Make.com - Berechtigungskonzept

Anwendungssicherheit

Strenge Schwachstellenmanagementprozesse zur Erkennung und Behebung von Bedrohungen. Regelmäßige Penetrationstests durch unabhängige Dritte, um zu gewährleisten, dass die Make Plattform sicher und geschützt ist.

Zugangskontrolle

Robuste Maßnahmen zur Zugangskontrolle. Die Hosting-Umgebung von Make ist nur über das private Netzwerk via VPN zugänglich und unterstützt keinen direkten Zugriff aus dem öffentlichen Internet.

SSO

Make unterstützt die einmalige Authentifizierung mit Google, Facebook und GitHub. Erweiterte Rollen- und Teamverwaltungsfunktionen innerhalb des Profils einer Organisation. Unternehmenskunden haben die Möglichkeit, ihre eigene SSO-Implementierung zu verwenden.

Rechenzentrum

Das Make Cluster ist über zwei Zonen verteilt, um die Verfügbarkeit zu gewährleisten. Die Infrastruktur befindet sich in privaten Amazon AWS EC2-Instanzen (Amazon VPC) mit Amazon Enterprise-Support.

Kodierungs- und Entwicklungsstandards

Make Entwickler halten sich an Kodierungsstandards gemäß dem Open Web Application Security Project (OWASP). Static Application Security Testing (SAST) ist ebenfalls vorhanden, um den Software Development Life Cycle (SDLC) von Make zu verbessern.

Sicherheit der Kundendaten

Make verpflichtet sich, die Daten der Kunden zu schützen und setzt fortschrittliche Sicherheitsverfahren ein, um die Daten sicher zu halten. Standardmäßig werden die Protokolldaten für 30 Tage gespeichert. Die Enterprise Lizenz bietet die Möglichkeit, Daten über einen längeren Zeitraum zu speichern.

Bewegungs- und Stammdaten

Jede Verbindung zwischen Make und einem Drittanbieter wird auf die sicherste verfügbare Weise hergestellt. In einigen Fällen (z.B. FTP, Datenbanken) haben die Kunden die Möglichkeit, die Sicherheitsstufe manuell einzustellen. Make sichert die Netzwerkkommunikation mit TLS-Version 1.2 und 1.3 mit AES 256 Verschlüsselung. Alle Passwörter werden in einem verschlüsselten Format gespeichert und können von niemandem reproduziert werden - auch nicht von Make-Mitarbeitern. Make verwendet eine Festplattenverschlüsselung mit dem branchenüblichen AES-256-Verschlüsselungsalgorithmus und AWS Key Management Service (KMS) für die Verwaltung kryptografischer Schlüssel.