Playbook: Unberechtigter Zugriff in Cloud-Umgebungen

Übersicht

Dieses Playbook beschreibt die Erkennung, Analyse und Reaktion auf unbefugte Zugriffsversuche und -vorfälle in cloudbasierten IT-Umgebungen. Es enthält strukturierte Vorgehensweisen für Sicherheitsteams zur effektiven Bewältigung von Sicherheitsverletzungen dieser Art.

Anwendungsbereich

- AWS, Azure, Google Cloud und andere Cloud-Service-Provider
- SaaS-Anwendungen mit Unternehmensnutzung
- Hybride Cloud-Umgebungen
- Multi-Cloud-Architekturen

Verantwortlichkeiten

Rolle	Verantwortlichkeiten
SOC-Analyst (L1)	Initiale Alarmüberwachung, Triage und Eskalation
Incident Response Team (L2)	Detaillierte Untersuchung und Eindämmung
Cloud Security Architect	Technische Beratung und Cloud-spezifische Maßnahmen
CISO/Security Manager	Geschäftliche Entscheidungen und Kommunikation mit Stakeholdern
Rechtsabteilung	Bewertung rechtlicher Verpflichtungen und Compliance-Anforderungen

1. Erkennung

1.1 Primäre Erkennungsmechanismen

- **Cloud-Provider-Logs**: CloudTrail (AWS), Activity Logs (Azure), Cloud Audit Logs (GCP)

- **IAM-Ereignisse**: Ungewöhnliche Anmeldeversuche, Rollenänderungen, Policy-Modifikationen
- **CASB-Lösungen**: Anomalieerkennung im Cloud-Zugriff
- **Endpoint Detection und Response (EDR)**: Verdächtige Aktivitäten auf verbundenen Endgeräten
- **Cloud Security Posture Management (CSPM)**: Änderungen an Sicherheitskonfigurationen

1.2 Alarmindikatoren (IoAs)

- Anmeldeversuche außerhalb üblicher Geschäftszeiten oder von unbekannten Standorten
- Erhöhung der Berechtigungen ohne genehmigten Change-Request
- Mehrfache fehlgeschlagene Authentifizierungsversuche gefolgt von erfolgreicher Anmeldung
- Plötzliche API-Aufrufe von unbekannten IP-Adressen oder geografischen Standorten
- Aktivierung oder Deaktivierung von Sicherheitsfunktionen
- Ausführung privilegierter Befehle oder ungewöhnlicher API-Aufrufe
- Massenhafte Datenzugriffe oder -exporte

1.3 Früherkennung und Alarmierung

- **SIEM-Integration**: Korrelation von Cloud-Provider-Logs mit anderen Sicherheitsdaten
- **Benutzer- und Entitätsverhaltensanalyse (UEBA)**: Erkennung von Abweichungen vom normalen Benutzerverhalten
- **Echtzeit-Alarmierung**: Automatische Benachrichtigung des SOC-Teams bei kritischen Ereignissen

2. Initiale Analyse und Triage

2.1 Sofortige Bewertung (15-30 Minuten)

1. **Verifizieren des Alarms**: Bestätigen Sie, dass es sich nicht um einen False Positive handelt
2. **Kontext erfassen**:
    a. Betroffene Cloud-Ressourcen und -Dienste identifizieren
    b. Involvierte Benutzerkonten oder Identitäten bestimmen
    c. Zeitlichen Ablauf der Ereignisse rekonstruieren

3. **Erste Risikobewertung**:
    a. Sensibilität der betroffenen Daten und Systeme
    b. Potenzielle Auswirkungen auf Geschäftsprozesse
    c. Mögliche Compliance-Implikationen

2.2 Initiale Datensammlung

- Cloud-Provider-Protokolle für den relevanten Zeitraum
- IAM-Audit-Logs und Authentifizierungsdaten
- Netzwerkverkehrslogs (VPC Flow Logs, Security Groups)
- Endpunkt-Telemetrie für relevante Systeme
- Konfigurationsänderungen an Cloud-Ressourcen

2.3 Schweregrad-Klassifizierung

Schweregrad	Kriterien	Reaktionszeit
Kritisch	- Zugriff auf sensible Kundendaten oder Geschäftsgeheimnisse - Kompromittierung privilegierter Zugänge - Aktive Lateral Movement-Anzeichen	Sofort (< 15 Min.)
Hoch	- Zugriff auf interne Daten - Unberechtigte Änderung von Produktionsumgebungen - Verdacht auf gezielte Angriffe	1-2 Stunden
Mittel	- Unberechtigter Zugriff auf nicht-kritische Systeme - Verdächtige, aber eingeschränkte Aktivitäten	4-8 Stunden
Niedrig	- Einzelne fehlgeschlagene Zugriffe - Verdächtige Aktivitäten ohne bestätigten Zugriff	24 Stunden

3. Untersuchung

3.1 Detaillierte Forensik

- **Zugriffspfad rekonstruieren**:
    - Wie wurde Zugang erlangt (gestohlene Credentials, Fehlkonfiguration, API-Keys)?

    - Welche Methoden wurden zur Umgehung von Sicherheitsmaßnahmen verwendet?
- **Aktivitäten nach Zugriff analysieren**:
    - Welche Aktionen wurden durchgeführt?
    - Welche Ressourcen wurden angesehen, verändert oder extrahiert?
    - Wurden weitere Backdoors oder persistente Zugänge eingerichtet?

3.2 Cloud-spezifische Untersuchungstechniken

- **CloudTrail/Activity Logs Analyse**:
    - API-Aufrufe nach Zeitstempel, Benutzer und IP filtern
    - Ungewöhnliche Aktivitätsmuster identifizieren
- **IAM/Identitätsanalyse**:
    - Berechtigungsänderungen überprüfen
    - Service-Principals und verwaltete Identitäten untersuchen
    - OAuth-Anwendungsberechtigungen und Token-Nutzung analysieren
- **Ressourcenanalyse**:
    - Änderungen an Netzwerkkonfigurationen (Security Groups, NACLs, Firewall-Regeln)
    - Neue oder modifizierte Compute-Ressourcen (VMs, Funktionen, Container)
    - Änderungen an Datenbanken und Speicherdiensten

3.3 Lateral Movement und Privilegien-Eskalation

- Überprüfung von Zugriffserweiterungen über verschiedene Cloud-Dienste
- Korrelation zwischen Cloud-Aktivitäten und On-Premises-Ereignissen
- Analyse der Nutzung von vertrauenswürdigen Beziehungen zwischen Ressourcen

3.4 IoC-Extraktion

- Verdächtige IP-Adressen, Domains und Geolokationen
- Kompromittierte Benutzerkonten oder Dienstprinzipale
- Ungewöhnliche API-Aufrufe oder Befehlssequenzen
- Neu erstellte oder modifizierte Cloud-Ressourcen
- Zeitliche Muster der Aktivitäten

4. Eindämmung

4.1 Sofortige Eindämmungsstrategien

- **Isolation kompromittierter Ressourcen**:
  - Temporäre Firewall-Regeln oder Security Groups anwenden
  - Zugriff auf betroffene Subnets einschränken
- **Identitätsmanagement**:
  - Betroffene Benutzerkonten sperren oder deaktivieren
  - API-Schlüssel, Zugriffsschlüssel und SAS-Token rotieren
  - MFA für kompromittierte Konten erzwingen
- **Zugriffskontrolle**:
  - Just-in-Time-Zugriff für administrative Aktionen implementieren
  - Break-Glass-Prozeduren für kritische Ressourcen aktivieren

4.2 Erweiterte Eindämmungsmaßnahmen

- **Netzwerkisolation**:
  - VPC Service Endpoints einschränken
  - Private Link/Endpoint-Konfigurationen überprüfen
  - Öffentliche Endpunkte temporär deaktivieren
- **Workload-Sicherung**:
  - Verdächtige VMs oder Container isolieren oder beenden
  - Serverless-Funktionen einschränken oder deaktivieren
  - Datenbankzugriffe auf Read-Only setzen
- **Automatisierte Reaktionen**:
  - Security Orchestration and Automated Response (SOAR) Playbooks auslösen
  - Auto-Remediation über Cloud Security Posture Management aktivieren

4.3 Beweissicherung

- Snapshots von betroffenen VMs oder Datenbanken erstellen
- Relevante Log-Daten in forensisch sichere Speicher exportieren
- Konfigurationsänderungen dokumentieren (vor und nach dem Vorfall)
- Metadaten kompromittierter Ressourcen sichern

5. Beseitigung

5.1 Entfernung von Angreifern

- Identifizierte Backdoors und persistente Zugänge entfernen
- Unbekannte oder unerwünschte Cloud-Ressourcen terminieren
- Automatisierungen und Scheduling-Jobs überprüfen und bereinigen
- Widerrufen aller während des Angriffs erstellten Zugriffsberechtigungen

5.2 Wiederherstellung sicherer Zustände

- **Identitätsmanagement**:
  - Rotation aller Credentials in betroffenen Umgebungen
  - Überprüfung und Neukonfiguration von IAM-Richtlinien nach Least-Privilege
  - Implementierung zusätzlicher Authentifizierungskontrollen
- **Ressourcen-Wiederherstellung**:
  - Restore aus Pre-Incident-Snapshots oder Backups
  - Infrastructure-as-Code Deployment für saubere Rekonfiguration
  - Überprüfung aller Konfigurationen auf versteckte Änderungen

5.3 Bereinigungsüberprüfung

- Sicherheitsbewertung nach der Bereinigung durchführen
- Penetrationstests oder Red-Team-Übungen zur Validierung
- Compliance-Check für betroffene Systeme

6. Wiederherstellung

6.1 Schrittweise Rückkehr zum Normalbetrieb

- Prioritätsbasierte Wiederherstellung kritischer Geschäftsfunktionen
- Überwachte Wiederaufnahme des normalen Betriebs
- Temporäre Erhöhung der Überwachung für wiederhergestellte Systeme

6.2 Kommunikation und Koordination

- Statusaktualisierungen an relevante Stakeholder
- Koordination mit Cloud-Provider (wenn erforderlich)
- Support für betroffene Geschäftsbereiche

6.3 Überwachung nach dem Vorfall

- Erhöhte Überwachung für kritische Cloud-Ressourcen
- Implementierung zusätzlicher Erkennungsregeln für ähnliche Angriffe
- Erweiterte Logging für relevante Ressourcen

7. Nachbereitung und Lessons Learned

7.1 Dokumentation und Berichterstattung

- Vollständige Dokumentation des Vorfalls und der Reaktionsmaßnahmen
- Root-Cause-Analyse
- Executive Summary für Management und Stakeholder
- Compliance- und regulatorische Berichterstattung (falls erforderlich)

7.2 Verbesserungen der Sicherheitslage

- **Technische Verbesserungen**:
  - Implementierung zusätzlicher Sicherheitskontrollen
  - Erweiterung der Erkennungsfähigkeiten
  - Automatisierung von Reaktionsmaßnahmen
- **Prozessverbesserungen**:
  - Aktualisierung des Incident-Response-Plans
  - Optimierung von Kommunikationswegen
  - Anpassung von Eskalationsverfahren

7.3 Schulung und Awareness

- Schulungsmaßnahmen basierend auf den Erkenntnissen
- Sensibilisierung für beobachtete Angriffstechniken
- Table-Top-Übungen für ähnliche Szenarien

Anhänge

A. Cloud-spezifische Reaktionstools und -befehle

AWS

```
# Benutzerzugriff einschränken
aws iam attach-user-policy --user-name [USERNAME] --policy-arn
```

```
arn:aws:iam::aws:policy/AWSDenyAll

# Zugriffsschlüssel deaktivieren
aws iam update-access-key --access-key-id [ACCESS_KEY_ID] --status
Inactive --user-name [USERNAME]

# Security Group isolieren
aws ec2 revoke-security-group-ingress --group-id [SECURITY_GROUP_ID]
--protocol all --cidr 0.0.0.0/0

# CloudTrail-Logs abfragen
aws cloudtrail lookup-events --lookup-attributes
AttributeKey=Username,AttributeValue=[USERNAME]
```

Azure

```
# Benutzerkonto sperren
az ad user update --id [USER_ID] --account-enabled false

# Notfallzugriff für Subscription entfernen
az role assignment delete --assignee [USER_ID] --scope
/subscriptions/[SUBSCRIPTION_ID]

# VM isolieren durch NSG
az network nsg rule create --name DenyAll --nsg-name [NSG_NAME] --
priority 100 --resource-group [RESOURCE_GROUP] --access Deny --
direction Inbound --source-address-prefix '*' --destination-address-
prefix '*' --destination-port-range '*'

# Activity Log abfragen
az monitor activity-log list --start-time [START_TIME] --
correlation-id [CORRELATION_ID]
```

Google Cloud Platform

```
# IAM-Berechtigungen widerrufen
gcloud projects remove-iam-policy-binding [PROJECT_ID] --
member='user:[USER_EMAIL]' --role='[ROLE]'

# API-Schlüssel deaktivieren
```

```
gcloud services api-keys update [KEY_ID] --state=DISABLED

# VM isolieren mit Firewall-Regeln
gcloud compute firewall-rules create deny-all-ingress --
direction=INGRESS --priority=100 --network=[NETWORK] --action=DENY -
-rules=all --source-ranges=0.0.0.0/0 --target-tags=[VM_TAG]

# Audit Logs abfragen
gcloud logging read 'resource.type=audited_resource AND
protoPayload.authenticationInfo.principalEmail=[USER_EMAIL]'
```

B. Incident Response Checkliste

Erste Reaktion

- [ ] Alarmbenachrichtigung und Informationsbeschaffung
- [ ] Incident Response Team aktivieren
- [ ] Betroffene Cloud-Ressourcen und -Dienste identifizieren
- [ ] Vorläufige Risikobewertung durchführen
- [ ] Sofortige Kommunikation mit relevanten Stakeholdern einleiten

Analyse und Eindämmung

- [ ] Relevante Cloud-Logs und -Protokolle sichern
- [ ] Angriffspfad und Zugriffsmethode identifizieren
- [ ] Betroffene Konten und Ressourcen inventarisieren
- [ ] Eindämmungsmaßnahmen entsprechend dem Schweregrad implementieren
- [ ] Sofortmaßnahmen zur Einschränkung des Zugriffs durchführen

Beseitigung und Wiederherstellung

- [ ] Alle unauthorisierten Zugänge entfernen
- [ ] Betroffene Credentials rotieren
- [ ] Kompromittierte Systeme aus sauberen Backups wiederherstellen
- [ ] Sicherheitskontrollen überprüfen und verstärken
- [ ] Schrittweise Rückkehr zum Normalbetrieb koordinieren

Nachbereitung

- [ ] Vollständigen Incident Report erstellen

- [ ] Root-Cause-Analyse durchführen
- [ ] Verbesserungsmaßnahmen identifizieren und planen
- [ ] Erkenntnisse mit relevanten Teams teilen
- [ ] Playbook basierend auf Erkenntnissen aktualisieren

C. Cloud-Sicherheitsressourcen

Best Practices für Cloud-Sicherheit

- AWS Well-Architected Framework - Security Pillar
- Microsoft Azure Security Benchmark
- Google Cloud Security Best Practices
- CIS Benchmarks für Cloud-Provider
- Cloud Security Alliance (CSA) Publikationen

Nützliche Tools

- Cloud Security Posture Management (CSPM) Lösungen
- Cloud Workload Protection Platforms (CWPP)
- Cloud-native Sicherheitstools des jeweiligen Providers
- Open-Source-Tools für Cloud-Forensik

Schulungsmaterialien

- Cloud-spezifische Sicherheitszertifizierungen
- Provider-spezifische Sicherheitsschulungen
- Incident Response in Cloud-Umgebungen