Azure-Spezifisches Playbook für Sicherheitsvorfälle

1. Ransomware-Vorfall in Azure-Umgebung

Sofortmaßnahmen

1. **Isolation betroffener Azure-Ressourcen:**
    a. Anwenden von Network Security Groups (NSGs) mit Deny-All-Regeln
    b. Erstellen und Anwenden von Application Security Groups (ASGs) für granulare Kontrolle
    c. Trennen von Virtual Networks durch Deaktivieren von VNet-Peering
    d. Nutzen von Azure Firewall für fortgeschrittene Filterung auf Protokollebene
2. **Azure-spezifische Beweissicherung:**
    a. Erstellen von Snapshots aller betroffenen verwalteten Datenträger
    b. Aktivieren von Azure Diagnostic Settings für umfassende Logging
    c. Sichern von Azure Activity Logs in einem separaten Storage Account
    d. Verwenden von Azure Disk Encryption für die Sicherung neuer Datenträger
3. **Azure Identity-Sicherung:**
    a. Durchsetzen sofortigen Passwort-Resets für potentiell kompromittierte Benutzer
    b. Deaktivieren verdächtiger Service Principals und App Registrations
    c. Auditieren und Einschränken von Azure AD Privileged Identities
    d. Überprüfen und Entfernen von ungewöhnlichen Conditional Access Policies
4. **Azure-spezifische Überwachung aktivieren:**
    a. Aktivieren von Microsoft Defender for Cloud für alle Abonnements
    b. Konfigurieren von Azure Monitor-Warnungen für verdächtige Aktivitäten
    c. Implementieren von Azure Sentinel für fortgeschrittene Bedrohungserkennung
    d. Aktivieren von Network Watcher für tiefgreifende Netzwerkdiagnostik

Wiederherstellung

1. **Clean VM-Erstellung:**
    a. Bereitstellen neuer VMs aus verifizierten Azure Marketplace Images
    b. Wiederherstellen von Daten aus Azure Backup oder Azure Site Recovery
    c. Verwenden von Azure Resource Manager (ARM) Templates für sichere Bereitstellung
    d. Implementieren von Azure Bastion für sichere VM-Verbindungen
2. **Azure-Konfigurationsüberprüfung:**
    a. Nutzen von Azure Security Center Secure Score für Sicherheitsbewertung
    b. Überprüfen der Azure Storage Account-Konfigurationen auf unberechtigte Zugänge
    c. Scannen von Azure Container Registry Images mit Defender für Schwachstellen
    d. Überprüfen aller Azure Front Door und Application Gateway Konfigurationen
3. **Azure DDoS-Schutz:**
    a. Aktivieren von Azure DDoS Protection Standard
    b. Konfigurieren von Azure WAF-Richtlinien basierend auf dem Vorfall
    c. Implementieren von Rate-Limiting mit API Management
    d. Konfigurieren von geo-basierten Zugriffskontrollen mit Azure Front Door

2. Unbefugter Zugriff auf Azure-Konto

Sofortmaßnahmen

1. **Azure AD-Zugangsschutz:**
    a. Sofortiges Ändern des Administrator-Passworts
    b. Aktivieren von MFA für alle privilegierten Azure AD-Rollen
    c. Implementieren von Azure AD Privileged Identity Management (PIM)
    d. Überprüfen und Entfernen unbekannter oder verdächtiger Enterprise Applications
2. **Azure-Ressourcen-Überprüfung:**

   a. Identifizieren ungewöhnlicher virtueller Maschinen mit unbekannten Images
   b. Überprüfen aller Azure Functions auf nicht autorisierte Änderungen
   c. Überprüfen der Resource Manager-Deployments auf ungewöhnliche Aktivitäten
   d. Scannen aller Storage Accounts auf öffentliche Zugänglichkeit oder Policy-Änderungen
3. **Azure Subscription-Maßnahmen:**
   a. Implementieren von Azure Management Groups und Azure Policy für Beschränkungen
   b. Überprüfen der Azure Subscription Activity Logs auf ungewöhnliche Aktivitäten
   c. Temporäres Einschränken der Azure Resource Provider-Registrierungen
   d. Überprüfen aller RBAC-Zuweisungen und Azure AD B2B-Gastkonten
4. **Azure-spezifische Logging-Verstärkung:**
   a. Sicherstellen, dass Azure Activity Log für alle Ressourcen aktiviert ist
   b. Aktivieren von Storage Analytics Logging für alle Storage Accounts
   c. Einrichten von NSG Flow Logs für alle Virtual Networks
   d. Konfigurieren von Azure Diagnostics für detaillierte Ressourcenprotokolle

Wiederherstellung

1. **Azure AD-Sicherheitsposture:**
   a. Implementieren von Azure AD Identity Protection für risikobased Policies
   b. Durchsetzen von Azure AD Conditional Access Policies
   c. Konfigurieren von Azure AD Password Protection gegen schwache Passwörter
   d. Implementieren von Azure AD PIM für Just-in-Time Administrative Zugänge
2. **Azure-spezifische Sicherheitsüberprüfung:**
   a. Durchführen eines Azure Well-Architected Reviews mit Fokus auf Sicherheit
   b. Überprüfen der Azure Key Vault-Zugriffe und -Berechtigungen
   c. Scannen aller Container Registry Images mit Security Center Scans

d. Überprüfen der API Management Gateway-Konfigurationen

3. Datenexfiltration aus Azure Storage

Sofortmaßnahmen

1. **Azure Storage-spezifische Sicherung:**
    a. Sofortige Überprüfung und Korrektur aller Storage Account Shared Access Signatures (SAS)
    b. Rotieren der Storage Account-Schlüssel
    c. Identifizieren und Entfernen aller unautorisierten CORS-Konfigurationen
    d. Aktivieren von Soft Delete und versioning für Container zur Schadensermittlung
2. **Azure-Datenverkehr-Analyse:**
    a. Überprüfen von Storage Analytics Logs für ungewöhnliche Zugriffsoperationen
    b. Analysieren von NSG Flow Logs für große ausgehende Datenübertragungen
    c. Überprüfen von Event Grid Subscriptions auf unautirisierte Datenweiterleitung
    d. Identifizieren von unerwarteten Geo-Replikationen oder Datenübertragungen
3. **Azure Storage-Zugriffssteuerung:**
    a. Implementieren des Azure AD Authentifizierung für Storage
    b. Überprüfen und Durchsetzen von Azure Storage-Verschlüsselung
    c. Konfigurieren von Azure RBAC mit Storage-spezifischen Rollen
    d. Implementieren von Azure Policy für Storage-Compliance-Durchsetzung

Wiederherstellung

1. **Azure Storage-Sicherheitsoptimierung:**
    a. Implementieren von Immutable Storage für kritische Daten
    b. Konfigurieren von Lifecycle Management für sichere Datenverwaltung
    c. Implementieren von Private Endpoints für Storage Accounts
    d. Verwenden von Azure Storage Firewalls für netzwerkbasierte Zugriffssteuerung
2. **Azure Purview Integration:**

a. Aktivieren von Azure Purview für automatische Datenerkennung und -klassifizierung
b. Konfigurieren von Purview-Scans für alle Storage Accounts
c. Erstellen von Purview-Klassifikationen für PII und sensible Daten
d. Integration von Purview mit Defender for Cloud für verbesserte Sicherheitseinblicke