Veille n 3 - Active Directory et les ransomwares

En 2025, les intrusions via Active Directory ont augmente de 37 % en un an (ANSSI). On recense 4 701 incidents ransomware, soit +46 % par rapport a 2024 (Gridinsoft, fevrier 2026).

Comment les ransomwares exploitent Active Directory

Apres un acces initial (phishing, identifiants compromis), les attaquants cartographient l'AD, elevent leurs privileges via Kerberoasting ou Pass-the-Hash, puis deployent le ransomware sur toutes les machines via les GPO. Le delai median entre l'intrusion et le chiffrement est desormais de seulement 5 jours (Gridinsoft, 2025).

Cas reels d'attaques (2025)

En janvier 2025, un prestataire de sante suisse a vu 3 000 postes chiffres en 51 secondes, avec 800 Go de donnees exfiltrees. Le groupe Play ransomware a touche 900 entites selon le FBI. En France, 74 % des organisations ont ete ciblees en 2024 et plus d'une sur deux a subi une attaque reussie (Semperis, aout 2025).

Impact sur les entreprises

Le cout moyen mondial d'une attaque atteint 5,08 millions de dollars en 2025. En France, l'arret du SI coute plus de 200 000 euros pour une PME. Les ransomwares pratiquent desormais la triple extorsion : chiffrement, vol de donnees et attaques DDoS simultanees. 69 % des entreprises attaquees ont paye la rancon, dont 30 % plusieurs fois.

Moyens de prevention

Segmenter le reseau via le Tier Model, maintenir des sauvegardes isolees et immutables, activer le MFA sur tous les comptes privilegies (63 % des incidents debutent par un compte compromis), deployer des outils EDR/XDR pour la detection en temps reel, et organiser des exercices de simulation d'attaques reguliers pour tester la resilience de l'organisation.

Sources

- AVTIS - Cybersecurite 2025 : nouvelles attaques ciblant les entreprises francaises, janvier 2026
- ctrlaltnod - Ransomware-as-a-Service 2025 : kits automatises, novembre 2025
- Solutions Numeriques - Ransomwares : 74% des organisations francaises ciblees, aout 2025
- Gridinsoft - Ransomware 2025 : Statistiques et Tendances, fevrier 2026