aircall

Überblick zum Thema Sicherheit

Um diese Themen geht es

Einführung 03

Organisation von Sicherheit 03

Sicherheit in der Personalabteilung 04

Identifizierung und Zugriffsverwaltung 05

Produktinfrastruktur von Aircall 06

Anwendungssicherheit 08

Krisenbewältigungsmaßnahmen 09

Vendor Management (Verwaltung von Anbietern) 10

Endgerätesicherheit 10

Datenschutz und -speicherung 10

Einführung

Aircall nimmt Sicherheit und Compliance sehr ernst. Mit diesem Dokument möchten wir unseren Kundinnen und Kunden die Sicherheit geben, dass ihre Daten in Übereinstimmung mit den jeweiligen Datenschutz- und Compliance-Anforderungen bearbeitet werden und dass Transparenz und Sicherheit die oberste Priorität für uns sind.

Unsere Sicherheitskontrollen und -mechanismen basieren auf der ISO-27001-Zertifizierung zu Informationssicherheitsstandards sowie den NIST-Standards. Folgende Themen werden darin abgedeckt: Richtlinien und Vorgehensweisen, Zugriffskontrolle, Geschäftskontinuität, Sicherheit in der Personalabteilung, Netzwerkinfrastruktur-Sicherheit, Sicherheit der Dienste von Drittparteien, Schwachstellenmanagement sowie Krisenbewältigungsmaßnahmen.

Organisation von Sicherheitsmaßnahmen

Bei Aircall gibt es ein offizielles IT-Security-Team, welches für alle Sicherheitsangelegenheiten im Unternehmen zuständig ist.

Unser Sicherheitsteam verfügt über viele Zertifizierungen und weitere Bescheinigungen, die die Expertise des Teams auf diesem Gebiet nachweisen.

Sicherheit in der Personalabteilung

Hintergrundprüfung und Geheimhaltungsvereinbarungen

Mitarbeiter:innen von Aircall werden eingehend durch Drittparteien geprüft, bevor sie ein offizielles Stellenangebot erhalten, sofern örtliche Regelungen und Einstellungsstandards dies erlauben. Alle Mitarbeiter:innen von Aircall müssen Geheimhaltungsvereinbarungen unterzeichnen, bevor sie den Zugang zu Systemen oder Daten erhalten.

Sensibilisierung und Schulungen

Weiterbildung ist ein zentraler Bestandteil eines effektiven IT-Security-Programms. Nur durch kontinuierliche Schulungen können Kunden- und andere sensible Daten mithilfe technischer Kontrollen ausreichend geschützt werden.

Jede:r neue Mitarbeiter:in muss im Rahmen des Onboardings an einer IT-Security-Schulung teilnehmen. Durch diese Schulung sollen neue Teammitglieder mit ihren Pflichten vertraut gemacht werden. Sie sollen zudem für interne Bedrohungen, Ransomware, Social Engineering, die ordnungsgemäße Verwendung von Ressourcen und andere Angelegenheiten in diesem Zusammenhang sensibilisiert werden.

Nach den Onboarding-Schulungen erhalten Mitarbeiter:innen mindestens alle zwei Monate Updates, Mitteilungen und interne Kommunikation.

Identifizierung und Zugriffsverwaltung

Aircall befolgt eine offizielle Vorgehensweise, um den Zugriff auf seine Ressourcen zu gewähren oder zu widerrufen. Der Zugriff auf das System basiert auf den Konzepten „Least-Privilege-Zugriff“ und „Kenntnis nur, wenn nötig“, um sicherzustellen, dass der autorisierte Zugriff mit den definierten Verantwortlichkeiten übereinstimmt. Alle Mitarbeiter:innen benötigen eine persönliche Kennung, um auf die Unternehmenssysteme zuzugreifen.

Aircall beruft sich auf eine Passwortrichtlinie für Unternehmen gemäß Industriestandards. In Übereinstimmung mit dieser Richtlinie müssen Passwörter alle 90 Tage geändert werden. Sie legt außerdem eine Mindestlänge für Passwörter von 10 Zeichen fest, sowie weitere Sicherheitsanforderungen, darunter Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen. Wir nutzen darüber hinaus eine Mehrfaktor-Authentifizierung (z. B. physische Sicherheitsschlüssel) und Single-Sign-on-Lösungen.

Autorisierungen werden regelmäßig überprüft (mindestens alle drei Monate), um festzustellen, ob diese für die jeweiligen Aufgaben einer Person erforderlich sind.

Vorgehensweise bei Beendigung des Arbeitsverhältnisses

Aircall befolgt einen dokumentierten Kündigungsprozess, der die Zuständigkeiten für die Einholung von Datensätzen und den Widerruf der Zugriffsrechte für Teammitglieder festlegt, die das Unternehmen verlassen.

Produktinfrastruktur von Aircall

Physisch und umgebungsbezogen

Amazon Web Services (AWS) ist unser Cloud-Infrastrukturanbieter. AWS verfügt über ein geprüftes Sicherheitsprogramm, das unter anderem nach PCI, ISO 27000 und SOC 2 zertifiziert ist. Dieses Programm umfasst Folgendes:

- Überwachungskameras (CCTV)
- Sicherheitskräfte
- Back-up-Stromversorgung
- Temperatur- und Feuchtigkeitskontrolle
- Rauchmelder
- Leckortung

Aircall hostet Produktsysteme nicht in seinen Büroräumen.

Netzwerksicherheit

Aircall teilt sein System in separate Netzwerke auf, um sensible Daten besser zu schützen und öffentliche Dienstleistungen von internen Dienstleistungen zu trennen. An Aircall übermittelte Kundendaten dürfen nur innerhalb des Produktionsnetzwerks vorkommen. Wir verwenden eine Kombination aus Security Groups, Firewalls, Intrusion-Detection-Systemen (Angriffserkennungssystemen) und Präventionssystemen (IDS/IPS) sowie Web-Application-Firewalls zum Schutz von Kundendaten.

Geschäftskontinuität und Notfallwiederherstellung

Wir haben ein Vorgehen zur Gewährleistung der Geschäftskontinuität und für die Notfallwiederherstellung entwickelt. Unsere Dienstleistungen beruhen dabei auf AWS-Verfügbarkeitszonen an unterschiedlichen geografischen Standorten, um eine verlässliche Funktionsweise auch zu gewährleisten, wenn ein Standort ausfällt. Unser Notfallwiederherstellungsplan wird mindestens einmal pro Jahr aktualisiert.

Wir möchten jegliche Probleme, die negative Auswirkungen für unsere Kundinnen und Kunden haben, schnell und transparent eingrenzen und beheben. Wir unterhalten eine Aircall Status-Seite **(https://status.aircall.io/)**. Dort wird der Status einer Anfrage regelmäßig aktualisiert und für den Anfragesteller verfügbar gemacht sowie aktualisiert wird, bis das jeweilige Problem behoben wurde.

Back-up und Wiederherstellung

Jeden Tag werden regelmäßige Back-ups durchgeführt, die im Rechenzentrum von AWS gehostet werden. Die Back-ups werden mit einer AES-256-Verschlüsselung gesichert. Die Tests zur Wiederherstellung von Back-ups werden mindestens einmal pro Jahr durchgeführt.

Verschlüsselung

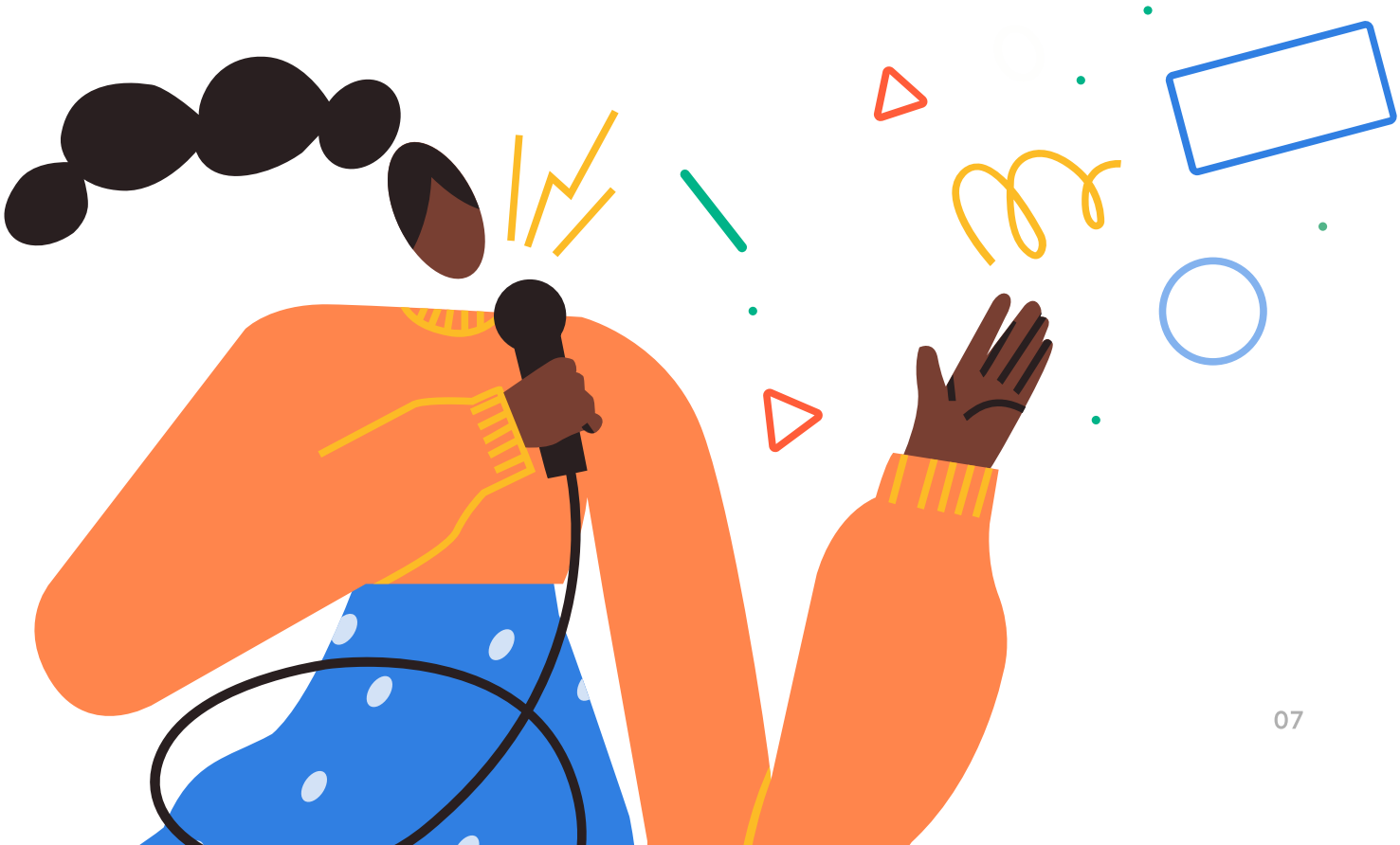
Aircall gewährleistet, dass alle sensiblen Kundendaten sowohl bei der Übermittlung als auch bei der Speicherung jeweils unter Einhaltung der Industriestandards TLS 1.2 und AES-256 verschlüsselt werden. Unser Ingenieurteam nutzt den AWS KMS (Key Management Service). Alle Schlüssel werden zentral von unserem Sicherheitsteam verwaltet.

Überwachung

Aircall nutzt Überprüfungs- und Überwachungstools zur Identifizierung von Unregelmäßigkeiten oder unsachgemäßem Gebrauch. In solchen Fällen prüft das jeweilige Team den Fall und leitet die notwendigen Korrekturmaßnahmen ein.

Multi-Tenant-Cloud

Aircall ist ein Multi-Tenant-Cloud-Dienst. Unsere Kundendaten sind logisch getrennt. Das heißt Aircall prüft, ob ein:e Nutzer:in berechtigt ist, die Anfrage auszuführen, indem wir überprüfen, ob das Unternehmen der Person mit dem Unternehmen der angeforderten Daten übereinstimmt.



Anwendungssicherheit

Schwachstellenanalyse und Patch-Management

Aircall führt regelmäßig Schwachstellenscans seiner IT-Systeme durch. Die Ergebnisse erscheinen in unserem Ticketingsystem, werden hinsichtlich Risiko und Priorität bewertet und eingestuft, dem System hinzugefügt und anschließend behoben. Alle Probleme oder Patches, die als hohes Risiko eingestuft werden, werden innerhalb von 30 Tagen behoben.

Penetrationstest

Aircall führt regelmäßig Penetrationstests durch und beauftragt zweimal pro Jahr unabhängige Drittanbieter mit der Durchführung von Penetrationstests auf Anwendungsebene. Nachdem Sicherheitsbedrohungen und Schwachstellen identifiziert wurden, werden sie eingestuft, kategorisiert und schnell beseitigt. Berichte stehen auf Anfrage und nach Unterzeichnen einer Geheimhaltungsvereinbarung zur Verfügung.

Darüber hinaus verfügt Aircall über ein Bug-Bounty-Programm. Unabhängige Sicherheitsforscher:innen werden für das Aufspüren von Sicherheitslücken bei Aircall Produkten belohnt.

Änderungsmanagement

Aircall verfügt über offizielle Änderungsmanagementprozesse, um Änderungen der Produktionsumgebung für die Dienstleistungen zu verwalten, darunter Änderungen an zugrundeliegender Software sowie zugrundeliegenden Anwendungen und Systemen.

Alle Änderungen an Quellcodes, die für Produktionssysteme bestimmt sind, werden vor der Übergabe einer Codeprüfung durch eine:n qualifizierte:n technische:n Mitarbeiter:in unterzogen, die eine Analyse der Sicherheit, der Leistung und des Missbrauchspotenzials umfasst.

Krisenbewältigungsmaßnahmen

Aircall befolgt eine dokumentierte Vorgehensweise für den Empfang von Berichten zu Sicherheitsvorfällen. Das Aircall Security Team arbeitet mit einem dokumentierten Krisenbewältigungsprozess, der Folgendes umfasst:

- Protokollierung
- Kategorisierung
- Recherche
- Eindämmung
- gewonnene Erkenntnisse

Als Reaktion auf jeden Vorfall identifizieren wir zuerst die Offenlegung der Daten und anschließend nach Möglichkeit die Quelle der Sicherheitslücke. Wir benachrichtigen die Kundin oder den Kunden (sowie alle anderen betroffenen Kundinnen/Kunden) per E-Mail oder telefonisch (falls die Benachrichtigung per E-Mail nicht ausreicht). Wir liefern nach Bedarf regelmäßig einen Überblick über die Entwicklung, um sicherzustellen, dass der Vorfall angemessen behoben wurde.

Sollten Sie Sicherheitsanliegen oder Kenntnis von einem Vorfall haben, senden Sie bitte eine E-Mail an: **report@aircall.io**.

Vendor Management (Verwaltung von Anbietern)

Aircall verfügt über ein Vendor-Management-Programm, um sicherzustellen, dass angemessene Sicherheitskontrollen durchgeführt werden. Aircall prüft regelmäßig alle Anbieter (wichtige Anbieter werden mindestens einmal pro Jahr geprüft) im Hinblick auf die Sicherheitsstandards und fortlaufende Funktionsweise von Aircall, darunter die Art des Zugriffs und ggf. die Klassifizierung der Daten, auf die der Zugriff erfolgt, notwendige Kontrollen zum Schutz von Daten sowie rechtliche/regulatorische Anforderungen.

Aircall schließt mit all seinen Anbietern schriftliche Vereinbarungen, darunter Geheimhaltungsvereinbarungen und Vereinbarungen zu obligatorischen Sicherheitsvorkehrungen, die ein angemessenes Maß an Schutz für alle Kundendaten bieten, die diese Anbieter ggf. bearbeiten.

Endgerätesicherheit

Alle Aircall Laptops werden zentral verwaltet und sind vollständig verschlüsselt. Die Endbenutzer:innen können Antivirus-Software oder Sicherheitsfunktionen nicht deaktivieren.

Unser IT-Team sorgt regelmäßig dafür, dass auf allen Geräten die neueste Software-Version installiert wird.

Datenschutz und -speicherung

Aircall verfügt über ein Datenschutzprogramm. Weitere Informationen zu Datenschutz und -speicherung erhalten Sie hier **(https://aircall.io/privacy-faqs/)**.