Fiche pratique

Advens
Security for the greater good

Réussir l'audit en boîte blanche de son Active Directory

Suivez la méthodologie d'Advens !

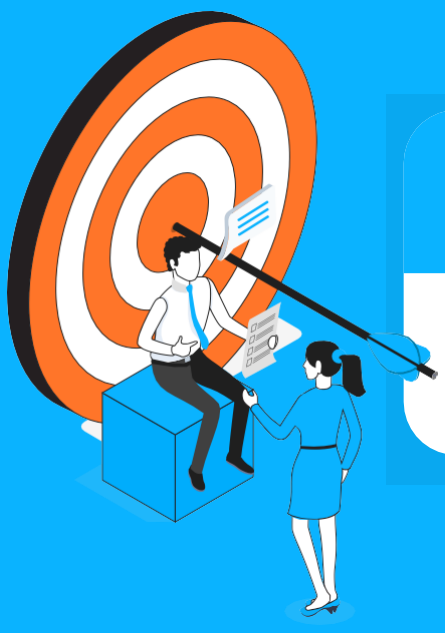
De toutes les phases nécessaires pour renforcer la sécurité de votre Active Directory (AD), l'audit en boîte blanche est sans doute l'une des étapes les plus indispensables et représentatives. Voici les 6 étapes clés pour réussir cet exercice : laissez-vous guider !

ÉTAPE 1

Régler les aspects juridiques

La procédure d'audit est très réglementée :

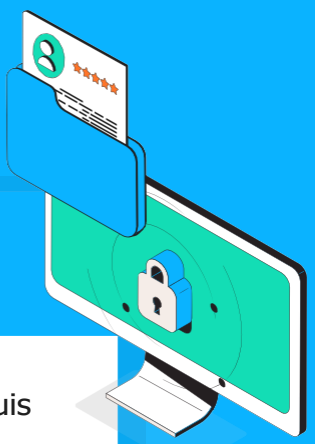
- La structure auditée doit officialiser le fait qu'elle accepte l'audit et que, dans certains cas, des simulations d'attaques peuvent être menées.



ÉTAPE 2

Identifier les besoins et spécificités du client

- Cette phase d'analyse permettra aux équipes de s'adapter et de mieux cibler les risques redoutés.



ÉTAPE 3

Récupérer les prérequis

En fonction de l'approche adoptée, les prérequis peuvent varier :

- Approche #1 - Test d'intrusion en boîte noire : seuls les accès au réseau sont nécessaires.
- Approche #2 - Test d'intrusion en boîte grise : il faut récupérer le compte utilisateur standard (et, en option le poste de travail).
- Approche #3 - Audit de conformité : il faut accéder au compte administrateur (ou à un extrait de la configuration des contrôleurs de domaine pour analyser).

ÉTAPE 4

Effectuer l'audit technique et organisationnel

Les tests techniques comprennent :

- la connexion sur le réseau ;
- le lancement des outils, pour identifier les vulnérabilités et les chemins qui mènent à l'AD.

Pour un test d'intrusion, cela consiste également à exploiter les chemins d'attaque identifiés pour valider si les risques associés sont avéré ou non.

L'audit organisationnel consiste en une interview :

- l'auditeur pose des questions sur la configuration de l'AD, afin de comprendre la maturité de l'entreprise vis-à-vis de son SI.

Les types de questions à poser

- Les procédures sont-elles rédigées et formalisées dans un document ?
- De quelle manière l'Active Directory est-il sécurisé et administré ?

ÉTAPE 5

Formaliser un rapport

L'auditeur récupère des preuves techniques et les réponses aux questions organisationnelles.

Il rédige un rapport dont l'objectif est :

- de mettre en exergue les points faibles et les points forts de ce qui a été trouvé sur le réseau ;
- d'attribuer un niveau de criticité aux vulnérabilités, en prenant en compte le contexte de l'entreprise et la priorité de traitement ;
- de proposer un plan d'action et de remédiation.

Meftez toutes les chances de votre côté !

- Nous vous recommandons de réaliser un audit en boîte blanche une fois par an, pour vous laisser le temps de renforcer votre sécurité et d'appliquer les mesures correctives.
- Pour résoudre toutes les failles de sécurité existantes, référez-vous à notre checklist dédiée à la reconstruction de votre Active Directory !

ÉTAPE 6

Déployer le plan d'action

Une fois le rapport reçu, l'entreprise déploie un plan d'action et une feuille de route pour les mesures correctives, selon les priorités et le niveau de criticité.

L'audit par boîte blanche est un processus qui demande une expertise poussée sur le sujet, et qui ne doit pas être sous-estimé – d'où l'importance de suivre ces quelques étapes pour le réussir !

Vous préférez laisser la main à des spécialistes ?

Advens vous accompagne

Advens
Security for the greater good