SafetyCulture

August 2024

Überblick: Sicherheit

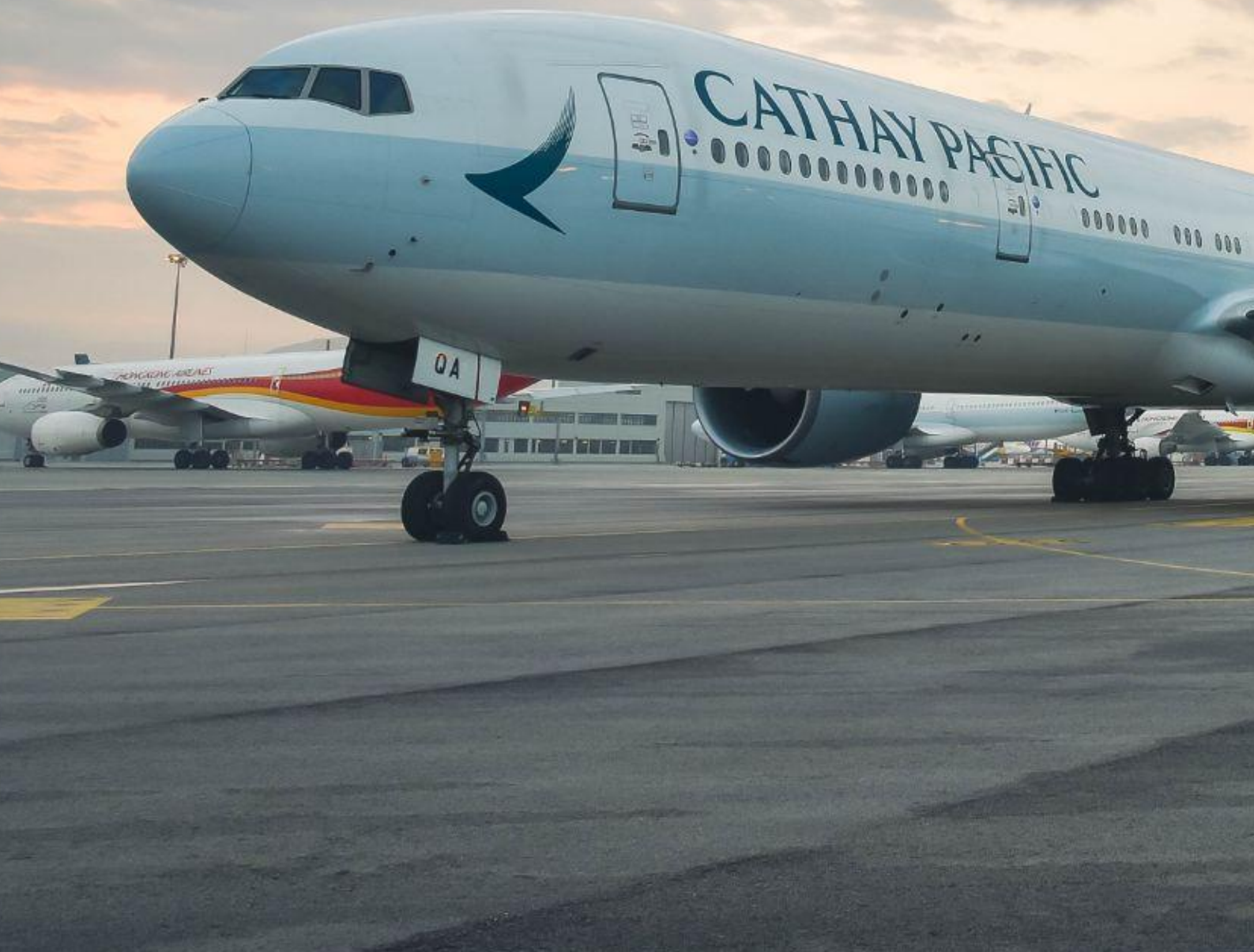
Verstehen Sie die SafetyCulture Cybersicherheit

Inhalt

SafetyCulture

Vor der Einführung von SafetyCulture mussten wir die Daten von Checklisten im Büro manuell abtippen und sie dann in Excel analysieren, bis wir sie endlich mit dem Team teilen konnten. Jetzt liefert uns das Analyse-Feature von SafetyCulture umfassendere Daten, die sich alle an einem Ort befinden und sich leicht teilen lassen.

Deaky Wong
Line Maintenance Engineer
Cathay Pacific



Unsere Mission

Die Mission von SafetyCulture ist es, Unternehmen dabei zu unterstützen, durch innovative, kostengünstige Mobile-First-Produkte sicherere und hochwertigere Arbeitsplätze auf der ganzen Welt zu schaffen.

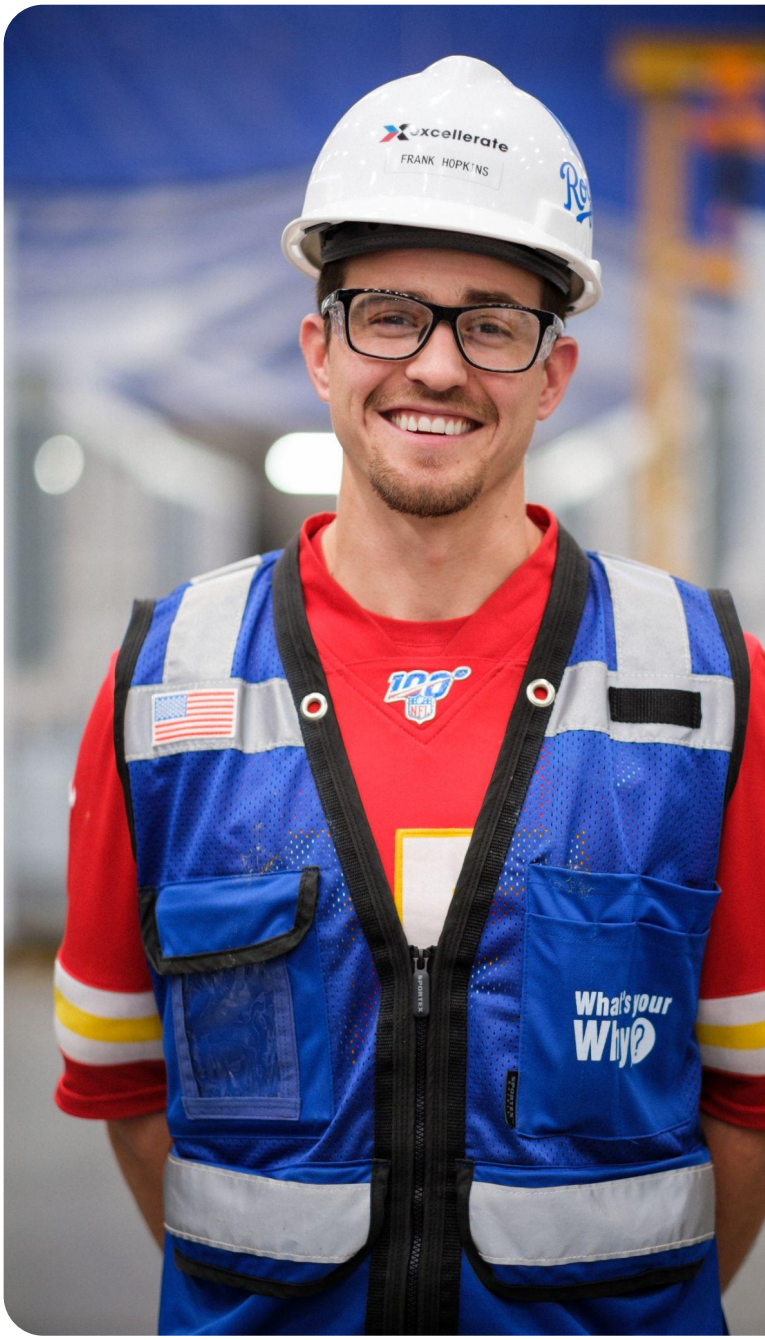
Wir erfüllen unsere Mission durch unsere Software-as-Service (SaaS)-Produkte.

Unsere Produkte werden täglich von mehr als 27.000 Unternehmen weltweit in zahlreichen Branchen und für eine Vielzahl von Anwendungsfällen eingesetzt.

Wir sind stolz darauf, dass SafetyCulture als ein weltweit führender Anbieter von Produkten zur Förderung von Sicherheit und Qualität geschätzt wird, und wir wissen, wie wichtig unsere Rolle ist, wenn es darum geht, unseren Kunden zu helfen, ihren täglichen Betrieb zu optimieren.

Wir sehen unsere Vorgehensweise bei der Cybersicherheit als eine wichtige tragende Säule, um unseren Status als führendes Unternehmen in diesem Bereich aufrechtzuerhalten, und dieser Inhalt gibt einen Überblick darüber, wie wir Cybersicherheit als Unternehmen angehen

SafetyCulture ist nach ISO 27001:2024 zertifiziert und wir befolgen die AICPA Vertrauensdienste Kriterien, die unser Engagement für die Sicherheit unserer Kunden bekräftigen.



Überblick

Cybersicherheitsprogramm

SafetyCulture verfügt über ein aktives, robustes und sich kontinuierlich verbesserndes Cybersicherheitsprogramm, um sicherzustellen, dass unser Unternehmen und die von uns bereitgestellten Produkte sicher sind. Das Cybersicherheitsprogramm von SafetyCulture setzt eine Reihe von Kontrollen auf technischer und operativer Ebene ein, um sicherzustellen, dass wir über einen effektiven, umfassenden Verteidigungsansatz verfügen, um uns vor Cyberangriffen zu schützen und die von unseren Software-as-a-Services (SaaS)-Produkten verarbeiteten Daten zu sichern.

Zu den wichtigsten Funktionen gehören:

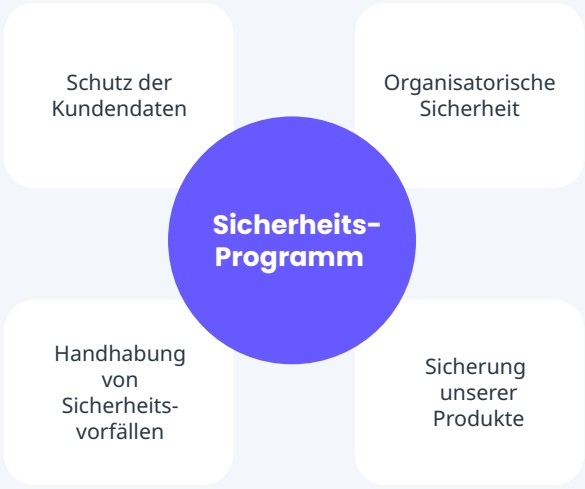
- Ein Sicherheitsprogramm, das an Best-Practice-Standards der Branche ausgerichtet ist, einschließlich der Verwendung von Cloud-Plattformen, die vertrauenswürdigen Sicherheits-Benchmarks wie ISO 27001 und SOC 2 entsprechen.

- Der Fokus darauf, die richtigen Grundlagen zu schaffen und zu erkennen, dass die Grundlagen der Sicherheit nach wie vor die kritischsten sind. Diese umfassen:

  - ➔ Schulung unserer Mitarbeiter über die Bedeutung der Sicherheit.
  - ➔ Ein engagiertes Sicherheitsteam zu haben, das dafür verantwortlich ist, unser Unternehmen vor tatsächlichen und möglichen Bedrohungen für unser Geschäft und die Daten zu schützen, die Kunden uns anvertrauen.
  - ➔ Einsatz robuster Mechanismen, um sicherzustellen, dass der Zugriff auf die Systeme und Kundendaten von SafetyCulture sorgfältig kontrolliert wird.
  - ➔ Verschlüsseln der von uns gespeicherten Kundendaten (sowohl während der Übertragung als auch im Speicher) mit robusten Verschlüsselungsmechanismen.
  - ➔ Sicherstellen, dass wir Patches in unserer IT-Umgebung und auf unseren Produkten so schnell wie möglich anwenden, um die Möglichkeit zu minimieren, dass Schwachstellen von Cyberangreifern ausgenutzt werden.
  - ➔ Aktive Überwachung und Prüfung unserer IT-Umgebung und unserer Produkte auf Schwachstellen und deren schnellstmögliche Behebung.
  - ➔ Ein klar definierter Prozess zur Bereitstellung effektiver Unterstützung und Reaktion im Falle eines Sicherheitsvorfalls.

Wir wenden die gebotene Sorgfalt an, um sicherzustellen, dass unsere Dienstanbieter die Industriestandards in Bezug auf Sicherheit erfüllen – wir wissen, dass die Sicherheit unserer Partner uns und unsere Kunden direkt betrifft, daher wählen wir sehr sorgfältig aus, mit wem wir zusammenarbeiten.

Die übrigen Teile dieses Dokuments bieten einen Überblick über die verschiedenen Teile unseres Sicherheitsprogramms.



Sicherheitpraktiken auf Unternehmens-ebene

Die Sicherheitsverfahren unseres Unternehmens orientieren sich an den empfohlenen Best Practices anerkannter Normen wie NIST, ISO 27001 und SOC.

Sicherheitsmanagement

SafetyCulture verfolgt eine Reihe dokumentierter Richtlinien, Standards und Verfahren, die das Sicherheitskonzept unserer Organisation definieren. Diese Richtlinien und Verfahren werden an alle Mitarbeiter weitergegeben und mindestens einmal jährlich überprüft und aktualisiert (häufiger, wenn wesentliche Änderungen erforderlich sind), um zu gewährleisten, dass unser Sicherheitskonzept aktuell bleibt.

Wir achten darauf, dass die Verantwortlichkeit für die Sicherheit im gesamten Unternehmen gewährleistet ist. Zu diesem Zweck haben wir ein Forum für Informationssicherheits-Management eingerichtet, in dem wichtige Interessenvertreter aus dem gesamten SafetyCulture-Konzern regelmäßig zusammenkommen, um sicherheitsrelevante Angelegenheiten zu prüfen und zu diskutieren und Entscheidungen zu treffen, die sich auf unseren Ansatz zur Cybersicherheit auswirken.

SafetyCulture ist nach ISO 27001:2024 zertifiziert und wir befolgen die AICPA Vertrauensdienste Kriterien, die unser Engagement für die Sicherheit unserer Kunden bekräftigen.

Zugriffskontrollen

Wir gewährleisten, dass der Zugriff auf die Systeme in unserer IT-Umgebung, einschließlich der von uns genutzten Cloud-Plattformen, auf Mitarbeiter beschränkt ist, die diesen Zugriff für ihre Arbeit benötigen.

Alle Zugriffe von Administratoren erfordern eine Multi-Faktor-Authentifizierung, und Mitarbeiter, die auf unsere Umgebung zugreifen, müssen eine genehmigte VPN-Lösung verwenden.

Die Berechtigungen für den Zugriff auf unsere Systeme werden regelmäßig für jeden einzelnen Mitarbeiter überprüft und nach Bedarf geändert. Im Rahmen unseres Off-Boarding-Verfahrens wird ausscheidenden Mitarbeitern jeglicher Zugriff auf Systeme und Dienste entzogen.

Sicherheit von Drittanbietern

Wir überprüfen von Anfang an und fortlaufend die Sicherheitspraktiken der von uns beauftragten Dienstleistern, um sicherzustellen, dass deren Praktiken den Branchenstandards entsprechen und mit unseren eigenen Datenschutz- und Sicherheitsrichtlinien und -verfahren übereinstimmen. Wenn solch ein Drittanbieter Zugriff auf unsere Systeme benötigt, stellen wir sicher, dass der Zugriff speziell auf den Zweck beschränkt ist, für den er beauftragt wurde.

Da Amazon Web Services (AWS) einer unserer wichtigsten Anbieter ist, arbeiten wir mit AWS nach dem Modell der geteilten Verantwortung für Sicherheit und Compliance zusammen, um sicherzustellen, dass klar definiert ist, wer welche Verantwortung für die Sicherheit übernimmt. AWS verfügt über Akkreditierungen vieler der neuesten Branchenstandards akkreditiert und erfüllt diese. Weitere Informationen finden Sie hier: *https://aws.amazon.com/de/artifact*

Für die Verarbeitung von Finanz- und Kreditkartendaten nutzt SafetyCulture mehrere Partner (Chargify, eWay und Stripe), deren Sicherheitspraktiken den Payment Card Industry Data Security Standard (PCI-DSS) erfüllen.

Netzwerksicherheit

Die Unternehmensnetzwerke von SafetyCulture sind durch Firewalls sowie ein Eindringerkennungssystem (Intrusion Detection System, IDS) und ein Eindringver- hinderungssystem (Intrusion Prevention System, IPS) an der Peripherie geschützt, die spezielle Netzwerksicher- heitsgeräte bereitstellen, damit wir jeglichen bösartigen Datenverkehr erkennen und verhindern können.

Für unsere Cloud-basierten Plattformen nutzen wir mit einer mehrschichtigen Strategie zum Schutz vor externen Angriffen hauptsächlich Amazon Web Services (AWS). Auf der Infrastrukturebene setzt AWS Strategien wie Kontrolle des Zugriffs auf Netzwerkgeräte, Trennung von Daten durch Firewalls und virtuelle private Clouds ein, um bösartigen Datenverkehr herauszufiltern, und nutzt umfangreiche Protokollierungs- und Überwachungsfunktionen, um netzwerkbasierte Angriffe zu verhindern. Auf Anwendungsebene nutzen wir die Web Application Firewall (WAF) und den DDoS-Schutz (Distributed Denial of Service) von Cloudflare, um webbasierte und Denial-of-Service-Angriffe auf unsere Produkte zu verhindern.

Unsere Entwicklungs-, Test- und Produktionsumgebungen sind voneinander getrennt.

Protokollierung und Überwachung

SafetyCulture verwendet ein zentralisiertes Protokollsystem, das Audit-Ereignisse für den Zugriff auf die Anwendung enthält. Diese Protokolle werden 90 Tage lang aufbewahrt. Wir verwenden auch Amazon Elastic Load Balancing (ELB)-Protokolle, um Zugriffe auf Dienste (erfolgreich oder nicht) zu verfolgen. Die in AWS gespeicherten Protokolle können nicht geändert werden, und der Zugriff ist auf die Personen beschränkt, für deren Aufgaben dies erforderlich ist.
Wir überprüfen die Protokolle regelmäßig, um böswillige Nutzeraktivitäten und potenzielle Schwach- stellen in unseren Produkten zu erkennen; wir haben eine automatische Überwachung, die uns vor bestimmten Arten von potenziell böswilligen Ereignissen innerhalb unserer globalen Infrastruktur warnt.

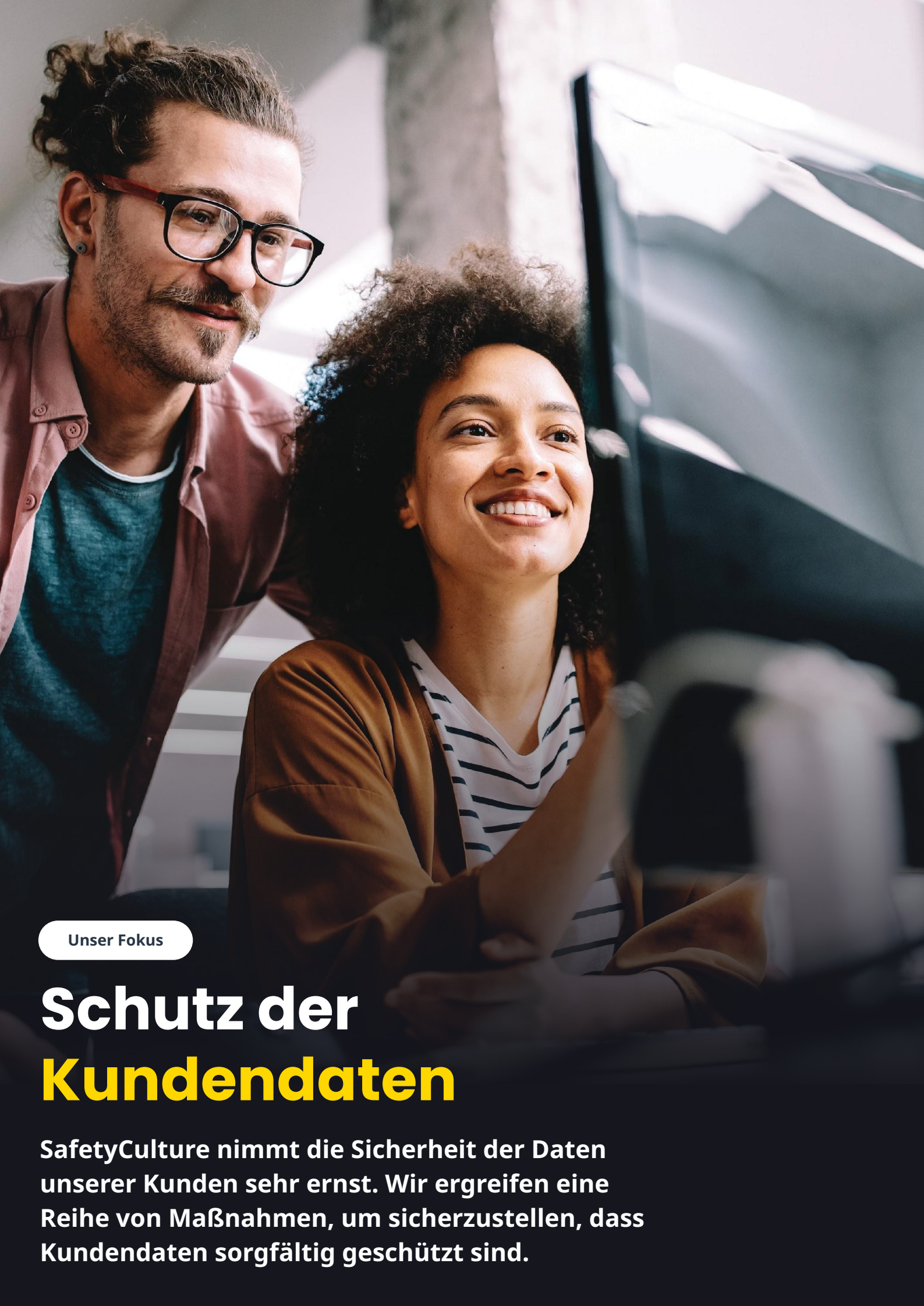
Schulungen zum Thema Sicherheit

Alle Mitarbeiter in Technischen und Nicht-Technischen Bereichen von SafetyCulture nehmen regelmäßig an Schulungen zum Thema Sicherheit teil. Zusätzliches Schulungsmaterial zum Thema Sicherheit wird den einzelnen Mitarbeitern bei Bedarf zur Verfügung gestellt, um sicherzustellen, dass sie für die spezifischen sicherheitsrelevanten Herausforderungen ihrer Rolle gerüstet sind.

Patching und Schwachstellenbehebung

Wir patchen unsere IT-Umgebung fortlaufend und betrachten dies als eine der wichtigsten Maßnahmen, um uns vor möglichen Sicherheitsverletzungen zu schützen:

- Wir verwenden AWS System Manager, um regelmäßig Patches für unsere Cloud-basierte Infrastruktur bereitzustellen.
- Wir nutzen Lösungen zur Verwaltung mobiler Geräte (MDM), um sicherzustellen, dass wichtige Patches schnell und effizient installiert werden.
- Unsere Geräte sind mit Endpoint Security-Technologien gesichert, um Sicherheitsbedrohungen wie Viren und Malware-Angriffe zu erkennen und zu verhindern, und überwachen sie auf bösartige Aktivitäten.
- Werden zuerst Patches für die kritischsten Schwachstellen installiert, und zunächst in unserer nicht produktiven Umgebung getestet, bevor sie schnell in der gesamten IT-Umgebung eingesetzt werden.



Unser Fokus

Schutz der Kundendaten

SafetyCulture nimmt die Sicherheit der Daten unserer Kunden sehr ernst. Wir ergreifen eine Reihe von Maßnahmen, um sicherzustellen, dass Kundendaten sorgfältig geschützt sind.

Schutz von Kundendaten

Eingeschränkter Zugriff auf Daten

SafetyCulture trifft verschiedene Maßnahmen zum Schutz der Kundendaten vor unberechtigtem Zugriff oder Verwendung durch Unbefugte (entweder extern oder intern). Kundendaten werden nur in unserer Produktionsumgebung gespeichert, und der Zugriff auf diese Daten durch SafetyCulture-Mitarbeiter ist auf Mitarbeiter mit der erforderlichen Zugriffs- berechtigung zur Erfüllung ihrer Standardaufgaben beschränkt. Der Zugriff auf Kundendaten wird über Zugriffskontroll- und Authentifizierungstools (einschließlich der Verwendung der Zwei-Faktor- Authentifizierung) verwaltet, die von Amazon Web Services und unseren anderen Cloud-Partnern bereitgestellt werden.

Kundendaten werden nur für Zwecke der Erbringung der vertraglich vereinbarten Dienstleistungen, z. B. zur Behebung von Problemen bei technischen Support-Anfragen verwendet. Ausführliche Informationen finden Sie in der SafetyCulture- Datenschutzrichtlinie hier: https://safetyculture.com/legal/privacy-policy/

Wenn die Support-Mitarbeiter von SafetyCulture auf bestimmte Kundendaten zugreifen müssen (zur Fehlerbehebung oder zu Support-Zwecken), dann verlangt SafetyCulture immer die Zustimmung des Kunden, bevor er auf diese Daten zugreift.

Wir speichern oder zwischenspeichern keine Finanz-daten von Kunden, die zur Abrechnung über die SafetyCulture-Plattform verwendet werden, und unsere Mitarbeiter haben keinen direkten Zugriff auf Abrechnungsdaten.

Physischer Zugriff auf Daten

Kundendaten werden auf einer Infrastruktur von Amazon Web Services gehostet, die die Sicherheit ihrer Standorte unter Verwendung von Best-Practice- Kontrollen der Branche aufrechterhält, wie auf ihrer Website für Sicherheit und Compliance beschrieben: https://aws.amazon.com/de/architecture/security-identity-compliance/.

In unseren Geschäftsräumen werden keine Kundendaten gespeichert.

Datenverschlüsselung

SafetyCulture verfügt über Mechanismen, die die Daten unserer Kunden stets schützten.

Im Ruhezustand werden alle in den Systemen gespeicherten Kundendaten mit AES-256 verschlüsselt und die Schlüssel über den Key Management Service von Amazon Web Services verwaltet. Alle Daten werden gemäß den Sicherheitsrichtlinien und -verfahren von AWS gespeichert.

Zum Schutz der Daten bei der Übertragung verwendet SafetyCulture Transport Layer Security (TLS) und setzt einen Mindeststandard von TLS v1.2 mit 128-Bit-Chiffrierschlüsseln durch. Wir unterstützen Verbindungen mit bis zu 256-Bit-Chiffre-Schlüsseln für die Verwendung einer AES-Chiffre.

Sicherheitskopien von Daten

SafetyCulture-Daten werden in regelmäßigen Abständen auf verschiedenen verschlüsselten Datenspeicherlösungen von Amazon Web Services gesichert. Die Sicherungen werden auf mehrere AWS-Standorte in der Region des Kunden (APAC, USA oder EU) repliziert.

Der Zugriff auf die Datensicherungen ist nur denjenigen Mitarbeitern von SafetyCulture vorbehalten, für die dieser Zugriff im Rahmen ihrer Rollenanforderungen erforderlich ist. Backups werden verschlüsselt und schreibgeschützt gespeichert.

Deletion and disposal of data

Unsere Kundendaten werden bei Amazon Web Services gespeichert und unterliegen deren Lösch- und Entsorgungsverfahren. Diese Verfahren umfassen einen Prozess zur Löschung von sicheren alten Medien. Gelöschte Medien werden inspiziert, um die erfolgreiche Vernichtung der Daten sicherzustellen.
SafetyCulture-Hardware, die vertrauliche Daten enthält (einschließlich SafetyCulture-Backups) unterliegt vor dem Recycling einer logischen Datenvernichtung nach branchenüblichen Standards.

Sicherung unserer Produkte

We recognize that for the bulk of customers, their principal experience with SafetyCulture will be through our products. Security forms an important part of the way our products are developed and operates.

Sichere Software-Entwicklungspraktiken

Als Teil unseres Produktentwicklungsprozesses wird jede Code- und Infrastrukturänderung in einem Versionskontrollsystem gespeichert, versioniert, geprüft und auf ihre Auswirkungen hin untersucht, bevor die Änderung für die Produktion freigegeben wird. Diese Überprüfung umfasst die Einhaltung bewährter Sicherheitsverfahren. Wir trennen auch unsere Entwicklungs-, Test- und Produktionsumgebungen und verwenden auch keine Kundendaten in unseren Nicht-Produktionsumgebungen.

Änderungskontrolle

Alle Änderungen an SafetyCulture-Produkten werden während ihrer Entwicklung aktiv getestet, um sicherzustellen, dass die Auswirkungen auf die Endbenutzer vor dem Einsatz bewertet werden, und alle wesentlichen Änderungen werden in die Produktions-Release-Notes aufgenommen.

SafetyCulture setzt Systeme zur Änderungsverfolgung und Versionskontrolle ein, um Änderungen an der Codebasis oder Konfiguration unserer Produkte aktiv zu überwachen und zu verwalten. Wir verwenden auch Amazon CloudTrail, um alle zugrunde liegenden Konfigurationsänderungen an der Cloud-Plattform zu verfolgen, auf der unsere Produkte betrieben werden.

Schwachstellenidentifizierung und Patch-Entwicklung

Wir arbeiten intensiv daran, die Anzahl der in unseren Produkten auftretenden Schwachstellen zu minimieren, und wir wissen, dass es wichtig ist, proaktive Schritte zu unternehmen, um sicherzustellen, dass wir alle Schwachstellen so schnell wie möglich beheben. Zu diesem Zweck führt SafetyCulture jährliche Penetrationstests durch und testet und überwacht unsere Anwendungen aktiv auf Schwachstellen. Wir führen ein privates Bug-Bounty-Programm durch, da wir wissen, dass eine Gemeinschaft unabhängiger Sicherheitsforscher, die dazu angeregt werden, unsere Produkte laufend zu testen, um potenzielle Probleme zu identifizieren, dazu beiträgt, die Sicherheit unserer Produkte zu erhöhen.

Wenn eine Schwachstelle identifiziert wird (intern oder extern), wird das Problem nachverfolgt und entsprechend der potenziellen Schwere der Auswirkung auf unsere Kunden priorisiert. Bei Problemen mit kritischem Schweregrad kann dies bedeuten, dass unsere Entwickler rund um die Uhr arbeiten, bis das Problem behoben ist.

Patches für Probleme werden entwickelt und durch einen kontinuierlichen Integrationsprozess (CI/CD) in die Produktionsumgebung freigegeben und so schnell wie möglich angewendet.

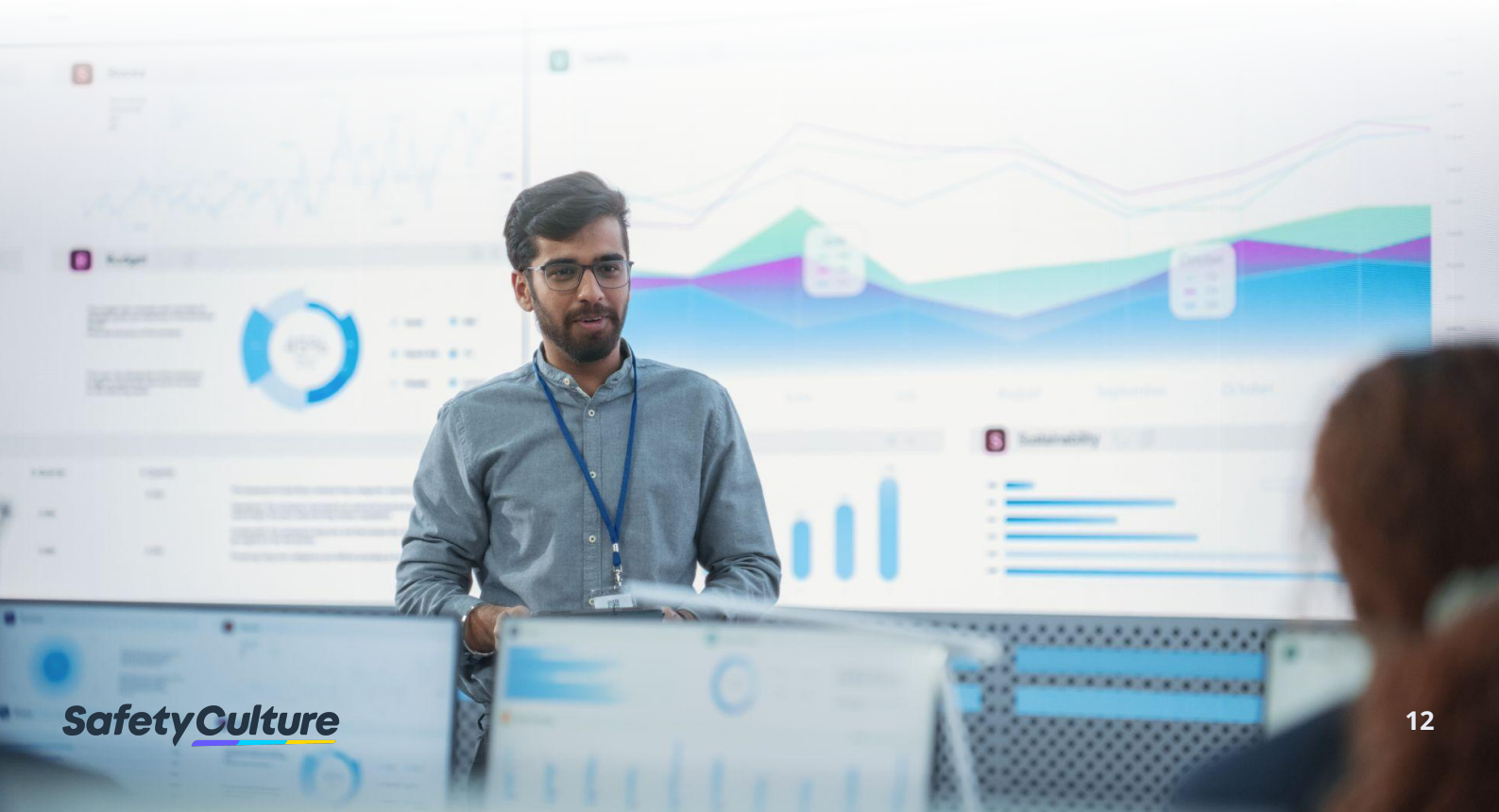
Handhabung von Sicherheitsvorfällen

Während wir unser Möglichstes tun, um Sicherheitsvorfälle zu verhindern, sind wir uns bewusst, dass wir auch darauf vorbereitet sein müssen, mit diesen Vorfällen umzugehen, sollten sie auftreten, um die möglichen Auswirkungen auf unsere Kunden und SafetyCulture zu minimieren.

Wir haben eine Reihe von Maßnahmen ergriffen, darunter:

- Ein dokumentiertes Incident-Management-Verfahren, das unseren Prozess zum Umgang mit der Vertraulichkeit, Integrität und Verfügbarkeit unserer IT-Umgebung und unserer Produkte definiert.
- Die garantierte Unterstützung eines globalen Unternehmens im Falle eines Vorfalls.
- Etablierte Disaster-Recovery-Pläne und Notfallstrategien, die uns dabei helfen können, die Betriebskontinuität während eines Vorfalls aufrechtzuerhalten. Dies umfasst die Verwendung mehrerer geografischer Verfügbarkeitszonen, die von Amazon Web Services bereitgestellt werden, und die Replikation von Daten über mehrere Systeme in jeder Zone. Dies gewährleistet einen kontinuierlichen Datenzugriff bei Vorfällen, die die Systemverfügbarkeit beeinträchtigen, und bietet Datenredundanz im Falle von System- oder Datenspeicherausfällen.

SafetyCulture benachrichtigt betroffene Kunden unverzüglich über schwerwiegende Vorfälle, die die Verfügbarkeit von SafetyCulture-Diensten oder -Daten beeinträchtigen, sowie über alle Vorfälle, die die Vertraulichkeit und Integrität ihrer Daten beeinträchtigen, gemäß unserer SafetyCulture-Datenschutzerklärung, die Sie hier finden: https://safetyculture.com/legal/privacy-policy

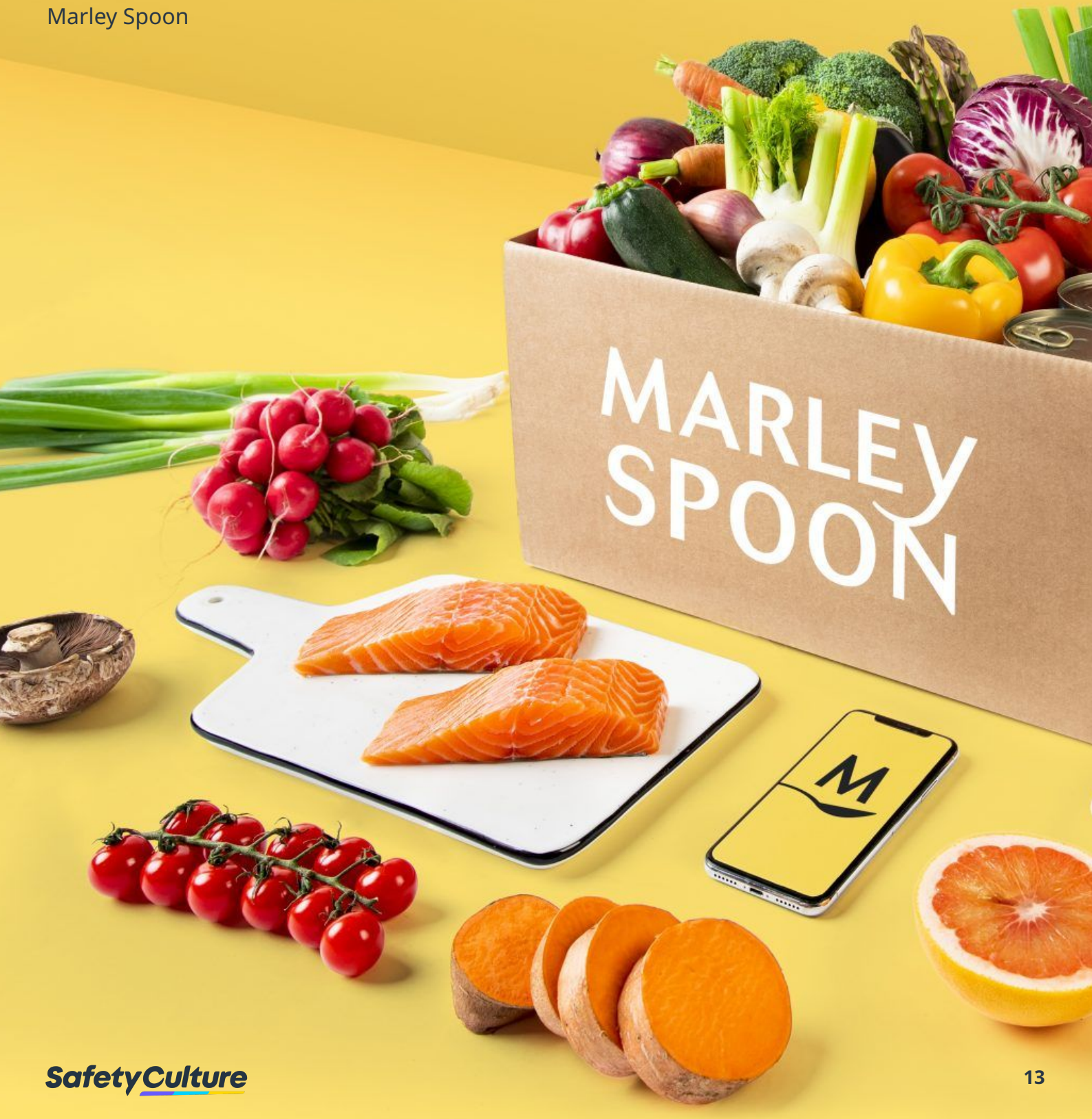


Mit den Daten, die wir mit SafetyCulture erfassen, haben wir Einblick in alles, was wir tun. Wenn es eine Schwellenwertausnahme oder einen Prozess gibt, der verbessert werden muss, müssen wir uns nur die Daten genau anschauen, und wir finden die Ursachen.

Sofia Dias

Food Safety & Quality Assurance Manager

Marley Spoon



Abschließende Gedanken

SafetyCulture betrachtet Cybersicherheit als grundlegenden Bestandteil unseres Geschäfts und der Dienstleistungen, die wir Unternehmen auf der ganzen Welt anbieten. Während die von uns eingerichteten Kontrollen und Maßnahmen erheblich über das hinausgehen, was hier behandelt wird, dient der vorliegende Inhalt dazu, ein allgemeines Verständnis für den vielschichtigen Ansatz, den wir verfolgen und unser Engagement für die Sicherheit zu vermitteln.

Wenn Sie Fragen zu diesen Inhalten haben oder weitere Informationen zu unserem Ansatz in Bezug auf Support, Sicherheit oder Datenschutz benötigen, kontaktieren Sie uns bitte unter den nachstehenden Kontaktdaten.

- **Support:** support@safetyculture.com
- **Datenschutz:** privacy@safetyculture.com

Um Sicherheitsprobleme zu melden, kontaktieren Sie uns unter security@safetyculture.com

Literaturhinweise

Unsere Sicherheitsseite: https://www.safetyculture.com/de/sicherheit/

Unser Datenschutzportal: https://safetyculture.com/de/rechtliches/datenschutz-portal/

Unsere Statusseite: https://status.safetyculture.com/