OwnBackup Security Controls

Content:

1. Introduction

OwnBackup was designed from the ground up with security in mind. The architecture implements multiple security tiers designed to address different security concerns.

OwnBackup is SOC2 compliant and undergoes annual SOC2 audit which verifies that information security practices, policies, procedures and operations meet or surpasses the rigorous SOC2 standards for security, availability, confidentiality and Processing Integrity.

OwnBackup utilizes Amazon Web Services (AWS) for all its computing and storage needs. AWS is a top-tier facility with the following accreditations: SOC1 - SSAE-16, SOC2, PCI DSS Level 1, ISO 27001, HIPAA, etc.

OwnBackup implements the following controls in accordance with security best practices.

2. Security Controls

2.1 Web-application security controls

- Access to the application is only via HTTPS.
- An OwnBackup account admin can provision & deprovision additional OwnBackup user access as necessary.

- All the user activities are audited (together with user, timestamp and source IP Address) & audits logs can be viewed by an OwnBackup Admin when logged into OwnBackup.com.
- Access to the OwnBackup account can be IP restricted (via the OwnBackup admin from the 'Account' tab).
- oAuth is used to obviate the need to store admin credentials wherever possible.
- Enterprise-grade password policy according to industry best practices.
- Two factors authentication for accessing the OwnBackup account.
- Single Sign-On (SSO) support via SAML 2.0 Identity Providers (IdP).

2.2 Encryption

- At rest: OwnBackup uses AES256bit encryption on Amazon EBS volumes (via LUKS: Linux Unified Key Setup Package) for storing the users' backed-up data.
- In transit, always over HTTPS:
    - Salesforce->OwnBackup (backup agent): API access always over HTTPS.
    - OwnBackup->Customer: Always over HTTPS (via TLS1.1 and 1.2).
- For internal DR purposes, OwnBackup takes twice-daily snapshots of the encrypted volumes onto Amazon S3.

2.3 Firewall

- OwnBackup utilizes Amazon's Security-groups to limit network access.

2.4 Monitoring and auditing

- OwnBackup collects application, network and OS events to a central syslog server. These logs are analyzed and reviewed to detect suspicious activity, and prevent threats. Any anomalies are escalated as necessary.
- OwnBackup uses intrusion detection system (IDS) to monitor network activity and alert on any suspicious behaviour.
- OwnBackup's Incident Response team (available 24x7) monitors security@ownbackup.com and works according to our Incident Response Plan (IRP) when necessary.

2.5 Isolation between accounts

- OwnBackup uses extreme Linux Sandboxes to isolate OwnBackup accounts' data. This ensures that any anomaly, either due to security issues, or an internal software bug, will always be confined to a single OwnBackup account.

2.6 Vulnerability management & security updates

- OwnBackup undergoes periodic penetration testing and vulnerability scanning to maintain the security of our application. In addition to scans conducted by our team, we undergo external security evaluations (most recently in February 2016).
- Puppet is used to maintain configuration across OwnBackups' instances such that security updates can be efficiently deployed.