SÉCURITÉ DU NUMÉRIQUE
RETROUVEZ DE LA VISIBILITÉ SUR VOTRE ANNUAIRE

Cible : Administrateurs AD, CHAINE SSI

- L'ANSSI met à disposition des opérateurs stratégiques de l'État une capacité d'audit des annuaires Active Directory (et Samba) au travers du service ADS (Active Directory Security).
- Cette capacité vise à redonner de la visibilité aux opérateurs stratégiques de l'État (ministères, OIV, OSE, 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 est basée sur l'expérience et l'expertise du bureau audits sur les sujets d'Active Directory (AD), et enrichie par les différentes opérations de cyberdéfense auxquelles le bureau participe.
- Le service ADS permet ainsi à la fois d'objectiver le niveau de sécurité et d'accompagner progressivement les opérateurs vers un niveau de sécurité à l'état de l'art. Cette capacité est pensée à la fois pour les chaînes SSI et pour les chaînes exploitation. Pour les unes, l'application présente les tableaux de bord avec les indicateurs ; pour les autres, elle présente les recommandations détaillées à appliquer et accompagne les bénéficiaires dans le pilotage de leurs prestataires.

1 Bénéficier du service ADS ?

Pour bénéficier du service, la procédure à suivre est particulièrement simple.

1. 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**].
2. Extraire les fichiers exécutables (exécutable ORADAD.exe et fichier de configuration).
3. 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>].
4. Envoyer l'archive tar contenant les résultats de la collecte (et présent dans le répertoire outputDirectory) à l'adresse club@ssi.gouv.fr. Si la taille du fichier est supérieure à 10 Mo, l'ANSSI met à disposition un serveur d'*upload* sur lequel déposer le fichier. L'URL et les comptes permettant d'accéder au serveur sont fournis à la demande (email à adresser à l'adresse **club@ssi.gouv.fr**)

Dès réception du fichier de collecte, l'ANSSI lancera les analyses et en partagera les résultats 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.

2 ADS pour les nuls

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

L'annuaire Active Directory est l'élément qui permet de gérer de manière centralisée 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.

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE
RETROUVEZ DE LA VISIBILITÉ SUR VOTRE ANNUAIRE

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 récurrent sur la sécurité des annuaires Active Directory. Ce défaut de sécurité affaiblit significativement le niveau global de sécurité de ces SI. Cette observation est confortée 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, le bureau Audits constate 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 t 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 donne une idée du niveau de sécurité à un instant donné, il ne mesure pas durablement l'évolution du niveau de sécurité.

Face à ce constat, le bureau Audits 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 Active Directories des ministères.

Une approche ludique et personnalisée

Les résultats sont rendus disponibles depuis une interface web qui répertorie et ordonne 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 sur une échelle de 1 à 5. Le niveau obtenu découle immédiatement 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 un lot de recommandations adaptées. Une fois ces dernières mises en œuvre, des scripts de contrôle sont aussitôt référencés dans l'interface pour permettre à l'administrateur de contrôler de manière autonome et indépendante la bonne application des recommandations.

L'évolution relative à chaque niveau est objectivée 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 que ses actions améliorent significativement le niveau de sécurité de l'AD et donc du SI.

Considérant l'enjeu majeur pour un réseau qu'est la bonne sécurisation de son AD (et son maintien), l'idée 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 un contexte plus ludique (*gamification*).

3 En savoir plus

Envoyer un email à club@ssi.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle Graphisme, Fabrication, Image – DSAF/DPSG – Octobre 2019.