OXFORD COMPUTER GROUP

Der Digitale Türsteher – IDABUS gegen Cyberbedrohungen

Rike Kouba & Rüdiger Berndt

HSD IDABUS® NEXIS TD SYNNEX

Szenario 1

- Angriff auf das IAM/IDABUS mit gültigem Konto (keine bis niedrige Berechtigungen)

Angriff auf das IAM / IDABUS mit bekannten Konten

Mögliches Szenario:

- Hacker meldet sich mit gültigem Konto an IDABUS an – z.B. kompromittiertes Entra-ID Konto

Angriff auf das IAM / IDABUS mit bekannten Konten

Mögliches Erkennungsszenario:

- IDABUS Auth Log auswerten und eine höhere Anzahl an fehlerhaften Anmeldungen erkennen

Angriff auf das IAM / IDABUS mit bekannten Konten

Mögliches Szenario:

- Ein Angreifer mit einem validen IDABUS Account versucht sich selbst mehr Rechte zu geben

RB

Angriff auf das IAM / IDABUS mit bekannten Konten

Mögliches Erkennungsszenario:

- IDABUS Event Log auswerten und auf eine ungewöhnliche Anzahl von abgelehnten Anfragen prüfen

RB

Angriff auf das IAM / IDABUS mit bekannten Konten – technische Erkennung (tags:alert_auth)

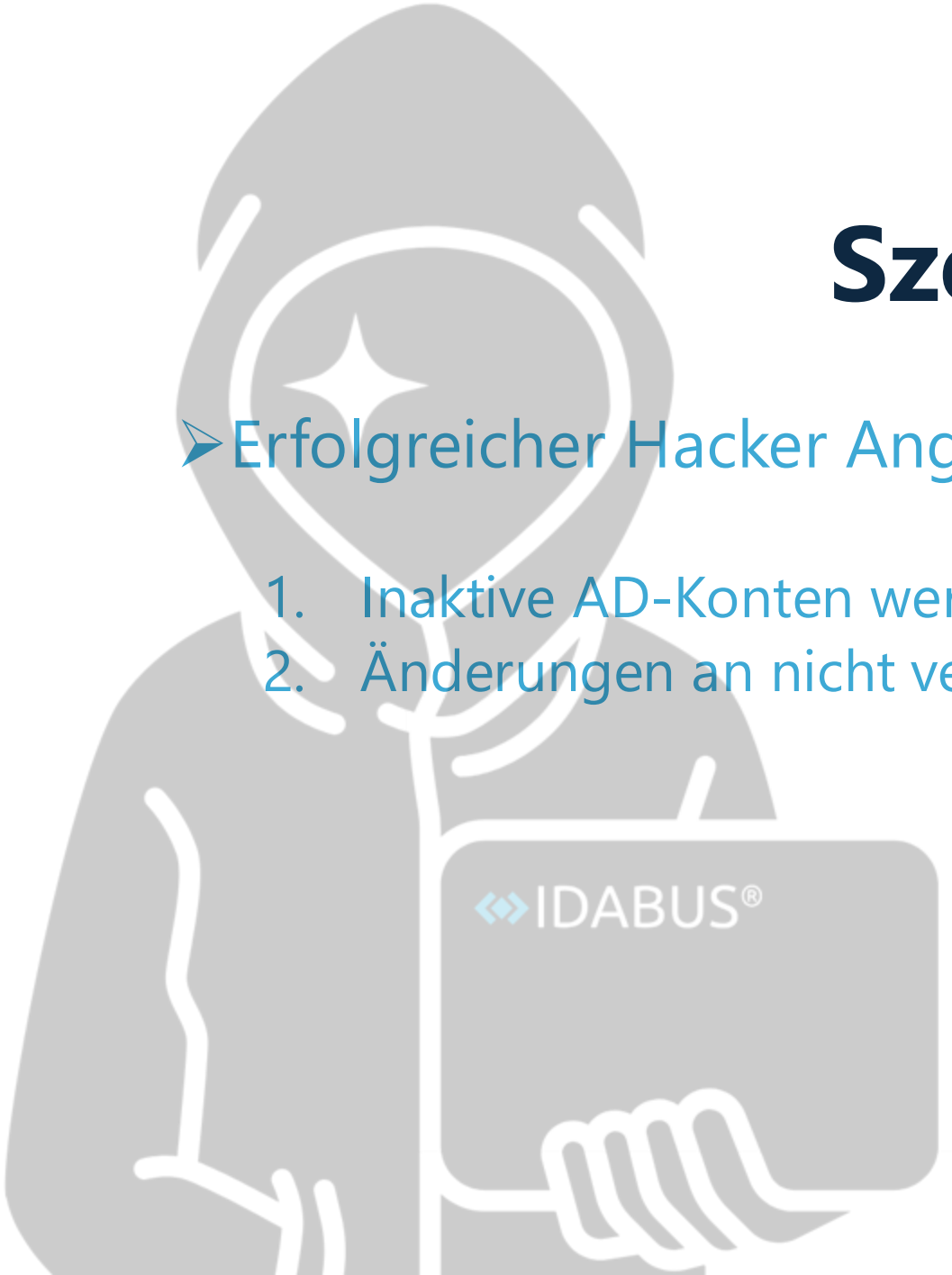
- Workflow (mit E-Mail versenden)
  - Alert: too many denied requests
- Report
  - Unauthorized Requests last 24h
- Trigger
  - Wenn mehr als 5 / Tag
- Dashboard
  - Widget mit Anzahl der fehlerhaften Requests

RB

Szenarien (2)

- Erfolgreicher Hacker Angriff auf das AD

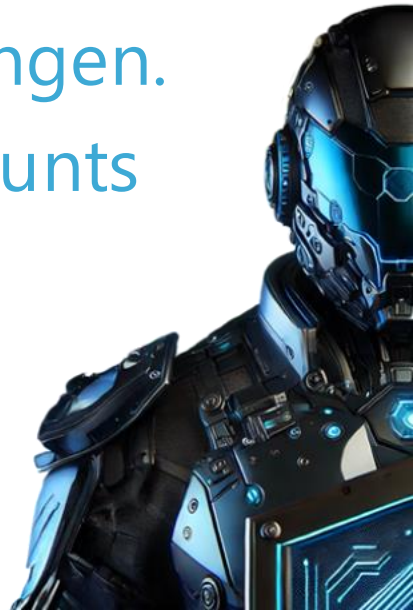
1. Inaktive AD-Konten werden plötzlich aktiv
2. Änderungen an nicht verwalteten Admin Gruppen im AD



Hacker Angriff auf AD

Mögliches Szenario:

- Ein Angriff auf das Active Directory war erfolgreich. Der Angreifer verfügt über teilweise administrative Berechtigungen.
- Der Angreifer aktiviert abgelaufene bzw. deaktivierte Accounts im AD



HE

Hacker Angriff auf AD

IDABUS
Soll-Zustand:
Benutzer = deaktiviert

Active Directory
Ist-Zustand:
Account = aktiviert

Delta erkannt!

Mismatch → Reaktion

Alarm/Workflow
z.B. SNOW Ticket oder
Auto-Aktionen

Hacker Angriff auf AD – technische Erkennung

- Sync: Attribut Flow
  - UAC über eigenes Attribut in IDABUS
- XPath Template
  - Active disabled user
- Trigger
  - detect active disabled users
- Workflow
  - notify when active disabled user is detected

Hacker Angriff auf AD

Mögliches Szenario:

- Ein Angriff auf das OnPrem AD war erfolgreich. Der Angreifer verfügt über teilweise administrative Berechtigungen.
- Der Angreifer verändert eine nicht verwaltete Gruppe direkt im AD

RB

2 - Hacker Angriff auf AD

Mögliches Erkennungsszenario:

- Das IAM System erkennt unerlaubte Änderungen im AD und liefert diese Informationen ins IDABUS
- Dort erfolgt *(mindestens)* eine Alarmierung

RB

2 - Hacker Angriff auf AD – technische Erkennung (tags:alert_groups)

- Sync: Attribut Flow
  - „Non managed“ Gruppen Mitgliedschaften fließen ins IDABUS
- Workflow
  - Alert: non manage group membership changed
- Mail Template
  - Alert: non managed Group Membership changed
- Trigger
  - SEC: trigger nonmanaged group membership

RB

Szenarien (3)

- Erfolgreicher Hacker Angriff mit administrativen Berechtigungen in IDABUS

1. Erkennung von ungewöhnlichen Änderungen an der Konfiguration
2. Adminverhalten abweichend vom Normalfall
3. Schnelle Rechte-Eskalation

1 - Hacker Angriff mit Admin Berechtigungen

Mögliches Szenario:

- Ein Angriff auf das OnPrem AD war erfolgreich. Der Angreifer verfügt über einen administrativen Account.
- Wegen eines eingestellten SSO zum Entra ID, kommt der Angreifer direkt ins IDABUS System

RB

1 - Hacker Angriff mit Admin Berechtigungen

Mögliches Erkennungsszenario:

- Erkennung von Anpassungen in der Konfiguration von IDABUS, wenn der (Angreifer) die internen Prozesse nicht kennt ☺
- Information (z.B. per Mail) an das IAM Team, wer gerade welche Konfigurationsobjekte ändert oder erstellt
  - Alternativ kann diese Änderung auch per Approval Schritt verhindert werden. Dadurch wird u.U. der Angreifer aber gewarnt!

RB

1 - Hacker Angriff mit Admin Berechtigungen (tags: alert_main)

- Workflow (mit MT)
  - „SEC - Post-Maintenance Monitoring Workflow“
  - SEC - Maintenance Mode Toggle Alert
- Trigger
  - „SEC - maintenance mode watch“
- Xpath
  - Template: „SEC all configuration resources“
- Mail Template
  - „Unexpected changes“
- Konfigurations Schalter (versteckt)
  - „ Maintenancemode“

RB

1 - Hacker Angriff mit Admin Berechtigungen

Mögliche Erweiterungen

- Die (unerlaubten) Änderungen per Approval Schritt verhindern
- Den potentiell betroffenen Account sofort sperren

RB

2 - Hacker Angriff mit Admin Berechtigungen

Mögliches Szenario:

- Ein Administrator führt unerwarteterweise Änderungen an Objekten wie Person/Gruppe/Rolle/OU durch

→ Das bedeutet eine Abweichung vom normalen Verhalten (mit Admin-Berechtigungen)

HE

2 - Hacker Angriff mit Admin Berechtigungen

Mögliches Erkennungsszenario:

- In IDABUS definieren, wer welche Änderungen an Objekttypen machen darf, z.B. Service Desk
- Regel: wenn Änderungen an Personen/Rollen/Gruppen/OUs außerhalb der genehmigten Gruppe → Alarm/Workflow

HE

2 - Hacker Angriff mit Admin Berechtigungen

Umsetzung

- XPath template – Service Desk
- Request-based Trigger
- Notification Workflow
- DEMO

HE

3 - Hacker Angriff mit Admin Berechtigungen

Mögliches Erkennungsszenario:

- Erkennung von einer nicht normalen Anzahl von (direkten) Rollenzuweisungen

RB

3 - Hacker Angriff mit Admin Berechtigungen – technische Erkennung

- Darstellung im Dashboard
  - Anzeige Anzahl RA der letzten 24h

RB

3 - Hacker Angriff mit Admin Berechtigungen

Mögliche Erweiterungen:

- Monitoring Integration (Abfrage des Count Wertes vom XPATH Template)
- Info Mail bei Schwellwertüberschreitung (im Monitoring oder IDABUS)

RB

Szenarien (4)

1. Users at Risk
2. PAM für IDABUS

1 – Users at Risk

Mögliches Szenario:

- Ein User wird zum Risiko für das System, weil er zu viele kritische Rollen/Berechtigungen besitzt oder zu viele fehlerhafte Anmeldeversuche aufweist

HE

2 – Users at Risk Umsetzung

⚠ Risikosignale
- Failed Logins
- Blocked requests
- High-Risk-Rollen

Konsolidierung

IDABUS Risk Tab
- Liste der Signale
- Rollen + Scores
- Login-Historie

Berechnung Risk Score

Risk Level: High (Gesamt-Score = 85)

HE

2 – PAM für IDABUS (tags:pam)

Mögliches Szenario:

- Ein SD Mitarbeiter benötigt kurzfristig mehr Rechte im IAM System
- Der betroffene SD Mitarbeiter ist bereits vorab als Kandidat in die PAM Gruppe aufgenommen worden
- Die PAM Gruppe hat den Scope „IDABUS IAM“

RB

Actions

- Sofortmaßnahmen
  - Konto sperren, PAM-Degradierung, Synchronisierung in Zielsysteme stoppen
- Alarmierung
  - Ticket, SIEM, E-Mail-Alert
- Analyse
  - Audit-Logs, Delta-Reports, Monitoring-Integration
- Recovery
  - Rollback, Berechtigungen neu zuweisen, Kommunikation, Backup
- Prävention
  - Policies härten, Risk Scores nutzen, intensivere PAM-Nutzung