Active Directory: beispiel

Sicherheitsbewertung

D-

53% der Prüfungen bestanden

34 gefundene IoE	**5** übersprungene IoE	**33** nicht gefundene IoE	**67** geprüfte IoE

4	6	15	7	2
Kritisch	**Hoch**	**Mittel**	**Niedrig**	**Info**

Kontakt

Nachfolgend finden Sie einen Überblick über Ihre Domäne und Ihre IT-Infrastruktur. Sollten Sie Rückfragen haben oder eine tiefergehende Untersuchung Ihrer Systeme benötigen, zögern Sie nicht uns zu kontaktieren. Wir unterstützen Sie gerne bei der Optimierung Ihrer IT.

Ihr SEC AUDITOR Team

+49 151 / 200 88 77 4

vertrieb@sec-auditor.com

Active Directory Sicherheitsuntersuchung

1.1 Einleitung

Der Schutz der IT-Infrastruktur ist für jedes Unternehmen von entscheidender Bedeutung. Ein zentrales Element dieser Infrastruktur bildet das Active Directory (AD) oder Entra ID, das als Herzstück einer IT-Infrastruktur fungiert. Schwachstellen können weitreichende Konsequenzen für die gesamte IT-Sicherheit eines Unternehmens haben.

Vor diesem Hintergrund wurde ein umfassender Scan durchgeführt. Ziel des Scans ist es, potenzielle Sicherheitslücken zu identifizieren, die die Integrität, Verfügbarkeit und Vertraulichkeit der im Active Directory und Entra ID verwalteten Informationen gefährden.

Es wurden **1 Forest, 1 Domäne, 8 Benutzerkonten, 55 Gruppen, 4 Computerkonten, 0 Exchange-OnPrem Mailboxen, 0 ManagedServiceAccount-Konten** und **142 Replikationsdaten** gescannt.

In diesem Bericht werden die Ergebnisse der Sicherheitsanalyse detailliert dargestellt und Maßnahmen zur Behebung der gefundenen Schwachstellen vorgeschlagen.

Es wurde eine automatisierte, gründliche Untersuchung Ihres Systems durchgeführt, dabei aktuelle technologische Standards, diverse Compliance-Anforderungen und bewährte Sicherheitsverfahren berücksichtigt.

1.2 Zusammenfassung der Untersuchung

Die Analyse legt nahe, dass Ihre Domäne eine verbesserte Sicherheitsinfrastruktur benötigt, um sowohl aktuellen als auch zukünftigen Bedrohungen entgegenzuwirken.

Die Analyse dient dazu, Ihnen ein fundiertes Verständnis für die bestehenden Sicherheitsprobleme Ihrer Domäne zu geben. Mit diesem Wissen können Sie gezielte Maßnahmen ergreifen, um Ihr Sicherheitsniveau nachhaltig zu erhöhen und Ihr System gegen potenzielle zukünftige Bedrohungen abzusichern.

Wir freuen uns darauf, Ihnen dabei zu helfen, die Sicherheit Ihrer Systeme zu verbessern und eine starke Verteidigung gegen mögliche zukünftige Bedrohungen aufzubauen.

1.3 Kritikalitätsstufen

Kritikalität	Risikoscore	Beschreibung
Kritisch	9.0 - 10.0	Schwachstellen, durch die eine Kompromittierung des Active Directory / Entra ID (oder Teilen davon) für unprivilegierte Benutzer ermöglicht wird
Hoch	7.0 - 8.9	Schwachstellen, die zur Kompromittierung oder zum Lateral Movement beitragen und gefährliche Fehlkonfigurationen, die nicht zur direkten Übernahme der Domäne führen.
Mittel	4.0 - 6.9	Fehlkonfigurationen, die Sicherheitsmechanismen umgehen und Schwachstellen, die sich nicht maßgeblich auf die Domäne auswirken
Niedrig	0.1 - 3.9	Empfohlene Security Best Practises in Bezug auf die Active Directory & Entra ID und Schwachstellen mit geringen Auswirkungen
Info	0.0	Informationen und Hinweise zu Konfigurationen

Mehr über die Kritikalitäten erfahren →

1.4 Übersicht der Ergebnisse

Kritikalität	Name	Objekte
Kritisch	**Uneingeschränkte Delegierung für Computer erlaubt** *Diese Option sollte nicht aktiviert werden.*	2
Kritisch	**NTLMv1 ist auf Domänencontroller aktiv** *GPO erlaubt NTLMv1*	1
Kritisch	**Veraltete Verschlüsselungsmethode für privilegierte Benutzer** *DES-Verschlüsselung ist veraltet und sollte nicht mehr verwendet werden.*	1
Kritisch	**Privilegierte Konten haben einen Service-Principal-Namen (SPN)** *Mitglieder in den privilegierten Gruppen sollten keinen SPN haben*	1
Hoch	**Veraltetes Betriebssystem erkannt** *Es wurden Betriebssysteme erkannt, die nicht mehr mit Sicherheitsupdates versehen werden*	1
Hoch	**Veraltete Verschlüsselungsmethode** *DES-Verschlüsselung ist veraltet und sollte nicht mehr verwendet werden.*	1
Hoch	**Passwortrichtlinie nicht stark genug** *Schwache Passwörter vereinfachen eine Accountübernahme*	1
Hoch	**Objekt mit Replikationsfehler** *Objekte beginnend mit "$Duplicate" weisen auf Replikationsfehler hin*	1
Hoch	**Passwortähnliche Zeichenkette gefunden** *Passwörter sollten nie im Klartext in AD-Objekten gespeichert werden*	1
Hoch	**Privilegierter Benutzer nicht in "Geschützte Benutzer"-Gruppe** *„Geschützte Benutzer" erhalten zusätzlichen Schutz vor der Kompromittierung von Anmeldeinformationen.*	3
Mittel	**Ein Notfalladministratorkonto wurde genutzt** *Der Built-In Administrator wurde in den letzten 30 Tage verwendet.*	1
Mittel	**Computer, bei denen kein Passwort erforderlich ist** *Computerkonten sollten immer ein Passwort haben*	3
Mittel	**Veraltete Domänenfunktionsebene** *Funktionsebene älter als windows 2016*	1
Mittel	**Veraltete Forestfunktionsebene** *Funktionsebene älter als windows 2016*	1
Mittel	**Kerberos Kennwort veraltet** *Letzte KDC-Passwortrotation ist älter als 365 Tage*	1
Mittel	**OU mit gefährlichen Berechtigungen** *Vom Standard abweichende Rechtebesitzer mit erhöhten Berechtigungen*	1
Mittel	**OU mit Berechtigungen für alle Objekte** *Es wurden zu weitreichende Berechtigungen gesetzt*	1

Kritikalität	Name	Objekte
Mittel	**Passwort eines privilegierten Benutzers wird reversible gespeichert** *Passwörter von privilegierten Benutzern im Klartext zu speichern ist ein sehr hohe Risiko*	2
Mittel	**Benutzer können Computer zur Domäne hinzufügen** *Jeder kann Computer mit der Domäne verbinden*	1
Mittel	**Benutzer kann Kennwort nicht ändern** *Benutzer ist auf die Hilfe von Dritten angewiesen um sein Kennwort zu ändern.*	1
Mittel	**Benutzer, bei denen kein Passwort erforderlich ist** *Jeder Benutzer sollte mit einem Passwort geschützt sein*	1
Mittel	**Nutzerkennwörter sind veraltet** *Letzte Passwortänderung ist älter als 365 Tage.*	8
Mittel	**Das Nutzerkennwort läuft nie ab** *Benutzerkonten, bei denen das Passwort nie abläuft*	5
Mittel	**Passwort eines Benutzers wird reversible gespeichert** *Passwörter, die im Klartext gespeichert wurden, sind einfach auszulesen*	3
Mittel	**Benutzer bei denen die Prä-Authentifizierung nicht erforderlich ist** *Diese Option sollte nicht aktiviert werden.*	1
Niedrig	**AD Papierkorb nicht aktiviert** *Ein gelöschtes Objekt ist damit unwiederbringlich gelöscht.*	1
Niedrig	**Zu wenige Domänencontroller vorhanden** *Domänendienste sind nicht redundant bereitgestellt*	1
Niedrig	**Computer wurde lange nicht am DC angemeldet** *Computer, die seit 180 Tagen nicht mehr angemeldet sind oder sich nie angemeldet haben*	3
Niedrig	**Passwort eines Computers ist zu alt** *Das Passwort ist älter als die Standardrotation von 30 Tagen*	3
Niedrig	**OU nicht vor versehentlicher Löschung geschützt** *Verhindert versehentlichen Datenverlust*	1
Niedrig	**Privileged Access Management ist nicht aktiviert** *Um eine höhere Sicherheit von priv. Benutzern zu ermöglichen, wird empfohlen eine PAM Lösung einzusetzen.*	1
Niedrig	**Inaktive Benutzerobjekte** *Benutzer, die seit 100 Tagen nicht mehr angemeldet sind oder sich nie angemeldet haben*	4
Info	**Leere Gruppen** *Gruppen ohne Mitglieder sollten gelöscht werden*	5
Info	**OU mit zusätzlichen Rechtebesitzern** *Es gibt vom Standard abweichende Rechtebesitzer*	1

1.4.1 Übersprungene Prüfungen

Kritikalität	Name	Objekte
Hoch	**Synchronisation privilegierter OnPrem-Konten** *Ermöglicht Übernahme des ADs aus der Cloud*	0
Hoch	**Externer Benutzer mit dauerhaften, erhöhten Entra-Privilegien** *Externe Benutzer sollten nach Möglichkeit keine erhöhten Berechtigungen haben*	0
Hoch	**Hybrider Benutzer mit dauerhaften, erhöhten Entra-Privilegien** *Cloud-Infrastruktur über OnPrem angreifbar*	0
Mittel	**Conditional Access: Keine Gerätecompliance** *Fehlende Geräte-Compliance-Richtlinie*	0
Niedrig	**Nur ein globaler Administrator (Entra ID)** *Es sollte mindestens einen Notfallzugriff geben*	0

1.4.2 Geprüft und nicht gefunden

Name
Benutzer mit falscher primärer Gruppen-ID *Benutzerobjekt hat abweichende Primary-Group-ID*
"Operator"-Gruppen nicht leer *Operator-Gruppen sind nicht leer*
Domänencontroller mit falscher primärer Gruppen-ID *Domänencontroller hat eine abweichende primäre Gruppen-ID*
Fehlende Updates auf Domaincontroller *Domänencontroller wurde seit mehr als 6 Monaten nicht neugestartet*
SMB v1 aktiviert *SMBv1 ist ein veraltetes Protokoll, das als unsicher gilt*
SMB v1 auf Domaincontroller aktiviert *SMBv1 ist ein veraltetes Protokoll, das als unsicher gilt*
Passwort des Domaincontrollers wird nicht regelmäßig geändert *Passwort wurde seit mehr als 60 Tagen nicht geändert*
LM (LanManager) ist aktiv *GPO erlaubt unsicheren LM- Passworthash*
Gastbenutzer mit falscher primärer Gruppen-ID *Gastbenutzer hat abweichende primärer Gruppen-ID*
Domaincontroller hat einen falschen Besitzer *Der Besitzer entspricht nicht "Domänenadministratoren"*
Gastkonto ist aktiviert *Gastkonto sollte nicht aktiviert sein*
Ungeschützer Recovery-Modus *Fehlender Administrator-Passwortschutz im Recovery-Modus*
Vorkonfigurierte Administratorengruppen in Verwendung *Nach Best-Practice sollen keine Benutzer in den Standardgruppen vorhanden sein.*
Ein Nutzerkonto hat oder hatte administrative Rechte *Ein nicht privilegiertes Nutzerkonto verfügte über administrative Rechte.*
Computer hat falsche primäre Gruppe *Das Computerobjekt befindet sich in der falschen primären Gruppe.*
Passwort des Computerobjektes läuft nie ab *Computer, bei denen das Kennwort nie abläuft*
Hohe Anzahl an Domänenadministratoren *Anzahl sollte nicht größer als 2 sein*
Eingeschränkte Delegierung auf Domaincontroller erlaubt *Dies kann zur Übernahme der Domäne ausgenutzt werden*

Name
Eingeschränkte Delegierung für Nutzer erlaubt *Kann zur unberechtigten Übernahme von Privilegien ausgenutzt werden*
Gruppe "Prä-Windows 2000 kompatibler Zugriff" erlaubt Zugang für authentifizierte Benutzer *Die Forgein Security Principal "Authenticated User" ist Mitglied der Gruppe*
Kennwortänderung von Computern verboten *GPO blockiert Computer-Kontopasswortänderung*
Gruppe "Abgelehnte RODC-Kennwortreplikationsgruppe" enthält nicht alle Standardmitglieder *Nicht alle Standardmitglieder enthalten*
LDAP Signierung deaktiviert *Ermöglicht Man-in-the-Middle-Angriffe*
Inaktive Domaincontroller *Ungenutzte Domaincontroller sollten herabgestuft werden*
Gruppe "Prä-Windows 2000 kompatibler Zugriff" erlaubt Zugang ohne Account *Die Gruppen "Jeder" oder "Anonym" sind Mitglieder der Gruppe*
GPO mit Autologin *Autologin per Registryeintrag*
Gruppenrichtlinie enthält Passwort *GPO enthält ein gespeichertes Passwort*
Deaktivierte, privilegierter Benutzer *Privilegierte Rechte von deaktivieren Benutzern sollten entfernt werden*
Computerobjekt kann sein Passwort nicht selbst ändern *Die automatische Rotation sollte eingeschaltet sein*
"Zulässige RODC-Kennwortreplikationsgruppe" enthält Benutzer *Es soll sichergestellt werden, dass die Gruppe "Zulässige RODC-Kennwortreplikationsgruppe" leer ist.*
Uneingeschränkte Delegierung für Nutzer erlaubt *Kann zur unberechtigten Übernahme von Privilegien ausgenutzt werden*
NTLMv1 ist aktiv *GPO erlaubt NTLMv1*
Eingeschränkte Delegierung für privilegierte Nutzer erlaubt *Dies kann zur Übernahme der Domäne ausgenutzt werden*

2 Detaillierte Analyse der identifizierten Schwachstellen

In diesem Kapitel werden wir uns eingehend mit den spezifischen Schwachstellen befassen, die während des Schwachstellenscans aufgedeckt wurden. Jede identifizierte Sicherheitslücke wird im Detail vorgestellt, analysiert und in ihrem Kontext erläutert.

Die Schwachstellen sind nach ihrer Kritikalität geordnet, beginnend mit den schwerwiegendsten Sicherheitsrisiken.

Ziel dieses Kapitels ist es, ein tiefgreifendes Verständnis der entdeckten Sicherheitslücken zu vermitteln und eine fundierte Grundlage für die Priorisierung von Korrekturmaßnahmen zu schaffen. Die hier präsentierten Informationen sollen IT-Administratoren und Sicherheitsverantwortlichen dabei helfen, fundierte Entscheidungen zur Verbesserung der Sicherheit zu treffen.

Dies ist ein grundlegender Sicherheitsüberblick Ihres Active Directory. Für eine detaillierte Analyse mit vollständigen Erkenntnissen, umfassenden Behebungsanleitungen und kontinuierlichem Monitoring wenden Sie sich bitte an Ihren IT-Dienstleister SEC AUDITOR.