monday.com Whitepaper: Sicherheit und Datenschutz

Datum	Version	Beschreibung der Änderung
November 2021	1.0	Endgültige Version

Dieses Whitepaper soll einen Überblick über die Sicherheits- und Datenschutzpraktiken von monday.com geben, die zum Zeitpunkt der Veröffentlichung dieses Whitepapers bestehen und die sich jederzeit ohne vorherige Ankündigung ändern können. Jegliche Beschreibung von Zukunftsplänen kann nach eigenem Ermessen von monday.com geändert oder verschoben werden. Dieses Whitepaper dient nur zu Informationszwecken und stellt keine Rechtsberatung dar und ist nicht als Ergänzung oder Bestandteil von Vertragsbedingungen zu betrachten.

Inhaltsverzeichnis

1. Einleitung

Das Work OS monday.com verwaltet die Daten von mehr als 127.000 Unternehmen auf der ganzen Welt und mit dieser Verantwortung verpflichten wir uns, unseren Kunden die höchsten Sicherheits- und Datenschutzstandards zu bieten. Wir verdienen uns das Vertrauen unserer Kunden, indem wir die Datensicherheit zu unserer obersten Priorität machen.

Unser Unternehmensleitbild

Wir möchten unseren Kunden ein sicheres Gefühl geben, während sie ihre Daten auf monday.com Work OS verwalten.

Unsere Teams

Die Bemühungen von monday.com im Bereich der Informationssicherheit werden von unserem CISO und unserem Sicherheitsteam sowie einem Sicherheitsforum, das sich aus Vertretern der Infrastruktur-, F&E-, Betriebs- und IT-Teams zusammensetzt, geleitet und überwacht.
Die Datenschutzbemühungen von monday.com werden von unserem Datenschutzforum, das sich aus Vertretern der Rechts-, Datenschutz- und Sicherheitsteams zusammensetzt und von unserem Datenschutzbeauftragten geleitet wird, gesteuert und überwacht.

Nützliche Links

Das Trustcenter von monday.com
Das Rechtsportal von monday.com
Die Statusseite von monday.com
Unterauftragsverarbeiter, Tochtergesellschaften und Support
Sicherheit und Datenschutz bei monday.com – FAQ
Schwachstellen melden
Support und Wissensdatenbank
Preise und Tarife
monday.Engineering Blog

---

2. Infrastruktursicherheit

Hosting-Anbieter

Um eine hohe Verfügbarkeit und Stabilität zu erzielen, wird unser Service auf der Infrastruktur von Amazon Web Services (AWS) in mehreren Regionen gehostet, vornehmlich in Nord-Virginia (USA) und Frankfurt (Deutschland)[1], und zwar in mehreren Verfügbarkeitszonen, wobei in verschiedenen Regionen spezielle Disaster-Recovery (DR)-Einrichtungen etabliert sind. Die Kundenkonten sind an eine einzige Region gebunden.

Beim AWS-Modell der gemeinsamen Verantwortung verwaltet AWS die Sicherheit der Cloud-Computing-Infrastruktur, während monday.com die Sicherheit der Software und der Daten, die sich in der Cloud-Computing-Infrastruktur befinden, verwaltet.

Unsere Aktivitätsprotokollfunktion (wie weiter unten in diesem Dokument beschrieben) sichert die Daten auf der Google Cloud Platform (GCP) in den USA.

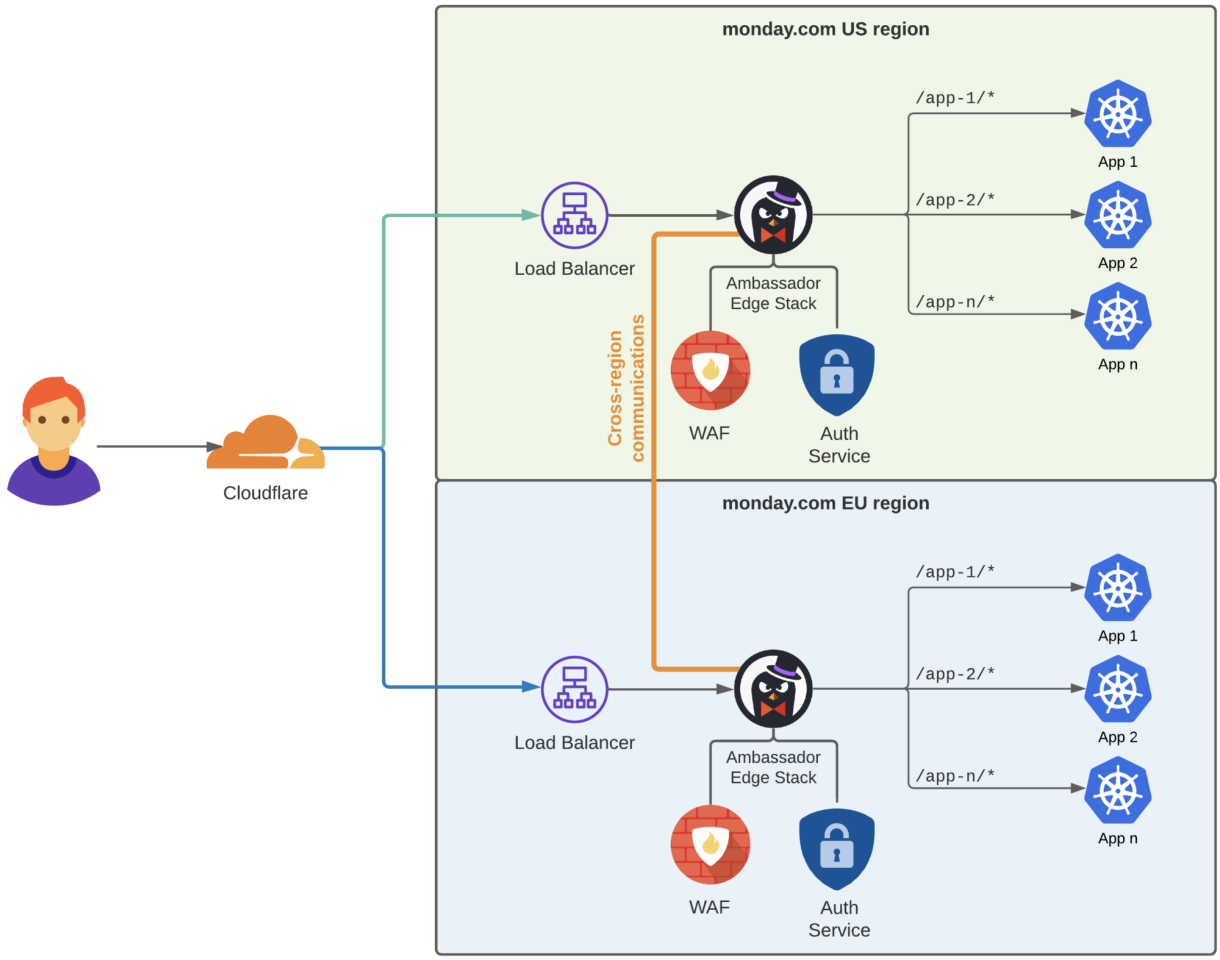
Netzwerkarchitektur

- Die Netzwerkarchitektur von monday.com ist nach den bewährten AWS-Verfahren aufgebaut, einschließlich der Trennung von öffentlichen und privaten Subnetzen.
- monday.com nutzt mehrere CDN-Anbieter, darunter Cloudflare und Fastly, um DDoS- und Brute-Force-Angriffe zu verhindern. Die Begrenzung der Übertragungsrate ist sowohl am Rand als auch auf der Anwendungsebene konfiguriert.
- Load Balancer befinden sich im öffentlichen Subnetz, während interne Netzwerkkomponenten wie die Webanwendungsserver und Datenbanken im privaten Subnetz untergebracht sind und ihnen keine öffentlichen IPs zugewiesen sind.
- Eine Web Application Firewall (WAF) ist für die inhaltsbasierte dynamische Angriffsabwehr vorhanden.
- Firewalls werden im gesamten Netzwerk eingesetzt, um IP-Whitelisting und den Zugriff auf Netzwerkressourcen nur über zugelassene Ports zu erzwingen. Die Regeln für Sicherheitsgruppen sind so konfiguriert, dass der Zugriff nur über die erforderlichen Ports möglich ist.
- Angriffserkennungssensoren im Netzwerk (NIDS-Sensoren) werden in Verbindung mit nativen AWS-Sicherheitsservices verwendet, die für alle Produktionsressourcen aktiviert sind.

Im Folgenden werden die Highlights des Netzwerkdiagramms von monday.com sowohl für die US-Datenregion als auch für die EU-Datenregion dargestellt:[2]

[1] Enterprise-Plan-Kunden können ihre Daten in unserem EU-Rechenzentrum in Frankfurt, Deutschland, hosten lassen.

[2] Ein hochrangiges Netzwerkdiagramm kann je nach Bedarf und MNDA-Signierung freigegeben werden.



„Infrastruktur als Code“ wird ausgiebig genutzt, um sicherzustellen, dass Konfigurationsänderungen nachverfolgt und geprüft werden. Das Infrastrukturteam von monday.com führt vierteljährlich eine gründliche Überprüfung der Netzwerkkonfiguration durch und nimmt alle zur Aufrechterhaltung oder Erhöhung der Sicherheit notwendig erachteten Änderungen vor.

aws partner network

AWS-Advanced Technology Partner

monday.com ist auch ein AWS-Advanced Technology Partner monday.com ist auch ein AWS-Advanced Technology Partner und dies bestätigt, dass AWS selbst unsere Organisation in Bezug auf Infrastruktur, Informationssicherheit, Best-Practice-Design und vieles mehr gründlich überprüft hat.

Netzwerksicherheit

Da monday.com eine rein Cloud-basierte Lösung ist, haben wir den Vorteil, moderne, Cloud-orientierte Kontrollen zu verwenden, um einen genauen Überblick über unsere Netzwerkumgebung zu erhalten. Wir sammeln und überwachen Netzwerkprotokolle mithilfe eines NIDS und Verkehrsprotokolle von Randgebieten und überprüfen relevante Alarme über unser Security Information und Event-Management (SIEM)-System. Wir verwenden Tools zur

Sicherheitsüberwachung, die regelmäßig unsere Sicherheitsgruppen- und Netzwerk-ACL-Konfiguration vom Cloud-Anbieter abrufen und so einen vollständigen Überblick über unser Netzwerk erstellen.

Das Infrastrukturteam von monday.com führt vierteljährlich eine gründliche Überprüfung der Netzwerkkonfiguration durch und nimmt alle zur Aufrechterhaltung oder Erhöhung der Sicherheit notwendig erachteten Änderungen vor. Darüber hinaus beauftragen wir jährlich einen unabhängigen Prüfer mit der Überprüfung unserer Netzwerkkonfiguration.

Zugang zur Produktion
Der Zugang zu den Produktionsanlagen wird rollenbasiert und in Übereinstimmung mit den „Need-to-know"- und „Least Privileges"-Prinzipien gewährt. Administrative Rechte werden nur den Mitarbeitern des Infrastrukturteams (einem kleinen und begrenzten Team erfahrener Ingenieure) gewährt. Für den Zugriff auf die monday.com-Server ist die Verwendung unseres VPN erforderlich, das über unseren Enterprise Identity Provider (IdP) authentifiziert und vollständig geprüft wird und die Passwortstärke sowie die Multi-Faktor-Authentifizierung (MFA) durchsetzt.
Der Zugriff auf Produktionsressourcen durch unsere Entwickler erfolgt über Kubernetes-Portweiterleitung und wird ebenso über unseren IdP authentifiziert.

Härtung
Die Server basieren auf der neuesten, gemäß den CIS-Standards (Center for Internet Security) gehärteten Ubuntu LTS-Version (20.04).

Datenbanken
Zu den Datenbanken, die von monday.com verwendet werden, gehören MySQL, Elasticsearch und Redis. Von unseren Integrationsfunktionen genutzte API-Schlüssel zu externen Systemen werden in einem dedizierten, selbstreplizierenden HashiCorp Vault-Cluster gespeichert.

Dateiablage
Die Dateiablage wird auf dem Simple Storage Service (S3) von AWS, der Anhänge und Datenbanksicherungen speichert, gehostet. Anhänge enthalten alle Dateien, die von einem Kunden auf der monday.com-Dienstleistung hochgeladen werden.
monday.com bietet einen automatischen Malware-Erkennungsdienst für Dateien, die von den Benutzern auf den Dienst hochgeladen werden, um sicherzustellen, dass fremde Dateien, die auf den Dienst hochgeladen werden, nicht infiziert sind. Außerdem haben wir eine Blacklist mit einer Liste von verbotenen Dateierweiterungen. Die Blacklist der Dateierweiterungen enthält Dateitypen, die als gefährlich angesehen werden können, wie z. B. ausführbare Dateien oder HTML. Durch die Sperrung dieser Dateitypen wird das Risiko einer Infizierung durch Malware signifikant reduziert.

Mehrregionen
Im Januar 2021 hat monday.com seine erste europäische Datenregion in Frankfurt, Deutschland, eröffnet (derzeit verfügbar für Enterprise-Plan-Kunden).
Aufgrund der identischen Infrastrukturprinzipien in der Region USA können monday.com-Kunden in der EU das monday.com-Erlebnis mit dem gleichen Maß an Sicherheitsmaßnahmen und -kontrollen genießen und darauf vertrauen, dass die CIA-Triade (Vertraulichkeit, Integrität und Verfügbarkeit) eingehalten wird.
Die Highlights des Netzwerkdiagramms von monday.com sind oben dargestellt.
Für die Zukunft planen wir, Rechenzentren in anderen Regionen zu eröffnen.

Verschlüsselung und Schlüsselmanagement

Verschlüsselung während der Übermittlung

Daten, die über offene Netze übertragen werden, werden mit TLS 1.3 (mindestens TLS 1.2) verschlüsselt.

Verschlüsselung im Ruhezustand

Daten im Ruhezustand werden mit AES-256 verschlüsselt. Die Verschlüsselungsschlüssel werden mit Hilfe von AWS Key Management Service (KMS) gespeichert. Ein jährlich rotierender Kundenhauptschlüssel (CMK) wird derzeit zur Verschlüsselung aller Kundendaten verwendet, die an den sertu.com-Dienst übermittelt und in dessen Namen verarbeitet werden.

Mandantentrennung

Unsere Umgebung ist eine Multi-Mandanten-Umgebung mit logischer Trennung zwischen den Kunden. Die Kundendaten werden auf der Anwendungsebene durch eindeutige IDs, die sich aus einer Kombination mehrerer Parameter ergeben, getrennt.

Wir arbeiten derzeit daran, unseren Kunden eine Verschlüsselung auf Mandantenebene (TLE) zu ermöglichen, wobei die TLE eine Schicht ist, die sicherstellt, dass Daten im Ruhezustand mit einem dedizierten Schlüssel pro Konto verschlüsselt werden und Schutz vor der Einsichtnahme von Daten durch nicht autorisierte Systeme oder Personen bietet.

Die TLE schützt vor zwei Hauptszenarien:

1. **Angreifer:** Die Daten in den Datenbankfeldern sind verschlüsselt, so dass ein Angreifer beim Zugriff auf die Datenbank und beim Extrahieren der Daten nur verschlüsselte Daten erhält.
2. **Unbeabsichtigte Weitergabe:** Die Daten werden mit einem speziellen Schlüssel pro Konto verschlüsselt, sodass versehentlich zwischen Konten ausgetauschte Daten niemals als Klartext weitergegeben werden.

Wir planen, Enterprise-Plan-Kunden in Zukunft die Möglichkeit zu bieten, ihre eigenen Verschlüsselungsschlüssel (BYOK: Bring Your Own Key) mitzubringen.

Backup

monday.com sichert die Daten seiner Kunden, die an die monday.com-Dienstleistung übermittelt und in deren Auftrag verarbeitet werden. Wir sichern die Nutzerdaten konsequent alle fünf Minuten und verteilen die verschlüsselten Backups über mehrere AWS-Verfügbarkeitszonen. Darüber hinaus haben wir zu Redundanzzwecken DR-Standorte in separaten AWS-Regionen eingerichtet. Die Aktivitätsprotokolldaten werden auf GCP gesichert.

Skalierbarkeit und Zuverlässigkeit

Wir verwenden eine Microservices-Architektur, um minimale Auswirkungen auf den Systemzustand, falls eine oder mehrere Komponenten ausfallen, zu gewährleisten. Die monday.com-Dienstleistung ist vollständig containerisiert, wobei Kubernetes für die Orchestrierung verwendet wird. Dadurch wird eine hochgradig skalierbare Infrastruktur geschaffen, die sich für die Bewältigung einer steigenden Kundennachfrage eignet und gleichzeitig ein hochwertiges Erlebnis für die Endbenutzer bietet.

„Infrastruktur als Code“ wird in großem Umfang über Terraform eingesetzt, um die Überprüfbarkeit und Wartbarkeit der Infrastrukturressourcen zu gewährleisten.

monday.com überwacht fortlaufend die Leistungskennzahlen aller seiner Infrastrukturkomponenten und baut seine Infrastruktur skalierbar auf. Darüber hinaus führen wir vierteljährliche Skalenprüfungen durch, und zwar sowohl mit den Infrastrukturingenieuren als auch mit dem Management durch, um sicherzustellen, dass unsere Roadmap eine qualitativ hochwertige Dienstleistung für eine ständig wachsende Anzahl von Kunden und Produktfunktionen bietet.

Dienstleistungsvereinbarung (Service Level Agreement – SLA)

Die Verfügbarkeit unsere Dienstleistung kann über unsere Statusseite überwacht werden. Systemstillstandszeiten für Wartungsarbeiten sind nur selten erforderlich. Wenn nötig und praktikabel, werden sie an Wochenenden und zu Zeiten geringer Aktivität eingeplant.

Benachrichtigungen über Ausfallzeiten sind sofort über die Statusseite verfügbar. Dort können Kunden Benachrichtigungen über die Verfügbarkeit und die Bemühungen unseres Teams zur Schadensbegrenzung per E-Mail oder Textnachricht abonnieren.

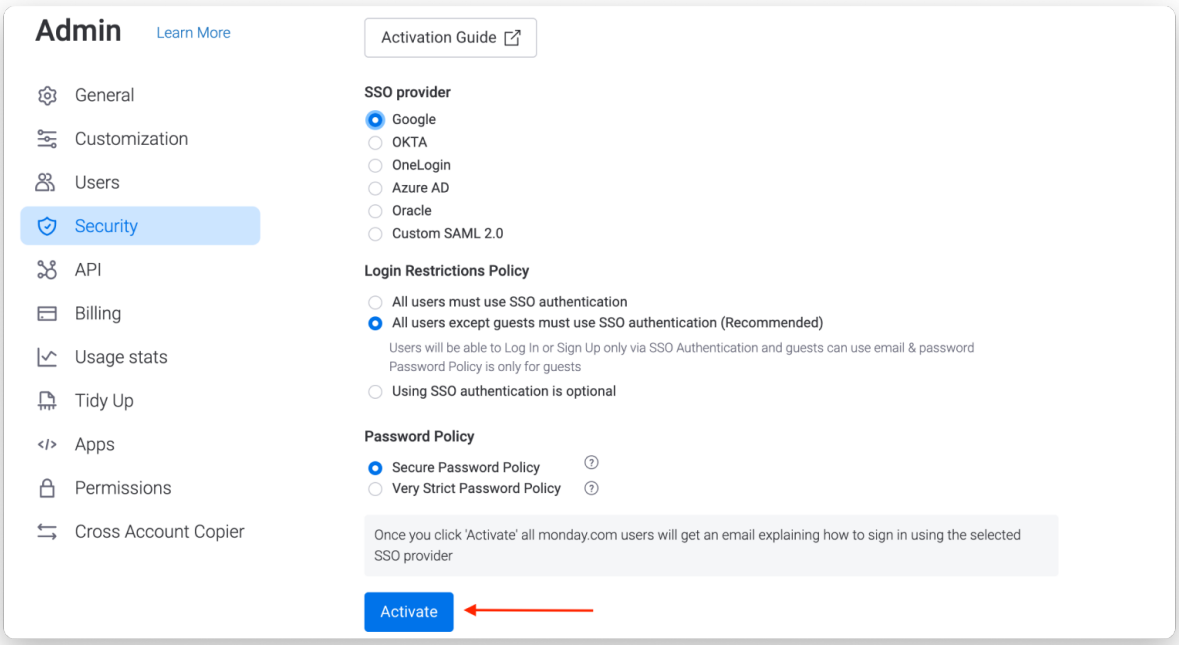
Enterprise-Plan-Kunden erhalten eine 99,9-prozentige Betriebszeitgarantie.

3. Sicherheitsmerkmale und -funktionalitäten

Authentifizierung
monday.com unterstützt die folgenden Authentifizierungsmethoden:
Berechtigungsnachweise
Sollten Sie sich dafür entscheiden, die Benutzer Ihres Kontos mit Anmeldeinformationen zu authentifizieren, können Administratoren zwischen zwei Passwortstärken für ihre Konten wählen:

1. Mindestens 8 Zeichen, wobei keine sich wiederholenden oder aufeinanderfolgenden Zeichen erlaubt sind, oder
2. Mindestens 8 Zeichen, wobei keine sich wiederholenden oder aufeinanderfolgenden Zeichen erlaubt sind und mindestens eine Ziffer (1, 2, 3), ein Kleinbuchstabe (a, b, c) und ein Großbuchstabe (A, B, C) enthalten sein müssen.

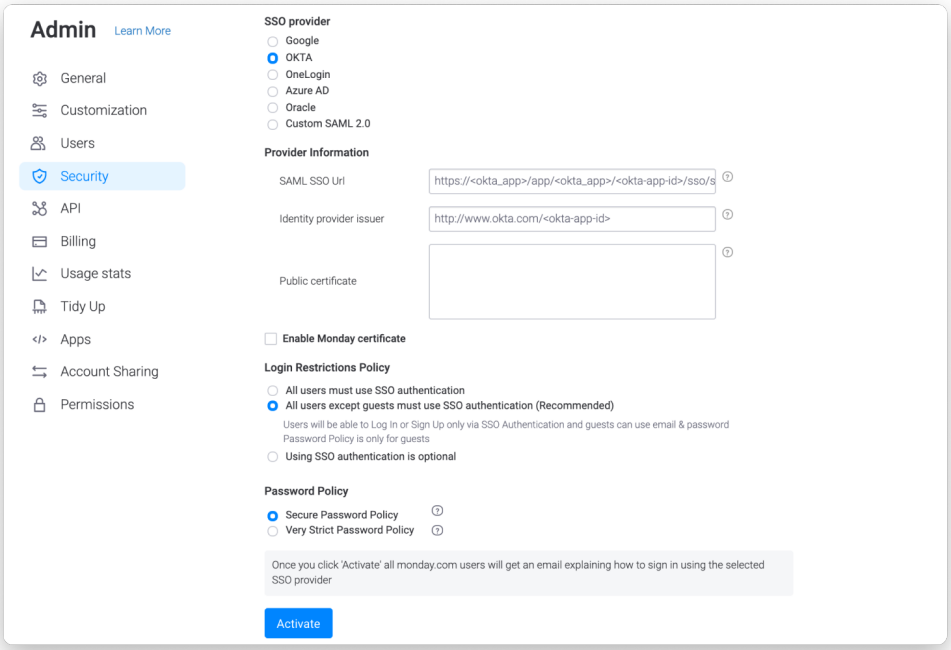
Einzelanmeldung bei Google (SSO)
Google SSO ist ein sicheres Authentifizierungssystem, das Benutzern die Möglichkeit gibt, sich mit ihrem Google-Konto bei monday.com anzumelden, ohne sich mehrere Passwörter merken zu müssen.
Diese Funktion ist nur für Pro- und Enterprise-Pläne verfügbar.



Identitätsprovider (IdP)
monday.com unterstützt derzeit drei Haupt-Identitätsprovider:

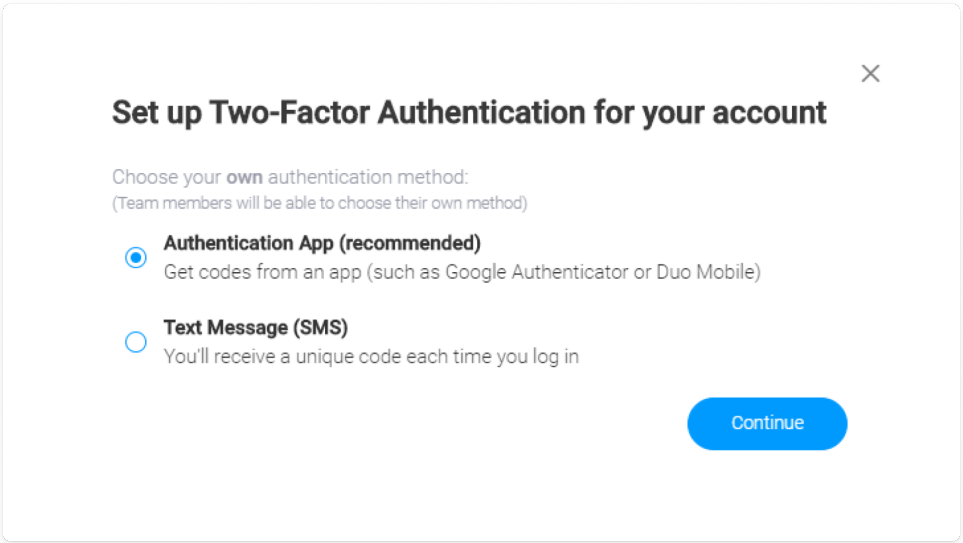
1. OKTA
2. Azure AD
3. OneLogin

Darüber hinaus haben die Kunden die Möglichkeit, ihren eigenen Provider zu nutzen, der SAML 2.0 verwendet.
Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.



Zwei-Faktor-Authentifizierung (2FA)

Zusätzlich zu den oben genannten Authentifizierungsmethoden können Administratoren eine zusätzliche Sicherheitsebene konfigurieren und 2FA über eine Textnachricht (SMS) oder über eine Authentifizierungs-App aktivieren.
Bitte beachten Sie, dass 2FA bei Ihnen aktiviert sein muss, wenn Sie sich für die Integration mit Ihrem IdP entscheiden.



Autorisierung

SCIM-Bereitstellung

Das System für domainübergreifendes Identitätsmanagement (System for Cross-domain Identity Management – SCIM) ist ein Protokoll für die anwendungsübergreifende Benutzerverwaltung, mit dem Sie auf einfache Weise Benutzer- und Teamdaten für mehrere Anwendungen gleichzeitig bereitstellen (hinzufügen), de-prosionieren (deaktivieren) und aktualisieren können. monday.com unterstützt drei Möglichkeiten zur Einrichtung der SCIM-Bereitstellung:

1. Bestehende monday.com SCIM-Anwendungen:
    a. OKTA
    b. Azure AD
    c. OneLogin
2. Benutzerdefinierte SCIM-Integration mit einem Identitätsanbieter Ihrer Wahl
3. SCIM-Bereitstellung unter Verwendung von API

Die folgende Tabelle zeigt alle **Benutzerattribute**, die von der SCIM-Integration von monday.com unterstützt werden:

monday.com-Attribut	SCIM-API-Attribut(e)	Beschreibung
Name (erforderlich)	name, displayName	Der Anzeigename des Benutzers.
Email-Adresse (erforderlich)	userName, email	Die E-Mail-Adresse, die der Benutzer für die Anmeldung bei monday.com verwendet.
Aktiv (erforderlich)	active	Beim Anlegen eines Benutzers muss dieses Feld auf 'true' gesetzt werden. Wird der Wert „active“ eines Benutzers auf „false“ geändert, wird er in der monday.com-Dienstleistung deaktiviert.
Position	title	Die Position des Benutzers in der Organisation.
Zeitzone	timezone	Die Zeitzone des Benutzers (alle Daten auf der Plattform beziehen sich auf diese Zeitzone).
Sprachraum	locale	monday.com wird eine lokalisierte Version für verschiedene Sprachräume anzeigen.
Telefonnummer	phoneNumbers	Die Telefonnummern des Benutzers (es wird nur die als „primär“ markierte angezeigt).
Privatanschrift	addresses	Die Anschriften des Benutzers (es wird nur die als „primär“ markierte angezeigt).
Benutzertyp	userType	Die Ebene jedes Benutzers innerhalb des Kontos. Die möglichen Werte sind: Admin, Mitglied, Betrachter oder Gast (der Standardwert ist „Mitglied“).

Die folgende Tabelle zeigt alle **Teamattribute**, die von der SCIM-Integration von monday.com unterstützt werden:

monday.com-Attribut	SCIM-API-Attribut(e)	Beschreibung
Name (erforderlich)	displayName	Der angezeigte Teamname.
Benutzer	members	Liste der Benutzer, die dem Team zugeordnet sind.

Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.

Berechtigungen

monday.com hilft Ihnen zu kontrollieren, wer was in Ihrem Konto tun darf. Wir bieten Ihnen verschiedene Arten von Berechtigungen, die Sie anpassen können, um die Anzeige oder Bearbeitung von Daten einzuschränken, darunter:

1. **Board-Berechtigungen**
    a. Arten: „Haupt"-, „gemeinsam nutzbare" und „private" Boards
    b. Einschränkungen: „Alles bearbeiten", „Inhalte bearbeiten", „Bearbeiten durch Beauftragten" und „Nur anzeigen"
2. **Spaltenberechtigungen**: „Spaltenbearbeitung einschränken" und „Spaltenansicht einschränken"
3. **Dashboard-Berechtigungen**
    a. Arten: „Haupt"- und „private" Dashboards
    b. Beschränkungen: Nur Dashboard-Besitzer können das Dashboard sowie die darin enthaltenen Anwendungen und Widgets bearbeiten.
4. **Arbeitsbereich-Berechtigungen**
    a. Arten: „Offene" und „Geschlossene" Arbeitsbereiche
    b. Beschränkungen: „Keiner", „Nur Administrator", „Arbeitsbereichseigentümer" und „Jeder"
5. **Kontoberechtigungen:** Kontoberechtigungen: Administratoren können Einschränkungen („Keiner", „Nur Administrator", und „Jeder") für die folgenden Funktionen festlegen:
    a. Dateien hochladen
    b. Boards übertragen
    c. Haupt-Boards erstellen
    d. Private Boards erstellen
    e. Freigabefähige Boards erstellen
    f. Integrationen erstellen
    g. Automatisierungen erstellen
    h. Arbeitsbereiche erstellen
    i. @alle Benutzer des Kontos für eine Aktualisierung oder ein Board erwähnen oder abonnieren
    j. Exportieren von Boards, Aktivitätsprotokollen, Suchergebnissen und Updates nach Excel

Bitte beachten Sie, dass einige der oben genannten Funktionen möglicherweise nicht in allen Plänen verfügbar sind.

Rollen innerhalb von monday.com

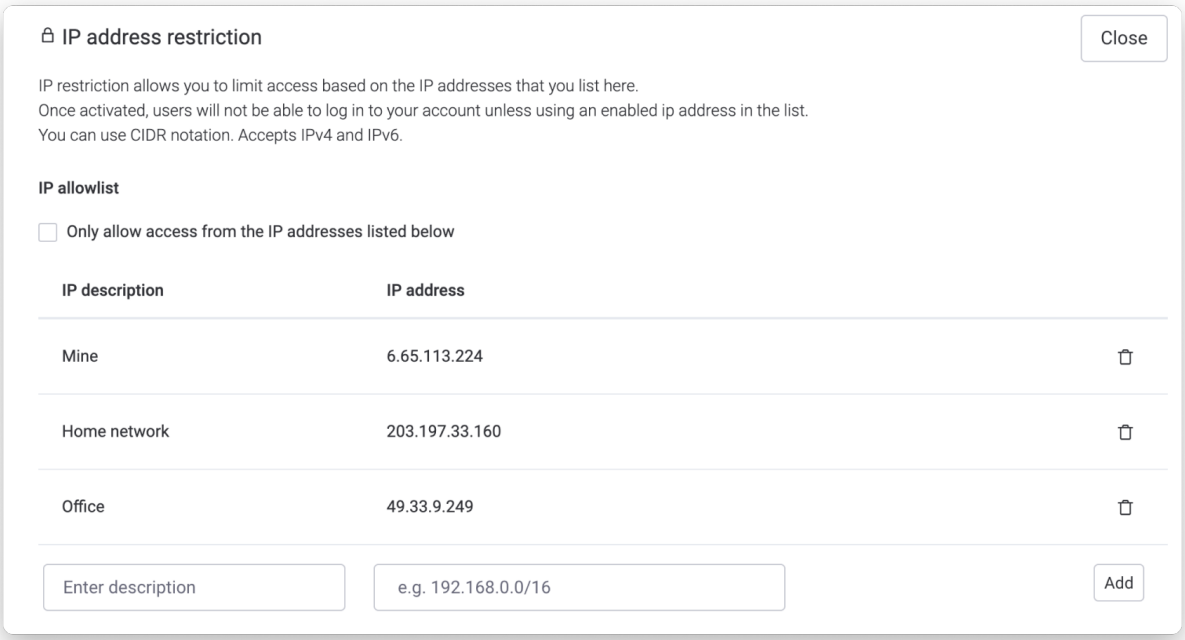
Zu den Rollen innerhalb von monday.com gehören:

Rolle	Beschreibung	Kann	Kann nicht
Administrator	Ein Teammitglied (oder mehrere, wenn Sie dies wünschen), das sein Team verwaltet	Das gesamte Konto überblicken Alles verwalten, von Benutzern und Boards bis hin zu Sicherheit und Abrechnung (wie im Abschnitt „Admin-Panel" weiter unten beschrieben)	

Mitglied	Hat Bearbeitungszugriff (Die Anzahl der Mitglieder, die Sie einladen können, hängt von Ihrem Plan ab)	• Boards, Artikel und Ordner erstellen • Andere Mitglieder innerhalb eines Boards und eines Artikels einladen • Sich alle Haupt-Boards anzeigen lassen • Zu gemeinsam nutzbaren oder privaten Boards eingeladen werden • Sein Profil bearbeiten • Anhänge kommunizieren und hinzufügen	
Betrachter	Nur in der Lage, Boards zu betrachten, und zwar ohne jegliche Bearbeitungsrechte (Sie können eine unbegrenzte Anzahl von Betrachtern einladen, und zwar unabhängig davon, welchen Plan Sie erworben haben)	• Sich alle Boards im Hauptarbeitsbereich des Kontos anzeigen lassen • Einen Artikel öffnen und Aktualisierungen lesen • Innerhalb eines Boards suchen oder filtern • Zu gemeinsam nutzbaren oder privaten Boards eingeladen werden • Seinen Profilbereich bearbeiten • Neue Betrachter einladen • Die Board-Ansichten öffnen • Einem Artikel zugewiesen werden • Zu einem Team hinzugefügt werden • Boards nach Excel exportieren	• Ein neues Board erstellen oder löschen • Irgendwelche Änderungen am Inhalt, der Struktur oder den Einstellungen eines Forums vornehmen • Aktualisierungen zu einem Artikel hinzufügen oder eine von einer anderen Person gepostete Aktualisierung mögen • Sich selbst und andere für einen Artikel/ein Board anmelden • Als Eigentümer eines Boards zugewiesen werden • Einen Gast zu einem gemeinsamen nutzbaren Board einladen • Ein Team erstellen
Gast	Externes Mitglied Ihrer Organisation, z. B. ein Anbieter, Kunde, freier Mitarbeiter oder externer Berater	• Zu gemeinsam nutzbaren Boards eingeladen werden • Als Mitglied fungieren	• Sich Informationen in Haupt- oder privaten Boards anzeigen lassen

Einschränkungen bezüglich der IP-Adresse

Der/Die Admin(s) hat bzw. haben die Möglichkeit, eine Reihe von zulässigen IP-Adressen festzulegen, die auf Ihr Konto zugreifen können. So können Sie den Zugriff auf das Konto auf Benutzer in bestimmten Kontexten beschränken, z. B. auf solche, die sich von einem bestimmten Standort aus (z. B. vom Büro aus) anmelden oder ein bestimmtes VPN verwenden. Jeder Benutzer, der versucht, sich mit einer IP-Adresse anzumelden, die nicht mit einer Adresse in der Liste der zugelassenen Adressen übereinstimmt, erhält eine Fehlermeldung und kann nicht fortfahren.
Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.

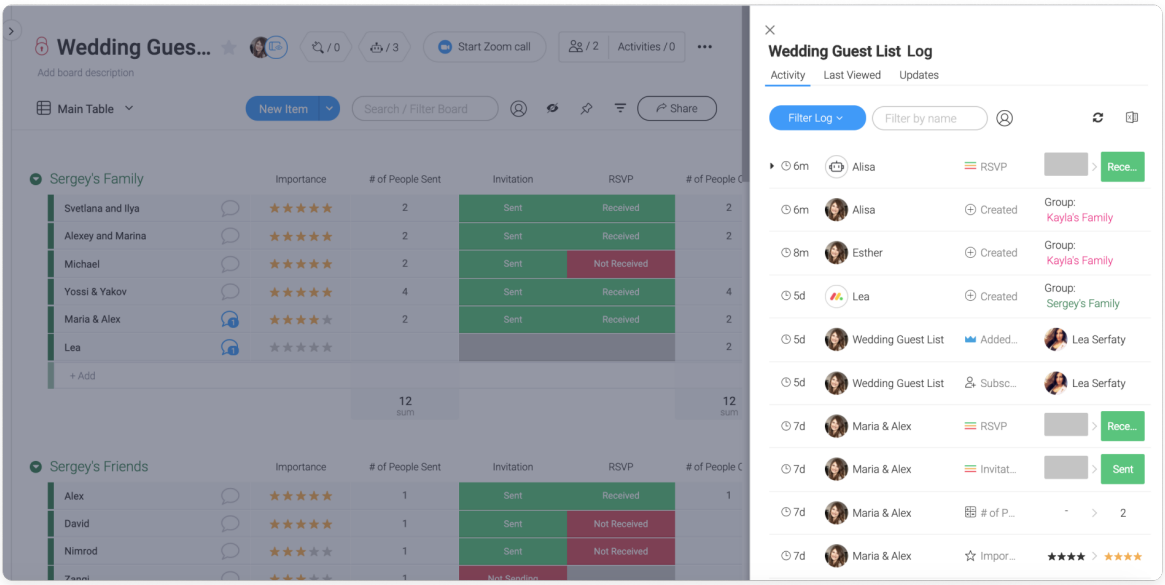


Protokolle

Aktivitätsprotokoll

Es gibt zwei Arten von Aktivitätsprotokollen:

1. **Das Board-Aktivitätsprotokoll** zeigt alle vergangenen Aktivitäten eines Boards in einer Liste an, einschließlich geänderter Daten, Status, Bewegungen zwischen Gruppen, Automatisierungen und Berechtigungen. Die Informationen, die im Aktivitätsprotokoll angezeigt werden, variieren je nach Stufe: Im Basic-Plan werden nur die Aktivitäten der letzten Woche gespeichert, im Standard-Plan 6 Monate und im Pro- und Enterprise-Plan bis zu 1 Jahr.

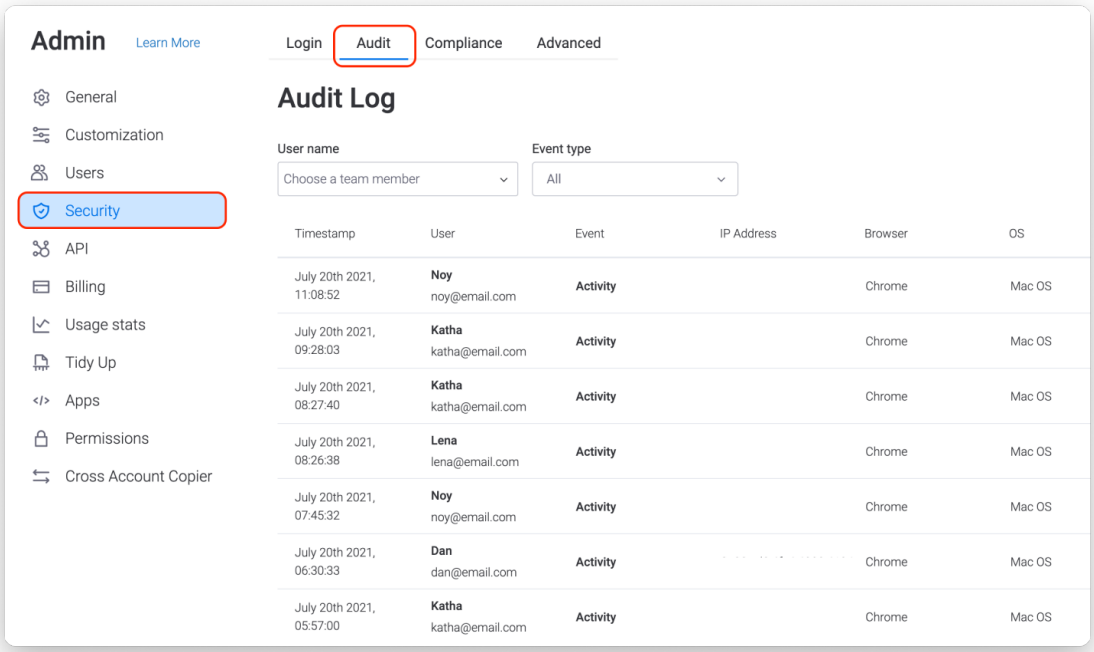


2. **Das Board-Aktivitätsprotokoll** zeichnet alle Aktualisierungen eines individuellen Artikels auf. Im Aufgaben-Aktivitätsprotokoll können Sie einen vollständigen Überblick über die Aktualisierungen des Artikels und den genauen Zeitpunkt ihrer Durchführung erhalten. Alle Aktualisierungen sind von der neuesten zur ältesten geordnet. Sie können für jede Aktualisierung eine Erinnerungsmeldung einrichten.

Mit einem Klick können Ihr Artikel- oder Board-Aktivitätsprotokoll mit einem Mausklick nach Excel exportieren.

Audit-Protokoll

Das Audit-Protokoll bietet dem/den Kontoadministrator(en) einen detaillierten Bericht über alle sicherheitsrelevanten Aktivitäten des Kontos. In diesem Abschnitt können Sie sehen, wann sich Benutzer das letzte Mal bei dem Konto an- und abgemeldet haben, von welchem Gerät aus und mit welcher IP-Adresse die Sitzung stattfand. Sie können auf diese Weise alle verdächtigen Aktivitäten überwachen und bei Bedarf den Panikmodus aktivieren.
Das Protokoll zeigt auch potenziell gefährliche Ereignisse wie fehlgeschlagene Anmeldungen, heruntergeladene Anhänge und exportierte Vorstandsdaten an. Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.



Interoperabilität und Übertragbarkeit

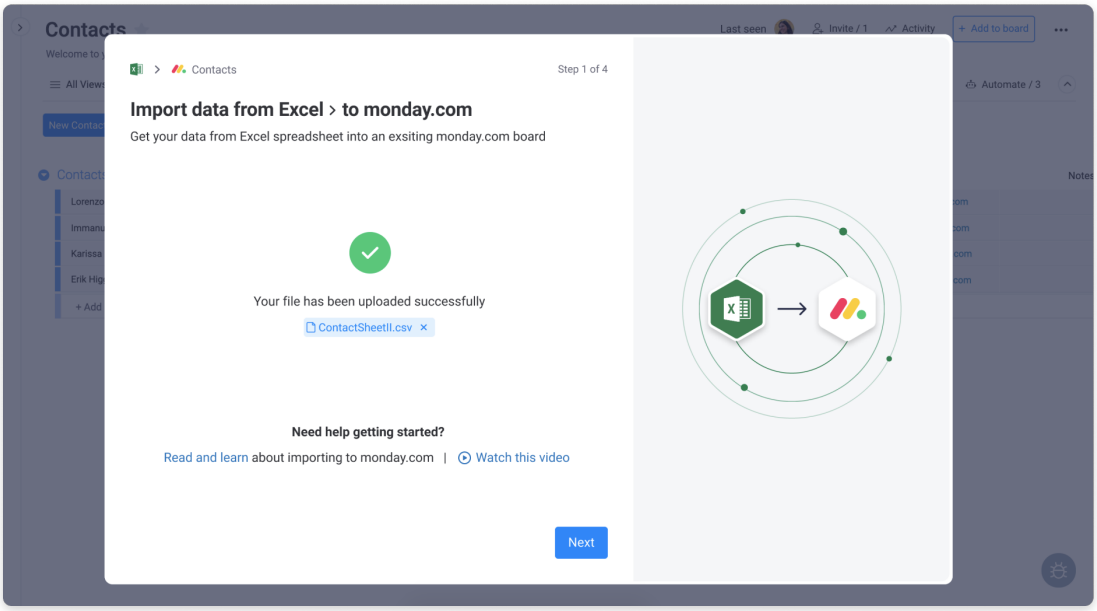
Integrationen

monday.com unterstützt Integrationen mit verschiedenen anderen Softwarelösungen, um individuelle Arbeitsabläufe zu erstellen. Sie können monday.com mit den Tools verbinden, die Sie bereits verwenden, um die Arbeit Ihres Teams an einem Ort zu verwalten.
Integrationen sind optional und können über das Admin-Panel deaktiviert werden.

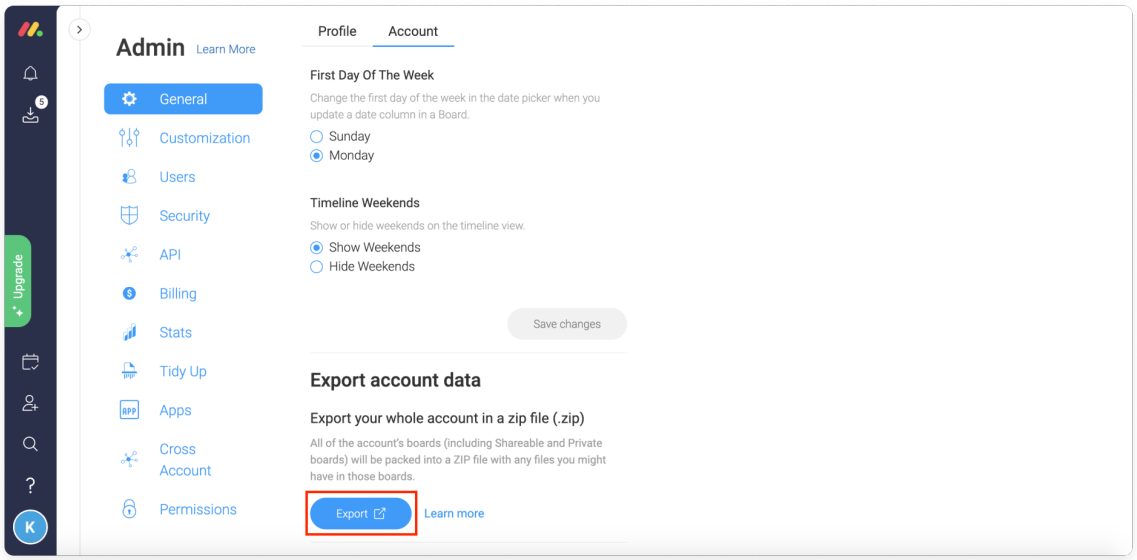
Excel-Import und -Export

monday.com bietet seinen Kunden zwei Datenmanagementfunktionen:

1. Daten aus einer Excel-Tabelle in ein monday.com-Board (neu oder vorhanden) übertragen.



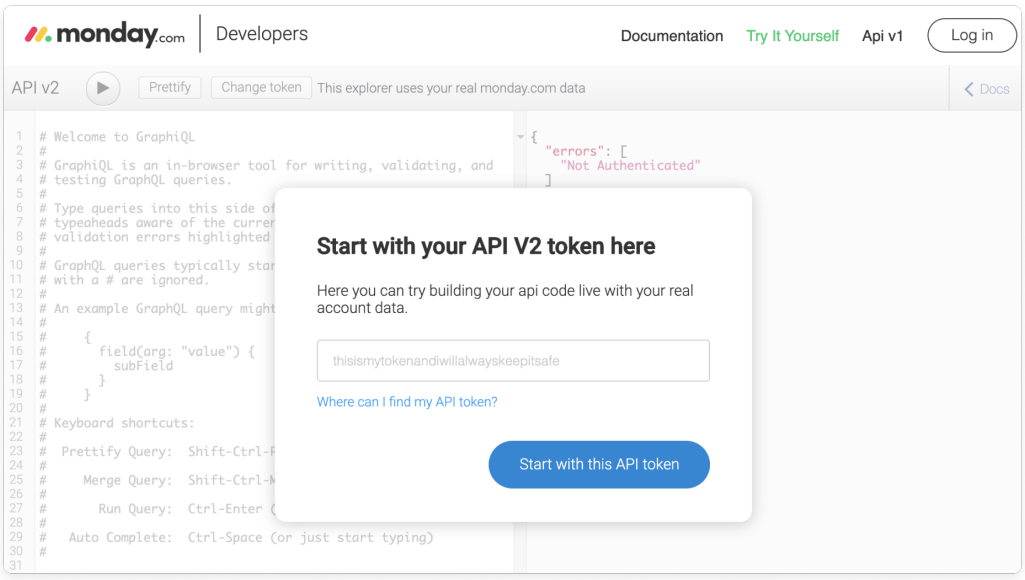
2. Daten von monday.com exportieren:
    a. Boards nach Excel exportieren.
    b. Daten des gesamten Kontos über das Admin-Panel exportieren. Der Export erfolgt als Zip-Archiv, das die Excel-Tabellen und die auf das Konto hochgeladenen Dateien enthält.



API

monday.com bietet eine GraphQL-API. Diese ist Teil des Frameworks der Monday-Apps und gestattet Entwicklern den programmatischen Zugriff auf und die Aktualisierung von Daten innerhalb ihrer monday.com-Konten.
Zu den Anwendungsfällen für die API gehören:

- Zugriff auf Board-Daten, um einen benutzerdefinierten Bericht innerhalb eines monday.com-Dashboards zu erstellen
- Erstellung eines neuen Artikels in einem Board, wenn ein Datensatz in einem anderen System erstellt wird
- Programmatischer Import von Daten aus einer anderen Quelle



Das Admin-Panel

Im Admin Panel kann der bzw. können die Admin(s) Ihres Kontos alles verwalten, einschließlich der Sicherheitseinstellungen, der Benutzer des Kontos, der Kontoanpassung, der Abrechnung und vieles mehr.

Autorisierte Domain

Administratoren können aus zwei Einstellungen wählen:

1. Nur Admins können Mitglieder und Betrachter von einer beliebigen E Mail-Domain zum Konto einladen.
2. Administratoren legen eine E-Mail-Domain, von der aus sich Benutzer für das Konto anmelden können, fest.

Blockierung von E-Mail-Domains

Admins können verhindern, dass Benutzer von bestimmten E-Mail-Domains aus neue monday.com-Konten erstellen. Diese Funktion ist nützlich, um redundante monday.com-Konten im gleichen Unternehmen zu vermeiden, und zwar insbesondere bei Unternehmen, die mehrere Unternehmensdomains besitzen, welches Auswirkungen auf die Einhaltung der Data-Governance-Regeln des Unternehmens haben kann.

Um die Erstellung neuer Konten zu blockieren, können E-Mail-Domains an den Service von monday.com übermittelt werden, um überprüft zu werden und die Eigentümerschaft zu verifizieren. Sie werden dann an den/die Admin(s) des Kontos weitergeleitet, um in das Konto der Hauptorganisation aufgenommen zu werden.
Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.

Panikmodus

Durch Aktivierung des Panikmodus wird Ihr Konto vorübergehend gesperrt. Niemand kann darauf zugreifen, bis der Admin des Kontos eine Anfrage an unser Kundenerfolgsteam sendet. Diese Funktion ist wichtig, wenn die Anmeldedaten eines Ihrer Teammitglieder kompromittiert wurden.
Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.

Sitzungsmanagement

Im Sicherheitsbereich des Admin-Panels können Admins auf die Registerkarte „Sitzungen“ klicken, um sich die Sitzungsdaten aller Benutzer anzeigen zu lassen und jede beliebige Sitzung zu kontrollieren und zurückzusetzen.
Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.

Generierung von API-Tokens

Nur Admins können in ihrem Konto die Berechtigung zur Erzeugung persönlicher GraphQL-API-Tokens erteilen (entweder für alle, nur für Admins oder für keinen). Dies verhindert, dass Benutzer API-Tokens generieren und sie versehentlich mit Tools von Drittanbietern teilen oder sie sogar öffentlich machen, indem sie sie in das öffentlich zugängliche Repository schieben und sensible Daten des Kontos preisgeben. Ein Benutzer, der keine Token generieren darf, wird mit einer Warnmeldung angezeigt.
Diese Funktion ist nur für Enterprise-Plan-Kunden verfügbar.

Inhaltsverzeichnis

Im Inhaltsverzeichnis finden Sie eine Übersicht über alle Arbeitsbereiche, Boards, Dashboards und Workdocs, die sich im Konto befinden. Darüber hinaus können Sie für jede dieser Funktionen die Eigentümer, Abonnenten, das Erstellungsdatum und das Datum der letzten Aktualisierung sehen und erfahren, ob sie für die übrigen Kontomitglieder öffentlich zugänglich ist oder nicht.

* Bitte beachten Sie, dass dieses Whitepaper nicht die vollständige Liste der Funktionen, die über das Admin-Panel verwaltet werden, enthält. Zusätzliche Informationen finden Sie in unseren Support-Artikeln.
Zusätzliche von den Konto-Admins verwaltete Funktionen, wie z. B. Anmeldung, Zwei-Faktor-Authentifizierung, SCIM-Bereitstellung, Berechtigungen, IP-Adressbeschränkung, monday-Apps, Audit-Protokoll, API-Tokens und HIPAA-Compliance-Konfiguration. können in verschiedenen Kapiteln dieses Dokuments behandelt werden.

---

4. Anwendungssicherheit

Sicherer Lebenszyklus der Softwareentwicklung (S-SDLC)

- monday.com verwendet die OWASP- Top-10-Methodik, um Sicherheit in unseren sicheren Softwareentwicklungslebenszyklus (S-SDLC) einzubauen.
- Der gesamte Code wird statisch analysiert (SAST) und im Rahmen des CI/CD-Prozesses begutachtet, um die Codequalität vor dem Einsatz in der Produktion sicherzustellen.
- Dynamische Anwendungssicherheitstests (DAST) werden mindestens einmal pro Woche durchgeführt.
- Wir legen besonderen Wert darauf, dedizierte Tests für neue Funktionen, die veröffentlicht werden, während ältere Funktionen bereits seit mehreren Jahren getestet werden, zu schreiben.
- Wir bewerten und überwachen während und nach der Bereitstellung unsere Anwendung kontinuierlich auf Schwachstellen.
- Alle serverseitigen Drittanbieter-Bibliotheken werden automatisch mit einem SCA-Tool (Software Composition Analysis) auf öffentlich bekannt gewordene Schwachstellen überprüft.

Web-Anwendungs-Firewall (WAF)

Eine Web-Anwendungs-Firewall (WAF) dient zur Filterung, Überwachung und Blockierung des Datenverkehrs auf Anwendungsebene, um bekannte Angriffe abzuwehren.

Schwachstellenmanagement

Schwachstellen werden zentral in einem Entwicklungsrückstand erfasst und auf der Grundlage unserer Bewertung ihrer Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der Dienstleistung und der Kundendaten klassifiziert. Der Schweregrad der Schwachstelle wird durch das Common Vulnerability Scoring System (CVSS) bestimmt. Unsere Forschungs- und Entwicklungsabteilung führt dann Abhilfemaßnahmen innerhalb eines vordefinierten, auf dem Schweregrad basierenden Zeitrahmens gemäß unserer internen Patch-Management-Richtlinie.

Sicherheitschampions

Unsere interne Gemeinschaft der Sicherheits-Champions umfasst Entwickler aus allen F&E-Teams. Die Sicherheitschampions erhalten eine fortgeschrittene Sicherheitsschulung und sind qualifiziert, bei Bedarf Sicherheitsanleitungen zu geben und Sicherheitscodeprüfungen durchzuführen.

Penetrationstests

Die Penetrationstests für Anwendungen werden jedes Jahr von einem anderen unabhängigen Unternehmen durchgeführt und umfassen manuelle und automatische Testmethoden.
Darüber hinaus führt unser internes Anwendungssicherheitsteam regelmäßig Sicherheitsaudits und Penetrationstests für vielfältige Funktionen, die ein tiefes Verständnis unserer internen Sicherheitsmechanismen und -architektur erfordern, durch.
Als Teil unserer externen und internen Penetrationstests werden Netzwerk-Scan-Tools gegen unsere Produktionsserver eingesetzt.

Bug-Bounty-Programm

monday.com unterhält ein intern verwaltetes privates Bug-Bounty-Programm auf HackerOne. Dieses gestattet Sicherheitsforschern aus aller Welt, auf ethische und verantwortungsvolle Weise Sicherheitslücken zu erforschen und unserem Sicherheitsteam mitzuteilen. Bestimmte Funktionen werden auf HackerOne besonders beworben, um die Forschung und die Bemühungen der Sicherheitsgemeinschaft auf diese Bereiche zu konzentrieren.

Als Teil des Programms unterhalten wir eine „Hall of Fame"-Anzeigetafel für Hacker.

---

5. IT-Sicherheit

Endpoint-Sicherheit

Alle Mitarbeiter-Workstations sind mit einer zentral verwalteten EDR-Lösung zur Erkennung und Quarantäne von Malware geschützt. Unsere EDR-Lösung wird von einem verwalteten SOC-Team rund um die Uhr und an 365 Tagen im Jahr kontinuierlich überwacht.
Alle Workstations sind mit FileVault/BitLocker verschlüsselt, passwortgeschützt und auf eine 10-minütige Bildschirmauszeit eingestellt.
Zusätzlich hinaus können wir über einen Gerätemanager Patches anwenden und einen Computer aus der Ferne löschen.

Passwort-Richtlinie

Unsere interne Passwort-Richtlinie schreibt vor, dass Passwörter mindestens 12 Zeichen lang sein und Folgendes beinhalten müssen:

1. Großbuchstaben
2. Kleinbuchstaben
3. Zahl
4. Symbol

Es wird eine Enterprise-Passwortmanagementlösung verwendet, die Standardpasswörter werden regelmäßig geändert, die Wiederverwendung von Passwörtern und häufig verwendeten Passwörtern ist technisch unzulässig und Passwörter laufen nach 120 Tagen ab.

Identitäts- und Zugriffsmanagement

Der Zugang zu den Systemen wird von unserem IT-Team rollenbasiert über unsere Enterprise Identity Provider (IdP)-Lösung gewährt, und zwar so wie es die Personalabteilung vorschreibt und in Übereinstimmung mit den Need-to-know- und Least-Privilege-Prinzipien.
Der Benutzerzugang wird innerhalb von bis zu 24 Stunden nach einem Beschäftigungswechsel oder einer Kündigung geändert. Darüber hinaus werden vierteljährliche Überprüfungen des Benutzerzugangs durchgeführt, um die Angemessenheit der Zugriffsrechte zu gewährleisten. Jeder Zugang, der nicht mehr benötigt wird, wird entfernt und dokumentiert.

E-Mail-Schutz

monday.com verwendet Google Workspace, das durch ein Drittanbieter-Mail-Relay geschützt ist, als unseren E-Mail-Anbieter. DMARC und SPF sind vorhanden. Die Mitarbeiter wurden kontinuierlich über die Best Practices zur Vermeidung von Phishing unterrichtet und es werden regelmäßig Tests durchgeführt.

Drahtlose Zugangspunkte

monday.com verwendet Industriestandardtechnologien, um sicherzustellen, dass die drahtlose Kommunikation in unserer Zentrale sicher ist. Wir setzen unter anderem WPA2 Enterprise ein, um eine rechtzeitige Deprovisionierung und Unfälschbarkeit im gesamten Netzwerk zu gewährleisten, und verfügen über eine Rogue-AP-Überwachung.

6. Betriebliche Sicherheit

Zugriff auf Kundendaten
monday.com behandelt alle Daten, die Kunden an die monday.com-Dienstleistung übermitteln und die von uns ausschließlich im Namen des Kunden verarbeitet werden, als „Black Box". Dies bedeutet, dass auf die Kundendaten für die Erbringung der monday.com-Dienstleistung grundsätzlich nicht zugegriffen wird und dass wir alle übermittelten Kundendaten mit höchster Vertraulichkeit behandeln.
Der Zugriff auf Kundendaten durch monday.com ist von Fall zu Fall gemäß unseren Geschäftsbedingungen oder der jeweiligen Vereinbarung mit dem Kunden beschränkt.

Personal
Hintergrundüberprüfungen
Unser Hauptsitz befindet sich in Israel, wo Hintergrundüberprüfungen unüblich und gesetzlich begrenzt sind. Zu den Überprüfungen, die wir durchführen, gehören die Überprüfung des beruflichen Werdegangs und Referenzgespräche mit früheren direkten Vorgesetzten.

Arbeitsvertrag
Alle Arbeitsverträge von monday.com enthalten Vertraulichkeitsbestimmungen und Bestimmungen, die eine sofortige Beendigung des Arbeitsverhältnisses bei Verstoß gegen bestimmte Pflichten und Verpflichtungen ermöglichen.
Zusätzlich unterhält monday.com eine HR-Sicherheitsrichtlinie, die die erforderlichen Sicherheitsaktivitäten und Verantwortlichkeiten während des Beschäftigungszeitraums, von der Einstellung bis zum Ausscheiden, definiert.

Zulässige Nutzung
monday.com unterhält eine Richtlinie zur zulässigen Nutzung, die jährlich von unserem Sicherheitsteam und dem erweiterten Sicherheitsforum überprüft wird. Unsere Mitarbeiter müssen die Richtlinie bei der Einstellung oder bei einer wesentlichen Änderung der Richtlinie unterschreiben.

Schulung und Sensibilisierung
Als Teil des anfänglichen Einführungsprozesses und danach mindestens einmal im Jahr erhalten die monday.com-Mitarbeiter eine Schulung zu den Verpflichtungen, die sie in Bezug auf Informationssicherheit und Datenschutz erfüllen müssen. Die Schulungen beinhalten sowohl Tutorials als auch schriftliche Aufgaben und werden vom Sicherheitsteam überwacht.
Es werden vierteljährliche Sicherheits- und Datenschutzwochen durchgeführt, um das Bewusstsein der Mitarbeiter weiter zu erhöhen.
Darüber hinaus werden bei Bedarf spezielle Schulungen durchgeführt (z. B. Schulungen zur sicheren Codierung für Entwickler).

Beendigung des Arbeitsverhältnisses
Der Benutzerzugang wird innerhalb von 24 Stunden nach einem Arbeitsplatzwechsel oder der Beendigung des Arbeitsverhältnisses geändert und die Firmengeräte müssen zurückgegeben werden. Es werden vierteljährliche Überprüfungen des Benutzerzugangs durchgeführt, um die Angemessenheit der Zugriffsrechte zu gewährleisten.

Red-Team-Bewertungen

Wir führen zweimal im Jahr Red-Team-Bewertungen unserer defensiven Struktur durch, die interne Penetrationstests, Infrastrukturangriffe und Simulationen von Sicherheitsverletzungen beinhalten. Die Red-Team-Bewertungen werden von führenden offensiven und defensiven externen Sicherheitsberatungsunternehmen durchgeführt. Diese setzen hochentwickelte Angriffstechniken, die einen einzigartigen Einblick in unsere potenziellen Sicherheitsrisiken und Schwachstellen bieten, ein.

Governance und Risikomanagement

monday.com unterhält einen fortlaufenden Risikomanagementprozess, der darauf abzielt, proaktiv Schwachstellen in den Systemen von monday.com zu identifizieren und neue und aufkommende Bedrohungen für den Betrieb des Unternehmens zu bewerten. monday.com unterzieht sich einer Risikobewertung im Rahmen der jährlich durchgeführten ISO 27001-Zertifizierung.

Störfallmanagement

Der Vorfallsreaktionsplan (Incident Response Plan – IRP) von monday.com enthält Richtlinien für die Erkennung von Sicherheits- und Datenschutzvorfällen sowie deren Eskalation an das zuständige Personal, die Kommunikation (intern und extern), die Schadensbegrenzung und die Post-Mortem-Analyse.
Das Incident Response Team (IRT) von monday.com besteht aus Vertretern der Sicherheit, der F&E, der Rechtsabteilung, aus Vertretern anderer Teams, die von Fall zu Fall hinzugezogen werden, und bei Bedarf aus einem externen Incident Response-Unternehmen.

Benachrichtigung

Gemäß den Bestimmungen in Abschnitt 7 unserer Ergänzung zur Datenverarbeitung („Datenstörfallmanagement und -benachrichtigung“) wird monday.com die betroffenen Kunden unverzüglich nach Bekanntwerden eines Datenvorfalls benachrichtigen.
Die betroffenen Kunden werden zum Zeitpunkt der Benachrichtigung über die Art des Verstoßes, die schädlichen Auswirkungen, die monday.com bekannt sind, die von monday.com ergriffenen Maßnahmen und die Pläne zur Behebung oder Milderung des Vorfalls informiert.

Disaster Recovery und Geschäftskontinuität

monday.com unterhält einen Geschäftskontinuitätsplan in Übereinstimmung mit ISO 27001 für den Umgang mit Katastrophen, die unser physisches Büro betreffen (wo kein Teil unserer Produktionsinfrastruktur aufbewahrt wird).
Darüber hinaus verfügen wir über einen Disaster Recovery Plan (DRP) für den Umgang mit unsere Produktionsumgebung betreffenden Katastrophen. Diese Tests werden mindestens zweimal im Jahr durchgeführt. monday.coms DR-Test kann in Form einer Begehung, einer simulierten Katastrophe oder eines Komponententests erfolgen.

Datenspeicherung und -vernichtung

Datenspeicherung

monday.com wird Ihre Daten, die monday.com kontrolliert, so lange aufbewahren, wie es notwendig ist, um die in unserer Datenschutzrichtlinie dargelegten Zwecke zu erfüllen. Daten, die monday.com im Auftrag unserer Kunden verarbeitet, werden in Übereinstimmung mit unseren Nutzungsbedingungen, unserer Ergänzung zur Datenverarbeitung und anderen kommerziellen Vereinbarungen mit diesen Kunden aufbewahrt.

Datenlöschung
Die Kunden von monday.com behalten die volle Kontrolle über die von ihnen übermittelten Daten und können diese jederzeit mit den über die Benutzeroberfläche der Dienstleistung verfügbaren Mitteln ändern, exportieren oder löschen.
Bei Beendigung oder Ablauf des Abonnements können die Kunden die Löschung ihrer Daten im Rahmen des Kontoschließungsverfahrens beantragen. Die Kundendaten werden dann innerhalb von 90 Tagen nach dem Antrag gelöscht, einschließlich einer 30-tägigen Frist für ein Rollback und einer weiteren 60-tägigen Frist für die Durchführung des Löschvorgangs.
Alternativ können die Kunden sich dafür entscheiden, die Kontodaten auf der Plattform zu belassen. In diesem Fall können wir die Daten weiterhin aufbewahren, sie aber auch jederzeit nach unserem Ermessen löschen.

Datenvernichtung2
Unsere Dienstleistung wird auf AWS gehostet, wobei bestimmte Daten auf GCP gesichert werden. Beide Cloud Computing-Anbieter setzen proprietäre Datenverteilungs- und -löschungsstrategien ein, um eine sichere Speicherung sensibler Daten in einer mandantenfähigen Umgebung zu ermöglichen. Die Stilllegung von Speichermedien wird von den genannten Anbietern unter Anwendung der in NIST 800-88 beschriebenen Techniken durchgeführt.

Überwachung und Protokolle

monday.com sammelt und überwacht Netzwerkprotokolle mithilfe eines Network Intrusion Detection System (NIDS) sowie mithilfe von Traffic-Protokollen von Edge-Standorten, Protokollen auf Anwendungsebene zur Nachverfolgung und Prüfung von Ereignissen und Protokollen auf Systemebene zur Prüfung des Zugriffs und hochprivilegierter Vorgänge. Die Protokolle werden in unsere SIEM-Lösung (Security Information and Event Management) eingespeist, wo sie kontinuierlich (24 Stunden an 7 Tagen in der Woche und 365 Tagen im Jahr) von einem verwalteten SOC-Team überwacht werden.

Lieferkettenmanagement

Unterauftragsverarbeiter
monday.com verlangt von seinen Unterauftragsverarbeitern (sowohl in der globalen Datenregion als auch in der EU-Datenregion) die Einhaltung von Industriestandards in Bezug auf die Datensicherheit und den Schutz der Privatsphäre und betrachtet beide Bereiche als entscheidend für den Auswahlprozess der Unterauftragsverarbeiter. Neben anderen Maßnahmen haben wir sichergestellt, dass für alle unsere Unterauftragsverarbeiter Ergänzungen zur Datenverarbeitung und andere relevante Unterlagen und Schutzmaßnahmen vorhanden sind, und wir führen Bewertungen des Datenschutzes, der Rechtslage und der Informationssicherheit sowie auf Fragebögen basierende Audits durch, die alle den Industriestandards und behördlichen Anforderungen entsprechen. Die Bewertungen unserer Unterauftragsverarbeiter werden mindestens einmal im Jahr durchgeführt.

Anbietermanagement
monday.com unterhält ein zentrales Repository Asset Management-Programm sowohl für die von uns genutzten Dienstleitungen als auch für die von uns genutzte Software. Das Repository wird laufend von unseren Teams für Sicherheit, Recht, Datenschutz und Beschaffung gepflegt, und der Genehmigungsprozess wird allen Mitarbeitern mitgeteilt.
Zu Beginn der Nutzung und Erneuerung von den Dienstleistungen oder der Software kategorisieren die verschiedenen Teams die Anbieter, mit denen wir zusammenarbeiten, nach der höchsten

Datensensibilitätsstufe, auf die sie Zugriff haben, um die entsprechende Risikostufe zu bestimmen und sie gemäß den Branchenstandards und gesetzlichen Anforderungen zu überprüfen.

Physische Sicherheit

monday.com-Büros

Die physischen IT-Bestände in den Büros von monday.com beschränken sich auf Laptops und Büronetzwerkgeräte. Die Netzwerkgeräte des Büros sind in einem passwortgeschützten, rund um die Uhr, an 7 Tagen die Woche und an 365 Tagen im Jahr CCTV-überwachten, umweltkontrollierten Serverraum geschützt. Der physische Zugang zu den Büros wird durch biometrische Identifizierung kontrolliert. Besucher werden beim Betreten unserer Büros registriert und müssen während ihres Aufenthalts im Büro stets von einem monday.com-Mitarbeiter begleitet werden. Alle Mitarbeiter sind verpflichtet, verdächtige Aktivitäten, unbefugten Zutritt zu den Räumlichkeiten sowie Diebstahl oder Verlust von Gegenständen zu melden.

Sicherheit im Rechenzentrum

monday.com verlässt sich auf die erstklassigen physischen und umwelttechnischen Sicherheitsmaßnahmen von AWS und GCP, welches in einer äußerst widerstandsfähigen Infrastruktur resultiert. Weitere Informationen über diese Sicherheitsmaßnahmen finden Sie unter den folgenden Links:
https://aws.amazon.com/security/, https://cloud.google.com/security/

7. Compliance, Datenschutz und Zertifizierungen

Audit-Sicherheit und -Compliance
monday.com hat seine Sicherheits- und Datenschutzprogramme in Übereinstimmung mit mehreren branchenüblichen Compliance-Programmen sowie mit den führenden Datenschutzbestimmungen in den Ländern, in denen wir unsere Dienste anbieten, entwickelt:

ISO 27001, 27017, 27018, 27032 und 27701
monday.com hält sich an die internationalen Standards der ISO (Internationale Organisation für Normung) und verwaltet seine Informationssicherheit, den Cloud-Service und den Datenschutz in Übereinstimmung hiermit. Wir werden jährlich von einer unabhängigen dritten Partei geprüft und halten 5 ISO-Zertifikate:

- **ISO/IEC 27001:201**3 ist der strengste globale Sicherheitsstandard für Informationssicherheitsmanagementsysteme (ISMS).
- **ISO/IEC 27018:2014** legt allgemein anerkannte Kontrollziele, Kontrollen und Richtlinien für die Umsetzung von Maßnahmen zum Schutz personenbezogener Daten (PII) in Übereinstimmung mit den Datenschutzgrundsätzen in ISO/IEC 29100 für die öffentliche Cloud-Computing-Umgebung fest.
- **ISO/IEC 27017:2015** bietet Kontrollen und Implementierungsleitlinien sowohl für Cloud-Service-Anbieter als auch für Cloud-Service-Kunden. Sie enthält Leitlinien für Informationssicherheitskontrollen, die auf die Bereitstellung und Nutzung von Cloud-Diensten anwendbar sind, indem sie zusätzliche Implementierungsanleitungen für relevante Kontrollen bietet.
- **ISO/IEC 27032:2012** bietet einen Leitfaden für die Verbesserung der Cybersicherheit, wobei die besonderen Aspekte der Cybersicherheit und ihre Abhängigkeiten von anderen Sicherheitsbereichen hervorgehoben werden, insbesondere: Informationssicherheit, Netzsicherheit, Internetsicherheit und Schutz kritischer Informationsinfrastrukturen (CIIP).
- **ISO/IEC 27701:2019** spezifiziert Anforderungen und bietet Anleitungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Privatsphären-Informationsmanagementsystems (PIMS)

Alle unsere Zertifizierungen finden Sie hier.

SOC 1, SOC 2 und SOC 3
monday.com hat Service- und Organisationskontrollen erreicht:

- **SOC 1 Typ II Audit**, bei dem Kontrollen untersucht werden, die für die Finanzberichterstattung von Kunden relevant sein können.
- **SOC 2 Type II Audit**, das unser Engagement für die Einhaltung der strengsten Sicherheits-, Verfügbarkeits- und Vertraulichkeitsstandards in der Branche unter Beweis stellt. Es bestätigt, dass die Sicherheitskontrollen von monday.com den Grundsätzen und Kriterien des AICPA (The American Institute of Certified Public Accountants) für Trust Services und den HIPAA-Sicherheitsanforderungen entsprechen.
- **SOC 3 Report**, der eine kürzere Version unseres SOC 2 Typ II-Berichts und öffentlich zugänglich ist.

Die Audits werden jährlich von einem unabhängigen Dritten durchgeführt und ein Bericht, der die Monate April bis März abdeckt, wird jährlich veröffentlicht.
Die SOC-Berichte von monday.com finden Sie unter den folgenden Links: SOC 1, SOC 2 und SOC 3.

Cloud-Sicherheitsallianz (CSA)

Die Cloud Security Alliance (CSA) ist eine gemeinnützige Organisation, deren Ziel es ist, „die Verwendung von Best Practices für die Gewährleistung der Sicherheit im Cloud Computing zu fördern und Aufklärung über die Verwendung von Cloud Computing zu leisten, um die Sicherheit aller anderen Formen des Computing zu unterstützen".

monday.com nimmt am freiwilligen CSA Security, Trust, Assurance, and Risk Registry (STAR)-Self-Assessment teil, um die Einhaltung der von CSA-veröffentlichten Best Practices zu dokumentieren. Der von uns ausgefüllte CSA Consensus Assessments Initiative Questionnaire (CAIQ) ist kostenlos und öffentlich auf der CSA-Website verfügbar.

Der Health Insurance Portability and Accountability Act (HIPAA)

Der Health Insurance Portability and Accountability Act (HIPAA) dient dem Schutz von Daten im Gesundheitswesen. Organisationen wie Krankenhäuser, Arztpraxen, Krankenversicherungen oder Unternehmen, die mit geschützten Gesundheitsinformationen (PHI) umgehen, sind verpflichtet, den HIPAA zu befolgen. Dies gilt auch für Unternehmen, die mit diesen Firmen zusammenarbeiten und in deren Auftrag mit PHI in Kontakt kommen.

monday.com bietet seinen Kunden des Enterprise-Plans eine HIPAA-konforme Kontokonfiguration, damit diese Kunden ihre sensiblen Gesundheitsdaten übermitteln können. Unsere HIPAA-Kunden müssen unsere Geschäftspartnervereinbarung (Business Associate Agreement – BAA) abschließen, um den Schutz und die ordnungsgemäße Verarbeitung von PHI in ihrem Namen zu gewährleisten, bevor sie HIPAA-Daten übermitteln.

monday.com und die DSGVO

Unser globales Datenschutzprogramm basiert auf den umfassendsten und fortschrittlichsten Datenschutzbestimmungen der Welt, wobei die allgemeine Datenschutz-Grundverordnung (DSGVO) der EU und Großbritanniens als unser „Polarstern" dient.

Unter anderem überwacht das Datenschutzforum von monday.com kontinuierlich die Produkt- und Prozessentwicklungen innerhalb unserer Organisation sowie die verschiedenen Aktivitäten, die mit der Nutzung personenbezogener Daten verbunden sind, um sicherzustellen, dass die DSGVO-Prinzipien eingehalten werden, wie z. B. die Prinzipien des Privacy-by-Design, der Datenminimierung und Speicherbegrenzung, der Rechtmäßigkeit und Fairness bei der Verarbeitung sowie der Transparenz unserer Aktivitäten und Zwecke.

Datenschutzrichtlinie

Die Datenschutzrichtlinie von monday.com, die unsere Datenschutz- und Datenverarbeitungspraktiken in Bezug auf personenbezogene Daten, die wir für unsere eigenen Zwecke als Datenverantwortlicher verarbeiten, beschreibt, finden Sie unter dem folgenden Link.

Ergänzung zur Datenverarbeitung (DPA)

Die Geschäftsbedingungen von monday.com und die Kundenverträge enthalten alle eine Ergänzung zur Datenverarbeitung, um den Schutz und die ordnungsgemäße Verarbeitung personenbezogener Daten im Namen unserer Kunden zu gewährleisten. Sie können unseren Datenverarbeitungszusatz (DPA) onlineeinsehen und ausführen.

Grenzüberschreitende Übertragungen von personenbezogenen Daten

monday.com hat seinen Sitz in Israel und verfügt über Niederlassungen in den USA, im Vereinigten Königreich, in Australien und in Brasilien sowie über Support-Teams in der Ukraine und in Guatemala. Unsere Unterauftragsverarbeiter sind ebenfalls in verschiedenen Ländern registriert, wie auf unserer Seite über Unterauftragsverarbeiter beschrieben.
Wenn wir personenbezogene Daten aus dem EWR und dem Vereinigten Königreich in andere Länder übermitteln, stützen wir uns auf die rechtmäßigen Übermittlungsmechanismen der DSGVO, wie z. B. die „Angemessenheitsbeschlüsse" der Europäischen Kommission (z. B. die Beschlüsse, die dem Vereinigten Königreich und Israel ein angemessenes Schutzniveau für personenbezogene Daten aus der EU bescheinigen) und die EU-Standardvertragsbestimmungen, die Sie hier und hier finden.

Controller und Auftragsverarbeiter

In der Datenschutz-Grundverordnung werden zwei Hauptrollen bei der Erhebung und Verarbeitung personenbezogener Daten definiert und unterschieden: Datenverantwortliche und Datenverarbeiter. Ein Datenverantwortlicher bestimmt die Mittel und Zwecke der Verarbeitung personenbezogener Daten, während ein Datenverarbeiter eine Partei ist, die Daten im Auftrag des für die Datenverarbeitung Verantwortlichen verarbeitet.

- monday.com ist der Datenverantwortliche für die personenbezogenen Daten seiner Kunden, Benutzer und Website-Besucher. Dies wird in unserer Datenschutzrichtlinie weiter ausgeführt.
- monday.com ist der Datenverarbeiter der personenbezogenen Daten, die seine Kunden und Benutzer auf der Plattform (in den Boards und Artikeln innerhalb ihres monday.com-Accounts) eingeben, und verarbeitet diese Daten im Auftrag seiner Kunden. Wir tun dies gemäß der mit unseren Kunden abgeschlossenen Ergänzung zur Datenverarbeitung. Die Drittanbieter, die uns bei der Verarbeitung dieser Daten helfen, sind unsere „Unterauftragsverarbeiter".

monday.com und der CCPA

Als „Dienstanbieter" verpflichtet sich monday.com, die geltenden Anforderungen des California Consumer Privacy Act von 2018 (CCPA) und die Vorschriften des Generalstaatsanwalts von Kalifornien im Lichte ähnlicher Vorschriften weltweit (wie der DSGVO) und sich entwickelnder Industriestandards einzuhalten – um sicherzustellen, dass unsere Kunden monday.com weiterhin ohne Unterbrechung nutzen können und personenbezogene Daten kalifornischer Verbraucher in Übereinstimmung mit dem CCPA verarbeiten können.

Weitere Informationen finden Sie hier.

Das australische Datenschutzgesetz (APA) und die australischen Datenschutzgrundsätze (APP)
Das australische Datenschutzgesetz (APA) und die australischen Datenschutzgrundsätze (APP) schaffen einen strukturierten Rahmen für die Erfassung, Verarbeitung, Verwendung und Weitergabe persönlicher Daten und geben dem Einzelnen mehr Kontrolle über die Art und Weise, wie seine Daten behandelt werden. monday.com verpflichtet sich, die Anforderungen des APA und der APP einzuhalten.
Weitere Informationen finden Sie hier.

Interne Audits
Unsere Teams für Sicherheit, Datenschutz, Infrastruktur, F&E, IT, Betrieb und Recht führen vierteljährliche Sicherheits- und Datenschutzwochen durch, die die Durchführung verschiedener Audits, einschließlich Überprüfungen des Benutzerzugriffs, Überprüfungen der Firewall-Konfiguration, Clean-Desk-Inspektionen, Sensibilisierungsschulungen und -aktivitäten und vieles mehr, beinhalten.

Offenlegung gegenüber Regierungsbehörden

monday.com gewährt staatlichen Stellen keinen unbegründeten Zugang zu den bei uns gespeicherten Kundendaten. Wir erhalten nur selten Anfragen von Behörden (in den USA oder anderswo) zur Offenlegung von Kundendaten. Die wenigen Fälle, in denen wir in den vergangenen Jahren solche Anfragen erhalten haben, waren vom Umfang her begrenzt und bezogen sich auf sehr legitime Gründe für die Anforderung solcher Daten (z. B. vermutete illegale Aktivitäten im Zusammenhang mit dem jeweiligen Konto).
Nachdem die Anfrage von unseren Rechts- und Datenschutzteams geprüft wurde, um sicherzustellen, dass sie gültig und gerechtfertigt ist, beschränkt sich die Offenlegung auf Daten, die nach dem Gesetz unbedingt erforderlich sind. Wir bemühen uns nach besten Kräften, unsere Kunden zu benachrichtigen, bevor wir eine solche Offenlegung vornehmen, es sei denn, wir sind dazu nicht berechtigt oder aufgrund eines potenziellen Risikos nicht in der Lage.[3] Wir verpflichten uns außerdem, alle wirtschaftlich vertretbaren Anstrengungen zu unternehmen, um vorbehaltlich der geltenden Gesetze jedem Ersuchen um Massenüberwachung in Bezug auf personenbezogene Daten zu widerstehen, die gemäß der GDPR oder der GDPR des Vereinigten Königreichs geschützt sind, u. a. auch gemäß Abschnitt 702 des FISA.

PrivacyTeam und DSB

monday.com wird von PrivacyTeam, der führenden Datenschutzberatung in Israel, geschützt und arbeitet intensiv mit PrivacyTeam zusammen, um zu garantieren, dass die Kundendaten und die Privatsphäre geschützt werden. Weitere Informationen finden Sie hier.
monday.com hat den erfahrenen Datenschutz-Veteranen Aner Rabinovitz von PrivacyTeam zu unserem Datenschutzbeauftragten ernannt, der die laufende Einhaltung der Datenschutzbestimmungen bei monday.com überwacht und berät und als Ansprechpartner in Datenschutzfragen für Betroffene und Aufsichtsbehörden dient.

---

[3] Weitere Informationen finden Sie in Abschnitt 4 („Datenweitergabe“) unserer Datenschutzrichtlinie.

8. Epilog

Dieses Whitepaper hat einen umfassenden Überblick über den Ansatz von monday.com zu Sicherheit und Datenschutz gegeben. Natürlich können Sie aufgrund der Komplexität dieser Themen weitere Fragen haben.
Weitere Informationen finden Sie in unserem Sicherheits-Trustcenter und im Rechtsportal.
Wenn Sie weitere Fragen zur Informationssicherheit oder zum Datenschutz bei monday.com haben, können Sie unsere Teams auch unter security@monday.com oder dpo@monday.com kontaktieren, und zwar zusätzlich zum allgemeinen Support, der Ihnen rund um die Uhr an 7 Tagen in der Woche und 365 Tagen im Jahr unter support@monday.com zur Verfügung steht.
Sie möchten Sie ein Sicherheitsproblem oder eine Sicherheitslücke melden? Senden Sie uns eine E-Mail an security@monday.com oder melden Sie es über unser HackerOne-Formular an https://monday.com/security/form/.

HAFTUNGSAUSSCHLUSS: Bei dieser Version handelt es sich um eine Übersetzung des englischen Originals, die nur zur Vereinfachung bereitgestellt wird. Das englische Original ist die offizielle und rechtlich verbindliche Version und hat im Falle einer Abweichung Vorrang.