Google Cloud-Spezifisches Playbook für Sicherheitsvorfälle

1. Ransomware-Vorfall in Google Cloud-Umgebung

Sofortmaßnahmen

1. **Isolation betroffener GCP-Ressourcen:**
    a. Anwenden von VPC Firewall-Regeln zur Isolation betroffener Instances
    b. Konfigurieren von GCP Network Tags für granulare Firewall-Steuerung
    c. Verwenden von VPC Service Controls zur Einschränkung des Ressourcenzugriffs
    d. Nutzen von Identity-Aware Proxy (IAP) für kontrollierten Zugriff auf isolierte Instances
2. **GCP-spezifische Beweissicherung:**
    a. Erstellen von Persistent Disk-Snapshots aller betroffenen Volumes
    b. Aktivieren von Stackdriver (Cloud Operations) Logging für detaillierte Überwachung
    c. Sichern von Cloud Audit Logs in einem separaten Projekt mit eingeschränktem Zugriff
    d. Erstellen von Machine Images betroffener Compute Engine-Instances
3. **Google Cloud IAM-Sicherung:**
    a. Identifizieren und Widerrufen kompromittierter Service Account-Schlüssel
    b. Rotieren aller Service Account-Schlüssel im betroffenen Projekt
    c. Überprüfen und Einschränken von IAM-Rollen mit temporären IAM Denials
    d. Überprüfen von IAM Policy Analyzer auf zu permissive Berechtigungen
4. **GCP-spezifische Überwachung aktivieren:**
    a. Aktivieren von Security Command Center Premium für erweiterte Bedrohungserkennung
    b. Konfigurieren von Custom Log-based Metrics für verdächtige Ereignisse

c. Implementieren von Cloud Monitoring-Alarmen für ungewöhnliche Aktivitäten
d. Aktivieren von Event Threat Detection für fortgeschrittene Bedrohungsanalyse

Wiederherstellung

1. **Clean Instance-Erstellung:**
   a. Bereitstellen neuer Instances aus verifizierten Gold-Images
   b. Wiederherstellen von Daten aus Cloud Storage-Backups
   c. Verwenden von Deployment Manager oder Terraform für sichere IaC-Bereitstellung
   d. Implementieren von OS Login für verbesserte VM-Zugriffssicherheit
2. **GCP-Konfigurationsüberprüfung:**
   a. Nutzen von Security Health Analytics für Sicherheitsbewertung
   b. Überprüfen der Cloud Storage-Bucket-Berechtigungen mit IAM-Analysen
   c. Scannen von Container Registry-Images mit Container Analysis API
   d. Überprüfen aller Load Balancer und Cloud Armor-Konfigurationen
3. **Google Cloud Armor:**
   a. Aktivieren von Cloud Armor für Web Application und DDoS-Schutz
   b. Konfigurieren von Cloud Armor-Sicherheitsrichtlinien basierend auf dem Vorfall
   c. Implementieren von Rate-Limiting mit Cloud Armor-Regeln
   d. Konfigurieren von geo-basierten Zugriffskontrollen

2. Unbefugter Zugriff auf Google Cloud-Konto

Sofortmaßnahmen

1. **Google Cloud Identity-Zugangsschutz:**
   a. Sofortiges Ändern des Administrator-Passworts
   b. Aktivieren von 2-Faktor-Authentifizierung für alle privilegierten Konten
   c. Implementieren von Security Keys für administrative Zugänge
   d. Überprüfen und Entfernen unbekannter API-Schlüssel und OAuth-Anwendungen
2. **GCP-Ressourcen-Überprüfung:**
   a. Identifizieren ungewöhnlicher Compute Engine-Instances

   b. Überprüfen aller Cloud Functions auf nicht autorisierte Änderungen
   c. Überprüfen der Deployment Manager-Deployments auf unbekannte Änderungen
   d. Scannen aller Cloud Storage-Buckets auf öffentliche Zugänglichkeit
3. **GCP Organizations-Maßnahmen:**
   a. Implementieren von Organization Policy Constraints zur Schadensbegrenzung
   b. Überprüfen der Cloud Audit Logs auf organisations- und projektübergreifende Aktivitäten
   c. Temporäres Einschränken neuer Projektregistrierungen über Resource Manager
   d. Überprüfen aller IAM-Bindings für externe Identitäten
4. **GCP-spezifische Logging-Verstärkung:**
   a. Sicherstellen, dass Cloud Audit Logs für alle Projekte aktiviert sind
   b. Aktivieren von Data Access Logs für alle sensiblen Ressourcen
   c. Konfigurieren von VPC Flow Logs für alle Netzwerke
   d. Einrichten von Log-Exports zu BigQuery für langfristige forensische Analysen

Wiederherstellung

1. **Google Cloud Identity-Sicherheitsposture:**
   a. Implementieren von Context-Aware Access für bedingte Zugriffssteuerung
   b. Konfigurieren von Access Boundary für Service-Konten
   c. Implementieren von Cloud Identity-Aware Proxy für web-basierte Anwendungen
   d. Bereitstellen von BeyondCorp Enterprise für Zero-Trust-Sicherheit
2. **GCP-spezifische Sicherheitsüberprüfung:**
   a. Durchführen eines GCP Architecture Review mit Fokus auf Sicherheit
   b. Überprüfen der Secret Manager-Geheimnisse und Berechtigungen
   c. Scannen aller Container Registry-Images mit Container Analysis
   d. Überprüfen der API Gateway-Konfigurationen auf korrekte Authentifizierung

3. Datenexfiltration aus Cloud Storage

Sofortmaßnahmen

1. **Cloud Storage-spezifische Sicherung:**
    a. Sofortige Überprüfung und Korrektur aller Cloud Storage IAM-Berechtigungen
    b. Widerrufen aller Signed URLs für sensible Buckets
    c. Identifizieren und Entfernen aller unautorisierten CORS-Konfigurationen
    d. Aktivieren von Object Versioning für betroffene Buckets zur Schadensermittlung
2. **GCP-Datenverkehr-Analyse:**
    a. Überprüfen von Cloud Audit Logs für ungewöhnliche Storage-Zugriffsoperationen
    b. Analysieren von VPC Flow Logs für große ausgehende Datenübertragungen
    c. Überprüfen von Pub/Sub-Abonnements auf unautirisierte Datenweiterleitung
    d. Identifizieren von unerwarteten Cross-Region-Replikationen
3. **Cloud Storage-Zugriffssteuerung:**
    a. Implementieren von Bucket Lock für kritische Daten
    b. Überprüfen und Durchsetzen der Cloud Storage-Verschlüsselung
    c. Konfigurieren detaillierter IAM-Rollen mit minimalen Berechtigungen
    d. Implementieren von VPC Service Controls für Storage-Zugriffsbeschränkung

Wiederherstellung

1. **Cloud Storage-Sicherheitsoptimierung:**
    a. Implementieren von Retention Policies für kritische Daten
    b. Konfigurieren von Lifecycle-Richtlinien für sichere Datenverwaltung
    c. Einrichten privater Google Access für Cloud Storage
    d. Verwenden von Cloud Storage-Firewalls (VPC Service Controls) für netzwerkbasierte Zugriffssteuerung
2. **GCP Data Loss Prevention Integration:**
    a. Aktivieren von Data Loss Prevention (DLP) für automatische Erkennung sensibler Daten

b. Konfigurieren von DLP-Scans für alle Cloud Storage-Buckets
c. Erstellen von DLP-Vorlagen für PII und sensible Daten
d. Integration von DLP mit Security Command Center für zentralisierte Warnungen