APP.6: Allgemeine Software

APP.bd.6 Secrets Management mit Hashicorp Vault

1 Beschreibung

1.1 Einleitung

Der Trend einer Umstellung von einer statischen On-Premise-Infrastruktur auf eine dynamische Infrastruktur mit mehreren Anbietern ändert den Sicherheitsansatz. Die Sicherheit in der statischen Infrastruktur hängt von dedizierten Servern, statischen IP-Adressen und einem klaren Netzumfang ab. Die Sicherheit in einer dynamischen Infrastruktur wird durch kurzlebige Anwendungen und Server, vertrauenswürdige Quellen für Benutzer- und Anwendungsidentität und softwarebasierte Verschlüsselung definiert.

Die Komponente Vault stellt einen Mechanismus zum Sichern, Speichern und kontrollierten Zugriff auf Token, Kennwörter, Zertifikate und Verschlüsselungsschlüssel zum Schutz von Geheimnissen und anderen vertraulichen Daten bereit. Bei den zu verwaltenden Geheimnissen handelt es sich zum Beispiel um vertrauliche Umgebungsvariablen, Datenbankanmeldeinformationen, API-Schlüssel oder Anmeldeinformationen der Mitarbeiter. Darüber hinaus stellt Vault alle nötigen Funktionalitäten für den Betrieb einer PKI bereit.

Dieser Baustein umfasst die Funktionalitäten Aufbewahrung und Verwaltung der Schlüssel, Schlüsselgenerierung sowie Inhaltsverschlüsselung von Daten durch encryption-as-a-service, sowie Identity-based Access. Der Zugriff auf Secrets kann mit Hilfe einer Benutzeroberfläche, einer CLI oder einer HTTP-API erfolgen.

1.2 Zielsetzung

Ziel des Bausteins ist der Schutz einer Vault Instanz und der Informationen, die durch Vault bereitgestellt oder im weitesten Sinne damit verarbeitet werden.

1.3 Abgrenzung und Modellierung

In diesem Baustein werden die für einen Secrets-Management-Dienst spezifischen Gefährdungen und Anforderungen betrachtet. Der Betrieb erfordert entweder einen Server oder Container, deren allgemeine Sicherheitsempfehlungen zusätzlich beachtet werden müssen (siehe z. B. SYS.1.3 *Server unter Linux und Unix*, SYS.1.2.2 *Windows Server 2012* bzw. SYS.1.6 *Container*). Zusätzlich sind die Anforderungen aus CON.3

Datensicherungskonzept sowie OPS.1.1.3 *Patch- und Änderungsmanagement* zu beachten. Da es sich bei Vault um allgemeine Software handelt, gelten auch hier die Anforderungen aus APP.6 *Allgemeine Software*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den benutzerdefinierten Baustein APP.bd.6 *Secrets Management mit Hashicorp Vault* von besonderer Bedeutung:

2.1 Kompromittierung von Vault durch unberechtigten Zugriff

Da in Vault Geheimnisse wie kryptographische Schlüssel oder Anmeldeinformationen auf Ressourcen verschiedener weiterer IT-Systeme verwaltet werden, kann eine Kompromittierung des IT-Systems den unberechtigten Zugriff auf weitere IT-Systeme und ggf. die Kompromittierung dieser IT-Systeme nach sich ziehen.

2.2 Fehlendes oder nicht zeitnahes Einspielen von Patches

Es werden regelmäßig Sicherheitsempfehlungen durch den Hersteller veröffentlicht. Bekannt gewordene Schwachstellen werden geschlossen („Patches“). Wenn die Sicherheitsempfehlungen und Patches ignoriert oder erst sehr spät umgesetzt werden, besteht die Gefahr, dass Angreifer Sicherheitslücken ausnutzen. Es besteht gegebenenfalls die Gefahr des Datenabflusses, Ausfalles von Funktionen und schließlich der Störung von wichtigen Prozessen.

2.3 Fehlende oder unzureichende Datensicherung

Wenn es für den Fall eines Datenverlustes keine oder nur eine unzureichende Datensicherung gibt oder sich gesicherte Daten nicht mehr zurückspielen lassen, könnten Geheimnisse nicht wieder herstellbar sein.

2.4 Fehlerhafte Konfiguration

Werden Authentifizierungsmethoden, Policies, Tokens, Ressourcenkontingente fehlerhaft konfiguriert, z. B. auf Grund manueller Anpassungen in diversen Umgebungen, kann dies zu unbeabsichtigten Sicherheitslücken führen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des benutzerdefinierten Bausteins APP.bd.6 *Secrets Management mit Hashicorp Vault* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den benutzerdefinierten Baustein APP.bd.6 *Secrets Management mit Hashicorp Vault* vorrangig erfüllt werden:

APP.bd.6.A1 Planung und Dokumentation des Einsatzes von Vault

Bevor Vault eingesetzt wird, MUSS die Institution den Einsatz sorgfältig planen. Dabei MUSS sie mindestens folgende Punkte beachten:

- Hinweise zum gewählten Betriebsmodell (Container, Application-Server),
- zu nutzende Funktionen (Secrets Management, Data-Encryption, Identity-based Access),
- Wahl des Storage Backends (z. B. Raft, Consul),
- Wahl der Anwendungsintegration (Trusted Platform, Trusted Orchestrator, direct Integration)
- Dokumentation des Vorgehens für Backup und Recovery.

Die Dokumentation MUSS die vom Hersteller bereitgestellte Dokumentation entsprechend den individuellen Anforderungen der Institution ergänzen, so dass die Planungen von Dritten nachvollzogen werden können. Die Dokumentation MUSS im späteren Betrieb entsprechend vorgenommener Änderungen aktualisiert werden.

APP.bd.6.A2 Root Rechte deaktivieren

Der Vault Dienst DARF NICHT mit Root Rechten laufen. Das Ausführen von Vault als regulärer Benutzer reduziert seine Berechtigungen. Für Konfigurationsdateien MÜSSEN Berechtigungen festgelegt sein, die den Zugriff nur auf den Vault-Benutzer beschränken.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den benutzerdefinierten Baustein APP.bd.6 *Secrets Management mit Hashicorp Vault*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.bd.6.A3 Hochverfügbarkeit

Da es sich um eine zentrale Komponente handelt, SOLLTE der Betrieb hochverfügbar ausgelegt werden (Cluster). Bei Virtualisierung SOLLTE darauf geachtet werden, dass die virtuellen Maschinen auf unterschiedlichen Hosts betrieben werden. Bei Verwendung von Container-Techniken SOLLTEN geeignete restart-on-failure Mechanismen konfiguriert sein.

APP.bd.6.A4 Verwendung von TLS

Die Kommunikation zwischen Clients und dem Server Cluster SOLLTE verschlüsselt erfolgen. Werden Load-Balancer oder Reverse-Proxies verwendet, SOLLTEN diese TLS nicht terminieren.

APP.bd.6.A5 Kein Mehrmandanten-System verwenden

Vault SOLLTE der einzige Hauptprozess sein, der auf einem Computer ausgeführt wird. Dies verringert das Risiko, dass ein anderer Prozess, der auf demselben Computer ausgeführt wird, kompromittiert ist und mit Vault interagieren kann.

APP.bd.6.A6 Kein SSH / Remotedesktop Zugriff

SSH bzw. Remotedesktop Verbindungen SOLLTEN deaktiviert sein. Ein Zugriff auf Vault SOLLTE immer über die API über das Netz stattfinden.

APP.bd.6.A7 Überwachung der Vault Instanzen

Die Vault Instanzen SOLLTEN geeignet überwacht werden. Es SOLLTE eine Einbindung in zentrale Monitoring- und Log-Management-Dienste erfolgen. Es SOLLTE dabei vor allem die Verfügbarkeit, die Ressourcenauslastung und Fehlerzustände überwacht und erkannt werden.

APP.bd.6.A8 Swap deaktivieren

Swap SOLLTE deaktiviert sein, damit verhindert wird, dass das Betriebssystem vertrauliche Daten auf die Festplatte überträgt. Vault verschlüsselt Daten während der Übertragung und im Ruhezustand.

APP.bd.6.A9 Core Dumps deaktivieren

Das Erstellen von Core Dumps SOLLTE deaktiviert sein, da ein Benutzer oder Administrator, der einen Core-Dump erzwingen kann und Zugriff auf die resultierende Datei hat, möglicherweise auf Vault-Verschlüsselungsschlüssel zugreifen kann.

APP.bd.6.A10 Root Token widerrufen

Das von Vault bereitgestellte Root-Token zur Initialisierung SOLLTE nach Fertigstellung der Einrichtung widerrufen werden, um das Risiko einer Preisgabe auszuschließen. Root-Token können bei Bedarf generiert werden.

APP.bd.6.A11 Versionsverwaltung für Konfigurationen

Notwendige Konfigurationen SOLLTEN nicht manuell erfolgen, sondern mit Hilfe von Konfigurationsdateien. Diese Konfigurationsdateien SOLLTEN an einer zentralen Stelle verfügbar sein sowie in die Versionsverwaltung und die Datensicherung eingebunden werden.

APP.bd.6.A12 Aktivierung Audit-Logging

Es SOLLTE das Audit-Logging aktiviert sein. Durch Aktivieren der Überwachung wird ein Verlauf aller von Vault ausgeführten Vorgänge angezeigt und ein forensischer Pfad für den Fall eines Missbrauchs oder einer Gefährdung bereitgestellt. In Überwachungsprotokollen werden vertrauliche Daten sicher gehasht, der Zugriff SOLLTE jedoch weiterhin eingeschränkt werden, um unbeabsichtigte Offenlegungen zu verhindern.

APP.bd.6.A13 Speicherzugriff einschränken

Der Zugriff auf das Speicher-Backend SOLLTE auf Vault beschränkt werden, um unbefugten Zugriff oder unbefugte Vorgänge zu vermeiden. Obwohl die Daten verschlüsselt sind, kann ein Angreifer durch Ändern oder Löschen von Schlüsseln zu Datenbeschädigung oder -verlust führen.

APP.bd.6.A14 Automatisiertes Ausrollen / Wiederrufen der Konfiguration

Die Konfiguration SOLLTE möglichst automatisiert in das laufende Cluster übertragen werden, um wiederholbare Prozesse zu etablieren und menschliche Fehler zu reduzieren.

APP.bd.6.A15 Verwendung feingranularer Policies verwenden

Die in dem ACL-System konfigurierten Policies SOLLTEN möglichst feingranular sein, um das Prinzip von „Least Privileges“ zu unterstützen.

APP.bd.6.A16 Verwendung kurzlebiger Tokens

Ein Token SOLLTE nur so lange gültig sein (Time To Live, TTL), wie Zugriff auf die Geheimnisse erforderlich ist, auf die er den Zugriff autorisiert.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den benutzerdefinierten Baustein APP.bd.6 *Secrets Management mit Hashicorp Vault* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.bd.6.A17 Master-Key austauschen

Im Falle von Personalwechsel (Eintritt oder Ausscheiden) SOLLTE bei den Inhabern von Shared-Keys der Master Key neu erzeugt und die Shared-Keys ausgetauscht werden. Zusätzlich SOLLTE der Encryption-Key rotiert werden.

APP.bd.6.A18 Verwendung von Ressourcenkontingenten (Quotas)

Um die Stabilität und das Netz der Vault-Umgebung sowie den Speicherressourcenverbrauch vor außer Kontrolle geratenem Anwendungsverhalten und DDoS-Angriffen (Distributed Denial of Service) zu schützen, SOLLTEN Ressourcenkontingente verwendet werden. Dabei SOLLTE die maximale Anzahl von Anforderungen pro Sekunde (RPS) oder Anzahl der Lease-Kontingente (nur Vault Enterprise) begrenzt werden.

4 Weiterführenden Informationen

4.1 Wissenswertes

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den benutzerdefinierten Baustein APP.bd.6 *Secrets Management mit Hashicorp Vault* finden sich unter anderem in folgenden Veröffentlichungen:

[DokVault]: Dokumentation Vault Security, https://www.vaultproject.io/docs/internals/security, zuletzt abgerufen am 28.05.2021

[DokVault2]: Dokumentation Vault Production Hardening, https://learn.hashicorp.com/vault/day-one/production-hardening, zuletzt abgerufen am 28.05.2021

[DokVault3]: Dokumentation Vault Rekeying and Rotating, https://learn.hashicorp.com/vault/operations/ops-rekeying-and-rotating, zuletzt abgerufen am 28.05.2021

[DokVault4]: Dokumentation Vault Tokens, https://learn.hashicorp.com/vault/security/tokens, zuletzt abgerufen am 28.05.2021

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für den benutzerdefinierten Baustein APP.bd.6 *Secrets Management mit Hashicorp Vault* von Bedeutung:

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

	Elementare Gefährdungen																	
Anforderungen	G 0.9	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.27	G 0.28	G 0.29	G 0.31	G 0.32	G 0.39	G 0.40	G 0.45	G 0.46
A1	X		X						X	X			X					
A2	X		X	X		X	X	X	X					X	X	X	X	X
A3	X								X	X						X	X	
A4		X		X			X											X
A5	X		X	X	X	X	X	X	X		X		X		X	X	X	X
A6	X		X			X		X	X				X	X				
A7	X					X	X	X	X	X		X					X	
A8			X	X			X										X	X
A9			X	X													X	X
A10			X	X		X	X	X	X								X	X
A11			X			X						X	X					X
A12						X	X	X										X
A13			X	X													X	X
A14						X							X					
A15			X				X	X										
A16			X	X			X	X									X	X
A17			X					X		X			X					
A18	X								X							X	X	X