ORP.6 Cloud-Identitäts- und Zugriffsmanagement

1. Beschreibung

1.1. Einleitung

Das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) in Cloud-Umgebungen unterscheidet sich grundlegend von traditionellen On-Premises-Ansätzen. Während es im eigenen Rechenzentrum primär um die Verwaltung von menschlichen Benutzern und Gruppen geht, erweitert sich das Spektrum in der Cloud dramatisch: Es umfasst eine Vielzahl nicht-menschlicher Identitäten wie Dienste, Anwendungen, Serverless-Funktionen und Container, die alle programmatisch über APIs auf tausende von Ressourcen zugreifen.
Die Verwaltung erfolgt über komplexe, oft in JSON definierte Richtlinien (Policies), die in einer dynamischen und ephemeren Umgebung angewendet werden. Konzepte wie föderierte Identitäten, temporäre Sicherheitsanmeldeinformationen und die gemeinsame Verantwortung (Shared Responsibility Model) zwischen Cloud-Anbieter und Kunde sind zentral. Ein Fehler in einer IAM-Konfiguration kann sofort weitreichende Konsequenzen für die Sicherheit der gesamten Cloud-Infrastruktur haben.

1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg auf, um ein robustes und sicheres Identitäts- und Zugriffsmanagement für Cloud-Umgebungen aufzubauen. Ziel ist es, den Grundsatz des geringsten Privilegs (Least Privilege) für alle Identitäten – menschlich wie maschinell – durchzusetzen, unautorisierte Zugriffe zu verhindern und eine lückenlose Nachvollziehbarkeit aller sicherheitsrelevanten Aktionen zu gewährleisten.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.6 ist auf alle genutzten Public- und Private-Cloud-Umgebungen anzuwenden.
Er konkretisiert die allgemeinen Anforderungen aus ORP.4 Identitäts- und Berechtigungsmanagement für den Cloud-Kontext. Er steht in enger Wechselwirkung mit OPS.2.3 Nutzung von Cloud-Diensten und ist eine wesentliche Grundlage für die Sicherheit von DevOps-Prozessen (siehe OPS.1.1.8), Container-Umgebungen (CON.5) und Cloud-Speichern (APP.4.9).

2. Gefährdungslage

Für den Baustein ORP.6 sind folgende spezifische Bedrohungen und Schwachstellen von besonderer Bedeutung:

Überprivilegierte Identitäten

Benutzer und insbesondere Dienste (Service Principals) erhalten weitaus mehr Berechtigungen, als für ihre eigentliche Aufgabe notwendig ist. Aufgrund der Komplexität von Tausenden von Einzelberechtigungen werden oft vordefinierte, zu breite Rollen wie

"Contributor" oder "Editor" vergeben. Eine Kompromittierung einer solchen Identität ermöglicht es einem Angreifer, weitreichenden Schaden anzurichten.

Kompromittierung von langlebigen Zugangsdaten

Für den programmatischen Zugriff werden langlebige statische Zugangsdaten (API-Schlüssel, Secrets) erstellt und in Anwendungen oder Konfigurationsdateien hinterlegt. Werden diese kompromittiert, hat ein Angreifer dauerhaft unbemerkten Zugriff auf Cloud-Ressourcen.

Unbeabsichtigte Berechtigungseskalation durch komplexe Richtlinien

Die Kombination mehrerer IAM-Richtlinien auf verschiedenen Ebenen (Organisation, Ordner, Projekt, Ressource) kann zu unbeabsichtigten und schwer nachvollziehbaren kumulativen Rechten führen. Ein Angreifer kann diese Komplexität ausnutzen, um seine eigenen Berechtigungen gezielt zu erweitern.

Unsichere Konfiguration von föderierten Identitäten

Eine fehlerhafte Konfiguration der Vertrauensstellung zwischen dem lokalen Identitätsprovider (z. B. Active Directory) und dem Cloud-IAM-System (z. B. Azure AD/Entra ID) kann es Angreifern ermöglichen, sich mit kompromittierten lokalen Konten unautorisiert Zugriff auf Cloud-Ressourcen zu verschaffen.

Mangelnde Übersicht und inkonsistente Richtlinien in Multi-Cloud-Umgebungen

Jeder Cloud-Anbieter (AWS, Azure, GCP) hat ein eigenes IAM-Modell mit unterschiedlichen Konzepten und Begrifflichkeiten. Dies erschwert die Durchsetzung einer einheitlichen Sicherheitsrichtlinie und führt zu einer fragmentierten und unübersichtlichen Berechtigungslandschaft.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.6 aufgeführt.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ORP.6.A1 Absicherung des Root-/Haupt-Administratorkontos (B)

Das initiale Haupt-Administratorkonto der Cloud-Umgebung (Root-Account) MUSS durch ein sehr starkes Passwort und Multi-Faktor-Authentifizierung (MFA) geschützt werden. Es DARF NICHT für alltägliche administrative Aufgaben verwendet werden.

ORP.6.A2 Einführung eines grundlegenden Rollenkonzepts (B)

Es MUSS ein grundlegendes, rollenbasiertes Zugriffskonzept (RBAC) umgesetzt werden, das mindestens zwischen Lesenden, Bearbeitern und Besitzern von Ressourcen unterscheidet.

ORP.6.A3 Erzwingung der Multi-Faktor-Authentifizierung (MFA) (B)

Für alle Benutzer, die über Berechtigungen zur Änderung von Konfigurationen oder Daten verfügen (nicht nur Administratoren), MUSS die Verwendung von MFA technisch erzwungen werden.

ORP.6.A4 Richtlinie zur Verwaltung von Cloud-Identitäten (B)

Es MUSS eine Richtlinie geben, die den Lebenszyklus von Cloud-Identitäten regelt. Dies umfasst die Erstellung, Änderung, Deaktivierung und Löschung von menschlichen und nicht-menschlichen Identitäten.

ORP.6.A5 Protokollierung von IAM-Aktivitäten (B)

Alle sicherheitsrelevanten IAM-Ereignisse, insbesondere Anmeldeversuche, API-Aufrufe und Änderungen an Berechtigungen, MÜSSEN protokolliert und an einem zentralen Ort gesammelt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.6.A6 Systematische Umsetzung des Prinzips der geringsten Rechte (S)

Berechtigungen SOLLTEN so granular wie möglich vergeben werden. Anstelle von breiten vordefinierten Rollen SOLLTEN benutzerspezifische Rollen erstellt werden, die nur die für die jeweilige Aufgabe notwendigen Berechtigungen enthalten.

ORP.6.A7 Nutzung von Föderation statt nativer Cloud-Benutzer (S)

Menschliche Benutzer SOLLTEN sich über einen zentralen, vertrauenswürdigen Identitätsprovider (z. B. Azure AD/Entra ID, Okta) authentifizieren. Die direkte Erstellung von Cloud-nativen Benutzern mit eigenen Passwörtern SOLLTE vermieden werden.

ORP.6.A8 Einsatz von temporären Anmeldeinformationen für programmatischen Zugriff (S)

Für den Zugriff durch Anwendungen, Skripte oder Dienste SOLLTEN Mechanismen für temporäre, rollenbasierte Anmeldeinformationen genutzt werden (z. B. IAM Roles bei AWS, Managed Identities bei Azure). Langlebige, statische API-Schlüssel SOLLTEN vermieden werden.

ORP.6.A9 Regelmäßige Überprüfung der Berechtigungen (Access Reviews) (S)

Die zugewiesenen Berechtigungen für alle Identitäten SOLLTEN in regelmäßigen Abständen überprüft werden. Nicht mehr benötigte oder überprivilegierte Zugriffe SOLLTEN entfernt werden. Dieser Prozess SOLLTE, wo möglich, automatisiert werden.

ORP.6.A10 Nutzung von bedingtem Zugriff (Conditional Access) (S)

Der Zugriff auf Cloud-Ressourcen SOLLTE an Bedingungen geknüpft werden. Richtlinien für den bedingten Zugriff SOLLTEN Faktoren wie den Standort des Benutzers, den Zustand des Endgeräts oder das Risikoniveau der Anmeldung berücksichtigen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Die folgenden Anforderungen sind exemplarische Vorschläge für ein Schutzniveau, das über den Stand der Technik hinausgeht. Sie SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden.

ORP.6.A11 Einsatz von Just-in-Time (JIT) Zugriff für administrative Rollen (H)

Hochprivilegierte Berechtigungen SOLLTEN nicht permanent zugewiesen sein. Sie SOLLTEN nur bei Bedarf, für einen begrenzten Zeitraum und nach einem Genehmigungsprozess über ein Privileged Access Management (PAM)-System aktiviert werden.

ORP.6.A12 Kontinuierliche Überwachung mit Cloud Security Posture Management (CSPM) (H)

Es SOLLTEN spezialisierte Werkzeuge (CSPM) eingesetzt werden, die die IAM-Konfiguration kontinuierlich auf Fehlkonfigurationen, öffentliche Zugriffe und übermäßige Berechtigungen scannen und automatisch alarmieren.

ORP.6.A13 Implementierung von Berechtigungsgrenzen (Permissions Boundaries) (H)

Um eine unkontrollierte Ausweitung von Rechten zu verhindern, SOLLTEN technische Berechtigungsgrenzen definiert werden. Diese legen die maximal möglichen Berechtigungen fest, die eine Identität jemals erhalten kann, selbst wenn ein Administrator versucht, ihr mehr Rechte zuzuweisen.

ORP.6.A14 Zentrales IAM für Multi-Cloud-Umgebungen (H)

In Multi-Cloud-Szenarien SOLLTE eine zentrale IAM-Lösung (Cloud Infrastructure Entitlement Management, CIEM) eingesetzt werden, um eine einheitliche Übersicht und Kontrolle über die Berechtigungen über alle Cloud-Anbieter hinweg zu gewährleisten.

ORP.6.A15 Absicherung von Workload-Identitäten (H)

Die Authentifizierung zwischen Diensten (z. B. zwischen einem CI/CD-Runner und einem Cloud-Dienst) SOLLTE über kurzlebige, zertifikatsbasierte Identitäten (Workload Identity Federation) anstelle von langlebigen Schlüsseln abgesichert werden.