Quick Facts zum Thema Applikation & Plattform Sicherheit

Mobile Event App by plazz AG

In der folgenden Auflistung geben wir eine Kurz-Beschreibungen zu den von uns umgesetzten Maßnahmen, welche zum Sicherheitsstandard der Services MEA, Polario, registr gehören.

Mandantentrennung:

Datenbanken und Dateiablagen sind kundenspezifisch getrennt. Business-Logik ist in Docker-Containern kapselt.

Penetrationstests:

Es werden regelmäßig jährlich externe Pentests durchgeführt, um Schwachstellen zu identifizieren und zu beheben. Die letzten Tests für MEA & Polario fanden Ende 2023 statt.

Schwachstellenscans:

Unsere DevOps nutzen Trivy für Schwachstellenscans in den Cloud-Umgebungen. Findings aus Scan-Reports werden ausgewertet und behoben.

Hacking:

Angriffszenarien werden in den Pentests abgedeckt und Schwachstellen behandelt.

Ethical Hacking Tests:

Bisher keine spezifischen Umsetzungen.

Plattformsicherheit:

Google Cloud bietet umfassende Dokumentation zu Sicherheitsmaßnahmen.

- https://cloud.google.com/solutions/security?hl=de
- https://cloud.google.com/docs/security?hl=de

Entwicklungsrichtlinien:

Vorgegebene Anforderungen für Mitarbeiter sind allen bekannt und werden kontrolliert.

Web Application Firewall:

Ist implementiert.

Verschlüsselung:

Daten at rest und in transit sind in der Google-Cloud verschlüsselt. Dokumentation steht zur Verfügung

- https://cloud.google.com/docs/security/encryption/default-encryption?hl=de
- https://cloud.google.com/docs/security/encryption-in-transit?hl=de

Zugriffskontrolle:

Es werden regelmäßig jährlich externe Pentests durchgeführt, um Schwachstellen zu identifizieren und zu beheben. Die letzten Tests für MEA & Polario fanden Ende 2023 statt.

Schwachstellenscans:

Alle Zugriffe sind gemonitored und auf das das Need-to-know Prinzip beschränkt. Google greift nur zu Supportzwecken auf Daten zu. API und CMS-Zugriffe werden vom Monitoring-System erfasst. Robuste Authentifizierung und Autorisierung, um sicherzustellen das nur berechtigte Nutzer auf die API/CMS/Plattform zugreifen können.

Vermeiden von sensiblen Infos in URLs:

Wir übertragen keine vertraulichen Daten wie Passwörter oder Zugriffs-Token in URLs. Wir nutzen stattdessen Header oder Anfragenkörper.

TLS-Verschlüsselung:

Wir verwenden eine sichere Transport Layer Security (TLS)-Verschlüsselung, um die Kommunikation zwischen Client und Server zu schützen.

Eng definierte Anfragen und Antworten:

Wir begrenzen die zulässigen Anfragen und Antworten für RESTful APIs, um unerwünschte Zugriffe zu verhindern.

Überwachung und Erkennung von API-Angriffen:

Wir haben eine Funktion zur Überwachung und Erkennung von Angriffen auf unsere API implementiert.

Patches und Updates:

Automatische Sicherheitspatches und Updates der Google Cloud. Individuelle Updates und Patches der Applikation.

Sichere Konfiguration:

Verbundene Services (GCP, All-Inkl) sind sicher nach Vorgaben des Providers konfiguriert.

Backups:

Tägliche Backups der Datenbanken mit 7-tägiger Vorbehaltszeit. Kann individuell festgelegt werden.

Notfallplanung:

ISO27001-konformes Notfallmanagement.

Monitoring:

Fortlaufende Überwachung von Zugriffen und weiterer Werte der Hosting Plattform. (Auslastung, Übertragung, Identifikation)

Detail- Beschreibungen und weitere Details finden sich in unserer AVV-Vorlage wieder.