VEILLE TECHNOLOGIQUE • SÉCURISATION D'ACTIVE DIRECTORY — FICHE 2

Microsoft prépare la désactivation de NTLM par défaut

Date de la veille : 22 octobre 2026

En suivant l'actualité de Windows Server, j'ai relevé la feuille de route de Microsoft (publiée en janvier et mise à jour en octobre 2026) visant à désactiver par défaut l'ancien protocole d'authentification **NTLM**. Le déploiement s'organise en trois étapes : d'abord une phase d'audit renforcé déjà disponible sur Windows Server 2025, suivie de correctifs fin 2026 pour combler les derniers blocages Kerberos (notamment via IAKerb), avant la désactivation native dans la prochaine version majeure de Windows Server.

L'enjeu de sécurité est majeur puisque NTLM est le vecteur principal des attaques par relais d'authentification et *Pass-the-Hash*. En basculant tout vers **Kerberos** et en imposant le *LDAP channel binding* par défaut, Microsoft élimine d'un bloc toute une famille d'exploitations réseau courantes.

Pour un administrateur système, le risque est toutefois opérationnel : couper NTLM sans préparation risque de faire tomber de vieilles applications métiers. Il faut donc activer l'audit dès maintenant en pré-production pour cartographier les flux existants et éviter d'avoir à réactiver le protocole dans l'urgence.

SOURCES

- Microsoft — *Advancing Windows security: Disabling NTLM by default* (29 janv. 2026, maj oct. 2026)
- Microsoft — *Guidance to help mitigate critical threats to Active Directory Domain Services* (9 déc. 2025)