Souhir ZAIMI

Veille n°2 – Les bonnes pratiques de securisation d'Active Directory

La securisation d'AD repose sur quatre piliers complementaires : les GPO pour appliquer des configurations centralisees, le principe du moindre privilege pour limiter les risques, la protection des comptes admin avec MFA et PAW, et une surveillance continue pour detecter les comportements anormaux.

GPO de securite

Les GPO permettent d'appliquer des configurations de securite de facon centralisee. Microsoft (2025) recommande de bloquer les protocoles obsoletes NTLMv1 et SMBv1, d'exiger la signature LDAP, de desactiver LLMNR et d'activer Windows LAPS pour les mots de passe administrateurs locaux. Toute modification incorrecte d'un GPO pouvant avoir des consequences graves, une surveillance des changements est indispensable.

Principe du moindre privilege

Il consiste a n'accorder que les droits strictement necessaires a chaque utilisateur. En pratique : limiter les membres des groupes privilegies (Domain Admins), creer des comptes de service dedies et appliquer le Tier Model. Ce modele segmente les ressources en trois niveaux (controleurs de domaine, serveurs metier, postes de travail) pour freiner la propagation laterale d'une attaque (Semperis, janvier 2026).

Securisation des comptes administrateurs

Le MFA doit etre active sur tous les comptes a privileges. Les administrateurs doivent utiliser des postes dedies (PAW), isoles du reseau standard. Les comptes Domain Admin ne doivent jamais servir a naviguer sur Internet. Microsoft recommande egalement les politiques de mots de passe a granularite fine (FGPP) pour imposer des exigences plus strictes selon le niveau de privilege.

Surveillance et audit

La securisation d'AD est un processus continu. Il faut activer l'audit avancee pour journaliser les connexions et modifications, et utiliser des outils comme Microsoft Defender for Identity ou PingCastle pour detecter les comportements anormaux et les chemins d'attaque.

Notions cles

MFA (Multi-Factor Authentication)
: Mecanisme de securite necessitant plusieurs preuves d'identite (mot de passe + code OTP, cle USB, biometrie) pour acceder a un systeme.

PAW (Privileged Access Workstation)
: Poste de travail dedie et isole utilise exclusivement par les administrateurs pour effectuer des taches privilegiees.

Tier Model
: Modele de segmentation d'Active Directory en trois niveaux (Tier 0: controleurs de domaine, Tier 1: serveurs metier, Tier 2: postes utilisateurs) pour limiter les risques.

NTLM et SMB
: Protocoles Windows utilises pour l'authentification et le partage de fichiers. Les anciennes versions sont vulnerables et doivent etre desactivees.

LDAP (Lightweight Directory Access Protocol)
: Protocole permettant de se connecter a un annuaire comme Active Directory. Sa signature garantit l'integrite des donnees echangees.

LLMNR (Link-Local Multicast Name Resolution)

Protocole permettant la resolution de noms locaux, mais qui peut etre exploite pour des attaques d'empoisonnement de cache.

Sources

• Microsoft Learn – Meilleures pratiques pour la securisation d'Active Directory
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

• Semperis – Active Directory Security Best Practices (janvier 2026)
https://www.semperis.com/blog/

• SpecOps Software – Active Directory Security Best Practices for 2025
https://specopssoft.com/blog/active-directory-security-best-practices/