlichen Audit.

Asana-Plattform

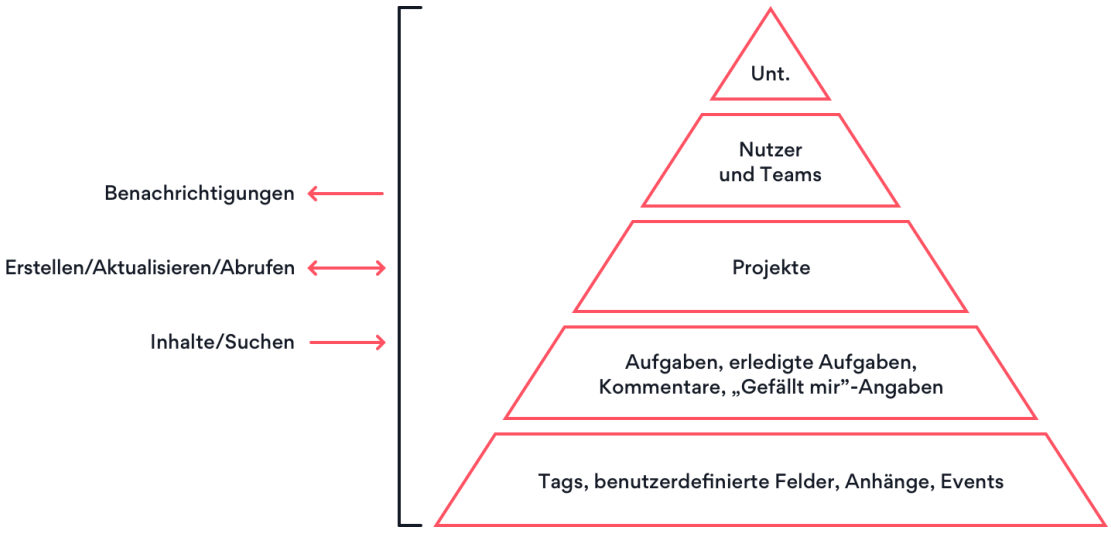
Integrationen

Asana ermöglicht seinen Nutzern den Zugriff auf ihre Konten über die Anwendungsschnittstelle (API). Die Asana-API ist eine „RESTful"-Schnittstelle, mit der Sie einen Großteil Ihrer Daten auf der Plattform programmgesteuert aktualisieren und darauf zugreifen sowie automatisch reagieren können, wenn sich etwas ändert. Sie stellt vorhersagbare URLs für den Zugriff auf Ressourcen zur Verfügung und verwendet integrierte HTTP-Funktionen, um Befehle zu empfangen und Antworten zu senden. Dies erleichtert die Kommunikation mit Asana in einer Vielzahl von Umgebungen, von Befehlszeilenprogrammen über Browser-Plugins bis hin zu nativen Anwendungen. Kunden können diese APIs verwenden, um kundenspezifische Lösungen zu erstellen oder Integrationen mit anderer Software zu ermöglichen. Asana unterstützt ein OAuth 2.0 oder Personal Access Token als Authentifizierungsmethode für die API.

Um mehr über die API von Asana zu erfahren, besuchen Sie asana.com/developers.

Die folgende Abbildung zeigt eine Zusammenfassung der ausführbaren Aktionen und Objekte, mit denen gearbeitet werden kann.

Standardmäßig hat jede Software oder jedes Skript die gleichen Berechtigungen wie der Nutzer, der sie



ausführt. Daher können nur die Daten bearbeitet werden, auf die der Nutzer Zugriff hat. Wenn zusätzliche Zugriffsrechte erforderlich sind, können Enterprise-Kunden Servicekonten nutzen. Weitere Details finden Sie weiter unten.

Servicekonten

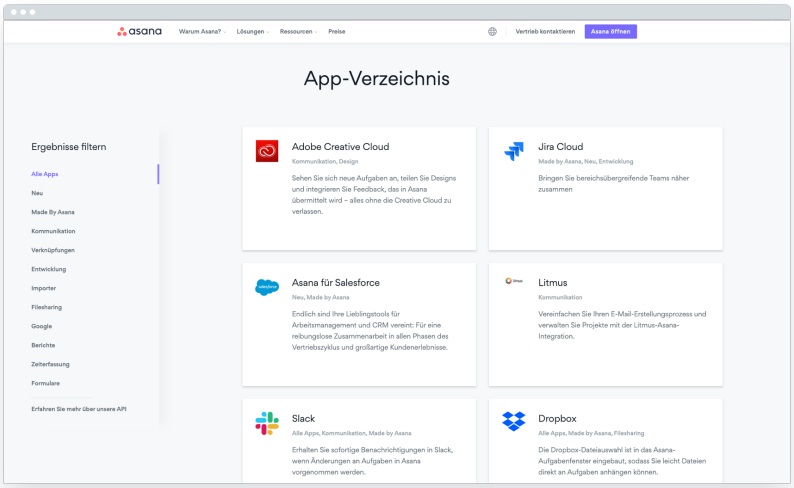
Asana Enterprise-Kunden können über Servicekonten auf alle ihre Inhalte zugreifen. Beispielsweise können sie mit diesen einen vollständigen Export von Unternehmensdaten durchführen oder die Teamaktivitäten nachverfolgen.

Anwendungen von Drittanbietern

Die API von Asana ermöglicht Hunderte Out-of-the-Box-Integrationen, mit denen Kunden ihre Asana-Anwendung erweitern oder ergänzen können. Asana lässt sich in viele Google- und Microsoft-Tools integrieren, um die Workflows der Kunden zu optimieren und die Produktivität zu steigern. Drittanbieter-Tools anderer Anbieter können ebenfalls integriert werden. Die Funktionen dieser Drittanbieter-Tools sind:

- Synchronisierung von Nachrichten zwischen verschiedenen Apps
- Workflow-Automatisierung
- Plattformerweiterungen
- Softwareentwicklung
- Datenimport
- Filesharing
- Berichte
- Zeiterfassung
- Datenerfassung

Ein Verzeichnis der Anwendungen von Drittanbietern finden Sie unter asana.com/apps.



Operative Sicherheit

Informationssicherheit bei Asana

Asana betreibt ein offizielles Programm zur Steuerung der Informationssicherheit, wobei das Sicherheitspersonal dem Chief Information Security Officer (CISO) von Asana untersteht. Diese Organisation ist mit der Durchführung von Sicherheitskontrollen und der Überwachung von Asana auf schädigende Aktivitäten beauftragt.

Vertrauliche Informationen

Asana behandelt alle Kundendaten unabhängig von der Klassifizierung als vertraulich. Durch diese Richtlinie dürfen nur diejenigen Mitarbeiter auf vertrauliche Informationen zugreifen, die im Rahmen ihrer Tätigkeit mit diesen Daten arbeiten und somit darauf zugreifen müssen. In diesen Fällen wird der Mitarbeiter angewiesen, nur auf ein Minimum an vertraulichen Informationen zuzugreifen, die zur Erfüllung der jeweiligen Aufgabe erforderlich sind.

Personalwesen

Alle Mitarbeiter oder Auftragnehmer von Asana sind verpflichtet, eine Vertraulichkeits- und Abtretungsvereinbarung zu unterzeichnen und bei der Einstellung und danach jährlich eine formelle Schulung zum Thema Sicherheitsbewusstsein zu absolvieren.

Alle unsere Entwickler unterzeichnen eine Vereinbarung über den Datenzugriff und durchlaufen vor ihrer Anstellung bei Asana eine Hintergrundprüfung. Darüber hinaus verfügen wir über Gateways für alle Zugangspunkte zu Kundendaten; jeder Datenzugriff wird protokolliert und unbegrenzt aufbewahrt.

Asana verfügt über eine Disziplinar- und Sanktionsrichtlinie für jegliche Verletzungen der Datenschutz- und Sicherheitsrichtlinien.

Nutzerzugriffsüberpüfung und -richtlinie

Das Management überprüft vierteljährlich den Nutzerzugriff auf In-Scope-Systeme auf seine Angemessenheit und entfernt jeden nicht mehr benötigten Zugriff. Bei Kündigung von Mitarbeitern wird der Zugang gelöscht.

Physische Sicherheit

Büroräume von Asana

Unsere Büroräume sind durch einen protokollierten Keycard-Zugang gesichert und verfügen über Einbruchalarmanlagen. Alle Besucher werden an unserer Rezeption registriert. Alle Mitarbeiter sind verpflichtet, verdächtige Aktivitäten, unbefugten Zutritt zu Räumlichkeiten oder Diebstahl/Verlust von Objekten zu melden.

Sicherheit im Rechenzentrum

Asana verlässt sich auf die erstklassigen physischen und umgebungsbezogenen Kontrollen von AWS.[4]

Netzwerksicherheit

Wir überwachen die Verfügbarkeit unseres Büronetzwerks und seiner Geräte. Wir dokumentieren Logs von Netzwerkgeräten wie Firewalls, DNS-Servern, DHCP-Servern und Routern zentral. Die Netzwerklogs werden für Sicherheitsanwendungen (Firewall), Wireless Access Points und Switches gespeichert.

IT-Sicherheit

Alle Laptops und Workstations sind durch eine vollständige Festplattenverschlüsselung gesichert und werden über ein zentral verwaltetes Image bereitgestellt. Wir führen gewissenhaft Updates auf den Rechnern der Mitarbeiter durch und überprüfen die Arbeitsplätze der Mitarbeiter auf Malware. Wir haben auch die Möglichkeit, kritische Patches anzuwenden oder einen Rechner über den Gerätemanager ferngesteuert zu bereinigen. Wo immer möglich, verwenden wir eine zweistufige Authentifizierung, um den Zugriff auf unsere Unternehmensinfrastruktur weiter zu sichern. Asana führt regelmäßig Sicherheitsscans durch.

Risiko- und Schwachstellenmanagement

Asana verfügt über einen laufenden Risikomanagementprozess, der darauf abzielt, Schwachstellen innerhalb der Asana-Systeme proaktiv zu identifizieren und neue und neu auftretende Bedrohungen für den Unternehmensbetrieb zu bewerten.

Asana pflegt einen Scanprozess für Schwachstellen sowohl für externe als auch für interne Systeme in der Production-Umgebung. Das Sicherheitsteam von Asana führt mindestens vierteljährlich Überprüfungen durch und behebt Schwachstellen auf der Grundlage der Bewertung. Überprüfungen von Schwachstellen werden auch nach einer wesentlichen Änderung der Production-Umgebung durchgeführt, entsprechend der Anweisung des Sicherheitsleiters.

Penetrationstests

Wir arbeiten mit Sicherheitsexperten von Drittanbietern zusammen, um unseren Code auf verbreitete Sicherheitslücken zu testen und setzen Netzwerk-Scanning-Tools auf unseren Production-Servern ein. Die Penetrationstests werden jährlich durchgeführt. Bestätigte Schwachstellen werden behoben und erneut getestet.

Bug-Bounty-Programm

Wir haben ein externes Programm zum Auffinden von fehlerhaftem Code[5], in dem wir Sicherheitsexperten für die Entdeckung von Schwachstellen bezahlen.

---

[4] http://aws.amazon.com/compliance/data-center/controls

[5] http://asana.com/bounty

Software-Entwicklungszyklus

Asana verwendet das Git-Revisionskontrollsystem. Änderungen an der Codebasis von Asana durchlaufen eine Reihe von automatisierten Tests und eine manuelle Überprüfung. Wenn Code-Änderungen das automatisierte Testsystem passieren, werden die Änderungen zunächst auf einen Staging-Server übertragen, auf dem unsere Mitarbeiter die Änderungen testen können, bevor sie schließlich auf Production-Server und unsere Kundendatenbank übertragen werden. Wir führen zudem eine spezifische zusätzliche Sicherheitsüberprüfung für besonders sensible Änderungen und Funktionen durch. Entwickler bei Asana haben außerdem die Möglichkeit, wichtige Updates auszuwählen und sofort auf die Production-Server zu übertragen.

Zusätzlich zu einer Liste, in der alle Änderungen an der Zugriffskontrolle veröffentlicht werden, haben wir eine Reihe von automatisierten Komponententests, um sicherzustellen, dass die Zugriffskontrollregeln korrekt geschrieben und wie erwartet durchgesetzt werden.

Reaktion auf Zwischenfälle

Asana verfügt über einen Reaktionsplan für Zwischenfälle, der darauf abzielt, eine angemessene und konsistente Reaktion auf Sicherheitsvorfälle und vermeintliche Sicherheitsvorfälle zu etablieren. Diese umfassen die zufällige oder rechtswidrige Zerstörung, den Verlust, den Diebstahl, die Veränderung, die unbefugte Offenlegung oder den Zugriff auf geschützte Daten oder personenbezogene Daten, die von Asana übertragen, gespeichert oder anderweitig verarbeitet werden. In diesen Vorfallsreaktionsverfahren wird im Einzelnen beschrieben, wie das Asana-Sicherheitspersonal die Sicherheitsvorfälle bewertet, untersucht, behebt und über sie berichtet. Asana hat Verträge mit digitalen Forensik-Firmen und Incident Response Firmen abgeschlossen, die im Falle einer Datenschutzverletzung tätig werden.

Notfallwiederherstellung und Geschäftskontinuität

Asana hat einen Plan für die Geschäftskontinuität für ausgedehnte Serviceausfälle aufgrund unvorhergesehener oder unvermeidlicher Katastrophen erstellt, um die Dienste in einem angemessenen Zeitrahmen so weit wie möglich wiederherzustellen. Asana hat eine Reihe von Richtlinien und Verfahren zur Wiederherstellung im Katastrophenfall dokumentiert, um die Wiederherstellung oder Fortsetzung wichtiger technologischer Infrastrukturen und Systeme nach einer Katastrophe zu ermöglichen.

Die primären Rechenzentren von Asana werden auf AWS in Virginia und in Frankfurt (Deutschland) gehostet, je eins für die USA und die EU, wobei die Redundanz in derselben AWS-Region liegt.[6] Im Falle des Ausfalls eines einzelnen AWS-Rechenzentrums würden Wiederherstellungsverfahren Datenknoten in einem anderen Rechenzentrum aktivieren. Um größere Katastrophen zu vermeiden, wird eine Disaster Recovery (DR) Plattform zur Wiederherstellung im Katastrophenfall in einem AWS Rechenzentrum in Ohio (USA) oder Dublin (Irland) gehostet, jeweils für die Daten in den USA und in der EU.

[6] Multiple Availability Zone durch RDS Multi-AZ-Bereitstellung.

Datenaufbewahrung und -löschung

Datenaufbewahrung

Wir speichern Ihre Daten für den Zeitraum, der zur Erfüllung der in unserer Datenschutzerklärung genannten Zwecke erforderlich ist. Für Enterprise-Kunden löschen wir auf Wunsch ihre Domain-Daten.

Datenlöschung

Auf Wunsch des Bevollmächtigten eines Kunden kann der Kunde den Export oder die Domainlöschung von Kundendaten verlangen. Asana kann sich auch verpflichten, die Vertraulichkeit der gespeicherten Kundendaten zu wahren und wird diese Kundendaten erst nach dem Anforderungsdatum aktiv verarbeiten, um die für sie geltenden Gesetze einzuhalten.

Monitoring

Asana verwendet Amazon CloudWatch in Kombination mit benutzerdefinierten Skripten, die wichtige Daten aus Protokollen extrahieren und an seine Überwachungsdienste weiterleiten. Asana überwacht die Auslastung der physischen und computergestützten Infrastruktur sowohl intern als auch für die Kunden, um sicherzustellen, dass die Leistungserbringung den Service Level Agreements entspricht. Wir führen automatisierte Sicherheitsscans in unserem Netzwerk und unseren Anwendungen durch. Ein wöchentlich ausgeführtes Überwachungsskript validiert, ob Code-Änderungen ordnungsgemäß überprüft wurden.

Bestimmte Anwendungs- und Geräteprotokolle werden auf unbestimmte Zeit aufbewahrt und in der Regel langfristig in S3 gelagert. Ausführlichere Geräteprotokolle werden nur auf dem Gerät gespeichert, auf dem sie erzeugt wurden und in der Regel für zwei Wochen aufbewahrt.

Subunternehmen und Dienstleisterverwaltung

Asana unternimmt angemessene Schritte, um nur Drittanbieter auszuwählen und weiter mit diesen zusammenzuarbeiten, die die Sicherheitsmaßnahmen im Einklang mit unseren eigenen Richtlinien aufrechterhalten und umsetzen. Bevor eine Software implementiert wird oder ein Softwareanbieter bei Asana eingesetzt werden kann, überprüft Asana-IT sorgfältig die Sicherheitsprotokolle, Datenspeicherungsrichtlinien, Datenschutzrichtlinien und Sicherheitsnachweise des Anbieters. Die IT-Abteilung kann die Verwendung von Software oder Softwareanbietern ablehnen, wenn nicht nachgewiesen wird, dass die Daten und Endbenutzer von Asana ausreichend geschützt werden können. Es werden einmal pro Jahr Anbieterbewertungen durchgeführt.

Unsere aktuellen Subunternehmen können Sie auf unserer AGB-Seite einsehen.[7]

[7] http://asana.com/terms#subprocessors

Datenschutz, Zertifizierungen und Compliance

Datenschutzerklärung

Die Datenschutzrichtlinie von Asana finden Sie auf unserer AGB-Seite.[8] Sie beinhaltet:

- Welcher Nutzertyp bin ich und welche Datenschutzbestimmungen gelten für mich?
- Datenschutzbestimmungen für Nutzer der kostenpflichtigen Versionen
- Datenschutzbestimmungen für Nutzer der kostenlosen Version
- Datenschutzbestimmungen für Besucher der Website
- Zusätzliche Datenschutzbestimmungen für alle Benutzer
- Kontaktdaten von Asana

Zertifizierungen und Rechtskonformität

Asana wurde bezüglich mehrerer Datenschutz- und Sicherheitsstandards bewertet und hat die folgenden Zertifizierungen erhalten:

Privacy Shield Framework

Asana ist zertifiziert nach EU-U.S. Privacy Shield und Swiss-U.S. Privacy Shield Framework[9] bezüglich der Erfassung, Verwendung und Speicherung personenbezogener Daten aus den Mitgliedsstaaten der Europäischen Union bzw. der Schweiz.

Service Organization Control (SOC 2)

Asana hat das SOC 2 (Typ II)-Audit für die von uns implementierten Kontrollen in Bezug auf Sicherheit, Verfügbarkeit und Vertraulichkeit erfolgreich abgeschlossen. Die Erlangung der SOC 2 (Typ II)-Zertifizierung bedeutet, dass wir Prozesse und Praktiken in Bezug auf diese drei Kontrollprinzipien etabliert haben, die von einem unabhängigen Dritten validiert wurden.

[8] http://asana.com/terms#privacy-policy

[9] https://www.privacyshield.gov/participant?id=a2zt0000000TNLRAA4&contact=true

DS-GVO

Die Datenschutzgrundverordnung („DS-GVO“) ist ein europäisches Gesetz zum Schutz der personenbezogenen Daten von EU-Bürgern, das am 25. Mai 2018 in Kraft getreten ist. Nach der DS-GVO müssen Unternehmen, die personenbezogene Daten von EU-Bürgern erheben, aufbewahren, verwenden oder anderweitig verarbeiten (unabhängig vom Standort des Unternehmens), bestimmte Datenschutz- und Sicherheitsvorkehrungen für diese Daten treffen. Asana hat ein umfassendes Programm zur DS-GVO-Konformität eingerichtet und ist bestrebt, mit seinen Kunden und Anbietern bei den Bemühungen zur DS-GVO-Konformität zusammenzuarbeiten. Einige wichtige Schritte, die Asana unternommen hat, um seine Praktiken an die DS-GVO anzupassen, sind unter anderem:

- Überarbeitung unserer Richtlinien und Verträge mit unseren Partnern, Anbietern und Nutzern
- Verbesserung unserer Sicherheitspraktiken und -verfahren
- Genaue Überprüfung und Zuordnung der Daten, die wir erheben, verwenden und weitergeben
- Erstellung einer stabileren internen Datenschutz- und Sicherheitsdokumentation
- Schulung der Mitarbeiter in Bezug auf die DS-GVO-Anforderungen und optimale Vorgehensweisen für Datenschutz und Sicherheit im Allgemeinen
- Sorgfältige Bewertung und Aufbau der Richtlinien und des Reaktionsprozesses bezüglich der Rechte von betroffenen Personen. Nachfolgend finden Sie weitere Details zu den Kernbereichen des DS-GVO-Konformitäts-Programms von Asana und wie Kunden ihre eigenen Initiativen zur DS-GVO-Konformität durch den Einsatz von Asana unterstützen können.

Datenverarbeitungsvereinbarung

Nach der DS-GVO sind „Datenverantwortliche“ (d. h. Instanzen, die den Zweck und die Art und Weise der Datenverarbeitung bestimmen) verpflichtet, Vereinbarungen mit anderen Instanzen zu treffen, die in ihrem Namen Daten verarbeiten (sogenannte „Datenverarbeiter“). Asana bietet seinen Kunden, die für die Verarbeitung personenbezogener Daten aus der EU verantwortlich sind, die Möglichkeit, ein solides Datenverarbeitungsabkommen zu schließen, in dem sich Asana verpflichtet, personenbezogene Daten gemäß den Anforderungen der DS-GVO zu verarbeiten und zu schützen. Dazu gehört auch die Verpflichtung von Asana, personenbezogene Daten in Übereinstimmung mit den Anweisungen des Datenverantwortlichen zu verarbeiten. Die Datenverarbeitungsvereinbarung finden Sie auf unserer AGB-Seite.[10]

Strafverfolgung

Asana befolgt die Richtlinien für die Anforderung von Daten zur Strafverfolgung, die auf unserer AGB-Seite aufgeführt sind.[11]

[10] http://asana.com/terms#data-processing

[11] http://asana.com/terms#law-enforcement-guidelines

Fazit

Wir verwenden Asana jeden Tag, damit unser Team organisiert, vernetzt und ergebnisorientiert arbeiten kann. Die Gewährleistung der Sicherheit unserer Plattform ist entscheidend für den Schutz unserer eigenen Daten und der Informationen unserer Kunden. Das hat für uns höchste Priorität.

Unser Ziel ist es, eine führende Position auf dem Markt für kooperatives Arbeitsmanagement einzunehmen, indem wir Asana benutzerfreundlich gestalten und gleichzeitig den Datenschutz als oberstes Gebot betrachten. Wenn Sie mehr über die kostenpflichtigen Angebote von Asana erfahren möchten, wenden Sie sich an unser Vertriebsteam unter sales@asana.com.

Möchten Sie uns über eine Sicherheitslücke informieren? Senden Sie eine E-Mail an security@asana.com.