Playbook: Ransomware-Reaktion in Cloud-Umgebungen

Übersicht

Dieses Playbook bietet strukturierte Anweisungen zur Reaktion auf Ransomware-Vorfälle in Cloud-Umgebungen. Es berücksichtigt die Besonderheiten von AWS, Azure und Google Cloud sowie unterschiedliche Cloud-Service-Modelle (IaaS, PaaS, SaaS).

Vorfallsphase: Identifikation

Anzeichen eines Ransomware-Angriffs

- Verschlüsselte Dateien mit ungewöhnlichen Dateiendungen
- Lösegeldforderungen in Text- oder HTML-Dateien
- Ungewöhnliche Verschlüsselungsaktivitäten (hohe CPU-/Speichernutzung)
- Verdächtige API-Aufrufe in den Cloud-Protokollen
- Massenhafte Dateisystemänderungen
- Plötzliche Erhöhung ausgehender Netzwerkaktivität

Erste Schritte

1. **Vorfall dokumentieren und ID zuweisen**
    a. Zeitpunkt der Entdeckung festhalten
    b. Betroffene Cloud-Ressourcen identifizieren
2. **Incident Response Team aktivieren**
    a. Über vordefinierten Kommunikationskanal (nicht über potenziell kompromittierte Systeme)
    b. Rollen und Verantwortlichkeiten zuweisen
3. **Cloud-spezifische Logs sichern**
    a. AWS: CloudTrail, VPC Flow Logs, S3 Access Logs
    b. Azure: Azure Activity Logs, Network Security Group Flow Logs
    c. Google Cloud: Cloud Audit Logs, VPC Flow Logs
4. **Ransomware-Variante identifizieren**
    a. Dateiendungen der verschlüsselten Dateien prüfen
    b. Lösegeldforderung analysieren
    c. Wenn möglich, Beispieldateien für forensische Analyse sichern

Vorfallsphase: Eindämmung

Sofortmaßnahmen

1. **Isolation der betroffenen Ressourcen**
    a. **AWS**:
        i. Netzwerkzugriff einschränken: Aktualisieren von Security Groups, um ein- und ausgehenden Verkehr zu blockieren
        ii. Betroffene EC2-Instances von Autoscaling-Gruppen trennen
        iii. VPC-Endpunkte für kompromittierte Dienste deaktivieren
    b. **Azure**:
        i. Netzwerkzugriff einschränken: Network Security Groups (NSG) aktualisieren
        ii. Betroffene VMs mit Network-Isolation versehen
        iii. Notfall-Firewall-Regeln implementieren
    c. **Google Cloud**:
        i. VPC Firewall-Regeln aktualisieren, um Verkehr zu isolieren
        ii. Betroffene Instanzen von Instance Groups entfernen
        iii. Identity-Aware Proxy (IAP) für kritische Ressourcen aktivieren
2. **API-Zugriffseinschränkungen implementieren**
    a. Temporäre restriktive IAM-Richtlinien anwenden
    b. Service-Principals/Managed Identities mit verdächtigen Aktivitäten deaktivieren
    c. Cloud-Zugriffsschlüssel rotieren
3. **Speichern von Snapshots/Backups**
    a. Erstellen von Snapshots für forensische Analyse (vor Wiederherstellung)
    b. AWS: EBS-Snapshots, RDS-Snapshots, AMIs
    c. Azure: Disk-Snapshots, SQL-Database-Backups
    d. Google Cloud: Persistent Disk-Snapshots, Cloud SQL-Backups

Ausbreitungsprävention

1. **Laterale Bewegung blockieren**
    a. Temporäre Segmentierung von Cloud-Netzwerken
    b. Überprüfung und Einschränkung von IAM-Vertrauensbeziehungen
    c. Cloud-übergreifende Verbindungen (Direct Connect, Express Route) überprüfen
2. **Privilegierte Zugänge sichern**
    a. Admin-Zugänge zu Cloud-Diensten temporär einschränken
    b. MFA für alle verbleibenden administrativen Zugänge erzwingen

c. Break-Glass-Konten überprüfen und absichern

3. **Backup-Systeme schützen**
    a. Zugriff auf Backup-Speicher isolieren
    b. Immutable Backups aktivieren, falls verfügbar
    c. Air-Gapped Backups überprüfen

Vorfallsphase: Beseitigung

Identifikation des Ursprungs

1. **Eintrittspunkt ermitteln**
    a. Cloud-Protokolle auf verdächtige Authentifizierungen überprüfen
    b. API-Aufrufe vor dem Vorfall analysieren
    c. Kompromittierte Anmeldeinformationen identifizieren
2. **Malware-Analyse**
    a. Ausführbare Dateien oder Skripte identifizieren, die für den Angriff verantwortlich sind
    b. Temporäre Cloud-Sandbox für sichere Analyse nutzen
3. **Verbreitungswege identifizieren**
    a. Cloud-Ressourcen-Beziehungen (z.B. IAM-Rollen, gemeinsame VPCs) dokumentieren
    b. Automatisierte Prozesse identifizieren, die zur Verbreitung beigetragen haben könnten

Bereinigung

1. **Cloud-Ressourcen-Bereinigung**
    a. **Option 1: Neubereitstellung aus gesicherten Vorlagen**
        i. Cloud Formation (AWS), ARM Templates (Azure) oder Deployment Manager (GCP) nutzen
        ii. Infrastructure-as-Code-Repositories überprüfen und aktualisieren
    b. **Option 2: Selektive Bereinigung**
        i. Nur für nicht kritische Ressourcen oder bei begrenztem Befall
        ii. Verdächtige Anwendungen und Daten entfernen
        iii. Komplette Überprüfung der Cloud-Konfiguration
2. **Zugangsdaten rotieren**
    a. Alle API-Schlüssel, Dienstkonten und Geheimnisse rotieren
    b. IAM-Berechtigungen überprüfen und nach dem Prinzip der geringsten Berechtigung anpassen
    c. Passwörter für alle Cloud-Administratorkonten ändern
3. **Integration mit vorhandenen Sicherheitstools**

a. Cloud Security Posture Management (CSPM) zur Überprüfung von Fehlkonfigurationen
b. Cloud-native Anti-Malware-Lösungen bereitstellen
c. Erweiterte Erkennungsmechanismen aktualisieren

Vorfallsphase: Wiederherstellung

Wiederherstellungsstrategie

1. **Prioritäten festlegen**
    a. Kritische Geschäftsfunktionen identifizieren
    b. Wiederherstellungsreihenfolge basierend auf Abhängigkeiten definieren
    c. Wiederherstellungszeitpunkte für verschiedene Dienste festlegen
2. **Daten wiederherstellen**
    a. Datenintegrität von Backups validieren
    b. Backups stufenweise wiederherstellen (nach Überprüfung auf Schadsoftware)
    c. Bei verschlüsselten Daten ohne Backup: Decryption-Tools prüfen (No More Ransom)
3. **Umgebung wiederherstellen**
    a. Infrastructure-as-Code-Bereitstellung aus validierten Vorlagen
    b. Updates und Patches für alle wiederhergestellten Systeme anwenden
    c. Wiederhergestellte Systeme vor Produktivschaltung isoliert testen

Validierung

1. **Sicherheitsvalidierung**
    a. Vollständige Sicherheitsüberprüfung der wiederhergestellten Umgebung
    b. Vulnerability Scanning und Penetrationstests durchführen
    c. Cloud Security Posture Assessment durchführen
2. **Funktionsvalidierung**
    a. Anwendungs- und Dienstfunktionalität überprüfen
    b. Performance-Tests durchführen
    c. Datenkonsistenz verifizieren
3. **Überwachung verstärken**
    a. Erweiterte Überwachungsmaßnahmen implementieren
    b. Zusätzliche Alarme für ähnliche Aktivitäten konfigurieren
    c. Temporäre Überwachungsperiode für wiederhergestellte Systeme einrichten

Vorfallsphase: Nachbereitung

Dokumentation und Berichterstattung

1. **Vollständige Dokumentation des Vorfalls**
    a. Genaue Timeline mit allen ergriffenen Maßnahmen
    b. Betroffene Assets und Wiederherstellungszeiten
    c. Effektivität der Reaktionsmaßnahmen
2. **Berichterstattung**
    a. Management-Bericht mit geschäftlichen Auswirkungen
    b. Technischer Bericht für Sicherheitsteams
    c. Compliance-Bericht für regulatorische Anforderungen
    d. Meldepflichten gemäß DSGVO prüfen

Lessons Learned

1. **Nachbesprechung durchführen**
    a. Treffen mit allen beteiligten Teams
    b. Analyse der Reaktionseffektivität
    c. Identifikation von Prozess- und Technologielücken
2. **Empfehlungen für Verbesserungen**
    a. Technische Maßnahmen (z.B. verbesserte Segmentierung, bessere Logging-Strategien)
    b. Prozessverbesserungen (z.B. schnellere Eskalationswege)
    c. Schulungsbedarf identifizieren
3. **Aktionsplan entwickeln**
    a. Konkrete Maßnahmen mit Verantwortlichen und Zeitplan
    b. Updates für das CIRP-Dashboard und Playbooks
    c. Verbesserung der Cloud-Sicherheitsarchitektur

Cloud-spezifische Ressourcen

AWS-spezifische Ressourcen

- AWS Security Incident Response Guide
- AWS Security Hub für zentralisierte Sicherheitsüberwachung
- AWS GuardDuty für Bedrohungserkennung

Azure-spezifische Ressourcen

- Azure Security Center Incident Response
- Azure Sentinel für SIEM und SOAR-Fähigkeiten
- Azure Security Center für Sicherheitsempfehlungen

Google Cloud-spezifische Ressourcen

- Google Cloud Security Response
- Security Command Center für zentrale Sicherheitsüberwachung
- Event Threat Detection für erweiterte Bedrohungserkennung

Anhänge

Kontaktliste für Ransomware-Vorfälle

- Interne Kontakte: Sicherheitsteam, Rechtsabteilung, Kommunikation
- Externe Kontakte: Cloud-Provider-Support, Cybersicherheitsexperten, Strafverfolgungsbehörden

Checkliste für Ransomware-Reaktion

- [ ] Vorfall identifiziert und dokumentiert
- [ ] IR-Team aktiviert
- [ ] Betroffene Systeme isoliert
- [ ] Snapshots für Forensik erstellt
- [ ] Ursprung identifiziert
- [ ] Bereinigungsstrategie festgelegt
- [ ] Systeme wiederhergestellt
- [ ] Validierung durchgeführt
- [ ] Nachbereitung und Dokumentation abgeschlossen

Rechtliche Überlegungen

- Meldepflichten gemäß DSGVO, BSIG, etc.
- Dokumentationsanforderungen für Versicherungszwecke
- Kommunikation mit Strafverfolgungsbehörden