AD-Sicherheit

Sicherheit des Active Directory (AD)

AD – der Pförtner unseres IT-Netzwerks

Der Active Directory Verzeichnisdienst, dessen Kernkomponente auch als Active Directory Domain Services bezeichnet wird, ist eine der meistgenutzten Technologien zur Administration von Gruppen und Benutzern in Windows-Netzwerken. Als das zentrale Verwaltungstool für Windows-Domain-Netzwerke wird es zur Authentifizierung und Autorisierung sämtlicher User und Rechner in Unternehmen eingesetzt. Active Directory in der Cloud angebundenen Variante Microsoft Entra ID (Azure AD) bildet einen Authentifizierungsmechanismus für Cloud- und auch on prem Umgebungen und ist damit ein elementarer Bestandteil moderner Infrastrukturen. Da das AD eine außerordentlich wichtige Rolle in der IT-Infrastruktur spielt, wird es zu einem attraktiven Ziel für Bedrohungsakteure.
Sobald Angreifer ins Active Directory eines Unternehmens eingedrungen sind, können sie von dort aus Malware verteilen, neue Benutzerkonten mit Administratorrechten erstellen, dem Netzwerk neue Rechner hinzuzufügen, Backups löschen und Server verschlüsseln. Sie sind in der Lage neue Clients zur Domain hinzuzufügen, Ransomware im gesamten Netzwerk bereitzustellen, sensible Systeme zu kompromittieren, sensible Daten zu entwenden und vieles mehr.

Ihre Active Directory Sicherheit sollte daher an erster Stelle stehen!

Cybersecurity-Zahlen 2025 (Deutschland):

- **Ransomware-Angriffe:** Im 1. Halbjahr 2025 machten Ransomware-Angriffe rund 60 % des Wertes großer Cyber-Schadensfälle aus.
- **Wöchentliche Angriffe:** Im 2. Quartal 2025 wurden wöchentlich 1.286 Cyberangriffe auf deutsche Unternehmen registriert.
- **Wirtschaftlicher Schaden:** Laut einer Studie des Digitalverbands Bitkom belief sich der durch Cyberangriffe verursachte Schaden in Deutschland im Jahr 2024 auf 267 Milliarden Euro, was einer Steigerung von 29 % im Vergleich zum Vorjahr entspricht.
- **Zielplattformen:** Windows bleibt das Hauptziel von Cyberangriffen. Im Jahr 2023 wurden durchschnittlich 411.000 schädliche Dateien pro Tag entdeckt, wobei ein erheblicher Anteil auf Windows-Geräte abzielte.

Die gefährlichsten Bedrohungen für die Cybersicherheit haben sich verändert. Noch vor Jahren waren die Haupteinfallstore schwache Webseiten und Portsecurity, heute sind die User und ihre Postfächer die Hauptschwachstellen. Bedrohungen sind:

- Ransomware / Malware
- Phishing und Social Engineering
- Veraltete Software und mangelndes Patchmanagement

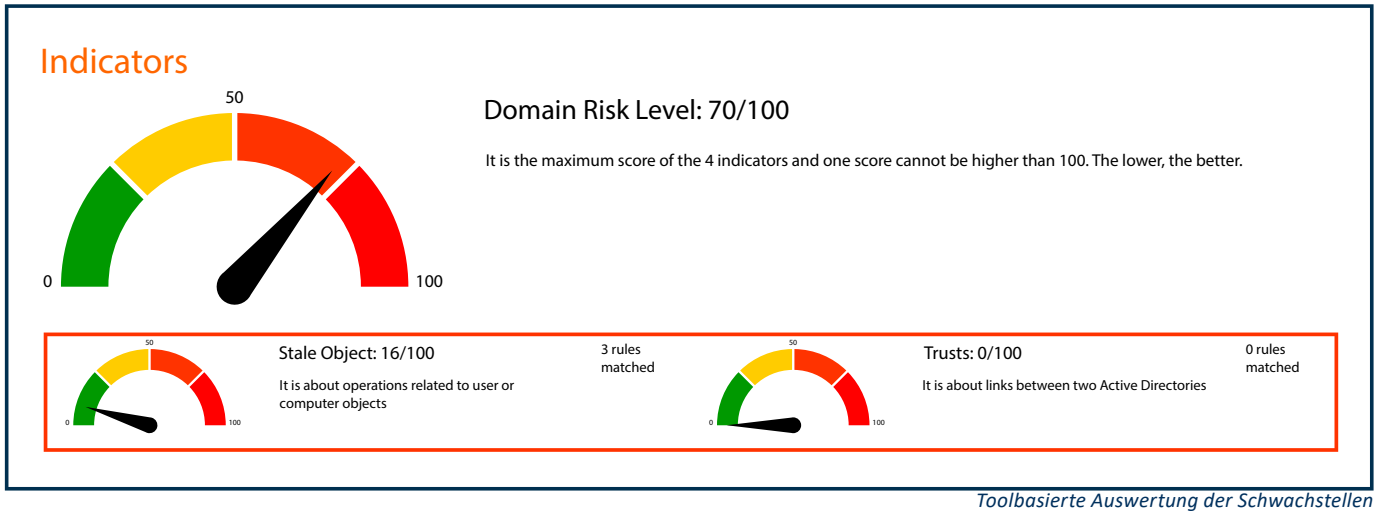
Wo befinden sich die Sicherheitslücken in Ihrem AD? Ein Check lohnt sich.

Wie sicher ist Ihr Active Directory?

Die beste Strategie besteht darin, das Active Directory ständig zu überprüfen und sich Transparenz über die Reichweite von Benutzerrechten und mangelnde Sicherheitsabgrenzungen auf allen Ebenen zu verschaffen. Identifizieren Sie Sicherheitslücken, priorisieren Sie Schutzmaßnahmen und investieren Sie in umfassende Lösungen, die Ihr Active Directory sicher machen. Bereinigen Sie Ihr AD und räumen Sie den Usern die minimal erforderlichen Berechtigungen ein, dass sie ihrer Arbeit voll-umfänglich nachgehen können, ohne dabei ein zu hohes Maß an Berechtigungen zu besitzen.

Wir prüfen - toolbasiert - Ihre AD- Sicherheit, bewerten und klassifizieren die in einem Bericht mit Dashboard-Ansichten dargestellten AD-Sicherheitslücken. Aufgrund unserer objektiven Sicht auf Ihr Windows Active Directory (WAD) und unserer jahrelangen Erfahrungen sind wir in der Lage die richtige Gewichtung und Reihenfolge festzulegen. Wir zeigen Ihnen auf, in welcher Priorisierung die Behebung der Schwachstellen stattfinden, sowie welche Maßnahmen ergriffen werden sollten. Beim AD-Check werden die folgenden vier Bereiche untersucht:

- Trusts (Vertrauensstellungen)
- Anomalies (Anomalien)
- Stale Object (verwaiste Objekte)
- Privileged Accounts (Accounts mit hohen Berechtigungen)



Toolbasierte Auswertung der Schwachstellen

Häufige Fehler, die bei einem Angriff am ehesten ausgenutzt werden können:

- Die Default-Einstellungen der Microsoft Produkte wurden nicht hinterfragt und entsprechend angepasst, so dass sie ggf. zu viel Spielraum lassen
- Fehlende Verschlüsselung und schwache Passwörter
- Passwortrichtlinien, die zu geringe Länge oder Komplexität vorgeben
- Inaktive Domain-Accounts, die vom Angreifer im Hintergrund reaktiviert werden können
- Service-Accounts, die als Domain-Admins konfiguriert sind
- Ungepatchte Sicherheitslücken auf AD-Servern
- Fehlende Automatisierung zur Prüfung und Alarmierung von Sicherheitsmissständen im AD

Angebot BLUE:

- Analyse und Active Diretory Scan
- Auswertung und Priorisierung der Schwachstellen
- Handlungsempfehlung und Unterstützung bei der Abwägung zwischen Selbsthilfe und externer Unterstützung
- Angebot zur Ergreifung sinnvoller Schutzmaßnahmen
- Umsetzungs- und Ablaufplanung nach Priorisierung

Benefits:

- Erfahrung in AD Security, Group Policies, Trusts sowie Patchmanagement
- Tiefe Fachexpertise von der Beratung über umfängliche Administration bis hin zu kontinuierlichem Austausch
- Maßgeschneiderte und optimierte Handlungs-empfehlungen mit Roadmap sowie Gewichtung der zu schließenden Sicherheitslücken
- Erhöhung des Sicherheitsbewusstseins

Kontakt

René Angenheister, BLUE Consult GmbH, Adolf-Dembach-Str. 2, 47829 Krefeld
experten@blue-consult.de, Telefon: +49 2151 6500 10

BLUE CONSULT.