AYI NEDJIMI Consultants

Sécuriser Active Directory : Le Gu

18 April 2026 • Mis à jour le 18 April 2026 • 60 min de lecture

> Guide définitif pour sécuriser Active Directory : Tiering Model, hardening K
> outils audit, AD CS, plan 90 jours.

Active Directory reste, en 2026, le socle d'identité de plus de 90 % des entreprise
2000 Server, ce service d'annuaire centralise l'authentification, les autorisations e
système d'information. Or, cette centralisation constitue précisément sa plus gran
à obtenir les clés de l'ensemble du royaume numérique. Les rapports de réponse
convergent sur un constat alarmant — dans 80 % des attaques par rançongiciel a
pour atteindre la domination du domaine. Les groupes APT comme FIN7, Conti ou
structurelles d'AD. Face à cette réalité, sécuriser Active Directory n'est plus un pro
de référence couvre l'intégralité des mesures de durcissement, de la théorie aux c
par un plan de remédiation actionnable en 90 jours.

État des lieux : pourquoi Active Directory est si vulnérable

Avant de déployer des mesures de protection, il faut comprendre pourquoi Active
Les raisons sont multiples, profondément ancrées dans l'histoire du produit et dan
sédimentées au fil des décennies.

L'héritage d'une architecture conçue pour la compatibilité

Active Directory a été conçu à une époque où la priorité absolue était la compatibi
protocole NTLM, maintenu pour la rétrocompatibilité avec des applications parfois
hachage (MD4) dont la faiblesse cryptographique est documentée depuis les anné
supporte encore par défaut le chiffrement RC4-HMAC — qui n'est autre qu'un wra
attaques comme le Kerberoasting. Les niveaux fonctionnels de domaine et de forê
domaine sous Windows Server 2012 R2, voire 2008 R2, dans un même environnem
impose le maintien de protocoles obsolètes et empêche l'activation de fonctionna

L'architecture plate : absence de segmentation par défaut

Par défaut, Active Directory ne propose aucune segmentation des privilèges. Un a
sur les postes de travail, les serveurs applicatifs et les contrôleurs de domaine. Ce
compromet un poste de travail sur lequel un administrateur s'est récemment conn
Mimikatz ou des techniques équivalentes) et pivoter directement vers les contrôle
entre les différents niveaux de criticité de l'infrastructure. Le modèle de tiering, qu
par défaut — c'est une surcouche architecturale que les organisations doivent con

La prolifération des comptes à privilèges

Les audits PingCastle révèlent systématiquement le même problème : une prolifér
élevés. Dans un domaine typique de 5 000 utilisateurs, on trouve fréquemment en