Beekeeper Security

White Paper

BEEKEEPER

INHALT

VERPFLICHTUNGSERKLÄRUNG

Die Produkte und Services von Beekeeper werden vielen Unternehmen weltweit und in einer Vielzahl von Marktsegmenten bereitgestellt. Unsere Kunden vertrauen uns ihre Datensicherheit und Privatsphäre an, und alle **Beekeeper-Mitarbeitenden setzen sich im Gegenzug mit vollem Engagement dafür ein, dieses Vertrauen zu wahren.**

Die Geschäftsleitung unterstützt die Umsetzung aller Tools und Prozesse, die für eine lückenlose Informationssicherheit notwendig sind. Wir halten vollumfänglich an unserer Verpflichtung fest, die **Vertraulichkeit, Integrität und Datenverfügbarkeit unserer Kundendaten zu wahren**.

Um das höchste Maß an Vertrauen bei unseren Kunden zu erreichen und unser Leistungsversprechen weiter auszubauen, haben wir ein ISMS (Managementsystem für Informationssicherheit) gemäß **des international anerkannten Industriestandards für Informationssicherheit und Datenschutz implementiert,** wie es im Zertifizierungsprozess nach ISO 27001:2013, ISO 27017:2015 und ISO 27018:2019 dargelegt ist.

Die nachfolgende Dokumentation bescheinigt unsere Verpflichtung zum Schutz von Kundendaten. Beekeeper wird auch in Zukunft aufmerksam und unermüdlich daran arbeiten, unser ISMS kontinuierlich zu verbessern und unsere Datenschutzverpflichtung gegenüber unseren Kunden und Mitarbeitenden aufrechtzuerhalten.

„Beekeeper wendet ausschließlich die höchsten Sicherheitsstandards bei Systemen und Prozessen an, um Ihr Recht auf Privatsphäre und Datenschutz zu gewährleisten.“

Cris Grossmann
CEO & Co-Gründer

SÄULEN DER BEEKEEPER-SICHERHEIT

Für Beekeeper haben Vertraulichkeit, Integrität und Datenverfügbarkeit höchste Priorität. Unsere Verpflichtung zum kontinuierlichen Schutz von Kundendaten- und Datenschutzprozessen umfasst die folgenden Punkte:

1. Beekeeper verwendet branchenführende Datensicherheitstechnologien und befolgt umfassende Defense-in-Depth-Konzepte zum Schutz von Daten.

2. Beekeeper betreibt ein hochleistungsfähiges Sicherheitssystem, das Produkt und Plattform kontinuierlich auf Schwachstellen überprüft.

3. Der technische Bereitschaftsdienst von Beekeeper gewährleistet rund um die Uhr schnelle Reaktionszeit, um jegliche Sicherheitsbedrohung zu erkennen und darauf zu reagieren.

4. Beekeeper ist bestrebt, erstklassige Sicherheitsstandards zu erreichen und hat die von der Internationalen Organisation für Normung (ISO) als Mindestanforderung definierten Kontrollen der Informationssicherheit vollständig implementiert.

5. Beekeeper verpflichtet sich zu höchsten Sicherheitsstandards und kontinuierlicher Weiterentwicklung. Daher unterzieht Beekeeper sich regelmäßig sowohl internen als auch externen Audits und Sicherheitsüberprüfungen.

Die Sicherheitsverfahren von Beekeeper entsprechen den sechs Säulen der Informationssicherheit, die auf der rechten Seite abgebildet sind. Jede Säule trägt zum Einsatz modernster Sicherheitstechnologien und -kontrollen bei und erfüllt in Kombination die Anforderungen unseres ISMS (Managementsystem für Informationssicherheit). Dies deckt sich mit und geht sogar noch über die Anforderungen des strengen Akkreditierungsverfahrens hinaus, wie unsere Zertifizierungen nach ISO 27001:2013, ISO 27017:2015 und ISO 27018:2019 belegen.

SÄULEN DER BEEKEEPER-SICHERHEIT

Virtual Private Cloud

Die Produkte und Services von Beekeeper werden in Virtual Private Clouds (VPCs) bereitgestellt, die mit stabilen Sicherheitsmaßnahmen und -kontrollen konfiguriert sind. Alle unsere VPCs werden in zertifizierten Rechenzentren gehostet, die von unseren Cloud-Anbietern (Cloud Service Providers) bereitgestellt werden. Unsere Produkte und Services werden unseren Kunden in verschiedenen Gerichtsbarkeiten zur Verfügung gestellt, und die Kunden haben die Wahl, ihre Daten entweder in der Schweiz, in der EU oder in den USA zu speichern.

Die Mandanten unserer Kunden innerhalb unserer VPCs sind so konzipiert, dass sie den höchsten Sicherheits- und Verfügbarkeitsstandards entsprechen. Jeder Kundenmandant ist außerdem vollständig logisch von anderen Kundenmandanten und -daten getrennt, wodurch für jeden Mandanten eine unabhängige Kundenumgebung sichergestellt ist.

Operative Sicherheit

Beekeeper hat führende Sicherheitsverfahren eingeführt, die auf einer „Shift-Left"-Mentalität beruhen. Sicherheit ist von Anfang an ein Faktor des auf Microservices basierenden Produktlebenszyklus, bei dem automatisierte Prozesse das jeweils zuletzt getestete und auf Qualität geprüfte Produkt mit einem Minimum an menschlicher Intervention in die Produktionsumgebung überführen.

Wir haben robuste und zeitgemäße Protokollierungs- und Überwachungsfunktionen implementiert, die durch modernste Technologien unterstützt werden. Unsere Sicherheitsprüfungen und -tests beinhalten ein umfassendes Verfahren zur Handhabung von Schwachstellen. Der Vorfallsreaktionsplan (Incident Response Plan) von Beekeeper ermöglicht es uns, Situationen und Szenarien bei Sicherheitsvorfällen auf standardisierte und konsistente Weise zu beheben.

Zugriffskontrolle durch Kunden

Beekeeper wurde als interne Kommunikationsplattform entwickelt. Der Kunde hat die vollständige Kontrolle über die Zugriffsbereitstellung zu seinem Mandanten. Ausschließlich administrative Rollen via den Beekeeper-Admin-Bereich oder automatisierte Kontrollprozesse wie Active Directory ermöglichen die Kontrolle über das Identitätsmanagement.

Komplette Verschlüsselung

Beekeeper verwendet in diversen Anwendungsfällen kryptografische Maßnahmen, einschließlich der Verschlüsselung aller externen Kommunikationskanäle sowie der Verschlüsselung von Daten im Ruhezustand, unabhängig davon, ob sich die Daten im Speicher oder auf dem mobilen Gerät des Endnutzers befinden.

SÄULEN DER SICHERHEIT

Einhaltung von DSGVO- und ISO-27001-Bestimmungen

Beekeeper richtet sich nach der Datenschutzgrundverordnung (DSGVO), die den Schutz personenbezogener Daten regelt, sowie nach anderen gesetzlich festgelegten Datenschutzbestimmungen. Beekeeper hat eine ISMS-Rahmenvereinbarung in Übereinstimmung mit den ISO-27001-Kontrollzielen implementiert und die Zertifizierung nach ISO 27001:2013 erreicht. Der Beekeeper-Datenverarbeitungsvertrag ist eine vertragliche Vereinbarung zwischen Beekeeper und seinen Kunden, in der alle diesbezüglichen Anforderungen festgelegt sind. Zusätzlich wurden die Zertifizierungen für ISO 27017:2015 und ISO 27018:2019 erlangt. Diese Sicherheitsstandardisierungen bestätigen nachweislich die Konformität von Beekeeper als SaaS-Anbieter, sowohl als Cloud-Anbieter wie auch bei der personenbezogenen Datenverarbeitung in Cloud-Lösungen.

Hohe Verfügbarkeit

Beekeeper verpflichtet sich im Rahmen des kommerziellen Abonnementvertrags mit seinen Kunden zu einer Verfügbarkeit von 99,9 %. Beekeeper kommt dieser Verpflichtung mit mehrfacher Redundanz und regelmäßig durchgeführten Tests der Serviceverfügbarkeit nach.

BEEKEEPER-ZERTIFIZIERUNG

Die Internationale Organisation für Normung (ISO) ist eine unabhängige, nichtstaatliche Organisation, die sich aus den Mitgliedern der nationalen Normungsgremien von 164 Ländern zusammensetzt. ISO 27001 setzt sich aus einer Reihe von Anforderungen für Informationssicherheit und Datenschutz in Bezug auf die Verwaltung von Kundendaten zusammen und entspricht den höchsten internationalen Datensicherheitsstandards. Wichtig dabei ist, dass die ISO-Normen das Ergebnis eines konsensbasierten und von Experten aus aller Welt erarbeiteten Prozesses sind, in dem umfangreiche internationale Erfahrungen und Kenntnisse aus allen Wirtschaftssektoren gebündelt wurden.

Zu den Daten, die unter die von ISO 27001 eingeführten Risikomanagementkontrollen fallen, gehören Kunden- oder Mitarbeiterdaten oder alle uns anvertrauten persönlichen Informationen. Darüber hinaus legen die ISO-27017- und ISO-27018-Zertifizierungen den Rahmen der Kontrollziele fest, die für den Betrieb eines Cloud-Anbieters sowie für die Verarbeitung personenbezogener Daten in einer cloudbasierten Umgebung erforderlich sind.

Erfahren Sie mehr über den Beekeeper-Zertifizierungsprozess der ISO-27000-Reihe und die kontinuierliche Einhaltung der ISO-27001-, ISO-27017- und ISO-27018-Informationssicherheitsstandards.

Zertifizierte Rechenzentren

Beekeeper verwendet ausschließlich zertifizierte Rechenzentrumsanbieter, die international anerkannte und genehmigte Compliance-Zertifizierungen für das Informationssicherheitsmanagement erhalten haben:

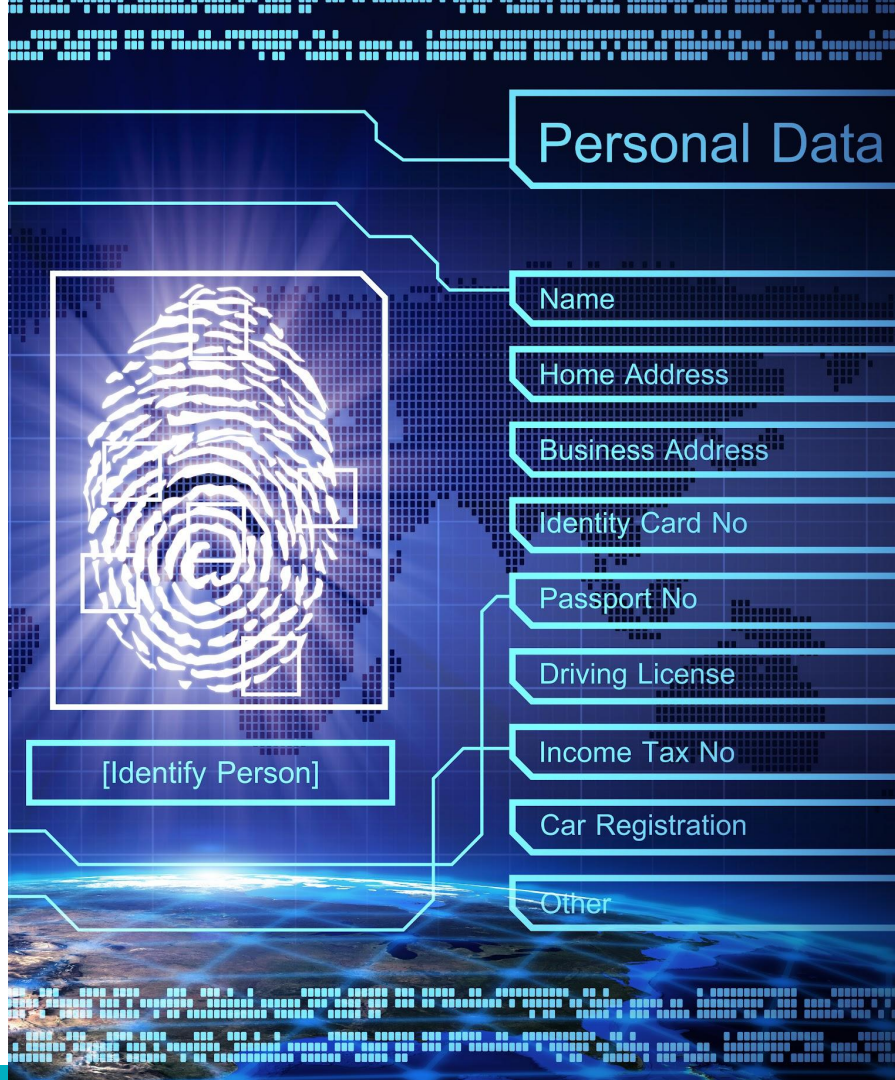
- Amazon Web Services: aws.amazon.com/compliance/
- Google Cloud Platform: cloud.google.com/security/compliance/

DATENSCHUTZ

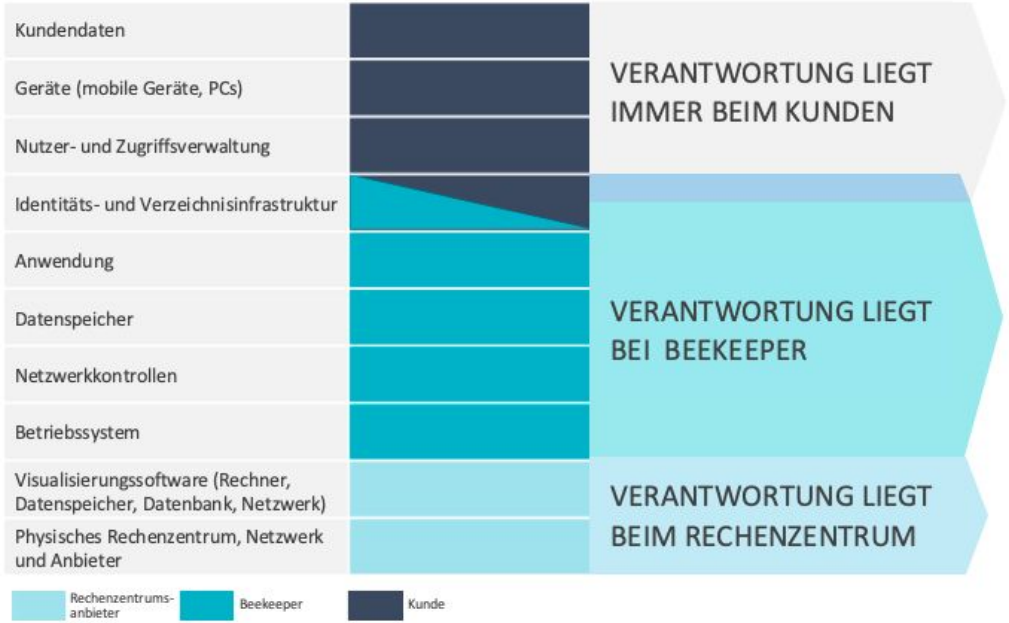
Beekeeper stützt sich auf die grundlegenden und striktesten gesetzlichen Anforderungen, wie sie in der Datenschutzgrundverordnung (DSGVO) und dem Schweizerischen Bundesgesetz über den Datenschutz (DSG) als Rahmen für die Datenschutzanforderungen personenbezogener Daten dargelegt und entsprechend in unserem Vertrag zur Auftragsverarbeitung und unserer Datenschutzbestimmung festgehalten sind.

Ihre Daten werden in Übereinstimmung mit den sieben Grundsätzen des Datenschutzes und der Rechenschaftspflicht verarbeitet, die in der DSGVO erläutert werden.

Technische Maßnahmen wie die Verwendung von Verschlüsselungstechnologien sind Standard und in die Produktlinien und Services von Beekeeper integriert. Verfahren wie die Durchführung von Datenschutz-Folgenabschätzungen (Privacy Impact Assessment) vor der Einführung neuer Produkte oder Services sind Teil unseres Produkt- und Services-Entwicklungszyklus. Die Liste der organisatorischen und technischen Maßnahmen findet sich im Vertrag zur Auftragsverarbeitung von Beekeeper (Anhang 2).



UNSER MODELL DER GETEILTEN VERANTWORTUNG



- In Beekeeper gespeicherte und verarbeitete Kundendaten
- Die für den Zugriff auf Beekeeper verwendeten Geräte sowie deren Verwaltung und Sicherheit
- Die Konten und Nutzer sowie deren Zugangsberechtigungen auf den Kundenmandanten von Beekeeper

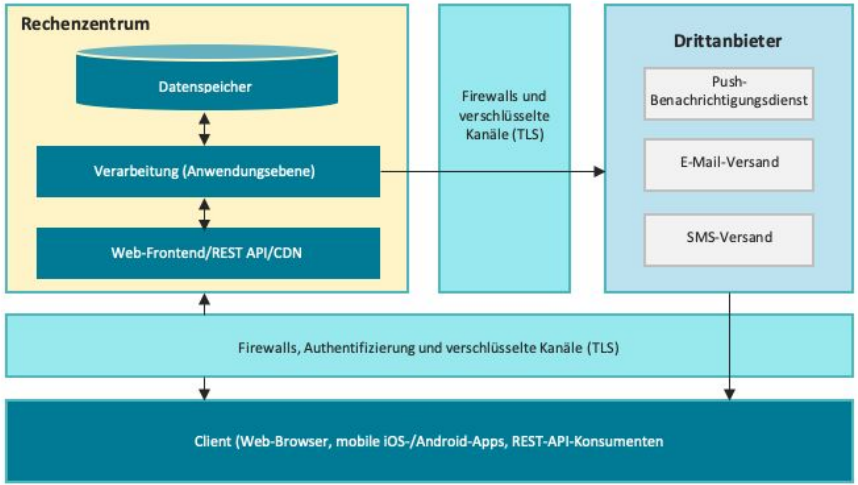
- *Die Integration von Identitäten und Konten kann als gemeinsame Aufgabe geregelt sein.*

- Vertraulichkeit, Integrität und Verfügbarkeit der Beekeeper-Plattform und der darin enthaltenen Daten
- Datenverschlüsselung bei der Übertragung und im Ruhezustand
- Hohe Verfügbarkeit, Datensicherung und Notfallwiederherstellung
- Netzwerk-, Cluster- und Hosting-Sicherheit, einschließlich VPC, Firewalls, Subnetze, gehärtete Ressourcen und Sicherheits-Toolings

- Beekeeper ist verantwortlich für die Beauftragung von Rechenzentrumsanbietern, die sich um Cloud-Management und Virtualisierungsdienste kümmern.
- Hohe Verfügbarkeitsanforderungen an Rechenzentrum
- Physische Überprüfungen und Umgebungskontrollen

SICHERHEITSARCHITEKTUR

Als SaaS-Anbieter (Software as a Service) maximieren wir die Sicherheit unserer Cloud-Plattform durch einen umfassenden Defense-in-Depth-Ansatz, der eine Hochverfügbarkeitsarchitektur, strenge Zugriffskontrolle, sichere Trennung, Datenverschlüsselung, Härtung und regelmäßige Backups umfasst. Unsere Services werden in Virtual Private Clouds (VPCs) mit höchster Sicherheit bereitgestellt, die kontinuierlich auf Sicherheitsbedrohungen und Schwachstellen überprüft werden.



Datenspeicherung: Die Daten werden unter Verwendung modernster Cloud-Speicherdienste gespeichert, die sich durch Sicherheit und Resilienz sowie konstante Betriebszeit und Leistung auszeichnen.

Mandantentrennung: Jeder unserer Kunden wird als unabhängiger Mandant definiert und seine Kundendaten werden logisch getrennt von anderen Kundenmandanten und -daten gespeichert.

Firewalls: Wir haben Perimeter-Firewalls in allen unseren VPCs konfiguriert. Zusätzlich haben wir eine Web Application Firewall (WAF) zum Schutz der Anwendungsebene eingerichtet.

Verbindungen zu Drittanbietern: Push-Benachrichtigungen, E-Mails und SMS-Textnachrichten werden über Drittanbieter gesendet. Alle Kommunikationskanäle mit Dritten werden mit sicheren Protokollen verschlüsselt.

VERSCHLÜSSELUNG UND SCHLÜSSELMANAGEMENT

Beekeeper verfügt über Kryptographie- und Schlüsselmanagementrichtlinien und -verfahren, um die Vertraulichkeit, Authentizität und Integrität von Informationen durch Verschlüsselung zu schützen.

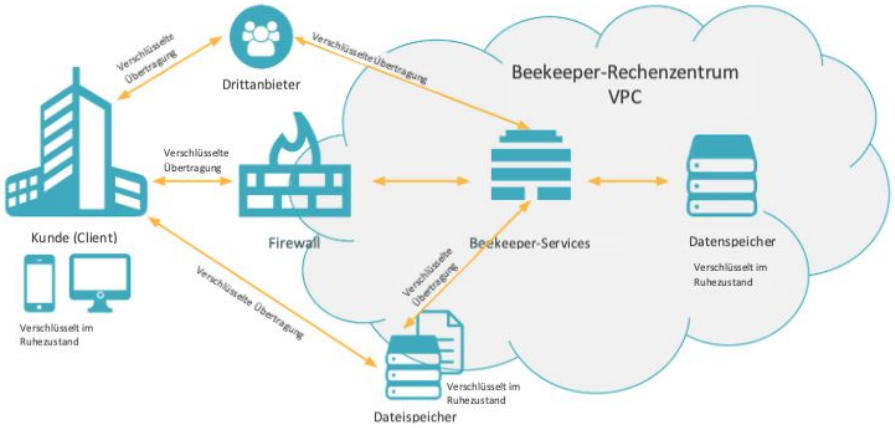
Im Ruhezustand: Daten im Ruhezustand werden verschlüsselt. Die Datenbanken in den Rechenzentren sind ebenso wie die Daten auf iOS- und Android-Geräten AES-256-verschlüsselt.

Bei der Übertragung: Die gesamte Kommunikation mit der Beekeeper-Plattform erfolgt über verschlüsselte Tunnel unter Verwendung von TLS 1.2 und 1.3, wobei starke Chiffrier-Suiten mit einer 256-Bit-AES-Verschlüsselung für sichere Verbindungen bei der Datenübertragung über das unsichere Internet verwendet werden.

Schlüsselmanagement

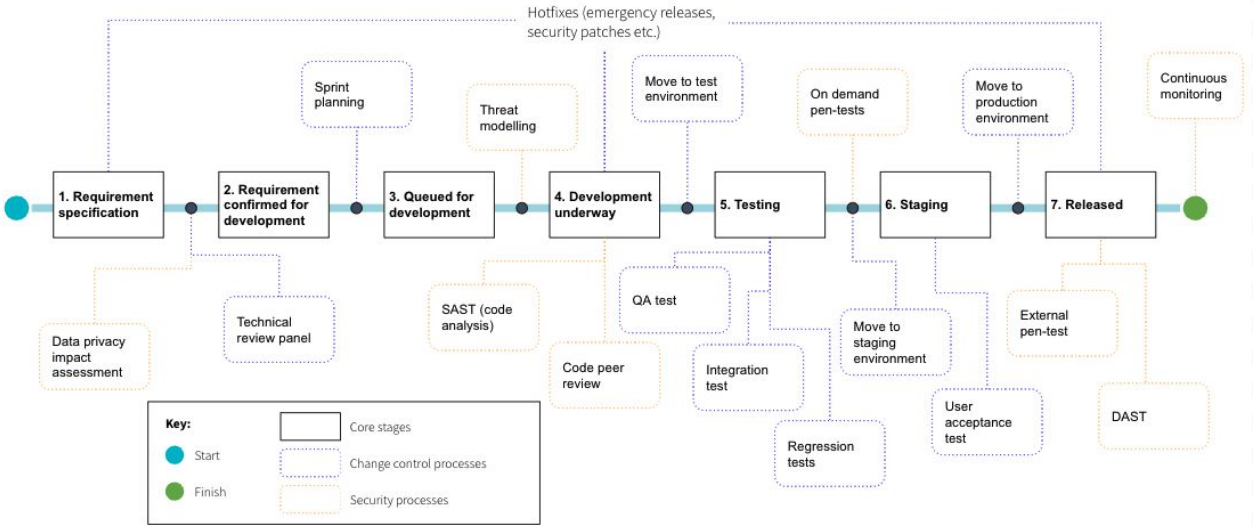
Nach dem Modell der geteilten Verantwortung werden alle Verschlüsselungsschlüssel für die physische Infrastruktur (d. h. die physischen Rechenzentren) von den jeweiligen Cloud-Anbietern verwaltet. Die Verschlüsselungsschlüssel, die für die Verbindung und den Zugriff auf virtuelle Server, Datenbanken, S3-/Speicher-Buckets und Backups verwendet werden, werden vollständig von Beekeeper verwaltet.

Datenflussdiagramm



LEBENSZYKLUS DER PRODUKTENTWICKLUNG

Beekeeper folgt bei der Implementierung von Code-Änderungen am Produkt und an den Services von Beekeeper einem klar definierten Change-Management-Prozess. Unser Entwicklerteam wendet sichere Programmiertechniken und Best Practices an, wie sie von OWASP oder SANS definiert sind. Entwickler werden bei ihrer Einstellung und im weiteren Verlauf in den Methoden der sicheren Anwendungsentwicklung geschult. Abgeleitet von den ISO-27001-Kontrollzielen schreiben die Informationssicherheitsregulierungen von Beekeeper eine strikte Aufgabenteilung sowie getrennte Umgebungen vor, um die Vertraulichkeit, Integrität und Verfügbarkeit unserer Informationssysteme zu maximieren.



- Beekeeper hat ein formelles Change-Management-Verfahren eingeführt, um bei Änderungen an Systemen/Anwendungen die Einhaltung formeller Prozesse sicherzustellen.
- Entwicklungs-, Staging- und Produktionsumgebungen sind voneinander getrennt.
- Der Zugang, um Änderungen an Produktionssystemen vorzunehmen, ist auf autorisierte Nutzer beschränkt.
- Sicherheitsprozesse sind vollständig in den Lebenszyklus von Änderungen und Produktentwicklung integriert.
- Beekeeper hat ein formelles Verfahren zur Handhabung von Sicherheitspatches eingeführt und umgesetzt.

SICHERHEITSPRÜFUNG UND GEWÄHRLEISTUNG

Externe Sicherheitstests

Unsere Richtlinien für die Informationssicherheit sehen vor, unabhängige externe Firmen für jährliche Penetrationstests an Beekeeper hinzuzuziehen. Alle Ergebnisse werden in unserem Risikoinventar festgehalten und es werden in Übereinstimmung mit unserem Change-Management-Prozess Maßnahmen zur Risikominderung definiert und umgesetzt.

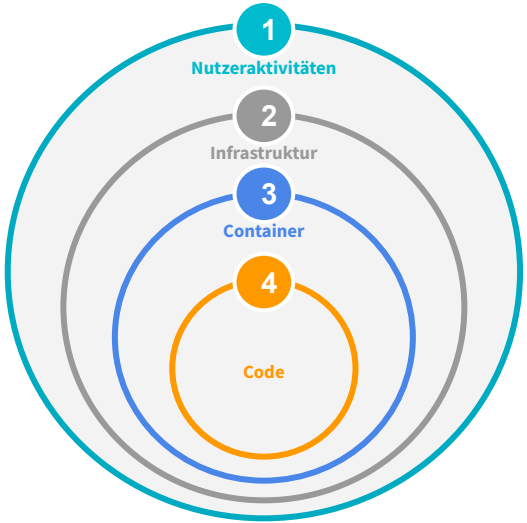
Interne Sicherheitstests

Folgende interne Schwachstellenprüfungen werden automatisch durchgeführt:

- Unabhängig von Code-Änderungen:
  - Tägliche Überprüfung der SSL-Zertifikate
  - Wöchentliches Scannen der Konfiguration, Aktivitätsüberwachung und Überprüfung anhand dokumentierter Best Practices
  - Wöchentliche dynamische Anwendungssicherheitstests
- Bei jeder Code-Änderung:
  - Obligatorisches Peer-Review-Verfahren
  - Statische Anwendungssicherheitstests
  - Reihe von Modul- und Integrationstests mit Schwerpunkt auf Zugriffsberechtigungen
  - Schwachstellenprüfungen der Systembibliothek

PROTOKOLLIERUNG UND ÜBERWACHUNG

Bei Beekeeper haben wir robuste und zeitgemäße Protokollierungs- und Überwachungsfunktionen implementiert, die durch modernste Technologien unterstützt werden. Wir verfügen über spezielle Tools und strenge Prozesse für die Erfassung, Korrelation und Aufbewahrung von Protokollen. Wir setzen WAF vor allen unseren Anwendungen ein, um verdächtigen Datenverkehr kontinuierlich zu überwachen und zu filtern. Wir verfolgen einen Zero-Trust-Ansatz und sind daher in der Lage, verdächtige Nutzeraktivitäten in unserem Netzwerk zu erkennen. Unser technischer Bereitschaftsdienst ist rund um die Uhr im Einsatz, um auch außerhalb der Geschäftszeiten auf alle Sicherheitsereignisse zu reagieren.



Ebenen der Protokollierung und Überwachung bei Beekeeper

1. Nutzeraktivitäten

Unter anderem protokollieren wir Nutzeraktivitäten, einschließlich Zeit- und Datumsstempel, IP-Adressinformationen, Benutzername und ID, Art der beabsichtigten Aktivitäten sowie Systeme, auf die zugegriffen wurde.

2. Infrastruktur

Zusätzlich zu den nativen Cloud-Services (z. B. GuardDuty) betreiben wir weitere Lösungen zur Protokollierung und Überwachung von IAM, VPC, DNS und anderen sicherheitsrelevanten Ereignissen.

3. Container

Wir haben hochentwickelte Tools implementiert, die uns die Protokollierung, Überwachung, Zusammenfassung und Meldung von Sicherheitsereignissen ermöglichen, die sich ausschließlich auf Container beziehen.

4. Code

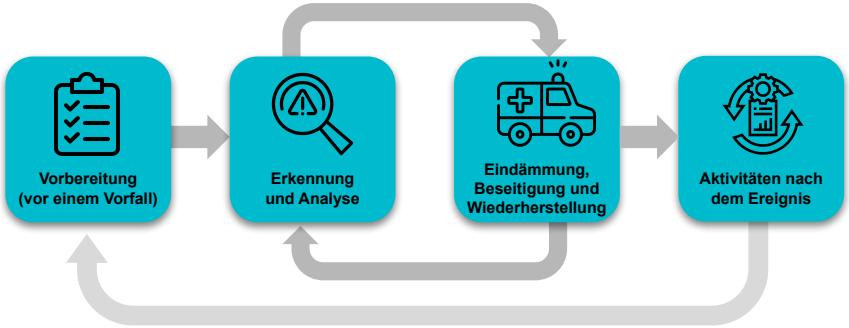
Wir überwachen aktiv unsere Codebasis und Bibliotheken, um bekannte/ aufgedeckte Schwachstellen zu identifizieren. Zusätzlich verwalten wir ein Inventar unserer öffentlichen Bibliotheken, Repos und Abhängigkeiten.

VORFALLSREAKTION UND BENACHRICHTIGUNG

Sollte ein Vorfall gemäß unserer Schweregradskala als schwerwiegend eingestuft werden, verfügen wir über einen präzise ausgearbeiteten Vorfallsreaktionsplan sowie einen Krisenkoordinationsplan, welche im Ernstfall zum Einsatz kommen. Unser Vorfallsreaktionsplan folgt dem Computer Security Incident Handling Guide von NIST, dem Branchenstandard zur Handhabung von Computersicherheitsvorfällen. Er wurde entwickelt, um Cyberangriffe in unserer Umgebung zu bewältigen, und umfasst vier Phasen:

Phase 1: Vorbereitung (vor einem Vorfall)
Phase 2: Erkennung und Analyse
Phase 3: Eindämmung, Beseitigung und Wiederherstellung
Phase 4: Nach dem Ereignis

Dies ermöglicht uns die nötige Flexibilität, Situationen und Szenarien bei Sicherheitsvorfällen auf standardisierte und konsistente Weise zu beheben.



Im Falle einer Verletzung des Schutzes personenbezogener Daten wird Beekeeper Sie im Einklang mit den geltenden Datenschutzbestimmungen (z. B. DSGVO, CCPA) unverzüglich und, sofern möglich, spätestens 72 Stunden nach Bekanntwerden der Verletzung des Schutzes personenbezogener Daten gemäß dem Beekeeper-Benachrichtigungsverfahren bei Sicherheitsvorfällen (Incident Management Notification Process) informieren.

Dieses Verfahren steht im Einklang mit den in ISO 27001/27017/27018 definierten Kontrollzielen zum Management von Informationssicherheits-Vorfällen sowie mit den Anforderungen der DSGVO nach Art. 33, 34. Beide sind im Vertrag zur Auftragsverarbeitung festgehalten.

PLAN ZUR NOTFALL-WIEDERHERSTELLUNG

Der Zweck unseres Notfallwiederherstellungsplans (Disaster Recovery Plan) ist es, Beekeeper auf längere Serviceausfälle vorzubereiten, die durch Faktoren verursacht werden, die außerhalb unserer Kontrolle liegen (z. B. Naturkatastrophen, von Menschen verursachte Ereignisse), und die Dienste innerhalb eines minimalen Zeitrahmens so weit wie möglich wiederherzustellen. Für alle unsere Rechenzentren wurde ein Notfallwiederherstellungsplan definiert und es werden vierteljährliche „Disaster Days“ durchgeführt, an denen wir die Wirksamkeit dieser Pläne testen und bewerten und basierend auf den Erkenntnissen Aktualisierungen vornehmen.

Datenerhalt und -wiederherstellung

In Übereinstimmung mit den ISO-27001-Kontrollzielen für Geschäftskontinuität und Notfallwiederherstellung nutzt Beekeeper die von seinen zertifizierten Rechenzentren verwalteten Dienstleistungen zur Datenerhaltung. Unsere Lösungen sind mit vollständig funktioneller Redundanz ausgestattet und werden im Laufe des Jahres mehrfach getestet. Alle Verfügbarkeitszonen sind auf denselben Gerichtsstand beschränkt wie das von Beekeeper genutzte Rechenzentrum. Die meisten unserer Dienste arbeiten in zustandslosem Modus. Bei einem Notfall können wir also neue Services zur Verfügung stellen, während die Daten in der Datenbank verfügbar bleiben.

Die Datenbank wird in mehreren Verfügbarkeitszonen betrieben, um Resilienz und Verfügbarkeit sicherzustellen (d.h. eine primäre Datenbank repliziert Daten synchron auf eine Standby-Instanz in einer anderen Verfügbarkeitszone). Im Notfall vertraut Beekeeper auf die automatischen Backups und Datenbank-Snapshots, die von unserem Rechenzentrumsanbieter durchgeführt werden. Die Verschlüsselung im Ruhezustand ist ebenfalls für alle Backup-Systeme implementiert.

ZUGRIFF AUF BEEKEEPER

Auf Beekeeper kann über eine Reihe von digitalen Schnittstellen zugegriffen werden. Jede Schnittstelle bietet Sicherheitseinstellungen, die sowohl die Benutzerdaten schützen als auch die Zugänglichkeit gewährleisten.

Web-Browser: Browser speichern nur ein sicheres Cookie, das den aktuellen Nutzer authentifiziert. Es findet keine lokale Speicherung von Kundendaten über diese Schnittstelle statt.

Mobile Apps: Auf Android und iOS werden die Zugangsdaten in verschlüsselten Containern gespeichert, die das Betriebssystem zur Verfügung stellt.

Benutzerdefinierte REST API: Beekeeper hat eine REST API entwickelt und stellt eine Dokumentation zur Verfügung, um die besten Sicherheitspraktiken bei der Programmierung benutzerdefinierter Clients hervorzuheben.

Verbindungen zu Beekeeper

Alle Verbindungen zu Beekeeper erfolgen über HTTPS (nur TLS 1.2 und 1.3). Jeder Versuch, eine Verbindung über HTTP herzustellen, wird zu HTTPS umgeleitet.

ZUGRIFFSKONTROLLE

Beekeeper definiert die Zugriffskontrolle als Komponenten bestehend aus zwei Schlüsselfaktoren:

- Authentifizierung
- Autorisierung

Zur Verwaltung der Zugriffskontrollanforderungen hat Beekeeper firmeneigene Systeme und Schnittstellen sowie ein Kontroll-Dashboard entwickelt.

Authentifizierung

Für interne Prozesse, die den Anforderungen der Zugriffskontrollgrundsätze für unsere Beekeeper-Produkte und -Services entsprechen, setzt Beekeeper für seine Mitarbeitenden eine Zwei-Faktor-Authentifizierung voraus.

Für den Kundenzugriff kann Beekeeper die Einhaltung der Unternehmensrichtlinien wahren, wenn die Zwei-Faktor-Authentifizierung über eine Single-Sign-on-Lösung (SSO) stattfindet. Beekeeper ist außerdem in der Lage, sich mit dem Personenverzeichnis des Unternehmens zu verbinden, und kann zudem andere Arten von Authentifizierungsmechanismus in Betracht ziehen.

Autorisierung

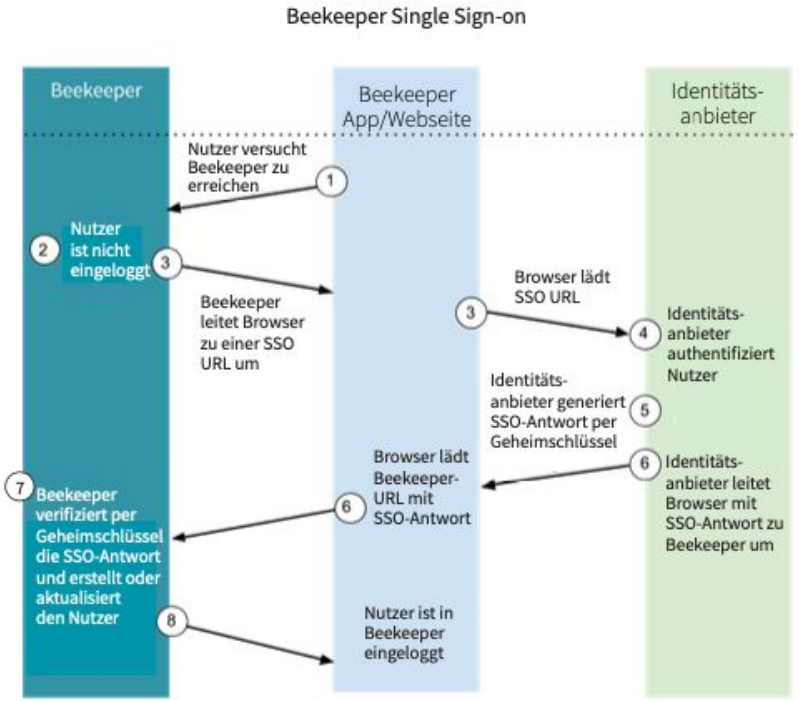
Beekeeper verwendet einen Autorisierungsserver nach Industriestandard, der für die Bereitstellung der Zugriffsrechte zum Beekeeper-System zur Anwendung kommt. Die Beekeeper-Berechtigungsfunktionen stehen dem vom Kunden bestimmten Administrator im Admin-Bereich zur Verfügung.

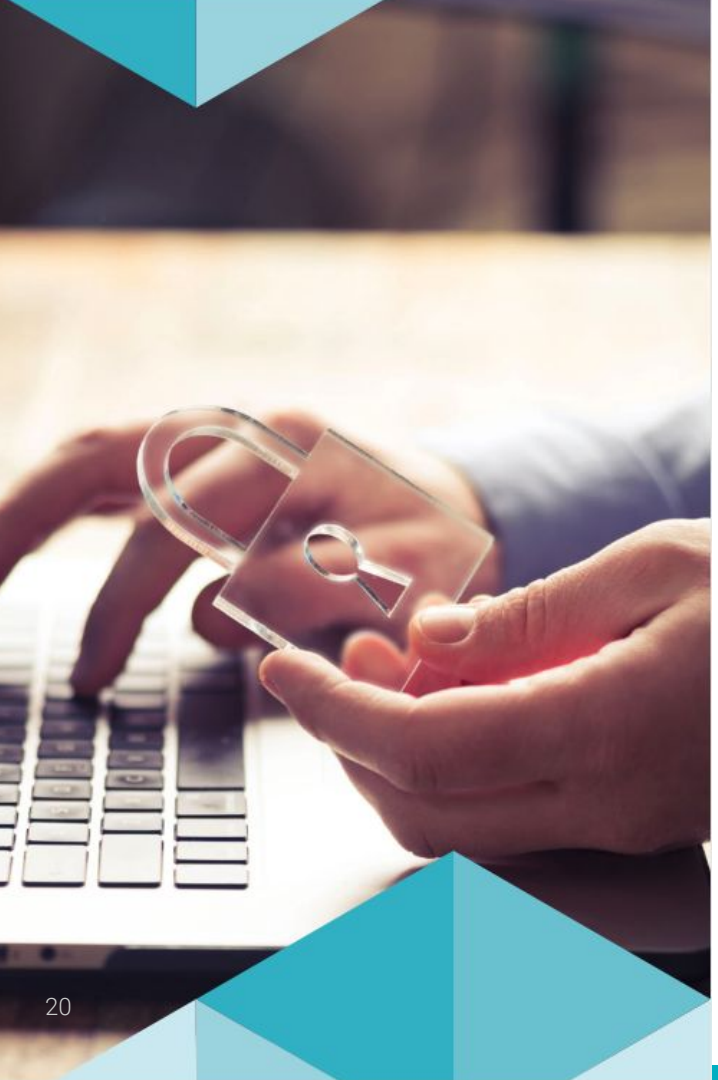
ZUGRIFFSKONTROLLE

Der Admin-Bereich von Beekeeper

Die vom Kunden bestimmten Administratoren können den Admin-Bereich von Beekeeper über sichere interne Kommunikationskanäle nutzen und verfügen über die folgenden Administrationsberechtigungen:

- Nutzer erstellen, aktualisieren oder löschen
- Einen aktiven Nutzer abmelden
- Nutzerzugang sperren
- SAML-Single-Sign-on konfigurieren
- Massenimporte und Aktualisierungen von Nutzern via Excel-Datei vornehmen





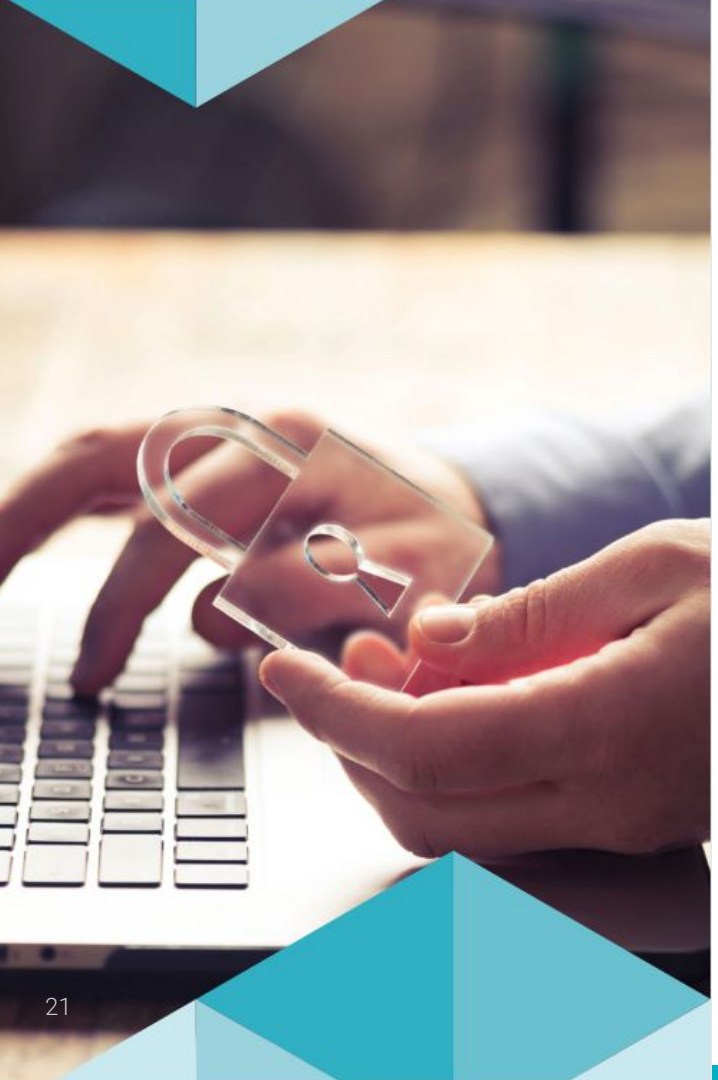
SICHERHEITSFUNKTIONEN BEI DER PRODUKTNUTZUNG

Authentifizierung

- Das Login erfolgt über E-Mail, Telefonnummer oder Benutzername in Kombination mit einem Passwort.
- Die voreingestellte Passwortstärke umfasst 8 oder mehr Zeichen (Groß- und Kleinbuchstaben und mindestens eine Zahl).
- Administratoren können Passwörter zurücksetzen.
- Nach dem ersten Login erfolgt die Aufforderung, das Passwort zu ändern.
- Wenn das Passwort zurückgesetzt wird, kann kein früheres Passwort verwendet werden.
- Nutzer werden nach X Tagen automatisch ausgeloggt (Anzahl Tage wird vom Admin bestimmt).
- Login auf dem mobilen Gerät erfolgt via QR-Code.
- Nutzer werden bei Login mit einem einmaligen QR-Code per E-Mail benachrichtigt.
- Administratoren können Nutzer ausloggen und Konten sperren.
- Das Ausloggen durch einen Administrator meldet den Nutzer auf allen seinen Geräten ab.
- Das Konto wird nach 10 erfolglosen Login-Versuchen gesperrt.

Autorisierung

- Jedem Nutzer ist eine Rolle zugewiesen, die definiert, was er innerhalb der Anwendung tun kann (siehe Admin Help Center).



SICHERHEITSFUNKTIONEN BEI DER PRODUKTNUTZUNG

- Timeout
  - Zeitbeschränkungen können für den Fall konfiguriert werden, wenn Nutzer von öffentlichen Computern auf Beekeeper zugreifen.
- Nutzer sperren
  - Administratoren können Nutzer jederzeit sperren. Ein gesperrter Nutzer wird sofort von allen Clients abgemeldet und verliert den Zugriff auf alle Daten. Die Daten eines gesperrten Nutzers bleiben erhalten und können für die forensische Datenanalyse zur Verfügung gestellt werden.
- E-Mail-Domains können vom Login gezielt ausgeschlossen oder zugelassen werden.
- Single Sign-on (SAML)
- Der Nutzer wird beim Einloggen von einem zuvor unbekannten Gerät per E-Mail benachrichtigt.
- Backup
  - Die regelmäßigen Backups der Benutzerinformationen sowie aller Daten werden aufbewahrt, um die Daten im Falle einer versehentlichen oder mutwilligen Zerstörung wiederherstellen zu können.
- Rollen
  - Verfügbare Rollen: Globale Admins, Admins für Organisationseinheiten, Standort-, Gruppen- und Stream-Admins und Inhaltsmoderatoren (siehe Admin Help Center)
- Aktivitätsüberwachung über das Meta-Dashboard (Kunden müssen den Datenzugriff anfordern, um diese Informationen einzusehen.)
  - Möglichkeit, das letzte Login anhand der Geräteinformation zu sehen
  - Liste mit den für das Login verwendeten Geräten
- Antivirusprogramm zur Überprüfung von Dateien, die innerhalb der Beekeeper-App gesendet werden
- Verbot oder Einschränkung, die App in einer anderen Seite einzubetten

HÄUFIG GESTELLTE FRAGEN

F: Können Daten und Nachrichten zur internen Archivierung oder Überprüfung exportiert werden?
A: Ja, auf der Grundlage eines festgelegten Prozesses kann Beekeeper für den Zweck der automatischen Archivierung Zugriff auf die Daten gewähren.

F: Können Berichte über Sicherheitspenetrationstests eingesehen werden?
A: Ja, auf Anfrage können Berichte früherer Penetrationstests zur Verfügung gestellt werden.

F: Findet das Hosting der Beekeeper-Plattform in einer gemeinsam genutzten Cloud-Infrastruktur statt?
A: Ja, aber unsere zertifizierten Rechenzentren verfügen über Virtual Private Clouds, um die Datenisolierung von verschiedenen Beekeeper-Kunden zu gewährleisten.

F: Bietet Beekeeper die Möglichkeit des lokalen Hostings (On-Prem) an?
A: Nein, wir bieten kein lokales Hosting an.

F: Ist ein Audit-Protokoll verfügbar?
A: Ja, ein Audit-Protokoll kann im CSV-Format zur Verfügung gestellt werden.

F: Sind die Produkte und Services von Beekeeper konform mit den HIPAA-Sicherheitsanforderungen?
A: Die Produkte und Services von Beekeeper erfüllen die Anforderungen der HIPAA-Sicherheitskontrollen, indem wir ein ISMS (Managementsystem für Informationssicherheit) implementiert haben, das nach den Industriestandards für Informationssicherheit der ISO-Akkreditierungsstelle zertifiziert ist. Es ist wichtig zu beachten, dass Beekeeper eine interne Kommunikationsplattform und keine Plattform zur Verarbeitung von Gesundheits- und Patientendaten ist.

F: Wie ist der Support und die Systemwartung von Beekeeper geregelt?
A: Der Support und die Systemwartung für das Beekeeper-Produkt (SaaS-Angebot) erfolgen durch die Support-Zentren in Zürich, Schweiz, und Krakau, Polen. Beekeeper bietet außerdem lokalen Kunden-Support durch unsere Niederlassungen in den USA und in Deutschland an.

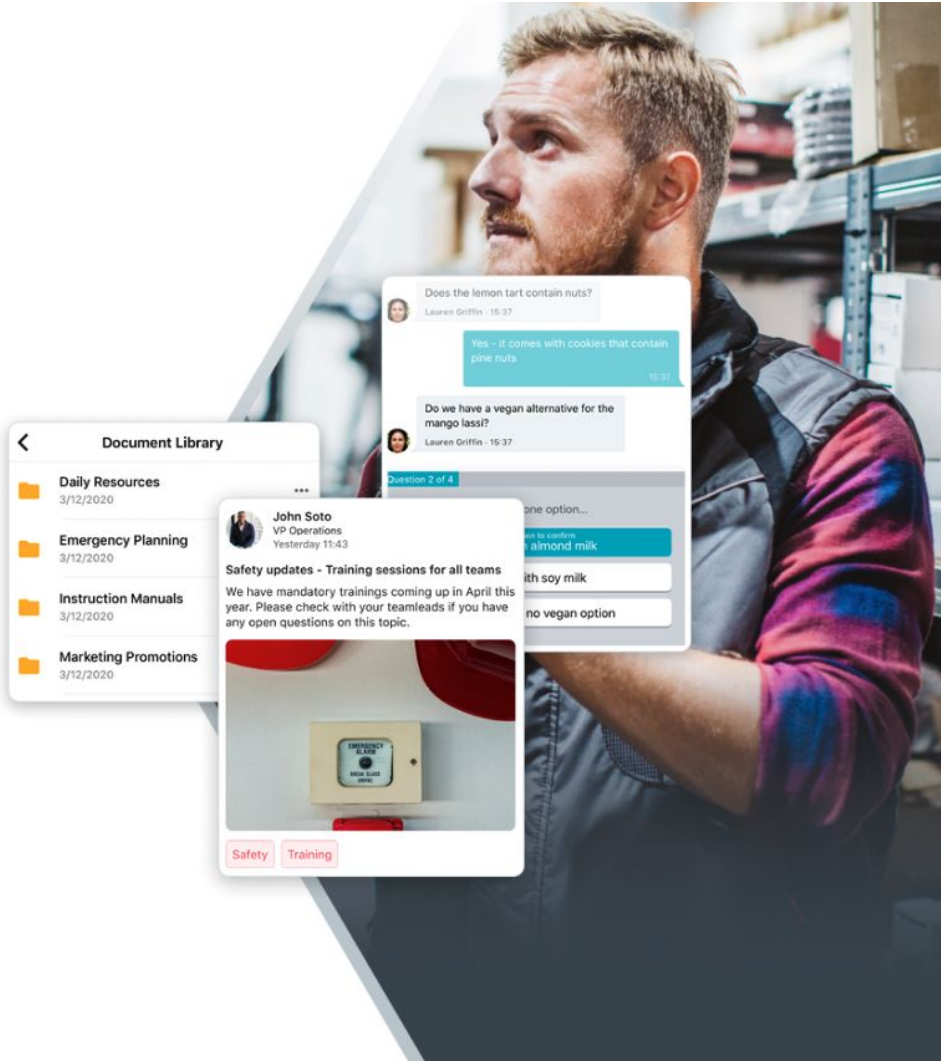
Weitere Informationen finden Sie unter beekeeper.io/datensicherheit.

Kontakt:
Wenn Sie weitere Fragen zur Datensicherheit haben, kontaktieren Sie uns unter security@beekeeper.io.

BEEKEEPER

Beekeeper revolutioniert die Arbeit in gewerblich geprägten Unternehmen. Mit unserem Success System für die Frontline können Firmen Schluss mit Papierkram und analogen Prozessen machen, Mitarbeitende besser einbinden und länger halten, sowie die Produktivität erhöhen.

Geben Sie Ihrem Team direkten Zugang zu allen Personen, Prozessen und Systemen, die sie für Bestleistungen benötigen. Beekeeper wird rund um den Globus genutzt, um Mitarbeitende zu verbinden, Tools zu zentralisieren und Unternehmen weiterzubringen.



Jetzt loslegen

Weitere Informationen finden Sie unter
beekeeper.io/datensicherheit

Veröffentlichungsdatum (R3.1): August 2022