RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SERVICE ADS

1. DESCRIPTION DU SERVICE

L'ANSSI met à disposition des opérateurs réglementés et de la sphère publique une capacité d'audit des annuaires *Active Directory* (et Samba) au travers du service ADS (*Active Directory Security*).

Cette capacité vise à donner de la visibilité aux opérateurs réglementés et de la sphère publique (ministères, Opérateurs d'Importance Vitale, Opérateurs de Service Essentiel, collectivités territoriales, etc.) sur le niveau de sécurité de leur annuaire et à les accompagner dans son durcissement par l'application progressive de mesures adéquates. Cette prestation s'appuie sur l'expérience et l'expertise de l'agence sur les sujets d'*Active Directory* (AD) et s'est enrichie par sa participation aux différentes opérations de cyberdéfense.

Le service ADS permet ainsi à la fois de quantifier le niveau de sécurité de l'annuaire et d'accompagner progressivement les bénéficiaires vers un niveau de sécurité à l'état de l'art. Cette capacité est pensée à la fois pour les chaînes SSI et les équipes d'exploitation. Pour les premières, l'application fournit une vision globale et synthétique à travers des tableaux de bord et indicateurs associés ; pour les secondes, elle détaille les recommandations à appliquer et accompagne les bénéficiaires dans le pilotage de leurs équipes techniques ou de leurs prestataires.

À ce jour l'ANSSI constate une nette amélioration du niveau de sécurité des annuaires des bénéficiaires ayant souscrit à ADS dans la mesure où ce service permet un suivi régulier et continu du niveau de sécurité tout en contrôlant la bonne application dans le temps des recommandations.

2. MODALITÉS D'ACCÈS AU SERVICE

Pour bénéficier du service, la procédure à suivre est la suivante :

1	Faire la demande de création d'un compte nominatif à la plateforme **https://club.ssi.rie.gouv.fr** par email à **club@ssi.gouv.fr** en indiquant les coordonnées de la personne (nom, prénom, email, fonction et n° de téléphone mobile).
2	Télécharger la dernière version de l'outil de collecte ORADAD (Outil de Récupération Automatique de Données de l'Active Directory) sur GitHub [**https://github.com/ANSSI-FR/ORADAD/releases**].
3	Extraire les fichiers exécutables (exécutable ORADAD.exe et fichier de configuration).
4	Ouvrir un terminal et exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine. Le fichier de configuration doit être positionné dans le dossier contenant l'exécutable ORADAD.exe [commande à lancer : ORADAD.exe <outputDirectory>]. Le compte utilisé n'a pas besoin de privilèges spécifiques.
5	Téléverser les résultats sur le portail **https://club.ssi.rie.gouv.fr/** après s'être préalablement authentifié en cliquant sur « Téléverser des captures d'ORADAD » depuis la page d'accueil.

Dès réception des fichiers de collecte, l'ANSSI lancera les analyses et en partagera les résultats avec le bénéficiaire dans un délai de 15 jours, sous forme d'un rapport détaillé présentant les différents points de contrôle qui ont révélé des défauts de configuration pouvant entrainer des risques de sécurité.

DES QUESTIONS SUR LE SERVICE ?
Envoyer vos questions par email à **club@ssi.gouv.fr**

3. UNE APPROCHE LUDIQUE ET PERSONNALISÉE

Les résultats sont rendus disponibles depuis une interface web qui détaille et classe les vulnérabilités et recommandations afférentes. Lors de chaque audit, le niveau de sécurité de la configuration de l'*Active Directory* est traduit par un niveau qui se situe sur une échelle de 1 à 5. Le niveau obtenu dépend de la gravité des vulnérabilités trouvées, le niveau 1 étant synonyme de défauts critiques et le niveau 5 d'un niveau à l'état de l'art.

Un niveau donne ainsi accès à une liste de recommandations adaptées. L'évolution relative à chaque niveau est quantifiée par un score et représentée sur l'interface graphique par une barre de progression. Même si elle ne permet pas toujours d'accéder aux vulnérabilités et recommandations du niveau suivant, la correction progressive des vulnérabilités à un niveau donné, se traduit néanmoins par l'obtention de points. L'administrateur peut ainsi justifier de manière objective et factuelle que les actions menées améliorent significativement le niveau de sécurité de l'*AD* et donc du SI. L'application de l'ensemble des recommandations portant sur les points importants d'un niveau permet de passer au niveau supérieur et d'accéder à une collection complémentaire de recommandations.

Pour un échelon donné, l'application détaille trois niveaux d'indications :

- Des problèmes importants : vulnérabilités critiques ordonnées qui devront être corrigées pour passer au niveau supérieur ;
- Des points d'attention : mauvaises pratiques manifestes du point de vue de la sécurité, mais non prioritaires au vu des autres vulnérabilités identifiées à ce niveau ;
- Des points d'information : informations sur certains points-clé de l'AD.

	Les niveaux sont échelonnés de la façon suivante :
1	L'annuaire Active Directory présente des problèmes critiques de configuration qui mettent en danger immédiat l'ensemble des ressources hébergées. Des actions correctrices sont à prendre dans les plus brefs délais ;
2	L'annuaire Active Directory présente des lacunes de configuration et de gestion suffisantes pour mettre en danger l'ensemble des ressources hébergées. Des actions correctrices sont à prendre à court terme ;
3	L'annuaire Active Directory possède un niveau de sécurité basique non affaibli depuis son installation ;
4	L'annuaire Active Directory dispose d'un bon niveau de sécurité ;
5	L'annuaire Active Directory dispose d'un niveau de sécurité à l'état de l'art.

Par conséquent, l'enjeu devient majeur pour les opérateurs réglementés et sphère publique de mettre en place et de maintenir un niveau de sécurité satisfaisant de leurs annuaires. Ainsi, l'ambition de l'ANSSI est d'accompagner progressivement vers un niveau de sécurité à l'état de l'art grâce à l'application de recommandations adéquates et dans une approche plus ludique.

4. EN SAVOIR PLUS

L'annuaire Active Directory, centre névralgique de la sécurité des systèmes d'information Microsoft

L'annuaire *Active Directory* (*AD*) est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI.

Le faible niveau de sécurité des annuaires met en danger les systèmes d'information

Les prestations d'audit effectuées par l'ANSSI auprès de ses bénéficiaires font apparaître un manque de maturité critique et récurrent sur la sécurité des annuaires *Active Directory*. Ce défaut de sécurité affaiblit significativement le niveau global de sécurité de ces SI. Ce constat est renforcé par la connaissance acquise au contact des différents réseaux compromis sur lesquels l'agence est intervenue lors d'opérations de cyberdéfense. Au-delà du manque de maturité, l'agence note par ailleurs que le niveau de sécurité des annuaires *Active Directory* décroît en fonction du temps et du cycle de vie du SI.

Développement d'une capacité spécifique et ouverture d'un service

Au sein de l'agence, les prestations d'audit sur un système d'information donnent habituellement lieu à la rédaction d'un rapport détaillé, répertoriant à un temps les vulnérabilités qui touchent le système d'information, les recommandations correspondantes et la priorité de leur déploiement. Ces rapports, souvent volumineux, ne permettent pas toujours de prioriser avec aisance les actions à mener. Par ailleurs, si un audit évalue le niveau de sécurité à un instant donné, il ne mesure pas dans la durée l'évolution du niveau de sécurité.

Face à ce constat, l'ANSSI a développé une nouvelle capacité dont l'objectif est d'auditer, à la demande du bénéficiaire et de manière autonome, le niveau de sécurité des annuaires *Active Directory* des opérateurs stratégiques de l'État.