Active Directory – Die Achillesferse Ihres Unternehmens?

Innovation & TechTalk 30.06.2022

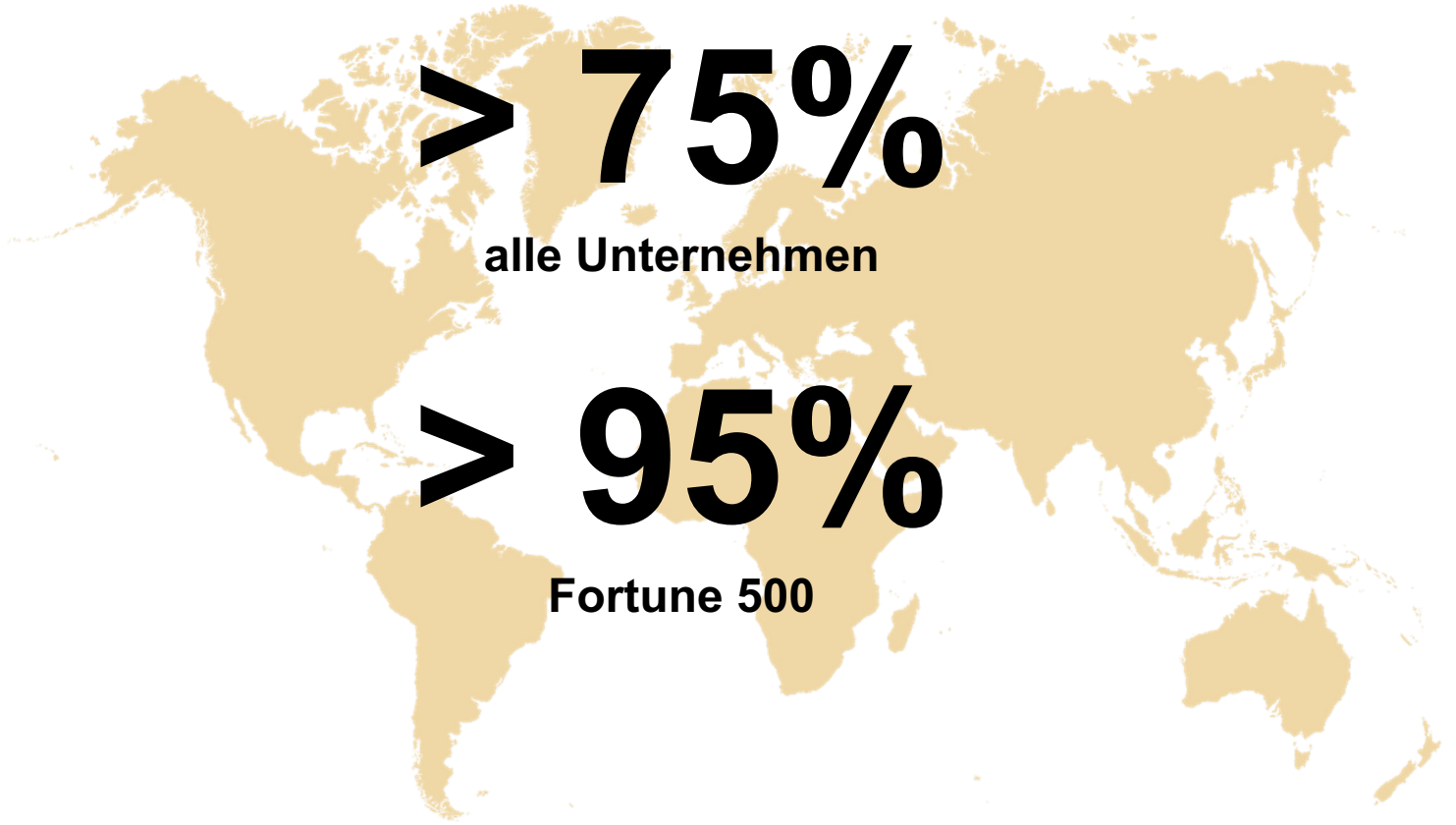
Dr. Tim Sattler (@sattlert)
CISO Jungheinrich AG

JUNGHEINRICH

Active Directory Refresher

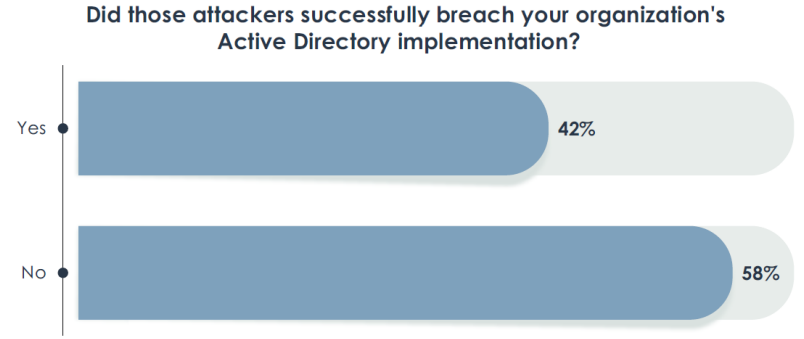
- Über 20 Jahre alt: Erstes Release mit Windows 2000
- Identitäts- und Zugriffsverwaltung für Benutzer und Computer im Netzwerk
- Repository für Benutzer, Gruppen, Computer, Dienste, Richtlinien usw.
- Verteilte, hierarchische Datenbank
- Server, die Kopien der Datenbank halten, heißen *Domänencontroller (DC)*
- AD-Objekte werden *Domains* zugeordnet
- Oberste Strukturebene und Vertrauensgrenze ist der *Forest*
- *Domain Admins* (+ „Tier 0“) besitzen höchste Rechte in der Domäne
- Richtlinien und Einstellungen können über *Group Policy Objects (GPO)* verwaltet werden
- Für die Authentisierung kommen die Protokolle *Kerberos* (bevorzugt) und *NT LAN Manager (NTLM)* zum Einsatz

Active Directory ist allgegenwärtig



Active Directory ist ein Paradies für Angreifer

- **Kompromittierung des AD = Generalschlüssel zum Unternehmensnetz**
  - durch Hybrid-Umgebungen mit Azure AD und Federation mit ADFS häufig auch darüber hinaus
- **Umfangreiches Arsenal an Tools und Methoden**
  - Mimikatz, PowerSploit, Cobalt Strike
  - Pass-the-Hash, Pass-the-Ticket, Golden Ticket, Kerberoasting, NTLM-Relay, DCSync
- **Komplex und schwierig abzusichern, „moving target“**
- **Nicht „secure by default“**
- **Zunehmende Zahl an „No-Fix“ Schwachstellen**



Quelle: EMA Research Report | The Rise of Active Directory Exploits

If an attacker has obtained *privileged access* to a *domain controller* or a *highly privileged account* in AD, […] you can *never restore* the directory to a *completely trustworthy state)**

*) Quelle: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/planning-for-compromise

Problem #1: Skills

- **Selbst in größeren Unternehmen i.d.R. nur wenige dedizierte AD-Administratoren**
- **Fokus der internen AD-Administratoren häufig auf Betriebsabläufen**
  - Personen mit AD- und Security-Expertise selten
- **Zusätzliche Herausforderung: Hybrid-Umgebungen mit Azure Active Directory (AAD)**
- **Engere Zusammenarbeit zwischen AD- und Security-Teams erforderlich**

Quelle: Unsplash.com

Problem #2: Altlasten

- **Legacy-Betriebssysteme**
  - Windows 2008 bzw. Windows 7 oder älter
- **Legacy-Protokolle**
  - z.B. SMBv1
- **Legacy-Authentisierung**
  - z.B. LM/NTLMv1, WDigest, CredSSP
- **Inaktive Benutzer- und Computerkonten**
- **Veraltete Domain Functional Level**
- **Zugangsdaten in Group Policy Preferences**

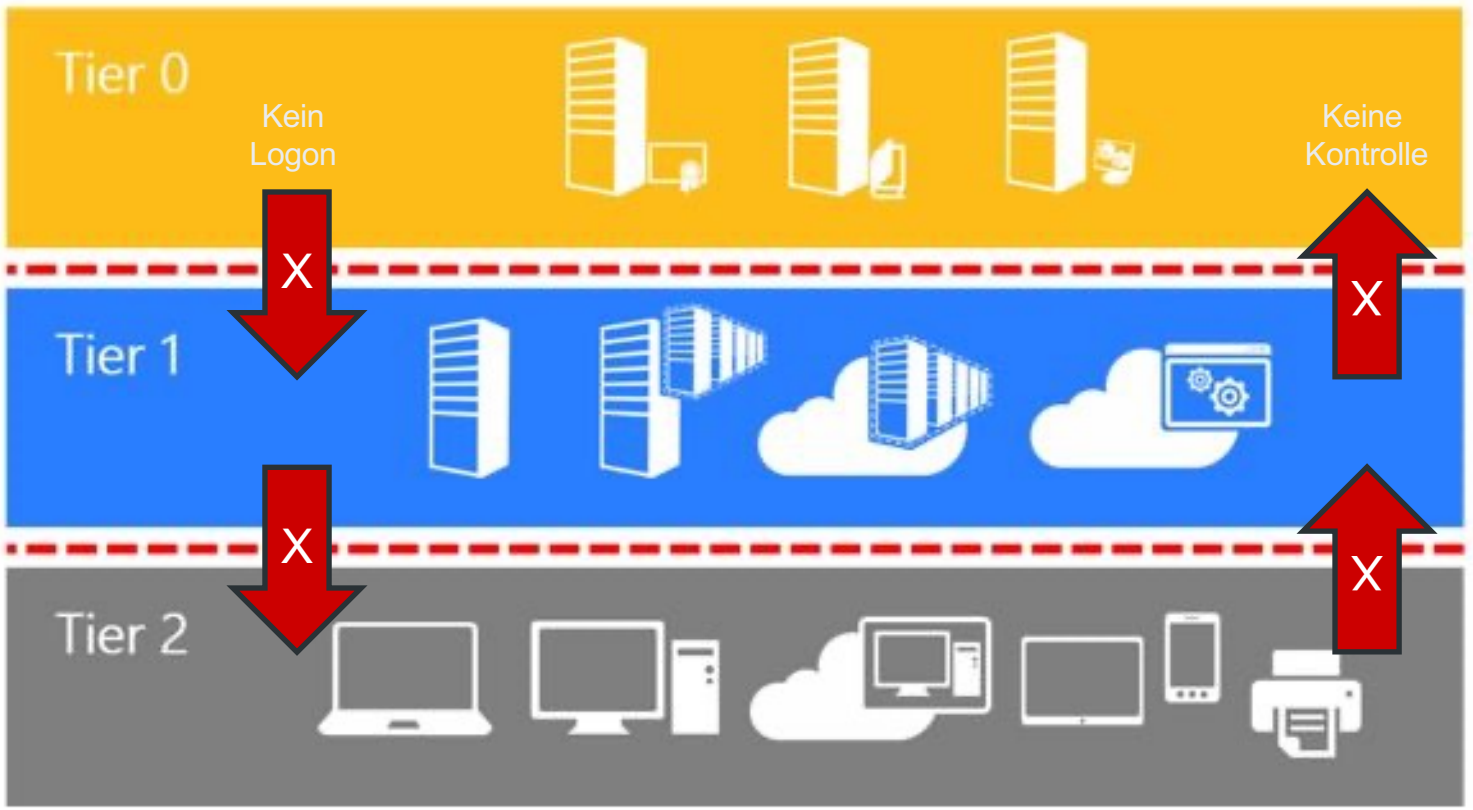
Quelle: Unsplash.com

Problem #3: Vertrauensgrenzen

- **Vertrauensgrenzen des Active Directorys ≠ Sicherheitsgrenzen des Netzwerks**
  - Viele Unternehmen betreiben nur 1-2 Forests
  - Sicherheitsgrenzen durch Segmentierung werden unterlaufen, z.B. DMZ, Backup Management
  - Hybrid-Umgebungen weichen Grenzen zusätzlich auf
- **Zu weitreichende Vertrauensstellungen**
  - Legacy-Trusts, z.B. aus M&A
  - Beidseitig, wenn einseitig reicht
  - Verzicht auf “Selective Authentication”

Quelle: Unsplash.com

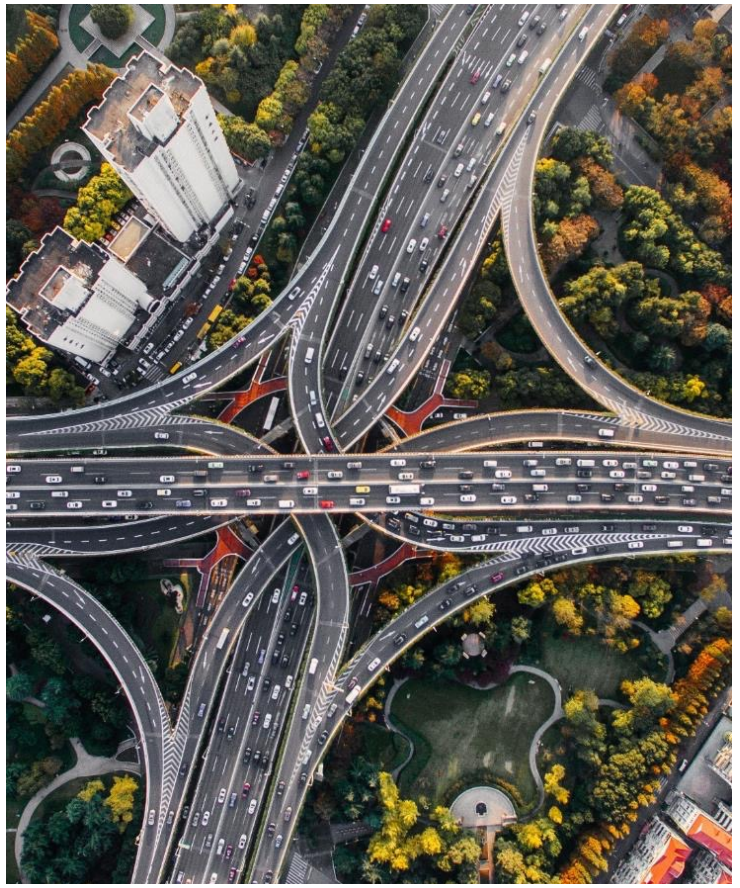
Problem #4: Trennung der Admin-Ebenen



- **Tier 0**: DCs, AD Admins & Assets mit direkter oder indirekter Kontrolle über DCs
- **Tier 1**: Server OS, Clouddienste, Business-anwendungen & Admins dieser Assets
- **Tier 2**: Clients & Client Admins

Problem #5: Trennung der Admin-Ebenen

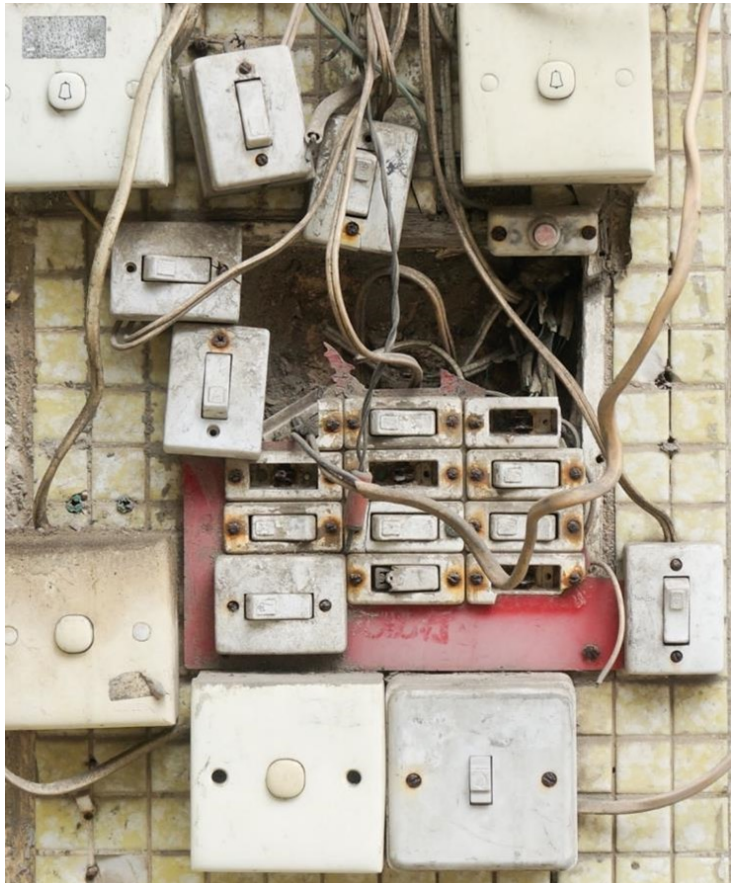
- **Trennung Tier 1/2 kaum konsequent umgesetzt**
- **Abgrenzung 0 in der Praxis schwierig**
  - Mehr als nur Domain Admins, z.B.
    - Account Operators, Server Operators, Backup Operators, DnsAdmins (wenn DNS auf DC)
    - Hypervisor-Administratoren
    - Exchange Server (in Standardkonfiguration)
    - Third-Party Software auf Domänencontroller
    - Berechtigungen auf Gruppenrichtlinien
    - Admin-Workstations
    - Mehrfachverwendung von Passwörtern
    - „Versteckte“ Berechtigungen



Quelle: Unsplash.com

Problem #6: Überprivilegierte Konten

- **Zu viele Domain Admins**
- **Servicekonten**
  - Häufig überprivilegiert
  - Zu schwache Passwörter
  - Kein Passwortablauf
- **Nutzen von Standardgruppen**
  - z.B. Service Desk in Account Operators
- **Undokumentierte oder uneingeschränkte Delegierungen**



Quelle: Unsplash.com

Problem #7: Hybrid-Umgebungen

- **Azure Active Directory (AAD) und AD sind grundverschieden, aber:**
- **Hybride Nutzung ermöglicht Sprung von Cloud zu On-prem und umgekehrt**
  - Azure Subscriptions mit Systemen im lokalen AD
  - „Hybrid Join“ von Endgeräten
  - Synchronisierung von Anmeldedaten
- **Azure AD Connect Server ist Tier 0**

Quelle: Unsplash.com

22 Quick Wins für mehr Sicherheit (1)

1. Anzahl der **Domain Admins und Global Admins** einschränken
2. **Servicekonten** aus Domain Admins usw. entfernen
3. Verwendung von privilegierten **Built-in-Gruppen** wie Account Operators vermeiden
4. Konten mit **uneingeschränkter Delegierung** reduzieren
5. Konten, die **Systeme zur Domäne hinzufügen** dürfen, einschränken
6. "**Pre-Windows 2000 Compatible Access**" einschränken
7. **Nicht benötigte Software und Dienste** auf DCs entfernen bzw. abschalten
8. **Print-Spooler-Dienst** auf allen DCs deaktivieren (*PrintNightmare*)
9. **Passwortlänge** auf mind. 12 Zeichen erhöhen
10. Für privilegierte Konten "**Fine-Grained Password Policies**" nutzen
11. Für hoch privilegierte Konten „Account is sensitive and cannot be delegated" konfigurieren und diese der Gruppe „**Protected Users**" hinzufügen
12. **OS und Patchstand** von DCs immer aktuell halten

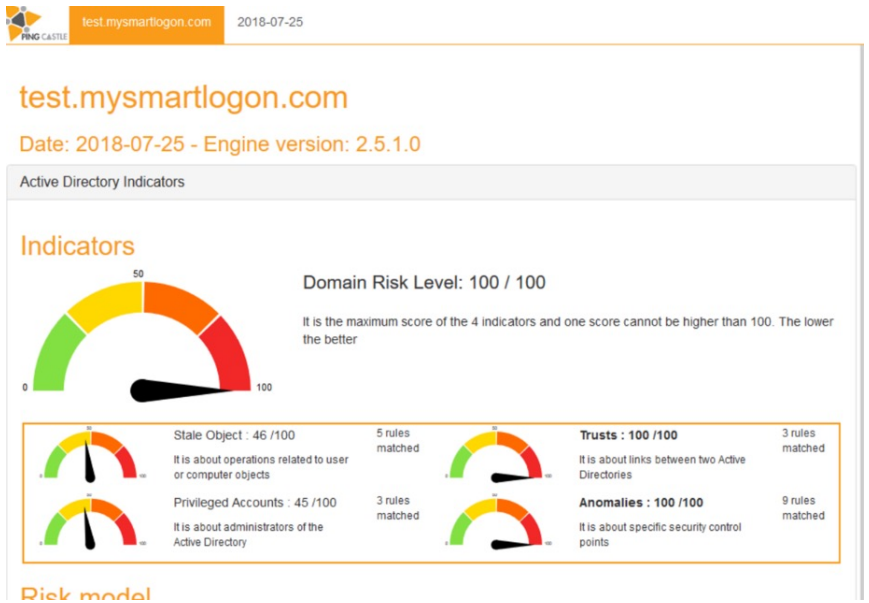
22 Quick Wins für mehr Sicherheit (2)

13. Wenn möglich, **Group Managed Service Accounts** (gMSA) nutzen
14. **Anmeldung von Domain Admins** usw. an Clients per GPO verhindern
15. **Anmeldung des lokalen Administrators** über das Netzwerk oder RDP per GPO verhindern
16. **Unterschiedliche Passwörter** für den lokalen Administrator per Local Administrator Password Solution (LAPS) o.ä. auf allen Systemen erzwingen
17. **Schwache Passwörter** per AAD Password Protection oder alt. Passwort Filter verhindern
18. Kerberos **Service Principal Name** (SPN) von allen Nicht-Servicekonten entfernen (*Kerberoasting*)
19. Passwortlänge für **Servicekonten mit SPN** auf 25 Zeichen erhöhen (*Kerberoasting*)
20. **Nicht benötige Protokolle** wie SMBv1, LLMNR oder WPAD deaktivieren
21. **MFA für AAD-Konten** aktivieren
22. Unnötige **laterale Kommunikation** über TCP-Ports 135 (RPC/WMI), 445 (SMB) und 3389 (RDP) einschränken

Nützliche Tools: Ping Castle

www.pingcastle.com

- AD Health Check: Identifiziert häufigste Mängel und Schwachstellen
- Entwickelt von Vincent Le Toux
  (Head of VINCI-CERT, Koautor Mimikatz)
- Kostenlose Nutzung für Anwenderunternehmen
  (sobald Umsatz generiert wird, Lizenz erforderlich)



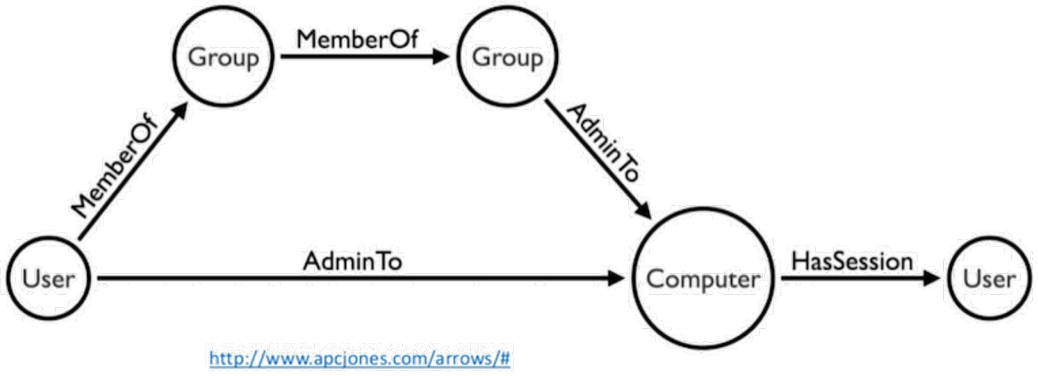
Nützliche Tools: BloodHound

github.com/BloodHoundAD

Full Report Details

2020-12-28

Title	Count	Further Details
Domain Users	8	Details
Domain Controllers	1	Details
Kerberoastable Users	2	Details
RDPable Servers	0	Details
Unconstrained Delegation Computers with SPN	1	Details
Admin Groups	9	Details
RDPable Groups	0	Details
RDPable Groups Count	0	Details
LocalAdminGroups	4	Details
LocalAdminGroupsCount	2	Details
LocalAdminUsers	6	Details
LocalAdminUsers	5	Details
Users Sessions	2	Details
Users Sessions Count	2	Details



"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."
– John Lambert, Microsoft

- Visualisiert Beziehungen innerhalb des AD in Form von Graphen
- Abfragesprache ermöglicht Suchen wie „Find Shortest Path to Domain Admins"
- Entwickelt von Will „harmj0y" Schroeder, Andy „wald0" Robbins et al.
- Kostenpflichtige Enterprise-Variante von SpecterOps
- Erweiterung „PlumHound" erzeugt gut auswertbare Berichte für Verteidigerseite: github.com/PlumHound

Weiterführende Informationen

- Best Practices for Securing Active Directory: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- Security Rapid Modernization Plan (RAMP): https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan
- AD Security Assessment Checklist (CERT-FR): https://www.cert.ssi.gouv.fr/uploads/guide-ad.html
- Sean Metcalf's Blog: https://adsecurity.org/
- Attacking Active Directory – 0 to 0.9: https://zer1t0.gitlab.io/posts/attacking_ad/
- The DFIR Report: https://thedfirreport.com/
- AD ACL Scanner: https://github.com/canix1/ADACLScanner


JUNGHEINRICH