ActionLogics

Summary of Security Policies and Standards for ActionLogics

Overview

The document outlines the security policies and standards adopted by ActionLogics, a SaaS-based solution hosted on Google Cloud Platform (GCP). ActionLogics' security leverages Google's robust infrastructure, ensuring comprehensive protection through layered physical, hardware, and software security measures, rigorous authentication and authorization processes, encrypted data storage and communication, extensive operational security protocols, and regular security scans. These standards are designed to safeguard user data and maintain the integrity and availability of services.

Key Aspects of Security Infrastructure

1. Physical Security
- Google designs and operates its data centers with multiple layers of physical security.
- Security measures include biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.
- Limited access to data centers, with additional measures for third-party hosted servers.

2. Hardware and Software Security
- Custom-designed server boards and networking equipment.
- Use of hardware security chips for device authentication.
- Secure boot processes with cryptographic signatures ensuring the integrity of BIOS, bootloader, kernel, and OS.

3. Data Encryption
- Data is encrypted at rest using keys managed by a central key management system.
- Automated key rotation and extensive audit logs.
- Network traffic encryption, including inter-VM traffic, with ongoing enhancements to extend encryption within data centers.

4. Service Deployment Security
- Services deployed on Google's infrastructure undergo rigorous authentication and authorization processes.
- Use of cryptographic credentials for service identity verification.
- Cluster orchestration services (Borg) manage the deployment, ensuring isolation and integrity.

5. User and Inter-Service Authentication
- Central identity service for user authentication, employing additional risk-based challenges and support for two-factor authentication (U2F).
- Inter-service communication authenticated and authorized using cryptographic methods.
- Role-based access control and rigorous code review processes.

6. Operational Security
- Continuous monitoring and incident response mechanisms in place.
- Red Team exercises to evaluate and enhance security defenses.
- Secure software development practices, including automated tools to detect vulnerabilities.

7. Security Scans
- Automated tools for detecting security bugs, such as fuzzers, static analysis tools, and web security scanners.
- Regular security scans of the infrastructure to identify and mitigate vulnerabilities.
- Integration of security scans into the development and deployment pipelines to ensure early detection of issues.

8. Data Management
- Scheduled deletion policies for data recovery and error correction.
- Secure data storage with lifecycle tracking of storage devices.
- Data marked for deletion undergoes a multi-step process to ensure complete removal, including physical destruction of devices when necessary.

9. Denial of Service (DoS) Protection
- Multi-tier, multi-layer protections to mitigate DoS attacks.
- Centralized DoS service coordinates response and mitigation strategies.