RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
REMÉDIATION

CYBERATTAQUES ET REMÉDIATION

LA REMÉDIATION DU TIER 0 ACTIVE DIRECTORY

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

TABLE DES MATIÈRES

V.0.0 – APPEL PUBLIC À COMMENTAIRES

INTRODUCTION

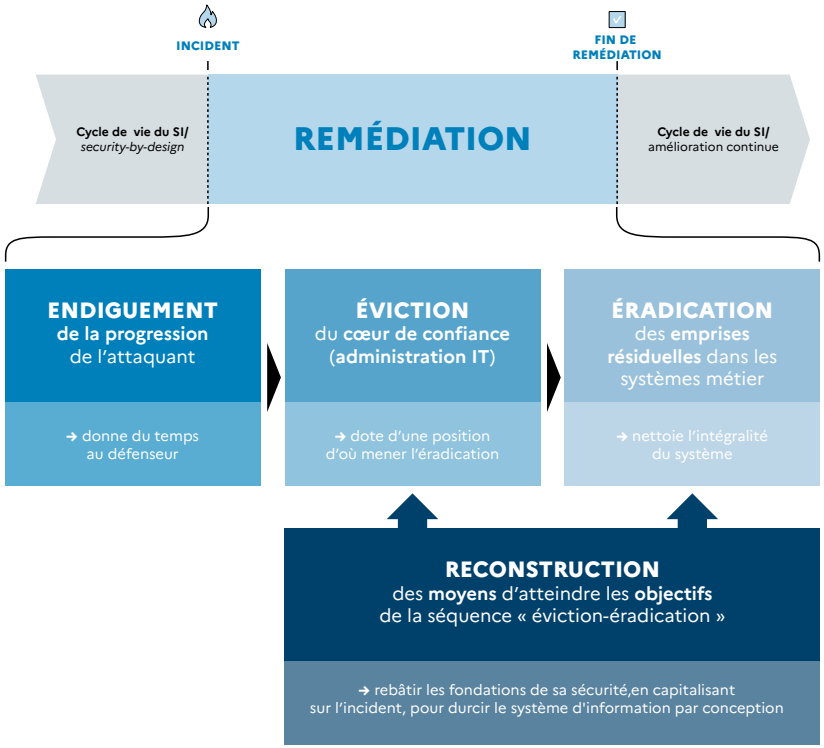
1 OBJET ET PÉRIMÈTRE DU DOCUMENT

L'objectif de cette publication est de fournir un cadre conceptuel aux opérations de remédiation qui succèdent aux incidents majeurs de sécurité informatique. La remédiation telle que considérée dans le présent document est la reprise de contrôle sur un système d'information (SI), s'appuyant sur Microsoft Active Directory, compromis dans le cadre d'un tel incident.

Ce document constitue un des volets techniques du corpus documentaire de l'ANSSI portant sur la remédiation. Il constitue une base technique présentant les piliers d'une opération de reconstruction du cœur de confiance[1] de l'Active Directory. Il est destiné à assister au déroulement du plan de remédiation en fournissant un ensemble synthétique de mesures clés à effectuer. Ainsi, il s'adresse principalement aux équipes techniques en charge de mettre en œuvre les opérations de reconstruction.

Reprenant la terminologie utilisée dans le volet opérationnel de ce corpus, la remédiation peut être résumée par le séquençage : endiguement, éviction, éradication, reconstruction ou « E3R ». Les opérations de remédiation du cœur de confiance de l'Active Directory s'inscrivent pour la plupart dans la séquence « éviction », sachant que d'autres actions de « reconstruction » sont menées en parallèle de cette phase. Cette étape est centrale dans la remédiation, puisqu'elle met le défenseur en position d'éradiquer totalement l'attaquant du SI.

1. Voir la définition, dans le chapitre 4. Concepts clés, b. Cœur de confiance.



L'objectif de ce document est de donner un cadre aux opérations de remédiation selon les trois scénarios présentés dans les volets stratégique et opérationnel :

SCÉNARIO 1 : « Restaurer au plus vite des services vitaux »

SCÉNARIO 2 : « Reprendre le contrôle du SI »

SCÉNARIO 3 : « Saisir l'opportunité pour préparer une maîtrise durable du SI »

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

En fonction du scénario choisi, des objectifs d'innocuité d'éviction et de sécurisation du Tier 0 doivent être définis[2]. Ces objectifs peuvent alors être atteints au travers d'actions techniques présentées dans ce document.

2 DESTINATAIRES DU DOCUMENT

Ce document s'adresse aux responsables de systèmes d'information et de la sécurité du SI amenés à piloter les aspects techniques d'une remédiation après un incident de sécurité des systèmes d'information.

Il est aussi destiné aux interlocuteurs des responsables : administrateurs, consultants, prestataires de services amenés à intervenir dans les opérations de remédiation et à réaliser les actions décrites dans le document.

3 LIMITES DU DOCUMENT

Ce document ne constitue pas une procédure de remédiation pas à pas.

Chaque incident de sécurité présente ses spécificités : mode opératoire de l'attaquant, impératifs métiers, etc. La feuille de route de la remédiation doit s'en nourrir et adapter les points d'attention techniques de ce document.

2. Voir le volet opérationnel du corpus, *Cyberattaques et remédiation : piloter la remédiation*.

De plus, les objectifs d'innocuité et de sécurisation peuvent parfois être garantis par des méthodologies différentes. Il est donc important de s'entourer d'experts Active Directory (support de l'éditeur, prestataires, etc.) en mesure de réaliser et d'adapter les actions décrites dans ce document ainsi que de diagnostiquer et de traiter les imprévus. Les impératifs de production et le contexte de crise ne doivent pas laisser place à l'improvisation de mesures techniques, lesquelles risqueraient de mettre en péril le bon fonctionnement du système au détriment de sa sécurité.

Les actions techniques d'éviction expliquées dans ce document traitent les chemins de contrôle les plus couramment utilisés par les attaquants. Des actions complémentaires, spécifiques à l'attaque en cours, peuvent être nécessaires pour finaliser l'éviction.

4 CONCEPTS CLÉS

a – Modèle d'administration en niveaux

Le modèle d'administration en niveaux se concentre sur la gestion de l'escalade non autorisée des privilèges dans un environnement Active Directory. Ce modèle, initialement proposé par Microsoft, définit trois niveaux d'administration qui sont les suivants :

Niveau Rouge, Tier 0, ou encore cœur de confiance de l'Active Directory, qui contient l'ensemble des ressources ayant un contrôle sur les identités de l'entreprise et donc sur l'ensemble des ressources intégrées à l'AD. Une démarche permettant de définir les éléments à intégrer dans le T0 est détaillée en annexe[3].

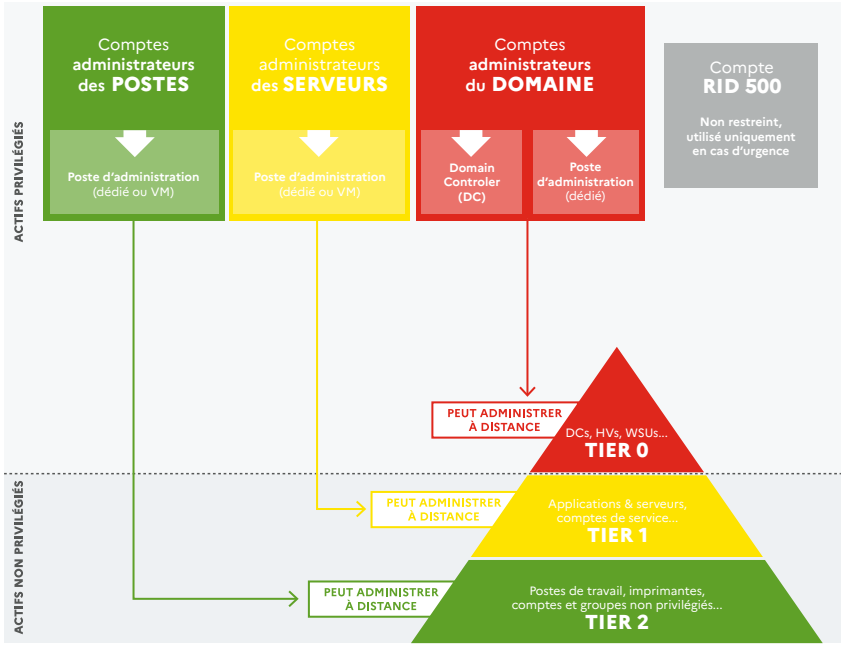
3. Voir l'annexe A. Démarche permettant de définir le périmètre du Tier 0 Active Directory.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Niveau jaune, ou Tier 1, qui contient l'ensemble des ressources ayant le contrôle des valeurs métier, incluant les serveurs et les applications de l'entreprise.

Niveau vert, ou Tier 2, qui contient l'ensemble des ressources ayant le contrôle des postes de travail utilisateurs et autres machines (les imprimantes par exemple).

Les principes d'un modèle d'administration en Tiers finalisé sont représentés dans la figure suivante :



b – Cœur de confiance

Dans ce document, l'expression « cœur de confiance » est utilisée pour désigner la partie d'un SI dont la compromission par un attaquant conduirait à une suspicion de compromission de l'ensemble du SI. Le cœur de confiance contient notamment : la gestion des identités, la gestion de la virtualisation, de l'administration, des composants assurant la supervision de sécurité. Les architectures sécurisées visent à minimiser la taille et la complexité du cœur de confiance afin d'en simplifier la sécurisation et de réduire les risques d'erreur de configuration. Ce caractère minimal du cœur de confiance est particulièrement important dans un incident, car chaque partie peut avoir fait l'objet de compromission.

Dans un environnement Active Directory, le cœur de confiance contient notamment le référentiel d'authentification, et par extension l'ensemble des ressources du Tier 0 telles que définies à la section précédente[4].

c – Groupes privilégiés

Dans un environnement Active Directory, les groupes natifs privilégiés sont les groupes d'administration et les groupes opératifs ayant le niveau de droits et de privilèges maximal sur la forêt ou pouvant se les attribuer :

- « administrateurs » ;
- « contrôleurs de domaine » ;
- « administrateurs du schéma » ;
- « administrateurs de l'entreprise » ;

4. Par abus de langage, le terme « cœur de confiance » sera parfois utilisé dans ce document pour désigner les contrôleurs de domaine et les ressources de Tier 0. Ces ressources, bien qu'appartenant au « cœur de confiance » n'en constituent qu'un sous-ensemble au regard de la définition donnée à cette expression dans cette section.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

- « administrateurs du domaine » : ces administrateurs ont les privilèges de lire la base des secrets de tous les comptes et donc d'extraire les secrets de l'ensemble des comptes privilégiés ;
- « administrateurs de clés » ;
- « administrateurs de clés de l'entreprise » : ces administrateurs peuvent fixer des valeurs arbitraires aux attributs relatifs à Windows Hello for Business, pour tous les utilisateurs sauf ceux protégés par le mécanisme d'adminSDHolder. Si l'authentification basée sur les certificats a été activée, ils peuvent générer un certificat sous leur contrôle, l'assigner à un compte privilégié (par exemple, un contrôleur de domaine), et s'authentifier en tant que lui ;
- « opérateurs de compte » : ces opérateurs peuvent administrer tous les comptes d'utilisateurs, les machines et les groupes, à l'exception des comptes protégés par l'*adminSDHolder* ;
- « opérateurs de serveur » : ces opérateurs peuvent administrer les contrôleurs de domaine, et donc récupérer les secrets de tous les comptes privilégiés ;
- « opérateurs de sauvegarde » : ces opérateurs peuvent sauvegarder un contrôleur de domaine et donc extraire les secrets de tous les comptes privilégiés depuis cette sauvegarde ;
- « opérateurs d'impression » : ces opérateurs peuvent charger des pilotes d'impression sur les contrôleurs de domaine et donc charger un pilote malveillant pour, par exemple, extraire les secrets de tous les comptes privilégiés.

La prise de contrôle de l'un de ces groupes[5] par un attaquant pourrait lui permettre de compromettre l'ensemble de la forêt, ce qui explique leur statut de cible prioritaire dans de nombreuses attaques.

5. Cette liste n'est pas exhaustive.

d – Chemin de contrôle

Un chemin de contrôle est composé d'un ensemble de relations de contrôle direct, où chaque relation traduit la maîtrise d'un objet sur un autre au travers d'une propriété particulière. Ainsi, les chemins de contrôle représentent des moyens pour un attaquant d'atteindre des cibles. Leur analyse permet d'identifier des déviances dans la gestion du domaine, de valider l'application d'un périmètre de sécurité autour des cibles considérées, mais également de révéler des moyens de persistance laissés par un attaquant après une compromission.

e – Recueil des points de contrôle Active Directory

Au sein de ce document sont faites plusieurs références vers le recueil des points de contrôle Active Directory, publié sur le site du CERT-FR[6] pour répondre au risque croissant auquel sont confrontés ces environnements. Ce recueil a vocation à être enrichi régulièrement en fonction des travaux de recherche, des pratiques constatées en audit, et de l'analyse des modes opératoires adverses.

5 STRUCTURE DU DOCUMENT

Ce document est structuré en quatre parties :

→ **« Actions techniques d'investigation du Tier 0 Active Directory »**

- Lors de la remédiation, il convient de s'assurer de l'absence de compromission d'éléments clés.
- Cette investigation permet d'identifier sur quelles ressources du SI l'éviction a besoin d'être menée.

→ **« Actions techniques d'éviction du Tier 0 Active Directory »**

- Cette section propose un ensemble d'objectifs techniques à atteindre en fonction du scénario de remédiation désiré. Ces objectifs visent à pallier les faiblesses de sécurité de l'Active Directory qui pourraient conduire, post-éviction, à une nouvelle compromission.

→ **« Actions techniques de supervision du Tier 0 Active Directory »**

- Concomitamment à la remédiation, la mise en place d'une supervision adéquate est essentielle et repose sur différents éléments présentés dans cette section.

→ **« Annexes »**

- Les annexes fournissent des documents pratiques pour mettre en œuvre les concepts proposés dans le corps du document.

6. Le recueil est consultable sur le site du CERT-FR : https://cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/

V.0.0 – APPEL PUBLIC À COMMENTAIRES

PARTIE I

ACTIONS TECHNIQUES D'INVESTIGATION DU TIER 0 ACTIVE DIRECTORY

Les objectifs techniques d'investigation pour le Tier 0 Active Directory sont de s'assurer qu'aucun élément malveillant ne soit répliqué du contrôleur de domaine compromis vers les contrôleurs de domaine pivot (contrôleur de domaine utilisé durant la remédiation pour permettre la réalisation de modifications de l'Active Directory sur un environnement isolé) et reconstruits.

Les investigations s'appuient notamment sur des captures réseaux et des collectes d'éléments système sur les contrôleurs de domaine.

Objectifs principaux de ces analyses :

→ **Au niveau réseau :**

- S'assurer qu'aucun script ou programme malveillant, manipulation de compte utilisateur, tentative d'exploitation de vulnérabilité ou comportement s'apparentant à un trafic illégitime ne se produise pendant les réplications (entre contrôleur compromis et pivot, ainsi qu'entre pivot et contrôleur reconstruit).
- Porter une attention particulière aux comportements pouvant s'apparenter à des mouvements latéraux entre les deux serveurs en cours de réplication.

→ **Au niveau système :**

- Vérifier qu'aucun binaire, scripts malveillant ou mécanisme de persistance d'un acteur malveillant ne soit présent sur les contrôleurs de domaine pivot et reconstruits. Un différentiel du domaine contrôleur pivot est effectué avant et après réplication afin de faciliter l'examen des différences potentielles.

Des levées de doute sont effectuées afin de qualifier les comportements inconnus ou ne correspondant pas aux attendus. Ces investigations techniques sont nécessaires et garantes du succès d'une éviction du Tier 0 Active Directory.

PARTIE II

ACTIONS TECHNIQUES D'ÉVICTION DU TIER 0 ACTIVE DIRECTORY

1 INTRODUCTION

Les actions techniques d'éviction du Tier 0 Active Directory décrites dans ce document sont réparties selon les trois scénarios de remédiation détaillés dans les documents stratégique et opérationnel de ce corpus documentaire[7].

Pour le cœur de confiance de l'Active Directory, ces trois scénarios ont différents objectifs :

Scénario 1 : « Restaurer au plus vite des services vitaux ».
L'objectif est une reprise d'activité rapide, par la suppression des accès de l'attaquant ayant été identifiés lors des analyses et par la restauration d'un cœur de confiance minimal.

Scénario 2 : « Reprendre le contrôle du SI ».
L'objectif est de supprimer les accès de l'attaquant, mais également de sécuriser l'Active Directory contre les schémas d'attaques les plus fréquemment exploités.

Scénario 3 : « Saisir l'opportunité pour préparer une maîtrise durable du SI ».
L'objectif est de mettre à profit l'éviction d'un attaquant pour reprendre le contrôle du pilotage du SI. Différentes mesures ayant pour objectif de réduire le risque de persistance de portes dérobées de l'attaquant sont alors mises en place, permettant ainsi de retrouver un bon niveau de confiance dans l'intégrité et la sécurité du Tier 0.

Il est à noter que dans un environnement Active Directory, la limite de sécurité est la forêt, et non le domaine. Les objectifs techniques d'éviction définis dans ce guide peuvent donc être considérés comme atteints uniquement lorsqu'ils ont été réalisés sur l'ensemble des do-

7. Voir l'annexe C : Structure du corpus documentaire.

maines d'une forêt compromise[8]. De plus, cette réalisation doit être effectuée en parallèle pour empêcher la compromission d'un domaine déjà remédié depuis un domaine ne l'étant pas encore.

Les actions techniques listées ne traitent que des chemins de contrôle les plus couramment utilisés par les attaquants. Des actions complémentaires, spécifiques à l'attaque en cours, peuvent être nécessaires pour finaliser l'éviction.

2 TABLEAU RÉCAPITULATIF DES ACTIONS TECHNIQUES D'ÉVICTION POUR LES DIFFÉRENTS SCÉNARIOS

ÉLÉMENT TECHNIQUE	SCÉNARIO 1	SCÉNARIO 2	SCÉNARIO 3
Absence de compromission des machines du Tier 0			
Réinstallation de l'ensemble des contrôleurs de domaine.		√	√
Réinstallation de l'ensemble des machines du Tier.		√	√
Suppression des chemins de contrôle dangereux vers les contrôleurs de domaine.	√	√	√
Suppression des chemins de contrôle dangereux vers les éléments d'infrastructure ayant un impact sur les contrôleurs de domaine.		√	√
Suppression des chemins de contrôle dangereux vers les serveurs MicrosoftDNS.	√	√	√
Suppression de toutes les délégations d'authentification vers les contrôleurs de domaine.	√	√	√
Sécurisation des RODC.	√	√	√
Renouvellement des secrets pour prévenir de l'utilisation de comptes compromis			
Compte administrateur par défaut.	√	√	√
Compte *krbtgt*.	√	√	√
Autres secrets permettant la prise de contrôle du Tier 0.	√	√	√
Comptes compromis ou suspectés d'être compromis.	√	√	√
Secrets des relations d'approbation.	√	√	√
Compte DSRM.		√	√
Clés KDS.		√	√

8. En fonction de l'architecture Active Directory, c'est donc plusieurs forêts qui devront potentiellement être reconstruites.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Configuration de l'Active Directory ne présentant pas de faiblesses permettant la prise de contrôle du Tier 0			
Montée du niveau fonctionnel de la forêt.		√	√
Durcissement de la configuration de l'annuaire.		√	√
Suppression des chemins de contrôle dangereux vers les objets privilégiés de l'annuaire.	√	√	√
Suppression des permissions dangereuses sur l'objet *adminSDHolder*.	√	√	√
Utilisation du protocole DFSR pour la réplication du SYSVOL.		√	√
Durcissement des objets privilégiés de l'annuaire			
Sécurisation des attributs des comptes privilégiés.		√	√
Réinitialisation des attributs *admincount*.			√
Assainissement des GPO s'appliquant aux objets privilégiés			
Configuration sécurisée pour les GPO s'appliquant à la racine du domaine.		√	√
Suppression des chemins de compromission vers les GPO s'appliquant aux objets privilégiés.	√	√	√

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

Absence de faiblesses dans la configuration des relations d'approbation			
Suppression des faiblesses dans la configuration des relations d'approbation.		√	√
Configuration des services privilégiés ne mettant pas en défaut le Tier 0			
Configuration des services privilégiés ne mettant pas en défaut le Tier 0.		√	√
Adoption de pratiques d'administration sécurisées			
Structure d'OU cohérente pour la sécurisation du T0.		√	√
Utilisation de comptes dédiés à l'administration du T0.	√	√	√
Politique de mots de passe robuste pour les comptes d'administration.	√	√	√
Réduction du nombre de comptes privilégiés.		√	√
Absence de chemins de contrôle vers les membres de groupes privilégiés.	√	√	√
Création de postes d'administration sécurisés.	√	√	√
Pratiques d'administration empêchant la présence de secrets des comptes privilégiés dans la mémoire des machines non T0.		√ (mesures organisationnelles)	√ (mesures techniques)

3 ABSENCE DE COMPROMISSION DES MACHINES DU TIER 0

a – Réinstallation de l'ensemble des contrôleurs de domaine

Les contrôleurs de domaines sont les éléments centraux de l'Active Directory puisque ce sont ces serveurs qui l'hébergent. À ce titre, un attaquant ayant placé des moyens de persistance sur l'un des contrôleurs de domaine aura la capacité de compromettre à nouveau l'Active Directory, immédiatement après son éviction.

Pour se prémunir d'un retour de l'attaquant par ce biais, il est nécessaire de réinstaller l'ensemble des contrôleurs de domaine. Les systèmes d'exploitation ainsi réinstallés doivent être mis à jour pour assurer l'absence de vulnérabilités connues sur les nouveaux systèmes.

Cette opération peut se faire sans interruption de service, en réinstallant les contrôleurs de domaine un par un et en s'appuyant sur la robustesse de disponibilité qu'offrent aujourd'hui les architectures Active Directory, ou en acceptant une interruption de service, par le biais d'un contrôleur de domaine pivot.

Dans le cas d'une réinstallation des contrôleurs de domaines sans interruption de service, il est à noter qu'il existe un risque que l'attaquant compromette les nouveaux contrôleurs de domaine durant la phase de déploiement des nouveaux contrôleurs.

Le cas d'une réinstallation des contrôleurs de domaine avec interruption de service doit suivre plusieurs principes pour être pleinement efficace :

- Les nouveaux contrôleurs de domaine, qui porteront l'Active Directory suite à l'éviction, ne doivent pas être exposés directement aux anciens contrôleurs de domaine. Pour ce faire, il est par exemple possible d'utiliser un contrôleur de domaine pivot, sur lequel les données de l'Active Directory sont répliquées puis assainies selon les autres mesures précisées dans ce document. Ce contrôleur de domaine pivot doit être spécifiquement protégé et/ou supervisé pour apporter les garanties d'innocuité souhaitées par la victime (absence de persistance sur le disque, d'exploitation en mémoire, etc). Les nouveaux contrôleurs de domaines répliquent alors les données de ce pivot.
- Un contrôleur de domaine ne doit jamais être en service au même moment que son remplaçant.

Un exemple d'éviction incluant la réinstallation des contrôleurs de domaine avec interruption de service est présenté en annexe[9].

b – Réinstallation de l'ensemble des machines du Tier 0

Suite à la mise en place du modèle d'administration en Tiers, les administrateurs ayant le plus haut niveau de droits et de privilèges, aussi appelés administrateurs Tier 0, sont amenés à se connecter aux différentes machines de ce Tier. Les contrôleurs de domaine, cités dans le point précédent, sont un cas de machines du Tier 0, mais ne sont pas les seules. Les postes d'administration des administrateurs Tier 0, ou encore les serveurs AD Connect, sont d'autres exemples de ces machines.

Dans l'hypothèse où un attaquant disposerait d'un moyen de persistance privilégié sur l'une de ces machines, il serait possible de récupérer en mémoire les secrets d'un administrateur Tier 0. La récupération d'un tel secret revient à compromettre l'Active Directory.

9. Voir l'annexe B. Exemple de déroulement d'une opération d'éviction du Tier 0 Active Directory mono-domaine.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Pour se protéger d'un tel retour de l'attaquant, il est nécessaire de réinstaller l'ensemble des machines du Tier 0 afin d'assurer l'absence de persistance sur celles-ci.

Le processus d'identification des machines à inclure dans le Tier 0 Active Directory est détaillé en annexe[10] de ce document.

c – Suppression des chemins de contrôle dangereux vers les contrôleurs de domaine

La présence d'un chemin de contrôle vers un contrôleur de domaine permet la prise de contrôle complète de l'Active Directory par les comptes concernés. Un attaquant peut, par exemple, répliquer l'ensemble des secrets (dont ceux des administrateurs de domaine), les réutiliser et ainsi prendre le contrôle complet d'un domaine.

Durant la remédiation, il convient de supprimer l'ensemble des chemins de contrôle vers les contrôleurs de domaine pour les utilisateurs qui ne sont pas membres des groupes privilégiés et sont confirmés comme étant légitimes.

d – Suppression des chemins de contrôle dangereux vers les éléments d'infrastructure ayant un impact sur le Tier 0

Différents éléments d'infrastructure peuvent permettre la prise de contrôle des éléments du Tier 0, notamment :

- les services de mise à jour WSUS s'appliquant aux contrôleurs de domaine ou autres machines du Tier 0 ;
- les hyperviseurs hébergeant les contrôleurs de domaine ou les autres machines du Tier 0 ;

10. Voir l'annexe A. Démarche permettant de définir le périmètre du Tier 0 Active Directory.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

- les produits d'éditeurs utilisant un agent déployé sur le contrôleur de domaine ou les autres machines du Tier 0, comme par exemple les antivirus.

Dans le cadre de l'éviction du Tier 0, et afin d'empêcher une élévation de privilèges par le biais de ces services, il est nécessaire de :

- supprimer les éléments non nécessaires à la sécurisation du Tier 0, comme par exemple les agents déployés sur les contrôleurs de domaine ;
- dédier les services d'infrastructures du Tier 0 strictement nécessaires et de les administrer à l'aide des comptes d'administration Tier 0.

e – Suppression des chemins de contrôle dangereux vers les serveurs MicrosoftDNS

Les comptes ayant le droit d'écrire les propriétés du conteneur *CN=MicrosoftDNS,CN=System* ont la possibilité de faire exécuter du code arbitraire par le service DNS. Ce service est généralement hébergé sur un contrôleur de domaine. Par défaut, les membres du groupe *DnsAdmins* disposent de ce droit et peuvent donc se rendre maîtres de tout contrôleur de domaine portant le rôle DNS.

Il est recommandé de retirer la permission d'écriture sur les propriétés du conteneur *CN=MicrosoftDNS,CN=System* pour les comptes disposant de tels chemins de contrôle.

Si la mise en place d'une telle permission a été faite pour la gestion du DNS, il est possible de créer une délégation manuellement. Si des permissions spécifiques sont nécessaires, il convient de considérer que les comptes ou les groupes délégués sont eux-mêmes privilégiés. Ainsi, ils doivent être correctement protégés et leurs permissions ap-

pliquées doivent être au moins aussi restrictives que celles appliquées à l'*adminSDHolder*.

Des compléments d'informations sur ce point peuvent être retrouvés dans le recueil des points de contrôle Active Directory[11].

f – Suppression des délégations d'authentification vers les contrôleurs de domaine

Les délégations d'authentification vers les contrôleurs de domaine peuvent être de plusieurs natures :

- contrainte sur le service d'un contrôleur de domaine ;
- contrainte avec transition de protocole vers un service d'un contrôleur de domaine ;
- contrainte portant sur des ressources, sur des contrôleurs de domaine.

Ces différents types de délégation, détaillés dans le recueil des points de contrôle Active Directory, peuvent permettre aux comptes qui les possèdent d'élever leurs privilèges auprès des contrôleurs de domaine. Ces délégations doivent donc être supprimées durant la phase de remédiation.

g – Sécurisation des contrôleurs de domaine en lecture seule (RODC)

Les RODC portent une partie des secrets de l'Active Directory et peuvent, en cas de compromission, entraîner la prise de contrôle complète du SI.

11. Voir les points de contrôle Active Directory sur le site du CERT-FR : https://cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Durant la phase de remédiation, il est recommandé de corriger les différentes faiblesses de configuration qui peuvent se retrouver sur les RODC, et notamment :

- les comptes ou les groupes privilégiés présents dans les attributs de révélation des RODC ;
- la configuration dangereuse des contrôleurs de domaine en lecture seule (RODC) (*neverReveal*) ;
- la configuration dangereuse des groupes de réplication pour les contrôleurs de domaine en lecture seule (RODC) (*allow*) ;
- la configuration dangereuse des groupes de réplication pour les contrôleurs de domaine en lecture seule (RODC) (*denied*).

4 RENOUVELLEMENT DES SECRETS POUR PRÉVENIR L'UTILISATION DE COMPTES COMPROMIS PAR L'ATTAQUANT

a – Compte administrateur par défaut

Le compte « Administrateur intégré » (RID 500) est totalement exempté de certaines stratégies de sécurité. Ceci permet, en ultime recours, d'utiliser ce compte pour corriger une éventuelle erreur de configuration. Ce compte a un rôle « bris-de-glace » et ne doit jamais être utilisé au quotidien.

Pour ce compte, il est recommandé de générer un mot de passe complexe, aléatoire et de le conserver dans un coffre qui pourra être accessible en cas de perte de la maîtrise de l'Active Directory.

Le mot de passe doit également être testé pour garantir qu'il sera utilisable le moment venu.

Il est recommandé de le changer après qu'il en aura été fait usage.

b – Compte *krbtgt*

Le compte *krbtgt* est un compte d'infrastructure servant de support de stockage aux clés des centres de distribution des clés Kerberos. La compromission du compte *krbtgt* permet à un attaquant de forger des tickets Kerberos (souvent appelés *golden tickets*) et de pouvoir ainsi s'authentifier auprès de n'importe quelle ressource (serveur, poste de travail, etc.) du domaine Active Directory avec des droits d'administration, et ce, de manière relativement furtive. Le mot de passe du compte *krbtgt* n'étant pas changé automatiquement, si la base des comptes de l'Active Directory a été extraite (par exemple par un ancien administrateur, lors d'un audit ou pour un test de robustesse des mots de passe), il est possible, tant que ce mot de passe n'a pas été changé, d'utiliser les informations contenues dans la base afin d'en extraire les secrets. Une personne malveillante peut ainsi s'authentifier sur l'ensemble des services du domaine Active Directory plusieurs années après l'extraction de la base.

Le changement de mot de passe doit être effectué **deux fois** pour être efficace.

⚠ **Attention :** toute opération de changement du mot de passe du compte *krbtgt* doit être effectuée uniquement dans un environnement Active Directory où la réplication entre les contrôleurs de domaine est nominale. Ainsi, il est indispensable d'attendre un délai permettant la réplication du changement avant le deuxième changement de mot de passe.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

c – Compte d'administrateur du mode de restauration des services d'annuaire (DSRM)

Directory Services Restore Mode (DSRM) est une fonctionnalité des contrôleurs de domaine Active Directory permettant de conserver un accès de type « bris-de-glace » sur ces machines. Le mot de passe du compte utilisé par le service peut être différent pour chacun des contrôleurs de domaine.

Dans le cas où les contrôleurs de domaine ne sont pas réinstallés, il est recommandé de renouveler le mot de passe du compte DSRM sur chacun des contrôleurs.

Dans le cas où les contrôleurs de domaine sont réinstallés, il est recommandé d'attribuer un mot de passe différent des précédents pour le compte DSRM.

Comme pour le compte administrateur par défaut, il est recommandé de générer un mot de passe complexe, aléatoire et de le conserver dans un coffre qui pourra être accessible en cas de perte de la maîtrise de l'Active Directory. Le mot de passe doit également être testé pour garantir qu'il sera utilisable le moment venu.

d – Clés KDS

Pour assurer l'absence de porte dérobée utilisant des comptes de service administrés de groupe (gMSA), il est nécessaire d'ajouter une nouvelle clé racine au service de distribution de clés (KDS) puis de renouveler l'ensemble des comptes de service administrés de groupe faisant partie du Tier 0.

e – Secrets des relations d'approbation

Les secrets des différentes relations d'approbation configurées entre les domaines de la forêt et ceux d'autres forêts doivent également être renouvelés. Pour ce faire, il est nécessaire de renouveler les secrets du côté de l'approbation entrante puis d'utiliser le même mot de passe du côté de l'approbation sortante.

f – Autres secrets permettant la prise de contrôle du Tier 0

Pour protéger l'Active Directory d'une nouvelle compromission directe par utilisation d'un compte contrôlé par l'attaquant avant l'éviction, il est nécessaire de renouveler l'ensemble des secrets (mots de passe, certificats des cartes à puces, etc.) pouvant permettre la prise de contrôle du Tier 0, de manière directe ou indirecte. Cela inclut les comptes utilisateurs mais également les comptes de service et les comptes machines.

À titre d'exemple, les secrets suivants doivent être renouvelés s'ils sont présents dans l'infrastructure :

- un compte MSOL utilisé par le service AD Connect ;
- des clés privées utilisées par les autorités de certifications présentes dans le conteneur *NtAuthCertificate* ;
- un compte machine du serveur WSUS utilisé pour maintenir à jour les contrôleurs de domaine.

g – Comptes suspects identifiés durant l'investigation

De la même manière, il est recommandé de renouveler les secrets de l'ensemble des comptes suspects identifiés durant les investigations afin d'empêcher leur réutilisation.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

5 CONFIGURATION DE L'ACTIVE DIRECTORY NE PRÉSENTANT PAS DE FAIBLESSES ET PERMETTANT LA PRISE DE CONTRÔLE DU TIER 0

a – Montée du niveau fonctionnel de la forêt

Dans les environnements Active Directory, certains mécanismes sont liés aux niveaux fonctionnels qui peuvent être au niveau forêt ou domaine. Les niveaux fonctionnels sont caractérisés par un chiffre allant de 0 (Windows 2000) à 7 (Windows 2016/2019). Afin de bénéficier des dernières fonctionnalités de sécurité, il est important d'augmenter les niveaux fonctionnels des domaines ainsi que de la forêt. Chaque niveau fonctionnel apporte des fonctionnalités de sécurité :

- **Niveau de fonctionnalité 2** (Windows 2003) : ajoute les relations d'approbation de forêts et le support des contrôleurs de domaine en lecture seule (RODC).
- **Niveau de fonctionnalité 3** (Windows 2008) : permet la prise en charge des algorithmes de chiffrement robustes comme AES et DFS pour la réplication des partages SYSVOL.
- **Niveau de fonctionnalité 4** (Windows 2008R2) : permet l'utilisation de la fonctionnalité de corbeille AD (protection contre les suppressions accidentelles d'objets).
- **Niveau de fonctionnalité 5** (Windows 2012) : permet l'utilisation des fonctionnalités avancées de Kerberos comme l'authentification composée et les *claims*.
- **Niveau de fonctionnalité 6** (Windows 2012R2) : introduit de nombreuses fonctionnalités de sécurité comme les politiques et silos d'authentification et le groupe *Protected Users*.

- **Niveau de fonctionnalité 7** (Windows 2016/2019/2022) : améliore la sécurité des comptes lorsque l'authentification par carte à puce est utilisée et ajoute les relations d'approbation de forêt de type *Privileged Identity Management* (PIM).

Pour augmenter le niveau fonctionnel d'un domaine il est nécessaire de mettre à niveau l'ensemble des contrôleurs de domaine vers un système d'exploitation supportant le niveau désiré et de réaliser une migration au niveau fonctionnel supérieur.

De même, pour augmenter le niveau fonctionnel d'une forêt il est nécessaire que l'ensemble des domaines soient dans un niveau fonctionnel équivalent ou supérieur.

> **Note :** il est nécessaire de vérifier la compatibilité du niveau fonctionnel avec les logiciels utilisés au sein du SI, comme par exemple Microsoft Exchange[12].

b – Durcissement de la configuration de l'annuaire

Les paramètres de configuration de l'annuaire agissant sur la sécurité de l'environnement Active Directory doivent être positionnés à des valeurs ne mettant pas en danger le Tier 0. À titre d'exemple, les paramètres dangereux configurés dans la propriété *dSHeuristics* doivent être modifiés et réinitialisés à leur valeur par défaut :

- *fLDAPBlockAnonOps* ne doit pas être configuré ou avoir une valeur différente de 2 ;
- *fAllowAnonNSPI* doit valoir 0 ;

12. Voir le site de Microsoft, « *Exchange Server supportability matrix* », URL : https://docs.microsoft.com/en-us/exchange/plan-and-deploy/supportability-matrix?view=exchserver-2019

V.0.0 – APPEL PUBLIC À COMMENTAIRES

- *dwAdminSDExMask* doit valoir 0.

c – Suppression des chemins de contrôle dangereux vers les objets privilégiés de l'annuaire

La possession d'un chemin de contrôle vers un objet privilégié de l'annuaire peut permettre à un attaquant la prise de contrôle complet de l'Active Directory. Parmi ces objets privilégiés, se retrouvent notamment :

- la racine des *naming contexts* ;
- les clés DPAPI ;
- les clés gMSA ;
- les paramètres DFSR du SYSVOL ;
- les objets du schéma.

Les chemins de contrôles vers ces objets doivent ainsi être corrigés pour l'ensemble des objets n'étant pas légitimement membres du Tier 0.

d – Suppression des permissions dangereuses sur l'objet *adminSDHolder*

Les permissions de l'objet *adminSDHolder* sont régulièrement appliquées sur l'ensemble des objets protégés (membres des groupes administratifs et opératifs) de l'Active Directory. Par défaut, seuls les objets privilégiés possèdent des droits sur l'objet *adminSDHolder*. Ainsi, ce mécanisme permet de protéger les utilisateurs et les groupes les plus privilégiés de l'Active Directory.

Il est fortement déconseillé de changer les permissions par défaut de cet objet, la présence de permissions dangereuses pouvant casser l'étanchéité du Tier 0 dans un modèle d'administration en niveaux.

Ainsi, il est recommandé d'enlever les permissions dangereuses sur l'objet *adminSDHolder* afin de revenir à un état par défaut.

e – Utilisation du protocole DFSR pour la réplication du SYSVOL

Il est recommandé d'utiliser uniquement le mécanisme *Distributed File System Replication* (DFSR) pour synchroniser des répertoires sur différents serveurs, en particulier pour la réplication du SYSVOL.

Le protocole NTFRS est quant à lui obsolète et rajoute inutilement des interfaces d'administration aux contrôleurs de domaine. De plus, ce protocole n'est plus supporté par les dernières versions de Windows Server, ce qui empêche la migration vers les dernières versions. La désactivation de ce protocole est donc recommandée.

Le processus de migration vers DFSR est documenté par Microsoft[13].

6 DURCISSEMENT DES OBJETS PRIVILÉGIÉS DE L'ANNUAIRE

a – Sécurisation des attributs des comptes privilégiés

Les comptes privilégiés doivent être protégés pour empêcher leur compromission à la suite de l'éviction. Pour ce faire, un certain nombre d'attributs doivent être regardés. Le recueil des points de contrôle Active Directory détaille les différents attributs dangereux des comptes utilisateurs, notamment au travers des points de contrôle suivants :

13. Voir le site de Microsoft, « *Exchange Server supportability matrix* », URL : https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/migrate-sysvol-to-dfsr

- comptes privilégiés sans pré-authentification Kerberos ;
- comptes utilisateurs avec un chiffrement Kerberos faible ;
- comptes ou groupes ayant un historique de SID d'apparence non conforme ;
- comptes privilégiés avec SPN ;
- comptes avec un PrimaryGroupID modifié ;
- comptes privilégiés dont le mot de passe n'expire jamais ;
- comptes ayant leur mot de passe stocké de manière réversible.

b – Réinitialisation des attributs *admincount*

L'attribut *admincount*, positionné sur les objets utilisateurs, permet d'indiquer l'appartenance actuelle ou passée de l'utilisateur à l'un des groupes protégés[14]. Lors de l'ajout de l'utilisateur dans l'un de ces groupes protégés, l'attribut *admincount* est positionné à 1. Cette valeur de 1 est également réappliquée toutes les heures tant que l'utilisateur appartient à au moins l'un de ces groupes.

Lorsque l'utilisateur est retiré de l'ensemble des groupes protégés auquel il appartient, l'attribut *admincount* n'est plus modifié, et conserve sa valeur de 1. Ce mécanisme peut alors permettre d'identifier une élévation de privilèges temporaire d'un compte dans l'un des groupes protégés.

Lors de l'éviction du Tier 0, il est alors nécessaire de réinitialiser les attributs *admincount* des utilisateurs n'appartenant plus à aucun groupe protégé. Pour ce faire, il faut attribuer la valeur de 0 dans cet attribut.

14. Voir le site de Microsoft, « Annexe C : Comptes protégés dans Active Directory », URL : https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory#appendix-c-protected-accounts-and-groups-in-active-directory-1

7 ASSAINISSEMENT DES GPO S'APPLIQUANT AUX OBETS

a – Configuration sécurisée pour les GPO s'appliquant à la racine du domaine

Les GPO s'appliquant à la racine du domaine s'appliquent par défaut à l'ensemble des objets du domaine, y compris les objets privilégiés. Ces GPO doivent être vérifiées pour assurer que la configuration qu'elles appliquent n'entraîne pas de faiblesse de sécurité pouvant permettre la prise de contrôle des objets privilégiés.

b – Suppression des chemins de compromission vers les GPO s'appliquant aux objets privilégiés

Un attaquant ayant le contrôle d'une GPO peut l'utiliser afin d'exécuter du code sur les machines des utilisateurs sur lesquels elle s'applique et élever ses privilèges.

Les permissions positionnées sur les objets GPO s'appliquant aux objets privilégiés doivent donc être revues pour empêcher toute re-compromission de l'Active Directory par ce biais.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

8 SUPPRESSION DES FAIBLESSES DANS LA CONFIGURATION DES RELATIONS D'APPROBATION

Les relations d'approbation avec un domaine externe peuvent être sources de compromission si elles présentent des faiblesses de configuration. Un attaquant compromettant un domaine externe concerné peut usurper l'identité de n'importe quel utilisateur ou n'importe quelle machine du domaine (sauf comptes ayant un RID inférieur à 1000, ce qui exclut les utilisateurs ou les groupes présents par défaut). Il est alors possible pour cet individu malveillant d'accéder à l'ensemble des données du domaine. Si un chemin de contrôle existe pour le compte usurpé, il peut également élever ses privilèges vers « Administrateurs du domaine » et ainsi compromettre l'ensemble de la forêt.

Le recueil des points de contrôle Active Directory détaille les différentes configurations dangereuses et devant être évitées pour les relations d'approbation, notamment au travers des points de contrôle suivants :

- relations d'approbation sortantes de type domaine non filtré ;
- relations d'approbation sortantes de type forêt avec SID History activé ;
- relations d'approbation entrantes avec délégation ;
- comptes de relation d'approbation dont le mot de passe est inchangé depuis plus d'un an.

9 CONFIGURATION DES SERVICES PRIVILÉGIÉS NE METTANT PAS EN DÉFAUT LE TIER 0

En complément des contrôleurs de domaine et des comptes administrateurs du domaine, le Tier 0 doit inclure l'ensemble des comptes, des machines et des services pouvant permettre une élévation de privilèges maximale sur le domaine.

Par défaut, différents services disposent de privilèges importants pouvant permettre la compromission du cœur de confiance Active Directory. C'est par exemple le cas :

- du service DNS, souvent installé sur les contrôleurs de domaine, et dont certaines configurations peuvent mettre en défaut le Tier 0 ;
- de l'Active Directory Certificate Services (ADCS), qui, s'il est mal configuré, peut entraîner la présence de chemins de contrôle vers les conteneurs ou les modèles de certificats ;
- du service AD Connect, qui dispose dans certaines configurations des privilèges de réplication de l'ensemble des utilisateurs du domaine ;
- des serveurs WSUS depuis lesquels les contrôleurs de domaine ou les autres machines du Tier 0 récupèrent leurs mises à jour ;
- des serveurs de sauvegarde de l'Active Directory ;
- de nombreux services proposés par des éditeurs et demandant pour être installés de délégations de privilèges importantes sur le domaine, allant parfois jusqu'à la possession de comptes administrateurs du domaine.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

Pour l'ensemble des services ayant une capacité d'élévation de privilèges sur le cœur de confiance de l'Active Directory, il est nécessaire, par ordre de préférence de :

- limiter les privilèges au maximum en mettant en place les délégations de privilèges strictement nécessaires afin de leur retirer les délégations dangereuses, souvent non nécessaires pour le bon fonctionnement du service ;
- considérer les services comme appartenant au Tier 0 et leur appliquer les mêmes principes de durcissement que pour les autres éléments du Tier 0 (administration par les administrateurs Tier 0 et depuis les postes d'administration Tier 0 notamment).

10 ADOPTION DE PRATIQUES D'ADMINISTRATION SÉCURISÉES

a – Structure d'unités organisationnelles permettant la sécurisation du Tier 0

Pour faciliter la gestion et la sécurisation des éléments du Tier 0, il est recommandé de mettre en place une structure d'unités organisationnelles claire et respectant les principes suivants :

- l'organisation des unités organisationnelles (OU) dans l'annuaire doit permettre l'application de GPO aux seuls objets privilégiés et assurer que les GPO des autres éléments du domaine ne s'appliquent pas aux objets privilégiés (en dehors de la GPO du domaine par défaut) ;
- les contrôleurs de domaine doivent être conservés dans leur unité organisationnelle par défaut.

b – Utilisation de comptes dédiés à l'administration

L'administration des éléments du Tier 0 doit être réalisée à l'aide de comptes dédiés, identifiés comme administrateurs Tier 0. Ces comptes d'administration disposant des privilèges maximums sur le domaine (privilèges administrateurs de domaine), doivent être particulièrement sécurisés. De plus, ces comptes doivent exclusivement être utilisés pour la réalisation des actions d'administration nécessitant les plus hauts niveaux de droits et de privilèges. Ils doivent se connecter uniquement aux machines du Tier 0 afin d'éviter leur mise en danger et aucune exception n'est tolérée.

c – Politique de mots de passe robuste pour les comptes privilégiés

Comme indiqué dans le point précédent, les comptes privilégiés doivent faire l'objet d'une sécurisation particulière, commençant par la mise en place d'une politique de mots de passe robuste[15].

d – Réduction du nombre de comptes privilégiés

La prolifération des comptes privilégiés est une mauvaise pratique. Elle complexifie leur supervision, augmente les risques d'erreurs de configuration, de désactivation ou de suppression d'un compte, élargit les chemins de contrôle, etc.

Les groupes privilégiés de l'Active Directory permettent aux utilisateurs qui en sont membres de posséder tous les droits et les privilèges sur la forêt. L'utilisation de ces groupes, à l'exception des groupes « Administrateurs » et « Administrateurs du domaine », procure donc un faux sentiment de sécurité.

15. Voir les Recommandations relatives à l'authentification multifacteurs et aux mots de passe sur le site de l'ANSSI : https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/

V.0.0 – APPEL PUBLIC À COMMENTAIRES

Il est nécessaire de mettre en place un modèle d'administration permettant de réduire le nombre de comptes privilégiés. Pour cela, il convient de référencer les besoins d'administration de chaque compte et de faire les délégations *ad hoc*.

e – Suppression des chemins de contrôle vers les membres des groupes privilégiés

La présence d'un chemin de contrôle vers un membre de groupes privilégiés est un moyen direct pour un attaquant de reprendre le contrôle de l'Active Directory.

Durant la remédiation, il convient d'identifier et de supprimer l'ensemble des chemins de contrôle vers les membres des groupes privilégiés de domaine pour empêcher une nouvelle compromission par ce biais.

f – Création de postes d'administration sécurisés

Les actions d'administration du Tier 0, effectuées par les administrateurs Tier 0, doivent être initiées depuis des machines dédiées à cette administration. Ces machines, appelées postes d'administration Tier 0, doivent être sécurisées en respectant les principes suivants[16] :

- Ces postes doivent être maîtrisés, les pratiques de type BYOD étant à proscrire.
- Dans le cas où le poste mutualise un environnement d'administration Tier 0 et un ou plusieurs autres environnements (bureautique par exemple) par le biais d'un mécanisme de virtualisation ou de conteneurisation, le cloisonnement des environnements doit être réalisé par des mécanismes

16. Voir aussi les Recommandations relatives à l'administration sécurisée des systèmes d'information sur le site de l'ANSSI : https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/

évalués comme étant de confiance au niveau du système. Notamment, le passage d'un niveau de sensibilité bas (l'un des autres environnements) vers un niveau de sensibilité haut (l'environnement d'administration Tier 0) ne doit pas être possible.

- Dans le cas où une solution d'accès distant est utilisée, celle-ci ne doit pas permettre le passage d'un niveau de sensibilité bas (réseau bureautique par exemple) vers un niveau de sensibilité haute (poste d'administration Tier 0 par exemple).
- Aucun accès Internet, et notamment mail, ne doit être possible depuis ce poste d'administration.
- Le poste d'administration doit être durci au niveau de son socle logiciel et de sa configuration.
- Le disque dur du poste d'administration doit être chiffré.
- Le poste doit utiliser un système d'exploitation supporté, maintenu à jour par le même mécanisme que les contrôleurs de domaine (serveur WSUS identique par exemple).

g – Pratiques d'administration empêchant la présence de secrets des comptes privilégiés dans la mémoire des machines ne faisant pas partie du Tier 0

Les pratiques d'administration du Tier 0, ayant dans la plupart des cas eu un impact sur l'incident en cours de remédiation, doivent évoluer pour protéger le cœur de confiance de l'Active Directory d'une nouvelle compromission.

L'objectif d'une telle évolution est l'absence de mise en danger du Tier 0 grâce à l'utilisation de pratiques d'administration ne permettant pas la présence de secrets privilégiés sur des machines n'appartenant pas à ce Tier 0.

Dans un premier temps, seules des mesures organisationnelles peuvent être mises en place pour former les administrateurs à utiliser les comptes d'administration Tier 0 exclusivement sur les machines du Tier 0.

Dans un second temps, différentes technologies peuvent être étudiées pour empêcher tout écart (délibéré ou accidentel) à ces mesures organisationnelles. Par exemple, les technologies pouvant être retrouvées sont :

- la mise en place de silos d'authentification ;
- le mode « Restricted Admin » pour les connexions RDP ;
- la solution LAPS (*Local Administrator Password Solution*) ;
- le mécanisme « djoin » pour la création et jointure de nouvelles machines ;
- l'utilisation du groupe de sécurité « Protected Users ».

PARTIE III

ACTIONS TECHNIQUES DE SUPERVISION DU TIER 0 ACTIVE DIRECTORY

Dans le cadre de la mise en place du Tier 0, des secrets sont renouvelés car potentiellement possédés par l'attaquant. Si l'attaquant cherche à utiliser les anciens secrets, des erreurs seront générées et journalisées.

Par exemple, les traces suivantes pourraient être générées par un attaquant :

- erreur d'authentification à l'utilisation d'un mot de passe renouvelé ;
- erreur de demande de ticket Kerberos en cas de vol du *krbtgt* ;
- erreur d'authentification sur un compte dans un silo depuis une machine non-autorisée.

Ces événements peuvent permettre d'identifier un attaquant disposant encore d'accès au SI. L'élargissement du périmètre à l'ensemble des systèmes compromis, voire à l'ensemble du SI permet d'identifier où l'attaquant est encore présent et quelles sont les activités qu'il conduit pour poursuivre ses objectifs ou pour reprendre le contrôle du Tier 0.

La mise en place d'une politique de journalisation au bon niveau doit dans ce cas être envisagée. Les technologies Microsoft de centralisation des journaux sont intéressantes à déployer dans ce cadre car robustes et silencieuses du point de vue système.

Pour mettre en place cette journalisation, l'ANSSI a produit un guide[17] et fournit des ressources[18] telles que des scripts de configuration et une sélection d'événements pertinents pour la détection d'intrusion. Ce guide explique comment configurer un serveur pour qu'il assure le rôle de collecteur de journaux, et comment déployer une GPO pour que tous les ordinateurs du domaine envoient leurs journaux aux collecteurs.

17. Guide de l'ANSSI *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnements Active Directory*, 2022.

18. GitHub de l'ANSSI : https://github.com/ANSSI-FR/guide-journalisation-microsoft

Une fois la journalisation mise en place, il est nécessaire d'indexer les données dans un puit de log ou SIEM. Chaque fournisseur dispose d'outils pour l'ingestion des journaux et pour assurer une normalisation des données. Par ailleurs ces SIEM sont accompagnés d'un ensemble de règles par défaut qu'il convient d'affiner pour qu'elles ne génèrent pas trop de faux positifs[19].

19. Voir l'annexe C du guide de l'ANSSI : *Recommandations de sécurité pour l'architecture d'un système de journalisation*, 2022.

ANNEXES

A DÉMARCHE PERMETTANT DE DÉFINIR LE PÉRIMÈTRE DU TIER 0 ACTIVE DIRECTORY

Le Tier 0 Active Directory est défini comme l'ensemble des ressources ayant un contrôle sur les identités de l'entreprise et donc sur l'ensemble des ressources intégrées à l'AD. Pour le définir de manière précise, il est alors nécessaire de mener une réflexion itérative pour identifier les ressources pouvant prendre le contrôle de celles inclues au périmètre du Tier 0 actuel, jusqu'à ce que ce périmètre ne grossisse plus.

L'identification des ressources devant être intégrées au Tier 0 doit par exemple s'appuyer sur les éléments de réflexion suivants :

1. Les contrôleurs de domaine sont automatiquement inclus dans le Tier 0 puisque portant l'annuaire Active Directory.

2. Les comptes administrateurs de domaine ont la possibilité d'agir sur les contrôleurs de domaine, et doivent donc être également ajoutés au Tier 0.

3. Ces comptes sont utilisés depuis des postes d'administration dédiés, sur lesquels ils se connectent, laissant ainsi des éléments d'authentification. Les postes d'administration sont donc également à ajouter au Tier 0.

4. De plus, certains contrôleurs de domaine sont virtualisés. La possession de privilèges sur l'hyperviseur permet alors par exemple d'accéder au disque ou à la mémoire des contrôleurs de domaine. Les hyperviseurs sur lesquels sont virtualisés des contrôleurs de domaine doivent donc également être ajoutés au périmètre.

5. Certains contrôleurs de domaine disposent quant à eux d'interfaces iLO dont l'accès peut permettre la récupération des éléments de l'annuaire. Ces interfaces et les comptes associés sont donc inclus dans le Tier 0.

6. Un antivirus est installé sur les contrôleurs de domaine. Depuis la console antivirale, il est possible d'exécuter du code sur les machines disposant d'un agent, en l'occurrence les contrôleurs de domaine. La console antivirale, ainsi que le serveur sur lequel elle est installée, sont donc également à ajouter au périmètre du Tier 0.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

À la suite de cette identification, il est recommandé de minimiser le périmètre du Tier 0 en ayant pour objectif initial de le limiter aux seules ressources Microsoft, et en ajoutant d'éventuelles exceptions si elles sont jugées nécessaires. Ces exceptions, comme par exemple une solution de sauvegarde des contrôleurs de domaine, doivent alors être administrées selon les mêmes principes que les autres machines du Tier 0 et ne doivent pas le mettre en danger. Il est alors souvent recommandé de dédier ces solutions aux seules machines du Tier 0.

Dans l'exemple précédent, des hyperviseurs sont intégrés au périmètre du Tier 0. Dans le cas où une garantie doit être apportée face à une menace d'échappement de machine virtuelle (compromission de l'hyperviseur ou d'une machine virtuelle depuis une autre machine virtuelle), il est alors nécessaire de dédier les hyperviseurs en question aux seules machines du Tier 0.

Les contrôleurs de domaine étant les éléments les plus critiques du SI, il convient également de limiter, voire de proscrire, l'utilisation de logiciels tiers sur ceux-ci. Ces logiciels augmentent en effet la surface d'attaque des contrôleurs de domaine et sont souvent substituables par de la configuration ou des scripts. Par exemple, il est préférable d'exporter les journaux d'événements depuis les contrôleurs de domaine vers une machine dédiée, de générer et de chiffrer les sauvegardes localement avant de les envoyer vers une solution de stockage, d'utiliser uniquement les solutions antivirales intégrées au système d'exploitation, etc.

B EXEMPLE DE DÉROULEMENT D'UNE OPÉRATION D'ÉVICTION DU TIER 0 ACTIVE DIRECTORY MONO-DOMAINE

Les garanties d'innocuité et de sécurisation d'une opération de remédiation peuvent être atteintes de différentes manières. L'exemple suivant ne vise donc pas à imposer une méthodologie, ni même à détailler une procédure complète, mais à présenter les étapes clés d'un exemple d'opération d'éviction sur une forêt mono-domaine avec interruption de service.

Avant toute opération d'éviction, il est recommandé d'éteindre entièrement le SI afin de limiter les applications dont le fonctionnement peut être altéré de manière définitive du fait de l'absence de contrôleurs de domaine. À titre d'exemple, les serveurs Exchange peuvent s'avérer irrécupérables s'ils ne sont pas éteints durant l'opération. L'utilisation d'Exchange sans contrôleurs de domaine n'est d'ailleurs pas supportée par Microsoft.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

→ Les étapes de cette éviction sont alors les suivantes :

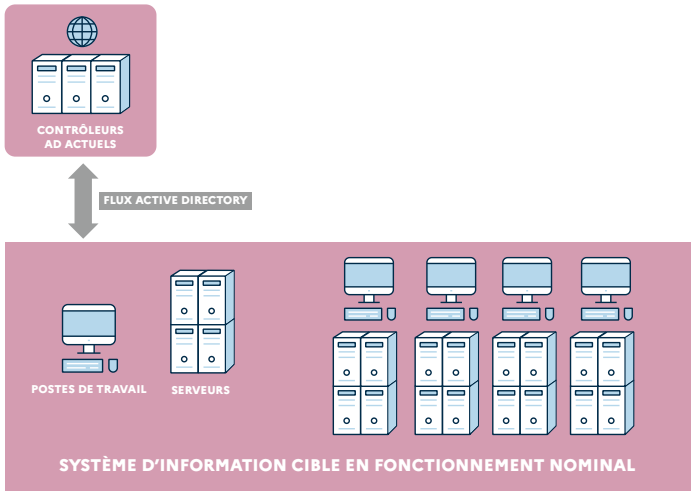


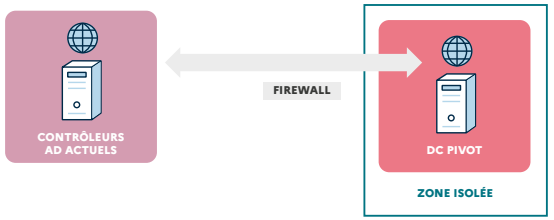
Figure 1 : Système d'information pré-bascule

1 - Installation d'un nouveau serveur qui servira de contrôleur de domaine pivot. Ce serveur doit être mis à jour et peut être durci à l'aide d'outils tels que WDAC. Il doit de plus être isolé du réseau de production, soit au travers d'une politique de filtrage, soit en lui attribuant son propre site.

2 - Arrêt de l'ensemble du SI à l'exception du dernier contrôleur de domaine sur lequel l'ensemble des rôles auront préalablement été transférés. Il est nécessaire au préalable de vérifier que l'ensemble des partitions sont répliquées vers ce dernier contrôleur de domaine.

3 - Réplication entre le dernier contrôleur de domaine et le contrôleur de domaine pivot.

Figure 2 : Réplication entre le dernier contrôleur de domaine de production et le contrôleur de domaine pivot



Remarque : la réplication peut également être effectuée sans lien réseau

4 - Une fois la réplication correctement réalisée, isolation du contrôleur de domaine pivot du dernier contrôleur de domaine.

5 - En parallèle du durcissement Active Directory mentionné dans le point suivant, réalisation d'une analyse système et réseau sur le contrôleur de domaine pivot dans l'objectif de valider sa non compromission.

6 - Réalisation des actions de durcissement Active Directory sur le contrôleur de domaine pivot jusqu'à atteindre le niveau de sécurité désiré.

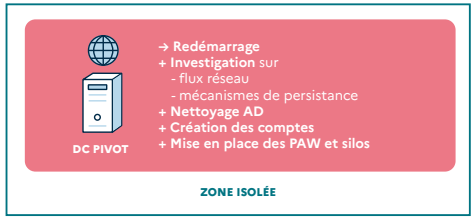


Figure 3 : Nettoyage et sécurisation de l'Active Directory

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

7 - En parallèle, installation de nouveaux serveurs pour remplacer les anciens contrôleurs de domaine (l'ensemble des contrôleurs de domaines doivent être remplacés). Pour minimiser les problèmes à la reprise, les nouveaux DC devront prendre les mêmes noms DNS, Netbios et mêmes IP que les anciens.

8 - Réplication depuis le contrôleur de domaine pivot vers un premier contrôleur de domaine reconstruit qui récupère l'ensemble des rôles.

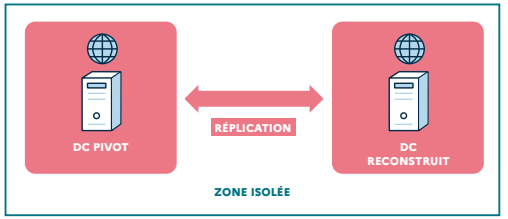


Figure 4 : Réplication vers un premier contrôleur de domaine reconstruit

9 - Dé-promotion et mise au rebus de manière sécurisée du contrôleur de domaine pivot qui contient les nouveaux secrets de production.

10 - Promotion des nouveaux contrôleurs de domaines réinstallés et réplication depuis le premier contrôleur de domaine reconstruit.

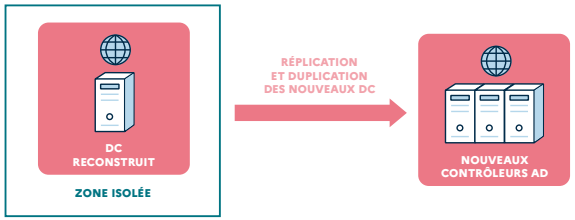


Figure 5 : Réplication vers les nouveaux contrôleurs de domaine

11 - Réouverture des flux et redémarrage du SI.

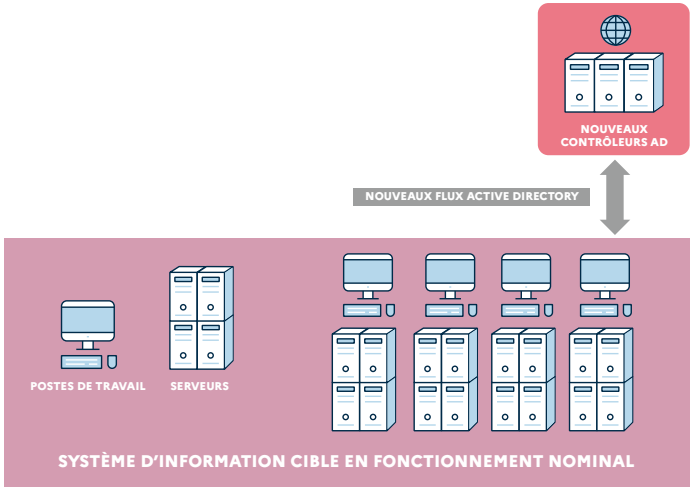
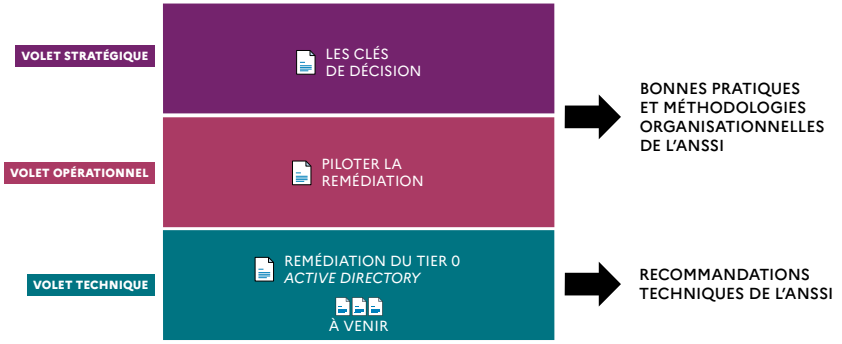


Figure 6 : Réouverture des flux

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

C STRUCTURE DU CORPUS DOCUMENTAIRE



La remédiation consiste en la reprise de contrôle d'un système d'information compromis. Le volet technique, qui traite de la reconstruction du cœur de confiance d'un système d'information s'appuyant sur Microsoft Active Directory, présente les mesures clés à respecter pour la reconstruction. Bien piloté, l'incident subi devient une opportunité d'amélioration significative.

La remédiation est l'une des dimensions majeures de la reprise de contrôle suite à une attaque cyber, avec l'investigation, la communication et la gestion de crise. C'est un travail qui commence dès l'endiguement de l'action adverse et qui peut s'étendre sur plusieurs mois.

Fruit d'une riche expérience dans l'accompagnement d'organisations victimes d'incidents de sécurité, l'ANSSI publie un corpus de guides sur la remédiation, décrivant les principes de son pilotage et de sa bonne mise en œuvre : le volet stratégique, le volet opérationnel et le volet technique.

Ce volet technique présentera les actions d'investigation, d'éviction et de supervision du Tier 0 Active Directory afin de reprendre le contrôle d'un SI.

Version 0.0 – Avril 2023
Dépot légal : avril 2023
ISBN papier : 978-2-11-167140-9
ISBN numérique : 978-2-11-167141-6

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr