Offre de service

Cyber Security

Technologies concernées :
- Microsoft PKI ADCS
- Microsoft Actve Directory (ADDS)

Charge estimée : 2-4 Jours

Budget estimé : 3-6 KCHF

Audit PKI Microsoft ADCS

Introduction

La gestion des identités et des certificats numériques est aujourd'hui au cœur de la sécurité des systèmes d'information. Authentification forte, chiffrement des communications, signature électronique ou encore protection des accès, tous ces mécanismes reposent sur une infrastructure à clés publiques (PKI) fiable et correctement configurée.

Dans de nombreuses organisations, la PKI a été déployée il y a plusieurs années pour répondre à un besoin spécifique (Ex : certificats serveurs, WiFi, VPN, etc.).

Avec le temps, l'infrastructure évolue, les usages se multiplient et les menaces se sophistiquent. Une configuration initialement correcte peut alors devenir fragile, obsolète ou exposée à des risques de sécurité importants.

Notre offre d'audit dédiée à Microsoft Active Directory Certificate Services (ADCS) vous permet d'évaluer en profondeur votre infrastructure PKI afin de garantir qu'elle reste fiable, sécurisée et alignée avec les bonnes pratiques actuelles.

La PKI constitue l'un des composants les plus critiques de votre architecture de sécurité.

Une mauvaise configuration peut avoir des conséquences importantes (émission de certificats non-autorisés, compromission de l'authentification utilisateurs ou machines, possibilité d'élévation de privilèges dans l'environnement Active Directory, ou encore perte de confiance dans l'ensemble des certificats émis.

Périmètre de la prestation

Un audit permet de vérifier que votre environnement Microsoft ADCS respecte les bonnes pratiques de sécurité de Microsoft, protège correctement les autorités de certification, contrôle strictement l'émission des certificats, limite les risques d'abus ou d'élévation de privilèges et répond aux besoins actuels et futurs de votre organisation. En d'autres termes, l'audit permet de sécuriser la racine de confiance de votre système d'information.

Notre audit repose sur une méthodologie structurée combinant analyse technique approfondie, expertise en cybersécurité et bonnes pratiques PKI. Nous analysons votre infrastructure ADCS dans sa globalité afin d'identifier les risques potentiels et de proposer des recommandations concrètes pour renforcer votre posture de sécurité.

Notre objectif est de garantir que votre PKI reste un pilier de confiance et non une source de vulnérabilités.

Microsoft

CloudEdge

Make IT more Human

Offre de service

Cyber Security

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 des scripts d'audit depuis le(s) serveur(s) de l'architecture PKI, optionnellement de l'AD, et de disposer de droits suffisants pour pouvoir exécuter les différents prélèvements d'informations.

Déroulement de la prestation

Le mandat d'audit de la PKI s'articule autour de différents axes d'analyse, en premier lieu l'architecture de la PKI, qui comprend l'étude de la structure globale de l'infrastructure (Ex: hiérarchie des CA, autorité root et autorités intermédiaires, architecture en ligne / hors ligne, intégration avec l'Active Directory, segmentation et isolation). Cette analyse permet d'évaluer si l'architecture actuelle respecte les principes fondamentaux de sécurité et de résilience d'une PKI moderne.

Le deuxième volet de l'analyse se concentre sur la configuration des autorités de certification, le cœur de la PKI. Leur configuration doit être irréprochable (configuration des services ADCS, paramètres de sécurité des autorités de certification, gestion des clés privées, durée de validité des certificats et politiques d'émission).

L'objectif est de s'assurer que les autorités de certification sont correctement protégées contre toute utilisation abusive.

Le troisième pan de l'audit s'intéresse aux modèles de certificats qui constituent l'un des points de vulnérabilité principaux des PKI Microsoft, et plus particulièrement les droits d'émission et d'inscription, les usages autorisés des certificats, les permissions associées, ou les risques d'élévation de privilèges. Cette analyse est complétée par une revue complète des accès et des permissions (Ex : groupes, comptes, permissions, délégations, mécanismes de traçabilité).

Le quatrième axe de l'analyse concerne le cycle de vie des certificats, soit les processus de demande et d'émission, de renouvellement automatique, ou de révocation des certificats, la publication des CRL et la gestion des certificats expirés ou compromis.

Le mandat est conclu par une évaluation de l'application des bonnes pratiques de sécurité (protection des clés, processus de sauvegarde/restauration, disponibilité des services, mécanismes de supervision). Ces éléments sont essentiels pour garantir une confiance totale en l'infrastructure PKI.

Bénéfices attendus par le client

La réalisation d'un audit PKI apporte des bénéfices immédiats, le renforcement de la sécurité de votre infrastructure, la réduction des risques d'attaque ou d'élévation de privilèges, l'amélioration de la gouvernance, l'optimisation de l'architecture et des configurations et l'alignement avec les bonnes pratiques de sécurité.

Microsoft

CloudEdge

Make IT more Human