AWS-Spezifisches Playbook für Sicherheitsvorfälle

1. Ransomware-Vorfall in AWS-Umgebung

Sofortmaßnahmen

1. **Isolation der betroffenen AWS-Ressourcen:**
    a. Modifizieren von Security Groups, um eingehenden/ausgehenden Verkehr zu blockieren
    b. Anwenden von Network ACLs zur Isolation auf Subnetz-Ebene
    c. Erstellung neuer Sicherheitsgruppen mit "Deny All" und Anwendung auf betroffene Instances
2. **Sichern der Forensischen Beweise:**
    a. Erstellen von EBS-Snapshots aller betroffenen Volumes
    b. Aktivieren von AWS Config für historische Konfigurationserfassung, falls noch nicht aktiviert
    c. Sichern von CloudTrail-Logs in einem separaten, gesicherten S3-Bucket
    d. Erstellen von AMIs betroffener EC2-Instances für forensische Untersuchung
3. **IAM-Zugriffskontrolle sichern:**
    a. Identifizieren und Deaktivieren kompromittierter IAM-Zugriffsschlüssel
    b. Rotieren aller IAM-Zugriffsschlüssel im betroffenen Konto
    c. Temporäres Einschränken von IAM-Berechtigungen mit expliziten Deny-Richtlinien
    d. Prüfen von AWS IAM Access Analyzer auf ungewöhnliche Berechtigungen
4. **AWS-spezifische Überwachung aktivieren:**
    a. Aktivieren von GuardDuty für erweiterte Bedrohungserkennung
    b. Konfigurieren von CloudWatch-Alarmen für verdächtige API-Aufrufe
    c. Implementieren von AWS Security Hub zur zentralisierten Sicherheitsüberwachung
    d. Prüfen von Logs mit Amazon Detective auf Angriffspfade

Wiederherstellung

1. **Clean Instance-Erstellung:**

   a. Bereitstellen neuer Instances aus verifizierten AMIs
   b. Wiederherstellen von Daten aus verifizierten Pre-Incident Backups (aus S3, Glacier oder Backup-Vaults)
   c. Verwenden von AWS CloudFormation oder AWS CDK für konsistente, sichere Neubereitstellung
   d. Implementieren von Instance Metadata Service Version 2 (IMDSv2) auf allen neuen Instances
2. **AWS-Konfigurationsüberprüfung:**
   a. Verwenden von AWS Trusted Advisor zur Identifikation von Sicherheitslücken
   b. Überprüfen der S3-Bucket-Berechtigungen mit S3 Access Analyzer
   c. Scannen von Elastic Container Registry (ECR) Images auf Schwachstellen
   d. Überprüfen aller Route-Tabellen und Internet Gateways auf unerwünschte Verbindungen
3. **AWS Shield und WAF:**
   a. Aktivieren von AWS Shield Standard/Advanced zum DDoS-Schutz
   b. Konfigurieren von AWS WAF mit angepassten Regeln basierend auf dem Vorfall
   c. Implementieren von rate-based Rules für verdächtige IP-Adressen
   d. Konfigurieren von geo-basierten Einschränkungen falls nötig

2. Unbefugter Zugriff auf AWS-Konto

Sofortmaßnahmen

1. **AWS-Zugangsschutz:**
   a. Sofortiges Ändern des Root-Benutzerpassworts
   b. Löschen oder Rotieren aller bestehenden IAM-Zugriffsschlüssel
   c. Aktivieren von MFA für alle IAM-Benutzer, insbesondere Root
   d. Überprüfen und Entfernen unbekannter IAM-Benutzer, -Rollen oder -Richtlinien
2. **AWS-Ressourcen-Überprüfung:**
   a. Identifizieren ungewöhnlicher EC2-Instances mit unbekannten AMIs
   b. Überprüfen aller Lambda-Funktionen auf nicht autorisierte Änderungen
   c. Überprüfen der CloudFormation-Stacks auf unbekannte Deployments

   d. Scannen aller S3-Buckets auf öffentliche Zugänglichkeit oder Policy-Änderungen
3. **AWS Organizations-Maßnahmen:**
   a. Implementieren von Service Control Policies (SCPs) zur Einschränkung des Schadens
   b. Überprüfen der AWS Organization Trail-Logs auf kontenübergreifende Aktivitäten
   c. Temporäres Einschränken des kontenübergreifenden Ressourcenzugriffs
   d. Überprüfen aller vertrauenswürdigen Identitäten und CrossAccount-Rollen
4. **AWS-spezifische Logging-Verstärkung:**
   a. Sicherstellen, dass CloudTrail Multi-Region aktiviert ist
   b. Aktivieren von S3-Access-Logging für alle Buckets
   c. Aktivieren von VPC Flow Logs für alle VPCs
   d. Sichern aller Cloudwatch Logs in einem isolierten forensischen Account

Wiederherstellung

1. **AWS Konten-Sicherheitsposture:**
   a. Implementieren von AWS Control Tower für standardisierte Multi-Account-Governance
   b. Anwenden von AWS Landing Zone Best Practices
   c. Konfigurieren von AWS Config-Regeln zur Überwachung von Compliance
   d. Implementieren von Least-Privilege-Berechtigungen mit AWS Permission Boundaries
2. **AWS-spezifische Sicherheitsüberprüfung:**
   a. Durchführen eines AWS Well-Architected-Reviews mit Schwerpunkt auf Sicherheit
   b. Überprüfen der AWS Secrets Manager- und Systems Manager Parameter Store-Einträge
   c. Scannen aller ECR-Images auf Schwachstellen mit ECR-Scans
   d. Überprüfen der API-Gateway-Konfigurationen auf korrekte Authentifizierung

3. Datenexfiltration aus S3 Buckets

Sofortmaßnahmen

1. **S3-spezifische Sicherung:**
    a. Sofortige Überprüfung und Korrektur aller S3-Bucket-Policies
    b. Temporäres Blockieren des öffentlichen Zugriffs auf Account-Ebene (S3 Block Public Access)
    c. Identifizieren und Entfernen aller unautorisierten Bucket ACLs
    d. Aktivieren von Versioning für betroffene Buckets zur Schadensermittlung
2. **AWS-Datenverkehr-Analyse:**
    a. Überprüfen von CloudTrail S3 Data Events für ungewöhnliche `GetObject`-Operationen
    b. Analysieren von VPC Flow Logs für große ausgehende Datenübertragungen
    c. Überprüfen von AWS Data Exchange auf unautirisierte Dataset-Freigaben
    d. Identifizieren von unerwarteten Cross-Region-Replikationen
3. **S3-Objektlevel-Sicherheit:**
    a. Implementieren von Object Lock für kritische Daten
    b. Überprüfen und Durchsetzen von S3 Server-seitiger Verschlüsselung
    c. Bereitstellen von IAM-Richtlinien mit S3-Condition-Keys für Zugriffseinschränkung
    d. Implementieren von S3 Intelligent Tiering für selten genutzte Daten zur Risikominimierung

Wiederherstellung

1. **S3-Sicherheitsoptimierung:**
    a. Implementieren von S3 Object Tagging für verbesserte Zugangskontrolle
    b. Konfigurieren von S3 Lifecycle-Richtlinien für sichere Datenverwaltung
    c. Einrichten von S3 Inventory zur regelmäßigen Objektüberprüfung
    d. Implementieren von S3 Batch Operations für massenhafte Sicherheitspatches
2. **AWS Macie Integration:**

a. Aktivieren von Amazon Macie für automatische Erkennung sensibler Daten
b. Konfigurieren von Macie-Klassifikationsjobs für alle S3-Buckets
c. Erstellen von Macie-Filtern für PII und sensible Daten
d. Integration von Macie-Erkennungen mit Security Hub für zentralisierte Überwachung