Offre de service

Cyber Security

Technologies concernées :
- Microsoft Active Directory (ADDS)
- Microsoft EntraID

Charge estimée : 3-5 Jours

Budget estimé : 5-8 KCHF

Audit Active Directory / EntraID

Introduction

L'identité numérique est devenue le socle de la sécurité des systèmes d'information modernes. Les services d'annuaire et de gestion des identités contrôlent l'accès aux applications, aux données et aux infrastructures critiques de l'entreprise.

Les environnements hybrides combinant Microsoft Active Directory et Microsoft Entra ID (anciennement Azure AD) offrent aujourd'hui des capacités puissantes d'authentification, d'administration et de gestion des accès. Toutefois, leur complexité croissante peut introduire des failles de configuration, des privilèges excessifs ou des vulnérabilités exploitables par des attaquants.

Notre offre d'audit de sécurité vous permet d'obtenir une vision claire et objective du niveau de sécurité de votre infrastructure d'identité, d'identifier les risques potentiels et de mettre en œuvre les meilleures pratiques pour protéger votre organisation.

Périmètre de la prestation

Notre audit s'appuie sur une méthodologie éprouvée combinant les bonnes pratiques de Microsoft, les standards de cybersécurité internationaux (CIS, ANSI, NIST), le retour d'expérience issu d'audits et d'incidents réels

Nous analysons vos environnements Microsoft Active Directory et Microsoft Entra ID dans leur globalité afin d'identifier les vulnérabilités potentielles et de proposer des recommandations concrètes pour renforcer votre posture de sécurité.

Notre objectif est de vous aider à sécuriser l'infrastructure d'identité qui protège l'ensemble de votre système d'information.

Prérequis du mandat

Ce mandat nécessite la pleine collaboration des équipes du client durant tout le déroulement de la prestation.

Les équipes de CloudEdge doivent pouvoir disposer d'un accès à distance durant la phase d'audit, l'autorisation d'exécuter un ou plusieurs scripts d'audit depuis le(s) serveur(s) de l'architecture Active Directory et le tenant Microsoft 365 du client, et de disposer de droits suffisants pour pouvoir exécuter les différents prélèvements d'informations techniques.

Déroulement de la prestation

Le mandat d'audit des gestionnaires d'identité Active Directory & EntraID s'articule autour de différents axes d'analyse, en premier lieu l'architecture des services d'annuaire ADDS, soit la structure des domaines et forêts, la configuration des contrôleurs de domaine, les éventuelles relations d'approbation (trusts), les notions de sites et de réplication, l'intégration avec le cloud.

Cette analyse permet de vérifier que l'architecture de Microsoft Active Directory est robuste, cohérente et conforme aux bonnes pratiques.

Microsoft

CloudEdge

Make IT more Human

Offre de service

Cyber Security

La seconde partie de l'analyse se concentre sur la gestion des identités et des comptes utilisateurs et administrateurs (Ex : comptes à privilèges, comptes de service, comptes inactifs ou obsolètes, stratégies de gestion des identités, mécanismes d'authentification), l'objectif est de réduire les risques liés aux comptes à privilèges excessifs ou mal protégés.

Le troisième pan de l'audit s'intéresse à la gestion des privilèges et des délégations (Ex : groupes administrateurs, délégations de contrôle, héritages de privilèges, accès aux contrôleurs de domaine, mécanismes d'élévation de privilèges). En effet, des droits administratifs mal maîtrisés représentent l'une des principales causes de compromission d'un environnement Active Directory. Cette analyse permet d'identifier les chemins d'attaque potentiels vers les privilèges les plus élevés.

Le quatrième axe de l'analyse concerne la sécurité de l'environnement Entra ID afin d'identifier les failles potentielles dans la gestion des identités Cloud (Ex : gestion des rôles administratifs, authentification multifacteur (MFA), politiques d'accès conditionnel, accès aux applications SaaS, gestion des identités externes).

L'objectif est de garantir une protection efficace des identités et des ressources Cloud.

Pour les environnements hybrides, nous nous intéresserons également à la synchronisation entre l'annuaire local et le Cloud (Ex : configuration de la synchronisation, comptes utilisés, permissions associées, afin de vérifier que l'intégration entre Microsoft Active Directory et Microsoft Entra ID ne crée pas de nouvelles vulnérabilités.

Enfin, le mandat est conclu par une analyse des politiques de sécurité et des configurations clientes (Ex : stratégies de groupe (GPO), politiques de mot de passe, mécanismes d'authentification, protocoles hérités, journalisation et supervision). Ces contrôles permettent d'évaluer la maturité globale de votre posture de sécurité.

Bénéfices attendus par le client

La réalisation d'un audit de vos gestionnaires d'identités permet de renforcer la sécurité de votre annuaire d'entreprise, de réduire les risques de compromission des comptes administrateurs, de sécuriser les accès aux services Cloud et aux applications SaaS, d'améliorer durablement la gouvernance des identités et des accès, et enfin d'aligner votre infrastructure avec les meilleures pratiques de cybersécurité

Vos environnements Microsoft Active Directory et Microsoft Entra ID devient ainsi un socle fiable pour la gestion des identités et la protection de votre système d'information.

Microsoft

CloudEdge

Make IT more Human