Sicherheitsbewertung

F

69% der geprüften IoEs wurden gefunden

21 gefundene IoE | **12** nicht gefundene IoE | **33** geprüfte IoE

5	3	10	3	0
Kritisch	**Hoch**	**Mittel**	**Niedrig**	**Info**

Mehr über die Kritikalitäten erfahren →

Kontakt

Nachfolgend finden Sie einen Überblick über Ihr Active Directory 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 CCVOSSEL Team

0800 2286773

info@ccvossel.de

Zusammenfassung

Dieser Bericht repräsentiert eine Sicherheitsanalyse Ihres Active Directory, mit besonderem Fokus auf potenzielle Bedrohungen und Mängel. Es wurde eine automatisierte, gründliche Untersuchung Ihres Systems durchgeführt, dabei aktuelle technologische Standards, diverse Compliance-Anforderungen und bewährte Sicherheitsverfahren berücksichtigt.

Es wurden **1 Forest, 1 Domäne, 8 Benutzerkonten, 50 Gruppen, 4 Computerkonten** und **197 AD-Änderungen** gescannt.

Die Analyse legt nahe, dass Ihr Active Directory eine verbesserte Sicherheitsinfrastruktur benötigt, um sowohl aktuellen als auch zukünftigen Bedrohungen entgegenzuwirken.

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

Unser Ziel ist es, Ihnen mit diesem Bericht die Informationen und das Verständnis zu liefern, die Sie benötigen, um fundierte Entscheidungen über die Verbesserung der Sicherheit Ihres Active Directory zu treffen. Wir freuen uns darauf, Ihnen dabei zu helfen, die Sicherheit Ihrer Systeme zu verbessern und eine starke Verteidigung gegen mögliche zukünftige Bedrohungen aufzubauen.

Gefundene Indicators of Exposure

Kritisch

Name	Objekte	Ausnahmen
SMB v1 auf Domaincontroller aktiviert SMBv1 ist ein veraltetes Protokoll, das als unsicher gilt	1	0
Uneingeschränkte Delegierung für Computer erlaubt Diese Option sollte nicht aktiviert werden.	2	0
Veraltete Verschlüsselungsmethode für privilegierte Benutzer DES-Verschlüsselung ist veraltet und sollte nicht mehr verwendet werden.	1	0
Privilegierte Konten haben einen Service-Principal-Namen (SPN) Mitglieder in den privilegierten Gruppen sollten keinen SPN haben	1	0
Passwort eines privilegierten Benutzers wird reversible gespeichert Passwörter von privilegierten Benutzern im Klartext zu speichern ist ein sehr hohe Risiko	2	0

Hoch

Name	Objekte	Ausnahmen
Veraltetes Betriebssystem erkannt Es wurden Betriebssysteme erkannt, die nicht mehr mit Sicherheitsupdates versehen werden	1	0
Objekt mit Replikationsfehler Objekte beginnend mit "$Duplicate" weisen auf Replikationsfehler hin	1	0
Passwort eines Benutzers wird reversible gespeichert Passwörter, die im Klartext gespeichert wurden, sind einfach auszulesen	1	0

Mittel

Name	Objekte	Ausnahmen
Ein Notfalladministratorkonto wurde genutzt Der Built-In Administrator wurde in den letzten 30 Tage verwendet.	1	0
Mindestkennwortlänge für Computer nicht festgelegt Leere Passwörter sollten nie erlaubt sein	3	0
Veraltete Domänenfunktionsebene Funktionsebene älter als windows 2016	1	0
Veraltete Forestfunktionsebene Funktionsebene älter als windows 2016	1	0
Benutzer können Computer zur Domäne hinzufügen 'Dies ist standardmäßig aktiviert. Es sollte nicht aktiviert werden.	1	0
Benutzer kann Kennwort nicht ändern Benutzer ist auf die Hilfe von Dritten angewiesen um sein Kennwort zu ändern.	1	0
Mindestkennwortlänge für Nutzer nicht festgelegt Leere Passwörter sollten nie erlaubt sein	1	0
Nutzerkennwörter sind veraltet Letzte Passwortänderung ist älter als 100 Tage.	7	0
Das Nutzerkennwort läuft nie ab Benutzerkonten, bei denen das Passwort nie abläuft	5	0
Benutzer bei denen die Prä-Authentifizierung nicht erforderlich ist Diese Option sollte nicht aktiviert werden.	1	0

Niedrig

Name	Objekte	Ausnahmen
AD Papierkorb nicht aktiviert Ein gelöschtes Objekt ist damit unwiederbringlich gelöscht.	1	0
Computer wurde lange nicht am DC angemeldet Computer, die seit 180 Tagen nicht mehr angemeldet sind oder sich nie angemeldet haben	4	0
Inaktive Benutzerobjekte Benutzer, die seit 365 Tagen nicht mehr angemeldet sind oder sich nie angemeldet haben	4	0