Deletec

Cybersécurité & Cloud services

Tech IT easy.

Hardening AD

Sécurisez votre Active Directory

Selon le Microsoft Digital Report de 2022, 20 % des comptes utilisateurs Active Directory subissent des tentatives d'attaques quotidienne.

Ces attaques n'ont qu'un seul but : récupérer des accès administrateur via l'exécution de code malveillant pour compromettre et rendre indisponible tout votre SI (messagerie, fichiers, applications, sauvegarde).

↘ Les vulnérabilités d'un Active Directory

- Une mauvaise gestion de l'Active Directory.
- Des systèmes obsolètes.
- Accès des prestataires externes.
- Des adhérences entre divers services favorisant l'escalade de privilèges.
- Une mauvaise surveillance de l'Active Directory.

L'Active Directory est le centre névralgique de votre système d'information...

... et de fait la cible des cyberattaquants.

↘ L'approche Deletec

Maturité 1.

- Mettre en œuvre une gouvernance de l'Active Directory, des postes de travail et des serveurs.
- Valider une arborescence permettant une première sécurité by design.
- Mettre en place un modèle d'administration basé sur le principe du moindre privilège.
- Déléguer les comptes d'administration.
- Nettoyer les objets obsolètes.
- Identifier les comptes critiques.
- Mettre en œuvre LAPS.
- Configurer les journaux d'événement des contrôleurs de domaine.
- Définir les dépendances à l'Active Directory.
- Valider l'EDR.

Maturité 2.

- Identifier et bloquer les protocoles obsolètes et vulnérables.
- Appliquer des stratégies de sécurisation sur les contrôleurs de domaine.
- Sécuriser les composants critiques liées à l'Active Directory (DC, CA, messagerie).
- Accompagner la rédaction de procédures d'onboarding et offboarding.
- Mettre à niveau les contrôleurs de domaine.
- Crypter les postes clients avec Bitlocker.

Maturité 3.

- Isoler les contrôleurs de domaine et modèle tiers.
- Mettre en œuvre les machines d'administration (PAW).
- Mettre en œuvre une surveillance AD sur notre SOC.
- Audit et test de pénétration

Les outils d'analyse et de suivi

Les principes de durcissement employés	Les technologies Microsoft employées	Les technologies tierces employées	Solutions technologiques
• Moindre privilège. • Isolation réseau. • Hardening des OS (serveurs, clients). • Modèle n-Tiers. • PAW (Privileged Acces Workstation).	• Windows laps. • Mot de passe fin. • Bitlocker. • GSMA. • Modèle tiers. • PAW.	• SIEM. • Zero trust. • Bastion pour les prestataires externes. • Bastion pour les administrateurs.	• Authentification à deux facteurs : Trustbuilder, Azure AD. • Bastion : Wallix. • Gouvernance : Netwrix. • Courriel : Vadesecure, Defender M365. • Gestion des événements : SIEM (Manageengine, FORTI SIEM, SEKOIA) • Endpoint Detection and Response: Sentinel1, Microsoft Defender, Carbon Black.

Notre offre

Grace à notre proposition complète, le sujet de la sécurité Active Directory est traité sur le court, moyen et long terme.

↘ Audit

- Analyse approfondie de l'infrastructure AD existante.
- Identification des vulnérabilités et des risques potentiels.
- Évaluation de la conformité aux meilleures pratiques de sécurité.
- Score de maturité et de sécurité.

↘ Mise en conformité

- Identification et blocage des protocoles obsolètes et vulnérables.
- Application de stratégies de sécurisation sur les contrôleurs de domaine.
- Définition d'une politique de mot de passe sécurisée.
- Application du principe du moindre privilège pour les comptes et groupes.
- Homogénéisation des postes de travail.
- Application des recommandations de l'ANSSI.

↘ Gouvernance

- Mise en place d'une gouvernance robuste et efficace.
- Mise en place de PKI et leur suivi.

↘ Migration & Mise à jour

- Migration des serveurs vers des versions OS supportées.
- Mise à jour des systèmes d'exploitation pour éliminer les vulnérabilités.

↘ Services managés

Apporter des réponses aux problématiques de gestion récurrente via notre équipe SOC.

- Surveillance par notre équipe SOC.
- Extraction des logs des contrôleurs de domaine vers notre SOC.
- Analyse des logs par notre SOC pour anticiper les risques.
- Audit et test de pénétration annuel.
- Génération de rapports réguliers sur l'état de sécurité.

↘ Formation

- Sessions de sensibilisation à la sécurité des courriels pour les utilisateurs.
- Formation sur les bonnes pratiques de gestion d'Active Directory pour les administrateurs.

↘ Les avantages de notre offre

- Réduction des risques de cyberattaques.
- Conformité aux normes de sécurité.
- Amélioration de la réactivité face aux menaces.
- Un partenariat pour vous accompagner de bout en bout.

À propos de Deletec

Deletec est une entreprise de services numériques à taille humaine, qui accompagne depuis près de 25 ans les entreprises et les organisations dans leur transformation digitale. Forts de notre équipe pluridisciplinaire et de notre écosystème partenaire, nous couvrons l'ensemble de la chaîne de valeur informatique et télécom.

Nous contacter

01 53 25 06 60
contact@deletec.fr