trengo

Trengo's Garantie: HÖCHSTE SICHERHEIT

September 2024

trengo.com

Trengo's Garantie: HÖCHSTE SICHERHEIT

Bei Trengo steht Sicherheit im Zentrum unserer Werte und ist fest in unserer Unternehmensphilosophie verankert. Sie ist mehr als nur eine technische Anforderung – sie ist ein Grundprinzip, das unser Handeln leitet und unsere Verpflichtung zu zuverlässigen und vertrauenswürdigen Dienstleistungen unterstreicht.

Wir sind uns bewusst, dass der Schutz von Daten und die Abwehr von Bedrohungen in der heutigen digitalen Welt einen umfassenden Ansatz erfordern. Deshalb betrachten wir Sicherheit durch ein ganzheitliches Quadrantenmodell, das alle Aspekte abdeckt – von den eingesetzten Systemen bis hin zu den Menschen, die sie nutzen.

Unser Sicherheitsansatz konzentriert sich auf vier wesentliche Bereiche: Systeme, Mitarbeiter, Kunden und Unternehmen. Dieses Modell verkörpert unser Verständnis, dass effektive Sicherheit eine gemeinsame Verantwortung ist. Bei Trengo sehen wir es als unsere Aufgabe, eine sichere Umgebung zu schaffen, doch wir verstehen, dass auch unsere Kunden eine entscheidende Rolle spielen. Unser Ziel ist es, durch kontinuierliche Kommunikation und gemeinsamen Einsatz ein sicheres Umfeld zu schaffen, in dem Trengo und undere Kunden erfolgreich agieren können.

Ein ganzheitlicher Sicherheitsansatz bei Trengo

Ihre Mitarbeiter

Bei Trengo wissen wir, dass menschliches Verhalten entscheidend für die Sicherheit ist. Wir setzen uns dafür ein, unseren Kunden benutzerfreundliche Werkzeuge, klare Anleitungen und informative Ressourcen bereitzustellen, um ihre Mitarbeiter zu befähigen, sichere Verhaltensweisen zu praktizieren. Durch die Bereitstellung intuitiver Tools und umfassender Unterstützung erleichtern wir es unseren Kunden, wirksame Sicherheitsmaßnahmen umzusetzen und potenzielle Risiken zu minimieren.

Auch mit unseren Ressourcen und Empfehlungen bleiben kontinuierliche Schulungen unerlässlich. Wir ermutigen unsere Kunden, ihre Mitarbeiter aktiv über Sicherheitstests und -updates zu informieren. Bei Trengo sehen wir dies als gemeinsame Aufgabe, bei der unser Support und die interne Schulung des Kunden zu einer starken Sicherheitsarchitektur beitragen.

Unsere öffentliche Produktdokumentation finden Sie in unserem Help Centre. Zusätzlich bieten wir eine exklusive Kundenakademie an, die Video-Kurse zur detaillierten Produktschulung für Trengo-Nutzer umfasst.

Systemkonfiguration

Unsere Plattform bietet robuste Sicherheitsfunktionen, ermöglicht individuelle Rollen- und Berechtigungsanpassungen und sorgt so für präzise Zugriffskontrolle. Des Weiteren bietet die Zwei-Faktor-Authentifizierung (2FA) eine entscheidende Sicherheitsebene und kann für alle Mitarbeiter verpflichtend gemacht werden, um den Schutz vor unbefugtem Zugriff zu erhöhen.

Um sichere Kommunikationswege zu gewährleisten, verwenden wir TLS-Verschlüsselung, die Daten während der Übertragung zwischen Ihren Systemen und unserer Plattform schützt. Zudem setzen wir OAuth2 ein, eine standardisierte Methode zur sicheren Authentifizierung, um Drittanbieter-Integrationen sicher und effizient zu gestalten. Diese Funktionen schützen vor Bedrohungen und geben Ihnen Vertrauen in eine sichere Systemkonfiguration.

Trengo's Mitarbeiter

Der Aufbau einer starken Sicherheitskultur ist ein zentraler Bestandteil unserer Arbeit. Regelmäßige Diskussionen über Sicherheitspraktiken und neue Bedrohungen sind fest in unserem internen Austausch verankert. Dieses kontinuierliche Engagement stellt sicher, dass jeder Trengoat über die neuesten Sicherheitsprotokolle und Best Practices informiert ist, was unser gemeinsames Bekenntnis zum Schutz unserer Systeme und Kundendaten stärkt.

Neue Mitarbeiter durchlaufen intensives Sicherheitstraining, um unsere hohen Standards von Anfang an zu erfüllen. Kundennahe Teams erhalten regelmäßige Schulungen, um sicherheitsrelevante Anfragen kompetent zu bearbeiten. So spielt jedes Teammitglied eine wichtige Rolle in unserer sicheren und widerstandsfähigen Umgebung.

Trengo's SaaS Lösung

Unser Service basiert auf dem grundlegenden Prinzip „Sicherheit durch Design", bei dem Sicherheit von Anfang an in jede Facette unserer Plattform integriert wird. Durch gezielte Designentscheidungen minimieren wir menschliche Fehler und potenzielle Schwachstellen, um höchste Schutzstandards zu gewährleisten.

Zur weiteren Stärkung unserer Sicherheitslage implementieren wir strenge Verfahren wie regelmäßige Zugriffsüberprüfungen und das Prinzip der minimalen Berechtigung. Diese Maßnahmen helfen, die Angriffsfläche zu begrenzen, indem sie sicherstellen, dass Benutzer und Systeme nur den für ihre Rolle notwendigen Zugriff erhalten, wodurch das Risiko unbefugter Zugriffe gemindert wird. Darüber hinaus sind sichere Backups und Datenverschlüsselung integrale Bestandteile unseres Services, die gewährleisten, dass Daten geschützt, privat und vollständig DSGVO-konform in Europe sind.

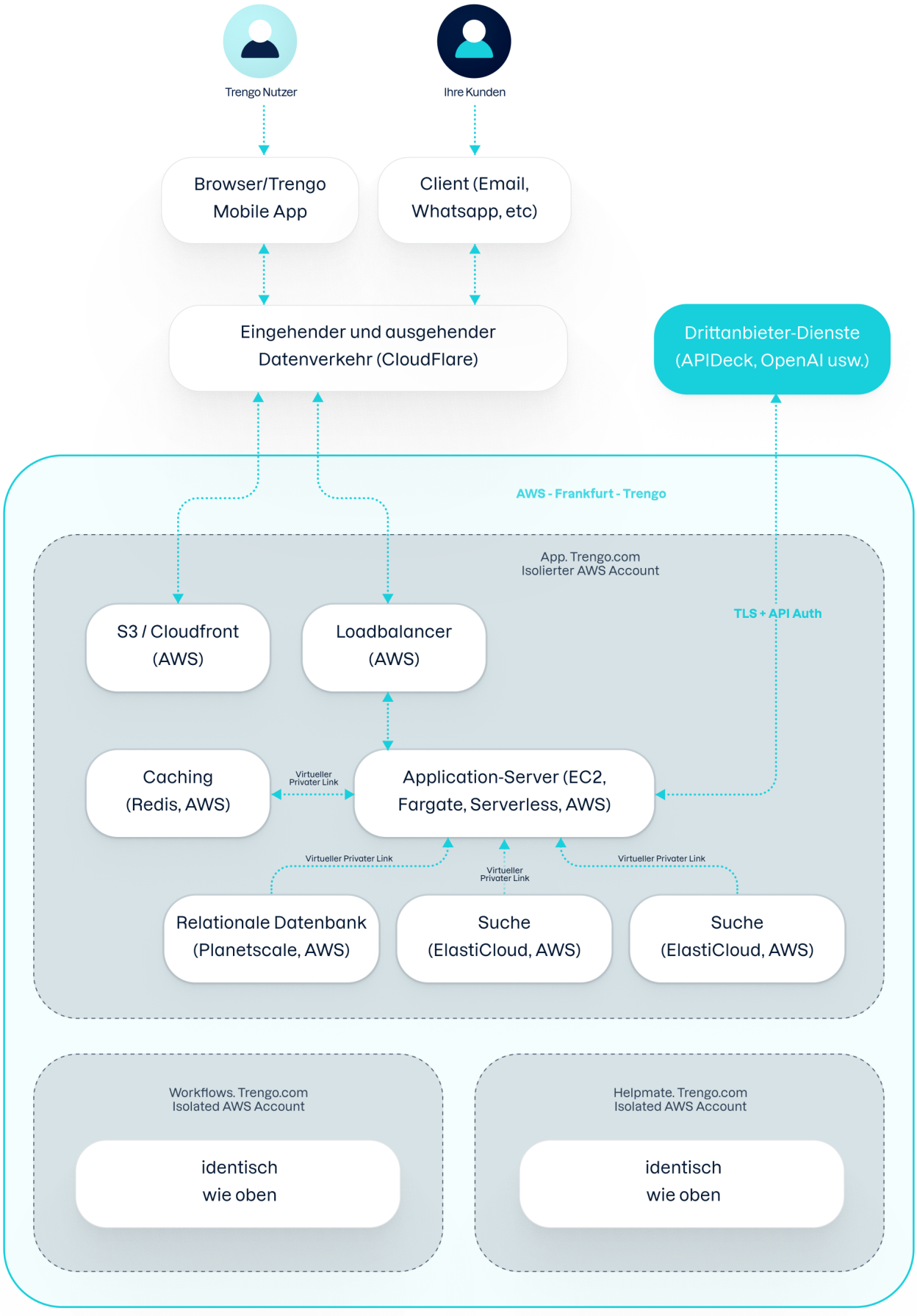
Zusätzlich sichern wir die Verbindungen zu Netzbetreibern durch fortschrittliche Verschlüsselungs- und Sicherheitsmaßnahmen, um einen umfassenden Schutz bei jeder Interaktion mit unserer Plattform zu gewährleisten.

Trengo Cloud Network / Architekturdiagramm

Trengo verwendet eine auf Platform-as-a-Service (PaaS) basierende Cloud-Architektur, um Betrieb und Änderungsmanagement zu optimieren und Best Practices einzuhalten. PaaS-Dienste ermöglichen eine effiziente Verwaltung unserer Infrastruktur und die Einhaltung etablierter Standards. Wir reduzieren die Exposition gegenüber offenen Netzwerken durch verkehrsspezifische Peer-to-Peer-Verbindungen via Virtual Private Links, was die Sicherheit erhöht und unbefugten Zugriff verhindert.

Unsere Anwendungen entwickeln wir nach einem konsistenten Architekturmodells, das Einfachheit fördert und das Risiko menschlicher Fehler reduziert. Diese Einheitlichkeit verbessert die betriebliche Effizienz und ermöglicht eine nahtlose Übertragbarkeit und Skalierbarkeit über verschiedene Systeme und Umgebungen hinweg.

Für optimale globale Verfügbarkeit und zentrale Überwachung sowie Kontrolle des Datenverkehrs—einschließlich Schutz vor DDoS-Angriffen—haben wir uns entschieden, über Cloudflare an das Edge-Netzwerk anzubinden. Diese Integration ermöglicht es uns, von Cloudflares umfangreichem Netzwerk zu profitieren, um Leistung, Sicherheit und Resilienz in allen Regionen zu steigern.


Trengo Nutzer
Ihre Kunden
Browser/Trengo Mobile App
Client (Email, Whatsapp, etc)
Eingehender und ausgehender Datenverkehr (CloudFlare)
Drittanbieter-Dienste (APIDeck, OpenAI usw.)
AWS - Frankfurt - Trengo
App. Trengo.com
Isolierter AWS Account
TLS + API Auth
S3 / Cloudfront (AWS)
Loadbalancer (AWS)
Caching (Redis, AWS)
Virtueller Privater Link
Application-Server (EC2, Fargate, Serverless, AWS)
Virtueller Privater Link
Virtueller Privater Link
Virtueller Privater Link
Relationale Datenbank (Planetscale, AWS)
Suche (ElastiCloud, AWS)
Suche (ElastiCloud, AWS)
Workflows. Trengo.com
Isolated AWS Account
identisch wie oben
Helpmate. Trengo.com
Isolated AWS Account
identisch wie oben

Häufig gestellte Fragen

Was ist der Unterschied zwischen SaaS und On-Premise Lösungen?

Eine On-Premise-Lösung ist ein System, das innerhalb eines bestimmten physischen Standorts gehostet und verwaltet wird, auch wenn es Unterstützung durch Drittanbieter erhalten kann. Im Gegensatz dazu sind Off-Premise-Lösungen, oft als cloudbasierte Lösungen bezeichnet, von externen Anbietern gehostet und unterstützt und können von verschiedenen Standorten aus zugegriffen werden. Während On-Premise-Lösungen auf einen einzelnen Standort beschränkt sind, operieren Off-Premise-Lösungen extern und bieten Remote-Zugriff.

SaaS (Software as a Service) ist ein Modell, bei dem der Dienstanbieter die Software hostet und wartet. Die Benutzer können Anwendungen und Daten aus der Ferne abrufen, was die Notwendigkeit eliminiert, Informationen von internen Unternehmensservern anzufordern und die Infrastruktur selbst zu verwalten.

Wie gewährt Trengo Datenverschlüsselung in Data-at-Rest und Data-in-Transit?

Zum Schutz der Vertraulichkeit und Integrität der Kundendaten nutzen wir umfassende Verschlüsselungsprotokolle für Daten im Ruhezustand und bei der Übertragung.

Data-at-Rest (Daten im Ruhezustand):

- **Verschlüsselungsstandards:** Wir verwenden Verschlüsselungsalgorithmen wie AES-256, um alle gespeicherten Daten, einschließlich Datenbanken, Dateispeicher und Backups, zu sichern.
- **Schlüsselverwaltung:** Wir verwalten Schlüssel sicher über ein zentrales Schlüsselmanagementsystem (KMS), das bewährte Verfahren wie regelmäßige Schlüsselrotation und strenge Zugriffskontrollen befolgt.
- **Zugriffskontrollen:** Der Zugriff auf verschlüsselte Daten ist auf autorisierte Personen beschränkt und wird regelmäßig überwacht und auditiert, um die Einhaltung unserer Sicherheitsrichtlinien sicherzustellen.

Data-in-Transit (Daten während der Übertragung):

- **Transport Layer Security (TLS):** Wir verwenden TLS 1.2 oder höher, um die Übertragung von Daten zwischen unseren Servern und den Kunden Geräten zu verschlüsseln.
- **Sichere APIs:** Alle API-Kommunikationen sind durch HTTPS gesichert, das TLS verwendet, um die Datenaustausche zwischen den Systemen zu schützen.

Häufig gestellte Fragen

Welche Sicherheitsstandards erfüllt Trengo's Plattform?

Unsere SaaS-Lösung erfüllt strenge Sicherheitsstandards, um den höchsten Schutz für die Daten unserer Kunden zu gewährleisten. Konkret halten wir uns an folgende Sicherheitsstandards:

- **NIST Cybersecurity Framework:** Wir orientieren uns am Cybersecurity Framework des National Institute of Standards and Technology (NIST). Dieses Framework bietet umfassende Richtlinien zur Verbesserung der Widerstandsfähigkeit und Sicherheit unserer Informationssysteme und umfasst Best Practices für die Identifizierung, den Schutz, die Erkennung, die Reaktion auf und die Wiederherstellung von Cyber-Bedrohungen.
- **DSGVO-Konformität:** Wir gewährleisten die Einhaltung der Datenschutz-Grundverordnung (DSGVO) für unsere Kunden in der Europäischen Union. Dazu gehören strenge Datenschutzmaßnahmen, transparente Datenverarbeitungspraktiken und die Wahrung der Rechte von betroffenen Personen.

Welche Protokolle nutzt Trengo zur Datensicherung?

Wir haben umfassende Backup-Protokolle eingerichtet, um die Integrität und Verfügbarkeit der Kundendaten zu gewährleisten und eine schnelle Wiederherstellung bei Störungen zu ermöglichen.

- **Regelmäßige Backups:** Wir führen regelmäßig automatisierte Backups aller kritischen Daten durch, einschließlich vollständiger wöchentlicher Backups und täglicher inkrementeller Backups, um Datenverlust zu minimieren.
- **Redundante Speicherung:** Backups werden an geografisch vielfältigen, redundanten Standorten gespeichert, um physische Katastrophen zu überstehen. Wir nutzen hochsichere Cloud-Speicherlösungen mit integrierter Redundanz und hoher Verfügbarkeit.
- **Verschlüsselung:** Alle Backup-Daten werden sowohl bei der Übertragung als auch im Ruhezustand mit fortschrittlichen Verschlüsselungsstandards (AES-256) geschützt, um unbefugten Zugriff zu verhindern.
- **Aufbewahrungsrichtlinien:** Wir pflegen eine strukturierte Aufbewahrungsrichtlinie, um sicherzustellen, dass Backups für angemessene Zeiträume gespeichert werden und eine Wiederherstellung zu verschiedenen Zeitpunkten möglich ist. Alte Backups werden sicher gelöscht, um Speicherplatz zu verwalten und gesetzliche Vorschriften einzuhalten.

Häufig gestellte Fragen

Wie geht Trengo mit Datenpannen um und was umfasst Trengo's Notfallplan?

Bei einer Datenpanne folgen wir einem strukturierten Plan, der darauf abzielt, Schäden zu minimieren und schnell eine effektive Lösung zu erreichen. Unser Ansatz umfasst:

1. **Erkennung und Identifizierung:** Wir nutzen fortschrittliche Überwachungswerkzeuge und Alarmsysteme, um potenzielle Pannen schnell zu erkennen und zu identifizieren. Jede ungewöhnliche Aktivität wird sofort zur Untersuchung gemeldet.
2. **Eindämmung:** Nach Bestätigung einer Panne isolieren wir umgehend die betroffenen Systeme, deaktivieren kompromittierte Konten und stoppen unbefugten Zugriff, um weiteren Datenverlust zu verhindern.
3. **Bewertung und Analyse:** Unser Sicherheitsteam führt eine gründliche Bewertung durch, um den Umfang und die Auswirkungen der Panne zu bestimmen. Dies umfasst die Analyse, wie die Panne zustande kam, welche Daten betroffen sind und welche Schwachstellen ausgenutzt wurden.
4. **Benachrichtigung:** Wir informieren umgehend die betroffenen Parteien gemäß den gesetzlichen und regulatorischen Anforderungen, einschließlich Kunden und Aufsichtsbehörden. Wir geben klare und zeitnahe Informationen über die Auswirkungen.
5. **Behebung:** Wir setzen Korrekturmaßnahmen um, um die Ursache der Panne zu beheben und zukünftige Vorfälle zu verhindern. Dies beinhaltet das Schließen von Sicherheitslücken, die Verstärkung von Sicherheitskontrollen und die Aktualisierung unserer Richtlinien und Verfahren.
6. **Wiederherstellung:** Wir arbeiten daran, die betroffenen Systeme und Dienste wieder in den Normalbetrieb zu versetzen und stellen sicher, dass keine verbleibenden Bedrohungen bestehen. Zudem überwachen wir die Systeme genau, um Anzeichen für wiederkehrende Probleme zu erkennen.
7. **Nachbesprechung:** Nach der Behebung der Panne führen wir eine umfassende Überprüfung durch, um unsere Reaktion zu bewerten und Verbesserungsmöglichkeiten zu identifizieren. Dies hilft, unseren Notfallreaktionsplan zu verfeinern und unsere Sicherheitslage insgesamt zu stärken.

Wie gewährleistet Trengo die physische Sicherheit der Rechenzentren?

Unsere SaaS-Lösung ist komplett in der öffentlichen Cloud gehostet. Alle Daten werden sicher in den hochmodernen Rechenzentren vertrauenswürdiger Anbieter wie AWS gespeichert. Weitere Details finden Sie im: AWS Compliance Centre .

Häufig gestellte Fragen

Wie geht Trengo mit Schwachstellenmanagement und Patching um?

Wir vermeiden nach Möglichkeit Hosting-Komponenten, die häufiges Schwachstellenmanagement erfordern, und beauftragen spezialisierte Anbieter mit Sicherheitszertifizierungen wie ISO 27001 und SOC 2 für maximale Sicherheit.

Für unsere eigenen Software-Komponenten automatisieren wir das Patchen von Abhängigkeiten, wann immer dies möglich ist. Unser Quellcode wird bei jedem Check-in gründlich gescannt, sodass identifizierte Schwachstellen vor dem Einsatz in der Produktion behoben werden. Zudem betreiben wir ein aktives Sicherheitsprogramm, das White-Hat-Hacker dazu ermutigt, Schwachstellen zu melden, was unsere Sicherheitslage weiter stärkt.

Welche Authentifizierungsmechanismen stehen Kunden zur Verfügung?

Trengo setzt ein umfassendes Authentifizierungs-Framework ein, um den sicheren Zugang für unsere Kunden zu gewährleisten. Wir bieten eine Standard-Kombination aus Benutzername und Passwort für die anfängliche Authentifizierung, ergänzt durch eine Zwei-Faktor-Authentifizierung (2FA) zur Erhöhung der Sicherheit. Kunden können 2FA als obligatorische Anforderung für alle Benutzer festlegen, um zusätzlichen Schutz zu gewährleisten. Dieser mehrschichtige Ansatz hilft, Konten vor unbefugtem Zugriff zu schützen und stellt sicher, dass nur verifizierte Personen auf sensible Informationen zugreifen können.

Häufig gestellte Fragen

Wie stellt Trengo die Einhaltung der Datenschutzbestimmungen (z. B. DSGVO) sicher?

Wir gewährleisten die Einhaltung der Datenschutzbestimmungen durch diese Maßnahmen:

1. **Datenverarbeitungsrichtlinien:** Wir verfügen über strikte Richtlinien und Verfahren zur Datenverarbeitung, die mit der DSGVO und anderen relevanten Vorschriften übereinstimmen. Dadurch wird sichergestellt, dass personenbezogene Daten rechtmäßig und transparent erhoben, verarbeitet und gespeichert werden.
2. **Datenschutzbeauftragter (DSB):** Wir benennen einen Datenschutzbeauftragten, der die Einhaltung der Datenschutzgesetze überwacht, Datenschutzaktivitäten koordiniert und als Ansprechpartner für Aufsichtsbehörden dient.
3. **Mitarbeiterschulungen:** Unsere Mitarbeiter werden regelmäßig zu Datenschutzbestimmungen und bewährten Praktiken geschult, um sicherzustellen, dass sie ihre Verantwortung und die Bedeutung des Datenschutzes verstehen.
4. **Rechte der betroffenen Personen:** Wir haben Prozesse implementiert, um die Rechte der Betroffenen zu wahren, wie z. B. Auskunft, Berichtigung, Löschung und Datenübertragbarkeit, gemäß der DSGVO.
5. **Sicherheitsmaßnahmen:** Wir setzen robuste Sicherheitsmaßnahmen wie Verschlüsselung, Zugangskontrollen und regelmäßige Sicherheitsüberprüfungen ein, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu gewährleisten.
6. **Drittanbieter-Compliance:** Wir prüfen Drittanbieter sorgfältig und fordern sie auf, Datenschutzvereinbarungen zu unterzeichnen, um die Einhaltung der Datenschutzbestimmungen sicherzustellen.

Welche Schulungsprogramme bietet Trengo zum Thema Cybersicherheit an?

Während des Onboardings absolvieren alle Mitarbeitenden eine umfassende Schulung zur Cybersicherheit. Mehrmals im Jahr organisieren wir zusätzliche Veranstaltungen, um dieses Wissen aufzufrischen und die Wachsamkeit zu fördern. Diese Schulungen informieren das Team über die neuesten Bedrohungen und bewährte Sicherheitspraktiken, damit sie sich der Risiken und ihrer Verantwortung zur Sicherung unserer Systeme bewusst bleiben.

Häufig gestellte Fragen

Wie gewährleistet Trengo die Sicherheit von APIs und Integrationen?

Um die Sicherheit unserer APIs zu gewährleisten, nutzen wir:

1. **Authentifizierung und Autorisierung:** Wir verwenden OAuth 2.0 und API-Schlüssel, um sicherzustellen, dass nur autorisierte Benutzer und Anwendungen Zugriff haben.
2. **Verschlüsselung:** Alle über unsere APIs übertragenen Daten werden mit TLS verschlüsselt, um Datenmissbrauch und Manipulationen zu verhindern.
3. **Rate-Limiting:** Wir setzen Rate-Limiting ein, um DDoS-Angriffe und Missbrauch zu verhindern.
4. **Eingabeprüfung:** Strikte Eingabeprüfung und -validierung verhindert gängige Schwachstellen wie SQL-Injection und XSS-Angriffe.
5. **Regelmäßige Sicherheitsüberprüfungen:** Unsere APIs werden regelmäßig durch Sicherheitsprüfungen und Schwachstellenanalysen auf Schwachstellen überprüft.
6. **Logging und Überwachung:** Um verdächtige Aktivitäten frühzeitig zu erkennen, führen wir umfassendes Logging und Monitoring der API-Aktivitäten durch.

Diese Maßnahmen gewährleisten maximale Sicherheit, Zuverlässigkeit und Widerstandsfähigkeit unserer APIs gegen Bedrohungen.

Welche Kontrollen gibt es zur Verwaltung von Zugriffsrechten und Benutzerrollen?

Für detaillierte Informationen zu den neuesten Autorisierungsfunktionen besuchen Sie bitte diesen Artikel im Hilfe Zentrum. Hier finden Sie umfassende Anleitungen zur effektiven Verwaltung und Nutzung unserer Autorisierungsoptionen.

Häufig gestellte Fragen

Welche Schritte unternimmt Trengo, um Entwicklungs- und Veröffentlichungsprozesse abzusichern?

Unser Quellcode wird bei jedem Check-in auf Schwachstellen gescannt, um Sicherheitsprobleme zu erkennen und zu beheben, bevor der Code in die Produktion geht. Dieser proaktive Ansatz gewährleistet die Integrität unserer Software.

Zusätzlich zur automatisierten Überprüfung wird der gesamte Quellcode einer Peer-Review unterzogen. Dieser Prozess hilft unserem Entwicklerteam, eventuelle übersehene Probleme zu identifizieren und so die Qualität und Sicherheit des Codes weiter zu erhöhen.

Wie oft führt Trengo Sicherheitsprüfungen und Schwachstellenanalysen durch?

Ja, wir führen regelmäßige Sicherheitsprüfungen und Penetrationstests durch, um die Robustheit unserer Sicherheitsmaßnahmen sicherzustellen. Diese werden jährlich von einem renommierten externen Sicherheitspartner durchgeführt, der mit seiner spezialisierten Expertise eine objektive Bewertung vornimmt. Dabei werden unsere Systeme, Prozesse und Kontrollen umfassend auf Schwachstellen geprüft, um sicherzustellen, dass wir den Branchenstandards entsprechen.

Zusätzlich zu den geplanten Prüfungen bieten wir unseren Kunden die Möglichkeit, nach vorheriger Absprache eigene Penetrationstests durchzuführen. Dabei bleibt unsere Sicherheitsinfrastruktur unangetastet, und es kann vorkommen, dass unsere Sicherheitsmaßnahmen bestimmte Testaktivitäten blockieren. Dies dient dem Ziel, die Sicherheit zu gewährleisten, während unsere Kunden ihre Interaktionen mit unseren Systemen prüfen können.

Mit Trengo lassen Sie keinen Kunden im Stich - Der Schlüssel zu zufriedenen Kunden!

Sie haben begonnen, Ihr Traumteam für den Kundenservice aufzubauen. Und was kommt danach? Jetzt ist es an der Zeit, Ihrem Team die Plattform zu bieten, die es sich immer gewünscht hat. Trengo ist die zentrale Plattform für Kundenkommunikation, die alle Ihre Kommunikationskanäle bündelt und hilft, wiederkehrende Aufgaben zu automatisieren. Mit Trengo haben Sie alle Kundenanfragen in einem einzigen Überblick – klingt fast zu gut, um wahr zu sein, oder? In den letzten sieben Jahren haben wir über 3000 Unternehmen geholfen, unvergessliche Kundenerlebnisse zu schaffen.

Möchten Sie mehr erfahren?
Unser Team hilft Ihnen gerne weiter.

trengo

Stadsplateau 30, 3521 AZ
Utrecht, Netherlands

© Trengo 2024

trengo.com/de