VEILLE TECHNOLOGIQUE • SÉCURISATION D'ACTIVE DIRECTORY — FICHE 5

Active Directory hybride : sécuriser la passerelle entre l'AD local et Entra ID

Date de la veille : 15 octobre 2026

Pour cette cinquième veille, je me suis penché sur la sécurisation des environnements hybrides reliant un Active Directory local à Microsoft Entra ID (ex-Azure AD), en m'appuyant sur les recommandations de l'ANSSI et de Microsoft Security. Aujourd'hui, la majorité des entreprises synchronisent leurs identités vers le cloud via *Entra Connect* (ou *Cloud Sync*), ce qui crée un pont critique : si l'un des deux côtés est compromis, l'attaquant peut rebondir vers l'autre.

Ce que je retiens, c'est que les attaquants ciblent en priorité les accès distants (VPN, portails cloud) par vol de jetons de session (*AiTM / phishing*) afin de contourner l'authentification multifacteur (MFA) classique. Pour verrouiller cette surface d'attaque, il est indispensable d'imposer un **MFA résistant au phishing** (clés FIDO2 ou Windows Hello Entreprise), d'appliquer l'accès conditionnel sur Entra ID et de sécuriser le serveur de synchronisation au même niveau qu'un contrôleur de domaine (modèle *Tier 0*).

Pour un administrateur système, cela signifie qu'on ne peut plus gérer la sécurité de l'AD local et du cloud séparément : la gouvernance des identités et les règles d'accès doivent être unifiées de bout en bout.

SOURCES

- ANSSI — *Recommandations de sécurité relatives à Active Directory et aux architectures hybrides*
- Microsoft — *Securing hybrid identity infrastructure (Microsoft Entra Connect & Cloud Sync)*