eventmobi

Sicherheit, Zuverlässigkeit, Wiederherstellung & Datenschutz

Letzte Aktualisierung: Januar 2023

Sicherheit

Physische Serversicherheit

Amazon verwaltet die Server von EventMobi via Amazon Web Services (AWS). AWS Datenzentren befinden sich in verdeckten Gebäuden. Besonders kritische Einrichtungen sind durch militärähnliche Berme mit Perimeterüberwachung sowie andere natürliche Grenzschutzmaßnahmen gesichert. Der physische Zugang wird sowohl am Perimeter als auch an den Gebäudeeintrittspunkten durch professionelles Sicherheitspersonal streng überwacht, welches Videoüberwachung, hochmoderne Einbruchmeldeanlagen und andere elektronische Mittel einsetzt. Autorisierte Mitarbeiter müssen die Zwei-Faktor-Authentifizierung nicht weniger als dreimal durchlaufen, um auf Datencenter-Etagen zugreifen zu können. Alle Besucher und Auftragnehmer müssen ihre Identität nachweisen und werden von autorisiertem Personal angemeldet und fortlaufend begleitet.
Amazon erteilt nur Mitarbeitern, die legitime betriebliche Gründe für solche Berechtigungen haben, Zugriff auf das Rechenzentrum und Informationen. Benötigt ein Mitarbeiter diese Privilegien nicht mehr, wird sein Zugriff sofort widerrufen, auch wenn er weiterhin Mitarbeiter von Amazon oder Amazon Web Services ist. Der gesamte physische und elektronische Zugriff auf Rechenzentren durch Amazon-Mitarbeiter wird routinemäßig protokolliert und überwacht.

Weitere Details finden Sie hier: https://aws.amazon.com/security/

Im Rahmen unserer internen Richtlinien erhalten nur Techniker, die unsere Einstellungsüberprüfungen (siehe Abschnitt *Interne Richtlinien*) und die Probezeit durchlaufen haben, Zugriff auf das Amazon Web Services-Portal. Zwei-Faktor-Authentifizierung ist erforderlich, und standardmäßig erhalten Techniker Zugriff mit der geringsten Berechtigung.

Amazon Web Services Datenverarbeitungsaddendum

EventMobi hat eine Kopie des Amazon Web Services Datenverarbeitungsaddendums mit Standard-Klauseln unterzeichnet. Eine Kopie dieses Dokuments ist auf Anfrage erhältlich.

Für weitere Informationen besuchen Sie : https://aws.amazon.com/compliance/eu-data-protection/

Physische Sicherheit der Büroräumlichkeiten und Inhalte von EventMobi

Die Mitarbeiter von EventMobi stimmen den Sicherheits- und Datenschutzrichtlinien zu, um vertrauliche Daten auf ihren Laptops, Telefonen und anderen elektronischen Geräten zu verwalten und zu speichern. Die Ausrüstung wird regelmäßig überprüft, um sicherzustellen, dass bestimmte Richtlinien vorliegen. Um Zugang zum Bürogebäude zu erhalten, ist jederzeit ein Mitarbeiterausweis erforderlich. Unsere internen Wi-Fi-Netzwerke werden mit WPA2-PSK-Passcodes gesichert.
Wir nutzen die Leistungsfähigkeit des Meraki MDM-Systems von Cisco auf all unseren Geräten, um eine Hardware-Richtlinie zu erstellen und alle unsere IT-Bestände zu inventarisieren. Wir prüfen regelmäßig die Konformität der Geräte und beseitigen Probleme persönlich und sofort, einschließlich der Aktualisierung der Betriebssystem-Patches und Anti-Virus-Software.
Die Festplatten aller Computer von EventMobi-Mitarbeitern sind mit dem AES-XTS-Modus von AES mit 128-Bit-Blöcken und einem 256-Bit-Schlüssel verschlüsselt. Computer müssen innerhalb kurzer Zeit der Inaktivität in den Schlafmodus wechseln und beim erneuten Aufwachen die Eingabe des Passworts fordern.
Es ist verboten, USB-Sticks aus dem Büro zu entfernen. Alle Datenspeichergeräte (NAS) sind physisch vor dem Entfernen gesichert.
Anwendungen von Drittanbietern, die von Mitarbeitern von EventMobi verwendet werden, sind nur über den One-Sign-On Anmeldedienst OneLogin zugänglich. Dies stellt sicher, dass wir eine angemessene Zugriffskontrolle für Daten in diesen Anwendungen haben. Um auf OneLogin zugreifen zu können, müssen die Mitarbeiter über ein ausreichend starkes Passwort verfügen, das alle sechs Monate geändert wird und eine Zwei-Faktor-Authentifizierung verwendet.

Passwortgeschützte Anmeldung

Alle Kennwörter für Benutzer- und Administratorenkonten werden mit dem einseitigen Hash-Algorithmus bcrypt mit Salt erstellt. Passwörter sind für alle Event-App-Nutzer erforderlich.

Verschlüsselung

Die gesamte Kommunikation zwischen Ihren Geräten und der Plattform und den APIs von EventMobi ist vollständig durch Secure Socket Layer-Verschlüsselung (SSL) geschützt, um Ihre Daten vor Man-in-the-Middle-Angriffen und Lauschangriffen zu schützen. SSL-Zertifikate werden von GeoTrust und GlobalSign bereitgestellt.

EventMobi nutzt die integrierte Verschlüsselung im RDS-Service von Amazon Web Services, die die Verschlüsselung von Daten in der Datenbank (und allen Backups) unter Verwendung der Industriestandard-AES-256-Verschlüsselung ermöglicht. Die Schlüssel werden von einem Hardwaresicherheitsmodul generiert und geschützt, das von AWS bereitgestellt wird.

Schwachstellenprüfung und Penetrationstests

Um unsere internen Systeme zu schützen, führt EventMobi routinemäßige Scans unserer Server auf bekannte Sicherheitslücken durch.

Mindestens einmal pro Jahr und zusätzlich nach großen Änderungen in der Codebasis behält sich EventMobi vor, eine Drittfirma mit der Dürchführung einer Schwachstellenanalyse für unsere Produkte zu beauftragen. Kunden, die einen eigenen Penetrationstest durchführen möchten, müssen eine Kopie des Penetrationstest-Antragsformulars ausfüllen und zurücksenden.

Zuverlässigkeit & Wiederherstellung

Redundante Server und Datenzentren

Die Architektur von EventMobi ist redundant und fehlertolerant ausgelegt. Wir verpflichten uns, ein hochverfügbares System bereitzustellen und zu pflegen. Dennoch ist es nahezu unmöglich, alle möglichen Fehlerfälle und Unterbrechungen zu berücksichtigen. Daher haben wir Sicherheitsvorkehrungen für diese Fälle getroffen.
EventMobi verwendet Amazon AWS-Dienste als primäre Hosting-Plattform. Informationen zu unseren Schutzmechanismen auf Infrastrukturebene und Details zu von AWS vorgenommene Vorkehrungen für Sicherheit, Verfügbarkeit und Wiederherstellung, finden Sie unter https://aws.amazon.com/security/. Wir nutzen EC2-Server-Instanzen (siehe http://aws.amazon.com/ec2-sla/ für EC2-SLA), hosten unsere Datenbank für RDS-Dienste, repliziert für Failover-Schutz und S3-Buckets für elf Neunen (99,9999999999) %) der Datenhaltbarkeit.

Datenbank-Backups

Die Daten in Ihrem EventMobi-Konto werden über mehrere Datenbankserver hinweg repliziert, um zu verhindern, dass ein einzelner Datenbankfehler zu Datenverlust führt.

Darüber hinaus werden diese Daten alle 20 Minuten gesichert und mit dem geografisch verteilten und fehlertoleranten S3-Dienst von Amazon sicher gespeichert. Dies stellt sicher, dass Ihre Daten bei einem katastrophalen Ausfall innerhalb des Rechenzentrums sicher sind und Ihre Aufzeichnungen innerhalb kurzer Zeit wiederhergestellt werden können.

Wir behalten alle Backups für einen Zeitraum von mindestens 7 Tagen in einem verschlüsselten Zustand und stellen das neueste Backup täglich wieder her, um sicherzustellen, dass es bei Bedarf in einem Vorfallszenario funktioniert.

Sicherheit von durch Benutzer hochgeladenen Daten

Alle vom Nutzer hochgeladenen Daten (einschließlich Bildern, Dokumenten und Videos) werden auf die Amazon S3-Plattform hochgeladen (siehe http://aws.amazon.com/s3-sla/ für S3 SLA), das eine Datenhaltbarkeit von 99,9999999999 (99,999999999%) und eine Verfügbarkeit von 99,99% aufweist und automatisch in mehreren Rechenzentren repliziert wird.

Service-Wiederherstellung

EventMobi hat in Cloud-Computing- und Deployment-Automation-Tools investiert und diese ausgebaut, um unsere täglichen Abläufe zu optimieren. Diese Automatisierung ist für unseren Disaster Recovery-Plan von entscheidender Bedeutung, da es sich bei jedem von uns durchgeführten Deployment um denselben Prozess handelt, der zur Wiederherstellung von Diensten aus einer Unterbrechung des Dienstes erforderlich ist, bei denen eine Wiederherstellung von Sicherungen erforderlich ist. Unser Deployment finden täglich statt und unsere automatisierten Tools werden regelmäßig auf ihre Funktionsfähigkeit überprüft. Unsere Architektur ermöglicht es uns, einen Disaster-Recovery-Plan zu erstellen, der Fehler in Rechenzentren in der Region von Amazon Web Services in Virginia aufrechterhalten kann. Wir haben Server, die über mindestens drei dieser Datencenter laufen, und können unsere vorhandene Deployment-Automatisierung auf allen fünf Servern nutzen.

Ausfallüberwachung und Performance-Benachrichtigungen

Unser Wiederherstellungsplan basiert auf den Benachrichtigungs- und Überwachungssystemen auf Unternehmensebene. Wir verwenden Pagerduty, einen geografisch verteilten Überwachungsdienst, um Uptime- und Performance-Checks auf unseren Systemen in einem 60-Sekunden-Intervall durchzuführen. Sollte es zu einer Alarmmeldung kommen, wird unser Entwicklerteam per Push-Benachrichtigung, E-Mail oder Telefonanruf informiert und folgt einem klar definierten Protokoll, um das Ereignis zu behandeln.

pagerduty

Kundenkommunikation

Kommunikation und Kundenservice stehen bei EventMobi immer im Vordergrund. Sollte es zu einer Dienstunterbrechung kommen, wird unser Support-Team proaktiv die betroffenen Parteien per E-Mail oder Telefon kontaktieren und sie über die Situation auf dem Laufenden halten. Offene Kommunikation und Einsicht in die Probleme sind der Schlüssel zum Erhalt des Vertrauens unserer Kunden.

Prozess nach einer Serviceunterbrechung

Innerhalb von 24 Stunden nach jeder Serviceunterbrechung wird unser Support-Team Ihnen die Ursache des Problems erklären und aufzeigen, wie wir es behoben haben und wie wir dies in Zukunft verhindern werden.

Datenschutzrichtlinien

Wir empfehlen unseren Kunden, unseren standardmäßigen Vertrag über die Auftragsverarbeitung (ADV) abzuschließen. Dieser legt dar, welche Rollen und Verantwortungsbereiche sowohl EventMobi (als Datenverarbeiter) als auch dem Veranstaltungsplaner (als Datenverantwortlicher) jeweils zuteil werden in Bezug auf die Sammlung, Speicherung und Verwendung persönlicher Daten während ihrer Nutzung der EventMobi-Plattform.

Wir haben unsere eigenen Richtlinien für den Datenschutz und die Datenverarbeitung überprüfen lassen und die Prozesse dokumentiert, wie wir auf Anträge zur Auskunftserteilung über personenbezogene Daten antworten, inklusive der Bereitstellung von Daten (unter dem Zugriffsrecht) und Vernichtung oder Anonymisierung von Daten (unter dem Recht aufs Vergessenwerden), wenn ein Datenverantwortlicher (die Organisation, die die Veranstaltung plant) uns damit beauftragt.

Wir bieten Kunden die Möglichkeit an, ihren Veranstaltungsteilnehmern eine Datenschutzrichtlinie und Allgemeine Geschäftsbedingungen anzuzeigen und stellen sprachliche Empfehlungen für beide zur Verfügung.

Skalierung

Die Systeme von EventMobi sind robust und auf die Anforderungen der Kunden zugeschnitten. Wir verfügen über eine Funktion zur automatischen Skalierung, mit der zusätzliche Server bereitgestellt werden, um übermäßige Belastungen zu bewältigen. Dies erfordert jedoch, dass bestimmte Lastschwellenwerte erreicht werden, sowie ~ 10-15 Minuten, damit neue Server bereitgestellt und zur Verwendung konfiguriert werden können. Leistungsprobleme sind möglich. Auch wenn dies selten vorkommt, halten wir einen vorinstallierten Server im Hot-Standby-Modus bereit.
Um diese Probleme zu vermeiden, teilen Sie uns einfach Ihre umfangreichen Nutzungspläne mit. Am Tag Ihrer Veranstaltung werden wir zusätzliche Server bereitstellen, um uns auf die Nutzung im großen Umfang vorzubereiten.

Interne Richtlinien

Die internen Richtlinien von EventMobi basieren auf dem Consensus-Assessment-Initiative-Fragebogen (CAIQ) der Cloud Security Alliance.

Weitere Informationen finden Sie unter: https://cloudsecurityalliance.org/group/consensus-assessments/. Alle EventMobi-Mitarbeiter und Auftragnehmer unterzeichnen Vertraulichkeitserklärungen bezüglich benutzerdefinierter Daten, mit denen sie interagieren. Darüber hinaus führt EventMobi Hintergrund-Checks für alle neuen Mitarbeiter durch. Wir erstellen und verteilen regelmäßig Schulungsmaterial über bewährte Sicherheitsverfahren und den richtigen Umgang mit vertraulichen Kundendaten.

Die Produktentwicklung bei EventMobi folgt dem OWASP Secure Software Development Life Cycle, um sicherzustellen, dass Sicherheitsexperten so früh wie möglich bei der Erstellung einer neuen Funktion eingesetzt werden, und um unseren Entwicklern zu helfen, sicherzustellen, dass unsere Produkte sicher sind.

Reporting-& Audit-Trails

EventMobi sammelt umfassende Audit-Trails für alle Aktivitäten auf den EventMobi-Systemen. Von Amazon Web Services erstellte Protokolle werden zentral in Amazon Web Services CloudTrail und CloudWatch gespeichert. Protokolle von EventMobi-Systemen werden zentral in Splunk gespeichert und 90 Tage aufbewahrt. Administratoren können Kontoaktionen, Benutzernamen, E-Mail-Adressen, IP-Adressen sowie Datum und Uhrzeit für alle Aktionen verfolgen.

Verantwortungsvolle Offenlegung

EventMobi hat es sich zur Aufgabe gemacht, Best Practices für die Sicherheit in jeden Aspekt der Entwicklung zu integrieren. Wir nehmen derzeit nicht an einem Bug-Bounty-Programm teil, nehmen aber Datenschutz und Schwachstellen sehr ernst. Wenn ein Mitglied Ihrer Organisation irgendwelche Sicherheitsprobleme feststellt, wenden Sie sich bitte an security@eventmobi.com.

Datenschutzbestimmungen & Allgemeine Geschäftsbedingungen

Die Datenschutzbestimmungen von EventMobi finden Sie hier: https://www.eventmobi.com/de/datenschutzbestimmungen/

Die Allgemeinen Geschäftsbedingungen von EventMobi finden Sie hier: https://www.eventmobi.com/de/agbimpressum/