Playbook: Phishing-Kampagne in Cloud-Umgebungen

Übersicht

Dieses Playbook bietet einen strukturierten Ansatz zur Erkennung, Untersuchung und Reaktion auf Phishing-Kampagnen, die auf cloudbasierte Unternehmensumgebungen abzielen. Es umfasst Maßnahmen zur Bewältigung von Vorfällen, bei denen Angreifer versuchen, über Phishing-Angriffe Zugang zu Cloud-Ressourcen zu erlangen.

Anwendungsbereich

- Alle cloudbasierten Unternehmensressourcen (AWS, Azure, GCP, etc.)
- Office 365, Google Workspace und andere Cloud-Produktivitätsplattformen
- Cloud-basierte Identitätssysteme und Single Sign-On (SSO) Lösungen
- Von Mitarbeitern genutzte Cloud-Anwendungen

Verantwortlichkeiten

Rolle	Verantwortlichkeiten
SOC-Analyst (L1)	Initiale Phishing-Analyse, E-Mail-Triage, Benutzerbenachrichtigung
Threat Hunter (L2)	Detaillierte Analyse, IoC-Extraktion, Kampagnen-Korrelation
Cloud Security Team	Bewertung der Auswirkungen auf Cloud-Umgebungen, spezifische Gegenmaßnahmen
IT-Support/Helpdesk	Benutzerunterstützung, Passwortrücksetzung, betroffene Endgeräte
Kommunikationsteam	Mitarbeiter-Benachrichtigungen, organisationsweite Warnungen
CISO/Sicherheitsleitung	Strategische Entscheidungen, Management-Kommunikation

1. Erkennung

1.1 Phishing-Erkennungsmechanismen

- **E-Mail-Sicherheitslösungen**: SEG, Anti-Phishing-Schutz, Anhangssandboxing
- **Endpoint Detection and Response (EDR)**: Verdächtige Prozesse nach Phishing-Interaktion
- **Cloud-Sicherheitstools**: Ungewöhnliche Anmeldeversuche, Standortanomalien
- **User-Reports**: Mitarbeiter-Meldungen über verdächtige E-Mails oder Webseiten
- **Web-Proxy/CASB**: Zugriffe auf bekannte Phishing-Domains

1.2 Phishing-Indikatoren (IoAs)

- E-Mails, die sich als Cloud-Dienste ausgeben (Office 365, Google Workspace, AWS, etc.)
- Aufforderungen zur dringenden Anmeldung aufgrund angeblicher Sicherheitsprobleme
- Links zu gefälschten Anmeldeseiten für Cloud-Dienste
- Ungewöhnliche Anmeldeversuche zu Cloud-Diensten außerhalb typischer Arbeitszeiten/Standorte
- API-Anfragen von unbekannten IP-Adressen nach erfolgreicher Anmeldung
- Massenhafte Datenzugriffe oder Download-Aktivitäten
- Änderungen an E-Mail-Weiterleitungsregeln oder Postfachberechtigungen

1.3 Früherkennung und Überwachung

- Proaktives Threat Hunting nach bekannten Phishing-Kampagnen
- Überwachung von Threat Intelligence Feeds für neue Phishing-IoCs
- Brand Monitoring für Nachahmungen der Unternehmensidentität
- DNS-Monitoring für Typosquatting- und Phishing-Domains

2. Initiale Analyse und Triage

2.1 Erstbewertung (15-30 Minuten)

1. **Phishing-E-Mail oder -Link analysieren**:
    a. Header und Metadaten untersuchen
    b. Identität des vermeintlichen Absenders verifizieren
    c. Zielgerichtete vs. allgemeine Kampagne unterscheiden

    d. Schweregrad der Gefährdung einschätzen
2. **Cloud-spezifischen Kontext erfassen**:
    a. Betroffene Cloud-Dienste identifizieren
    b. Zielgruppe innerhalb der Organisation bestimmen
    c. Potenziell gefährdete Benutzerkonten identifizieren
3. **Sofortige Maßnahmen identifizieren**:
    a. Notwendigkeit zur E-Mail-Quarantäne bewerten
    b. Blockierung von URLs/Domains priorisieren
    c. Benutzerbenachrichtigungen vorbereiten

2.2 Datensammlung für Analyse

- Originale Phishing-E-Mail mit vollständigen Headern
- URLs und Website-Screenshots/Inhalte
- Extrahierte Malware oder verdächtige Anhänge
- Benutzerberichte über Interaktionen mit dem Phishing-Inhalt
- Authentifizierungslogs aus betroffenen Cloud-Diensten

2.3 Schweregrad-Klassifizierung

Schweregrad	Kriterien	Reaktionszeit
Kritisch	- Gezielte Kampagne gegen C-Level/privilegierte Nutzer - Bestätigte Anmeldedaten-Kompromittierung mit Aktivität - Aktiver Zugriff auf kritische Cloud-Ressourcen	Sofort (< 15 Min.)
Hoch	- Gezielte Kampagne gegen spezifische Abteilungen - Wahrscheinliche Anmeldedaten-Kompromittierung - Fortgeschrittene Techniken oder Zero-Day-Ausnutzung	1-2 Stunden
Mittel	- Breit angelegte Phishing-Kampagne - Einzelne bestätigte Interaktionen - Bekannte Phishing-Techniken	4-8 Stunden
Niedrig	- Standard-Spam/Phishing ohne spezifisches Targeting - Keine bestätigten Interaktionen - Durch Sicherheitskontrollen bereits blockiert	24 Stunden

3. Untersuchung

3.1 Phishing-Inhaltsanalyse

- **E-Mail-Forensik**:
  - DKIM/SPF/DMARC-Validierung durchführen
  - Ursprüngliche Absender-IP und -Infrastruktur identifizieren
  - Analysieren von E-Mail-Routing und Relay-Pfaden
  - Vergleich mit bekannten Phishing-Kampagnen
- **URL und Webseiten-Analyse**:
  - Domain-Registrierungsinformationen prüfen
  - HTTPS-Zertifikate und deren Ausstellung analysieren
  - Website-Hosting-Informationen erfassen
  - Payload und Datenerfassungsmechanismen untersuchen
- **Malware-Analyse** (falls zutreffend):
  - Statische und dynamische Analyse von Anhängen
  - Verhaltensmuster und Funktionalität bestimmen
  - Identifizierung von Command & Control-Servern

3.2 Auswirkungsanalyse

- **Betroffene Benutzer ermitteln**:
  - Empfänger der Phishing-E-Mail identifizieren
  - Benutzer mit nachgewiesener Interaktion isolieren
  - Benutzer mit verdächtigen Anmeldeaktivitäten überprüfen
- **Cloud-Service-Überprüfung**:
  - Authentifizierungsprotokolle für verdächtige Anmeldungen analysieren
  - Ungewöhnliche API-Aufrufe oder Aktivitäten identifizieren
  - MFA-Events und Authentifizierungsanomalien untersuchen
  - OAuth-Berechtigungen und App-Registrierungen überprüfen
- **Datenzugriffs-Analyse**:
  - Zugriff auf sensible Daten nach verdächtigen Anmeldungen
  - Cloud-Storage-Zugriffe und Datei-Downloads
  - E-Mail-Weiterleitungsregeln und Postfachzugriffe

3.3 Kampagnenanalyse

- Abgleich mit aktuellen Threat Intelligence zu Phishing-Kampagnen
- Organisationsübergreifende Muster erkennen (falls mehrere Empfänger)
- Attribution an bekannte Bedrohungsakteure, falls möglich

- Bewertung der Kampagnenziele (Anmeldedaten, Datendiebstahl, Malware-Deployment)

3.4 IoC-Extraktion

- E-Mail-Absenderadressen und -Header
- Phishing-URLs und Domains
- Hosting-IP-Adressen und Infrastruktur
- Datenerfassungsmethoden und Exfiltrationsziele
- Malware-Signaturen und Verhaltensweisen
- C2-Infrastruktur und Kommunikationsmuster

4. Eindämmung

4.1 Sofortige Eindämmungsmaßnahmen

- **E-Mail-Containment**:
  - Quarantäne ähnlicher E-Mails im gesamten Unternehmen
  - Entfernung der identifizierten Phishing-E-Mail aus allen Postfächern
  - Blockierung der Absender-Domain und -IPs in E-Mail-Sicherheitslösungen
- **Web-Schutzmaßnahmen**:
  - Blockierung von Phishing-URLs und -Domains im Web-Proxy/Firewall
  - DNS-Sinkholing für identifizierte bösartige Domains
  - CASB-Richtlinien zur Blockierung verdächtiger Cloud-App-Zugriffe
- **Cloud-Zugriffssicherung**:
  - Password-Reset für nachweislich betroffene Benutzer erzwingen
  - Temporäre Zugangsbeschränkungen für verdächtige Konten
  - Implementierung zusätzlicher Authentifizierungshürden

4.2 Erweiterte Eindämmungsstrategien

- **Identitätsschutz**:
  - Überprüfung und Zurücksetzung von OAuth-Tokens und Sitzungen
  - Implementierung adaptiver MFA-Herausforderungen
  - Conditional Access-Richtlinien für geografische Einschränkungen
- **Berechtigungsbeschränkungen**:
  - Temporäre Einschränkung von Admin-Berechtigungen für gefährdete Konten
  - Just-in-Time-Zugriffskontrollen für kritische Ressourcen

    - Cloud-Entitlement-Review für potenziell kompromittierte Konten
- **Workload-Schutz**:
    - Verstärkte Überwachung sensibler Cloud-Workloads
    - Runtime-Schutz für Cloud-VMs und Container aktivieren
    - Temporäre Isolation betroffener Cloud-Ressourcengruppen

4.3 Beweissicherung

- Forensische Kopien der Phishing-E-Mails und -Inhalte erstellen
- Screenshots und HTML-Quellcode von Phishing-Webseiten sichern
- Authentifizierungs- und Aktivitätslogs in unveränderliche Speicher exportieren
- Netzwerkverkehrsdaten zu relevanten Interaktionen archivieren
- Chain of Custody für alle gesammelten Beweise dokumentieren

5. Beseitigung

5.1 Sicherung kompromittierter Konten

- **Credential-Management**:
    - Zurücksetzen von Passwörtern für betroffene Benutzer
    - Widerruf und Erneuerung aller Token, API-Schlüssel und Sessions
    - Erzwingen von MFA für alle wiederhergestellten Konten
    - Überprüfung auf versteckte Wiederherstellungsmethoden
- **Berechtigungsbereinigung**:
    - Entfernung unberechtigter Zugriffe und Berechtigungen
    - Überprüfung und Löschung unbekannter OAuth-Anwendungsberechtigungen
    - Bereinigung von Rechten in verbundenen Identity-Providern

5.2 Entfernung von Angreifer-Zugängen

- **Zugangskontrolle**:
    - Identifizierung und Entfernung von Angreifer-erstellten Konten
    - Kontrolle und Bereinigung von E-Mail-Weiterleitungsregeln
    - Überprüfung und Reset von SSO-Konfigurationen
- **Cloud-Ressourcenbereinigung**:
    - Identifizierung und Beseitigung verdächtiger Cloud-Ressourcen
    - Überprüfung auf Backdoors in IAM-Richtlinien und -Rollen
    - Entfernung schädlicher Automatisierungen und Scheduler-Tasks

5.3 Bereinigungsvalidierung

- Security Scans für betroffene Cloud-Konten und -Umgebungen
- Überprüfung der E-Mail- und Postfacheinstellungen
- Forensisches Assessment der betroffenen Endgeräte
- Validierung der erfolgreichen Entfernung aller bekannten IoCs

6. Wiederherstellung

6.1 Wiederherstellung normaler Operationen

- Schrittweise Wiederherstellung des normalen Zugriffs für betroffene Benutzer
- Entfernung temporärer Zugangsbeschränkungen bei bestätigter Sicherheit
- Wiederherstellung von Anwendungsfunktionalität und Diensten
- Normalisierung erhöhter Sicherheitskontrollen nach angemessener Überwachung

6.2 Erhöhte Überwachung

- Implementierung verschärfter Monitoring-Regeln für betroffene Konten
- Erweiterte Überwachung von Cloud-API-Aktivitäten
- Besondere Aufmerksamkeit für sensible Operationen und Datenzugriffe
- Temporäre Aktivierung von Session-Recordings für risikoreiche Konten

6.3 Benutzerkommunikation und -unterstützung

- Klare Kommunikation über Status und Wiederherstellungsmaßnahmen
- Schulungsmaßnahmen für betroffene Benutzer
- Support-Hotline für weitere Phishing-Erkennungen
- Feedback-Mechanismen für Benutzer über Sicherheitsmaßnahmen

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