Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Guide visant à sécuriser les services Active Directory de Microsoft dans votre organisation

Gestionnaires

TLP:CLEAR

Canada

Avant-propos

Le Guide visant à sécuriser les services Active Directory de Microsoft dans votre organisation (ITSM.60.100) est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le XX mois 202X.

Historique des révisions

Révision	Modifications	Date
1	Première version.	XX mois 20XX

D97-4/60-100-2023F-PDF
978-0-660-68379-9

Vue d'ensemble

Les services d'annuaire sont des composants fondamentaux essentiels pour les environnements d'architecture de technologies de l'information (TI) d'entreprise. Ils servent principalement à stocker et à gérer les justificatifs d'identité et les membres des groupes (rôles) connexes. Les services Active Directory (AD) de Microsoft comprennent un référentiel de données structuré que les organisations utilisent fréquemment pour stocker et gérer des objets de données d'annuaire d'entreprise, notamment des stratégies, des utilisatrices et utilisateurs, des dispositifs, des justificatifs d'identité ainsi que d'autres ressources réseau. Les services AD peuvent aussi être une cible intéressante pour les auteures et auteurs de menace qui cherchent des moyens pour entrer dans le réseau de votre organisation et accéder à vos systèmes et données.

La présente publication donne un aperçu des facteurs à considérer pour sécuriser les services AD de Microsoft dans votre organisation, plus particulièrement en ce qui a trait aux déploiements sur site. Ce guide fournit des recommandations sur le renforcement de la sécurité des déploiements sur site de Microsoft AD pour la gestion des environnements avec un niveau moyen de confidentialité, d'intégrité et de disponibilité, tel qu'il est décrit à l'annexe 2 de *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) [1]. Le modèle de menace prend en compte les scénarios de menace les plus courants et actifs, dont ceux dans lesquels des adversaires possèdent des ressources minimales, mais sont disposées et disposés à prendre des risques importants, comme les pirates informatiques dotées et dotés de moyens peu sophistiqués ou les cybercriminelles et cybercriminels solitaires. Il n'a pas pour objectif d'atténuer des menaces plus sophistiquées, comme les attaques du jour 0 ou les menaces internes spécialisées. Si une organisation est confrontée à un contexte de menace plus poussé, elle peut s'adresser au Centre canadien pour la cybersécurité (Centre pour la cybersécurité) pour obtenir de l'orientation additionnelle.

Étant donné que la présente publication n'est pas un guide de déploiement et de configuration complet, des ressources supplémentaires pour la configuration de services AD sont également offertes auprès de Microsoft, dans le Guide de mise en œuvre technique de sécurité (STIG pour *Security Technical Implementation Guide*) de la Defense Information Systems Agency (DISA) et dans les rapports sur les objectifs repères du Centre for Internet Security (CIS).

Les recommandations formulées dans cette publication ont été élaborées en collaboration avec Microsoft et conformément aux pratiques exemplaires générales pour sécuriser les environnements AD. Elles s'appliquent aux environnements AD de Microsoft exécutant Microsoft Windows Server 2019 ou toute version supérieure.

Table des matières

1 Introduction

Les services d'annuaire sont des composants essentiels pour les environnements d'architecture de technologies de l'information (TI) d'entreprise. Ils servent à stocker et à gérer des objets essentiels, comme les justificatifs d'identité et les autorisations s'y rattachant. Les services d'annuaire comprennent également des données sensibles comme les justificatifs administratifs qui peuvent autoriser l'accès à l'environnement complet de votre organisation. Les violations de réseaux et de données continuent de s'accroître alors que les auteures et auteurs de menace sophistiqués tirent de plus en plus avantage des lacunes de sécurité que l'on trouve dans les technologies gérées et non gérées. Les auteures et auteurs de menace cherchent à exploiter les faiblesses et les lacunes de configuration pour cibler des ressources conservées dans les services d'annuaire. Les organisations doivent impérativement prendre les mesures nécessaires pour sécuriser leurs services d'annuaire.

Le service Active Directory (AD) de Microsoft est un référentiel de données structuré que les organisations utilisent fréquemment pour stocker et gérer des objets de données d'annuaire d'entreprise. L'unité de sécurité de base dans AD est appelée une « forêt ». Ces forêts peuvent être divisées en sous-unités que l'on appelle des « domaines ». Si votre organisation devait être aux prises avec la compromission d'une quelconque partie de sa forêt, cette situation pourrait entraîner la compromission de la forêt dans son ensemble. L'historique continu des compromissions de services AD démontre la nécessité de renforcer sa sécurité, ce qui entraînerait des coûts d'exploitation potentiellement plus élevés et davantage d'efforts pour prévenir des violations plus importantes et onéreuses. Il est essentiel de protéger et de renforcer le service AD de Microsoft pour assurer la protection du réseau d'entreprise.

Avant l'acceptation générale des services AD, la délivrance de justificatifs d'identité était souvent « cloisonnée » pour chaque service. Les utilisatrices et utilisateurs devaient ouvrir une session dans chaque service. Les services AD ont permis de centraliser cette expérience en offrant à beaucoup d'utilisatrices et d'utilisateurs l'authentification unique (SSO pour *Single Sign-On*); toutefois, cette approche peut entraîner une source unique de compromission. Si les auteures et auteurs de menace sont en mesure de compromettre des justificatifs d'identité faisant partie de la SSO, alors ils ont la possibilité d'utiliser un ensemble unique de justificatifs pour déverrouiller d'autres systèmes ou magasins de données. On compte de nombreux exemples de compromissions de SSO attribuables à divers types d'attaques, comme les attaques par vol de justificatifs à authentification unique. La compromission de SSO est une tendance qui est appelée à continuer.

La présente publication donne un aperçu des facteurs à considérer pour sécuriser les services AD de Microsoft dans votre organisation, plus particulièrement en ce qui a trait aux déploiements sur site. Étant donné que la présente publication n'est pas un guide de déploiement et de configuration complet, des ressources supplémentaires pour la configuration de services AD sont également offertes auprès de Microsoft, dans le Guide de mise en œuvre technique de sécurité (STIG pour *Security Technical Implementation Guide*) de la Defense Information Systems Agency (DISA) et dans les rapports sur les objectifs repères du Centre for Internet Security (CIS).

Ce guide fournit des recommandations sur le renforcement de la sécurité des déploiements locaux de Microsoft AD pour la gestion des environnements avec un niveau moyen de confidentialité, d'intégrité et de disponibilité dans les contextes de menace les plus actifs.

Les recommandations énoncées dans la présente publication s'appliquent aux environnements AD de Microsoft exécutant Microsoft Windows Server 2019 ou une version plus récente, et elles s'appliquent à tous les environnements AD Domain

Services de Microsoft. Les recommandations mentionnées dans cette publication ciblent strictement les systèmes exécutant les services AD Domain Services, même si certaines peuvent s'appliquer à d'autres services au sein d'un environnement d'entreprise, comme le système de noms de domaine (DNS pour *Domain Name Service*), le protocole DHCP (pour *Dynamic Host Configuration Protocol*), ainsi que les services de fichiers et d'impressions. Pour les organisations exécutant des systèmes d'exploitation d'une version inférieure à la version Microsoft Windows Server 2019 recommandée, nous suggérons le passage à des forêts « séparées » distinctes.

1.1 Risques liés aux services AD

La fréquence et la sophistication des attaques contre AD sont en hausse et la sécurité traditionnelle pour les services AD n'est plus adéquate. Afin d'améliorer la protection des services d'annuaire, votre organisation devra investir des ressources additionnelles et davantage d'efforts. Une mesure que votre organisation peut prendre est d'assurer la séparation des tâches au moyen de procédures et de stratégies. Plusieurs fonctions de sécurité, comme celles des administratrices ou administrateurs des sauvegardes, des audits ou des alertes, devraient particulièrement être distinctes des fonctions d'administration des domaines. De plus, les organisations devraient tenir compte du fait que les administratrices et administrateurs de domaines (et d'autres rôles équivalents) peuvent s'accorder des autorisations à leur discrétion, puisque la capacité de restreindre techniquement une telle activité est limitée dans AD.

Votre organisation devrait également assurer la maintenance de son environnement AD en appliquant les plus récents correctifs disponibles pour atteindre le niveau de correction offert par Windows Server 2019. En mettant à jour et en corrigeant ses environnements de TI, votre organisation peut s'assurer que les vulnérabilités et les bogues ont été corrigés et ainsi empêcher les auteures et auteurs de menace de les exploiter. Votre organisation peut également choisir d'isoler les services dont la maintenance est déficiente pour les éloigner des menaces provenant d'Internet.

1.2 Considérations stratégiques

Votre organisation doit se doter de ressources informatiques d'entreprise pour soutenir son personnel et remplir sa mission. Elle devrait tenir compte du contexte opérationnel et de l'environnement de menace qui lui sont propres au moment d'appliquer les recommandations formulées dans cette publication pour protéger son infrastructure AD. Les piliers suivants ont pour but de soutenir l'environnement opérationnel d'entreprise et d'étayer le contexte de menace pour les services d'annuaire :

- Architecture de TI d'entreprise;
- Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA);
- Évaluations des menaces et des risques (EMR).

1.2.1 Architecture de TI d'entreprise

L'architecture de TI d'entreprise définit la manière dont la structure et le fonctionnement des biens de TI de votre organisation sont censés soutenir vos objectifs opérationnels stratégiques, en tenant compte de la sécurité et des risques. L'architecture de TI d'entreprise fournit une orientation stratégique qui permet de savoir comment les investissements dans les ressources d'information peuvent intégrer et favoriser les processus opérationnels. Votre organisation devrait comparer

les recommandations formulées dans cette publication avec son architecture de TI d'entreprise afin de mieux comprendre comment ces changements pourraient avoir une incidence sur ses objectifs opérationnels.

1.2.2 Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)

La GIJIA fait référence aux processus d'authentification et d'autorisation nécessaires pour que les utilisatrices, les utilisateurs et les dispositifs interagissent avec les ressources technologiques de votre organisation et se connectent à elles. Elle comprend un ensemble d'outils de sécurité, de stratégies et de systèmes qui aide votre organisation à gérer, à surveiller et à sécuriser l'accès à ses ressources technologiques. Les recommandations formulées dans cette publication auront une incidence sur les contrôles de GIJIA dans votre organisation.

Pour obtenir plus de renseignements sur la GIJIA, consultez l'ITSAP.30.018, Gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) [2].

1.2.3 Évaluation des menaces et des risques

La gestion de l'évaluation des menaces et des risques comprend l'identification, l'évaluation et l'atténuation des menaces auxquelles font face les biens de TI. Votre organisation doit réévaluer ses environnements et comprendre tous les risques associés à la mise en œuvre des recommandations formulées dans la présente publication. Si elle collabore avec un fournisseur de services, comme Services partagés Canada (SPC), pour gérer la mise en œuvre des contrôles, votre organisation demeure responsable de la gestion des risques. Ces conseils concernent un modèle de menace selon lequel des adversaires possèdent des ressources minimales, mais sont disposées et disposés à prendre des risques importants, comme les pirates informatiques dotées et dotés de moyens peu sophistiqués ou les cybercriminelles et cybercriminels solitaires. Ils ne visent pas à atténuer des menaces plus sophistiquées, comme les attaques du jour 0 ou les menaces internes spécialisées. Si une organisation est confrontée à un contexte de menace plus poussé, elle peut s'adresser au Centre pour la cybersécurité pour obtenir de l'orientation additionnelle.

2 Active Directory (AD) de Microsoft

AD de Microsoft est un référentiel de données structuré pour le stockage d'objets de données d'annuaire. Il peut être utilisé pour gérer l'accès à un bon nombre de ressources de TI de votre organisation en fonction de rôles ou de groupes, comme l'infrastructure réseau, les services de courriel, les services d'infrastructure à clé publique (ICP) et les services sans fil.

2.1 Capacités d'AD

Microsoft AD est un ensemble de services permettant à votre organisation d'identifier, d'organiser et de sécuriser des objets (par exemple, des dispositifs) et des comptes. Il se compose des services suivants, lesquels peuvent être fournis en totalité ou en partie et nécessitent une attention particulière pour acquérir une posture de sécurité globale :

- Services de domaine AD (AD DS – *AD Domaine Services*);
- Services de fédération AD (ADFS – *AD Federation Services*);
- Services de certificat AD (AD CS – *AD Certificat Services*);
- Services de gestion des droits AD (AD RMS – *AD Rights Management Services*);
- Services d'annuaire légers AD (AD LDS – *AD Lightweight Directory Services*).

Cette publication se concentre sur les capacités des services AD DS. Un addenda à cette publication sera fourni pour les autres services énumérés.

2.2 Architecture de déploiement des services AD

L'annuaire Microsoft AD peut être déployé dans différentes architectures, notamment dans une architecture exclusivement sur site (ou dans un centre de données directement contrôlé), dans une architecture en nuage hybride et dans des solutions complètes sur des plateformes infonuagiques.

2.2.1 AD sur site

À l'origine, les services AD étaient destinés à la gestion traditionnelle d'infrastructures et d'applications sur site. Cette option de déploiement permet à votre organisation de gérer pleinement son service d'annuaire de bout en bout. Les conseils relatifs au renforcement de la sécurité présentés dans cette publication sont axés principalement sur cette architecture de déploiement.

2.2.2 Services infonuagiques AD (sur site, autogérés dans le nuage)

Il faut soigneusement prendre en compte les déploiements et les migrations en nuage hybrides. Lorsqu'une fonction de service infonuagique est incluse, cela implique l'utilisation d'un hyperviseur, ce qui pourrait transformer radicalement la posture de sécurité d'un déploiement sur site, puisque l'on introduit également différentes préoccupations de sécurité et

fonctions de mise en réseau qui doivent être prises en considération. Cette publication mettra l'accent sur l'utilisation des services AD tels qu'ils sont contrôlés par les clients.

Pour obtenir de plus amples renseignements sur les déploiements dans de nouveaux systèmes des services d'annuaire au sein d'une infrastructure infonuagique, notamment ceux commençant par l'utilisation d'un fournisseur de services infonuagiques (FSI) ou d'un fournisseur de services GIJIA tiers, consultez l'ITSP.60.100, *Guide visant à sécuriser les services Active Directory de Microsoft dans votre organisation* [3].

Les services AD peuvent quand même être utilisés pour les capacités de GIJIA pour le nuage au moyen de solutions sur site existantes. C'est ce que l'on appelle généralement une architecture « hybride », puisque certains éléments sont contrôlés et exploités sur site, et que d'autres éléments sont connectés et ensuite synchronisés aux services d'annuaire du FSI. Dans certains déploiements, les configurations d'un serveur AD restent en soi les mêmes, puisque la différence ou le changement principal consiste à utiliser la plateforme d'infrastructure-service (IaaS pour *Infrastructure as a Service*) du FSI. Dans ce type de déploiement, le contrôle de certains aspects physiques et du réseau changera en fonction du modèle d'infonuagique fondé sur le partage des responsabilités lié à l'infonuagique.

Les deux principales approches à l'égard d'une architecture « hybride » sont :

- **Sur site (dans un centre de données de client) :** Les contrôleurs de domaine sont fédérés et affectés aux services infonuagiques par les services ADFS sur site.
- **Sur site étendue (autogérée) :** Les contrôleurs de domaine sur site et déployés sur une plateforme IaaS de FSI.
  - En utilisant la même forêt ou une approbation de forêt, les domaines déployés de cette façon sont techniquement hybrides, car ils se synchronisent et sont fédérés localement, et ils font aussi vraisemblablement appel à ADFS sur site et à la fédération.
  - Dans ce cas, il n'y a toujours pas une synchronisation directe ou complète des identités avec un fournisseur d'identité (IdP pour *Identity Provider*) pour constituer une identité native en nuage.
  - Bien qu'il s'agisse d'une approche possible, il est à noter qu'elle n'est pas recommandée à long terme, car elle implique des changements fondamentaux à la posture de sécurité, réduisant ainsi l'applicabilité des mesures de protection énoncées dans la présente publication et dans l'ITSP.60.100.
  - Cette approche devrait normalement être considérée comme une stratégie de transition ou de migration.

2.2.3 Services d'annuaire dans le nuage

L'authentification et l'autorisation dans un environnement infonuagique peuvent se faire sans avoir recours à des capacités sur site. Une authentification en nuage seulement fait référence aux processus de gestion de l'identité et de l'accès exclusivement offerts par une solution de GIJIA du FSI ou par une solution de gestion de l'identité hébergée par une tierce partie. Cette option permet à votre organisation de créer et de gérer des identités d'utilisateur, des droits et un contrôle d'accès au moyen d'une application tierce sans avoir à mettre en place, à posséder ou à exploiter une infrastructure sur site. Les solutions d'authentification en nuage seulement peuvent être utilisées pour gérer l'accès aux charges de travail sur un nuage public et aux applications sur site gérées par des particuliers (par exemple, l'utilisation d'Azure AD Domain Services). Plusieurs protocoles d'authentification régissent la façon dont sont créés, diffusés et gérés les identités, les droits et les autorisations. Votre organisation devrait effectuer une évaluation des risques afin de déterminer les risques auxquels sont exposés ses processus opérationnels et ses données avant d'opter pour cette option.

Remarque : La posture de sécurité dans ce déploiement est différente du modèle sur site, et plusieurs contrôles dans cette publication ne peuvent pas être appliqués.

Au moment de considérer un nouveau déploiement ou d'envisager de créer une stratégie réseau pour votre organisation, il est important de prendre note que cette approche – et les options hybrides mentionnées précédemment – est toujours valide, mais qu'il faudra tenir compte des dépenses en capital et des coûts opérationnels continus pour chacune de ces approches. Dans le cas où les services d'un FSI ou d'un IdP sont utilisés, le client permet que la totalité de l'identité ou des justificatifs d'identité de ses utilisatrices et utilisateurs soit formée et utilisée dans ces services. Cette façon de procéder offre des avantages, car des facettes de l'application des correctifs et des mises à niveau à la solution de GIJIA sont effectuées par le FSI conformément à l'abonnement auquel souscrit votre organisation.

Toutefois, cette approche implique un changement fondamental dans l'utilisation des services AD en ce sens que votre organisation est maintenant dépendante des services infonuagiques. En d'autres termes, plusieurs des recommandations formulées dans cette publication devront être revues, puisque le contrôle du matériel physique et l'étendue du contrôle sur d'autres fonctions changeront de manière radicale. En outre, la capacité de votre organisation est réduite en ce qui concerne la visibilité et le contrôle des justificatifs d'identité, car elle doit collaborer avec le fournisseur dans tous les cas où des mesures et des services additionnels, ou une utilisation des justificatifs en dehors des principales fonctions de service du fournisseur, sont requis.

3 Stratégies de renforcement et d'atténuation

Les déploiements sur site des services AD de Microsoft peuvent être protégés contre de nombreuses menaces en renforçant les défenses et les contrôles. Les stratégies de renforcement et d'atténuation demandent la mise en place de mesures visant à protéger les justificatifs, les systèmes, les processus et les identités. Dans la section ci-dessous, nous proposons des stratégies de renforcement et d'atténuation pour protéger les services AD.

Nous recommandons à votre équipe de gestion de faire appel à des praticiennes et praticiens de TI pour suivre, dans un premier temps, le guide de configuration et de mise en œuvre des services AD de Microsoft, et dans un deuxième temps, les données supplémentaires tirées des documents d'orientation du guide STIG de la DISA et du CIS.

3.1 Gestion des systèmes

La gestion des systèmes porte sur les contrôles liés à l'établissement de frontières pour le système et à la mise en œuvre d'un plan sécurisé pour assurer l'approvisionnement des services AD et l'accès sécurisé continu à ces services. Ainsi, les éléments suivants doivent être mis en œuvre pour établir un environnement d'exploitation fiable pour l'infrastructure AD renforcée :

- utiliser des postes de travail administratifs dédiés pour toutes les tâches administratives, avec une authentification multifacteur ayant recours à des jetons matériels;
- utiliser des comptes privilégiés distincts pour les tâches d'administration;
- mettre hors service ou séparer les applications et services AD patrimoniaux;
- limiter les connexions réseau vers les serveurs AD et en provenance de ceux-ci – aucune connectivité Internet entrante ou sortante;
- configurer des comptes privilégiés uniques et des mots de passe d'administration locale pour les serveurs et les postes de travail;
- bloquer les comptes privilégiés pour empêcher leur utilisation sur des systèmes non autorisés;
- l'administration à distance ne peut être effectuée que depuis un poste de travail administratif dédié, et seulement en utilisant le protocole RDP (pour *Remote Desktop Protocol*) chiffré au moyen du protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*).

3.2 Gestion des comptes

La gestion des comptes porte sur les contrôles fondamentaux qui permettent de gérer en toute sécurité tous les comptes privilégiés et d'utilisateur, et ce, de l'approvisionnement et à la mise hors service dans les environnements de services AD. Parmi les exemples de comptes privilégiés, notons les comptes administratifs locaux et de domaine, les comptes de services et les comptes administratifs intégrés.

Les mesures suivantes doivent être mises en œuvre pour la gestion des comptes :

- mettre en place l'authentification multifacteur ayant recours à des jetons matériels (par exemple, carte intelligente et clavier, clé USB) pour tous les comptes d'administrateur et d'utilisateur conformément aux conseils de Microsoft sur les services AD et pour tous les terminaux;
- utiliser le principe du droit d'accès minimal pour attribuer et gérer les droits et des privilèges d'administration;
- mettre en place et appliquer la création de comptes privilégiés « juste à temps »;
- s'assurer que l'accès à tous les comptes de services est accordé en fonction du principe du droit d'accès minimal et que des comptes de services gérés sont utilisés autant que possible;
- éviter d'attribuer des comptes de services dans des groupes privilégiés intégrés, dont les groupes d'administrateur locaux et les groupes d'administrateur de domaine;
- s'assurer que les comptes de services sont utilisés uniquement par des applications ou des services plutôt que par des utilisatrices et utilisateurs;
- empêcher que les comptes de services soient utilisés pour des connexions interactives et l'exécution de traitements par lots;
- mettre en œuvre le filtrage de mot de passe AD pour bloquer l'utilisation de mots de passe compromis ou de mauvais mots de passe.

3.3 Sécurité et renforcement des applications

En limitant les applications autorisées sur les serveurs AD et en permettant ou en installant uniquement les services et les applications qui sont essentiels à l'exécution et au soutien des fonctions des services d'annuaire, votre organisation aura une posture de renforcement plus solide pour ses services AD. Ainsi, votre organisation a un ensemble de services plus restreints qui s'exécutent sur ses serveurs AD, alors que les services cohébergés sont déplacés et mis à l'écart des services AD. Limiter le plus possible le nombre de logiciels exécutés est une étape essentielle du renforcement de la sécurité et de la réduction de la surface d'attaque. Il est recommandé de suivre des procédures de gestion des changements appropriées, comme celles de la bibliothèque d'infrastructure des TI (ITIL pour *Information Technology Infrastructure Library*).

La mise en œuvre de listes d'applications autorisées sur les serveurs et les postes de travail administratifs permet de garantir que seules les applications approuvées explicitement sont installées sur les systèmes de services d'annuaire. Des contrôles basés sur l'hôte et des contrôles basés sur les stratégies doivent aussi être mis en œuvre sur les serveurs AD et les postes de travail administratifs dédiés pour empêcher l'installation et l'utilisation non autorisées d'applications sur les serveurs.

3.4 Journalisation, audit et surveillance

Des mécanismes de surveillance, d'audit et de journalisation doivent être mis en place pour les activités liées aux services d'annuaire. Tous les événements doivent être transmis à un serveur distant auquel on ne peut pas accéder au moyen de justificatifs d'identité de base. Les journaux d'événements peuvent également être acheminés à un serveur de gestion des informations et des événements de sécurité (GIES) centralisé pour faciliter l'agrégation, le regroupement et l'analyse des

événements dans des journaux d'activités. Des mécanismes d'alerte automatisés doivent être mis en œuvre pour repérer les violations des stratégies ayant une plus grande incidence et permettre des mesures d'intervention plus rapides. Il est nécessaire de journaliser, de surveiller et de vérifier les événements qui ont échoué et ceux qui ont réussi, ainsi que les événements liés aux opérations sensibles et critiques du serveur. Votre organisation devrait également désactiver les comptes d'utilisateur périmés ou inactifs et mettre en place un système de surveillance pour les événements liés à l'utilisation de ces comptes.

Il est important que votre organisation surveille, journalise et vérifie l'utilisation de tous les comptes privilégiés ou d'administrateur. Vous pouvez activer les paramètres d'audit des systèmes de manière à vérifier régulièrement les comptes dotés d'un accès privilégié ou administratif. Pour obtenir de plus amples renseignements, consultez le document Recommandations de stratégie d'audit pour Microsoft Windows Server [4].

3.5 Détection des menaces et intervention

La détection des menaces et l'intervention doivent tenir compte de différents scénarios possibles, comme une compromission de vos biens AD par une auteure ou d'un auteur de menace, et des contrôles de détection à mettre en place.

Votre organisation peut améliorer la prévention et la détection de techniques d'attaque connues en se servant d'indicateurs de compromission (IC) et de technologies de prévention des menaces automatisées. Vous devriez surveiller les événements Windows sensibles liés aux services AD susceptibles d'indiquer une tentative de compromission ou une compromission fructueuse. En faisant appel à des solutions de détection et de prévention des menaces sur le réseau ou les terminaux, votre organisation peut détecter les tentatives de compromission de ses services AD et prendre les mesures nécessaires pour intervenir.

Pour ajouter un niveau supplémentaire de protection, vous devriez mettre en place des solutions d'antimaliciels et mettre à jour les antivirus et antimaliciels de tous les systèmes en temps opportun. Ces outils de détection devraient surveiller les tentatives visant à désactiver ou à neutraliser les solutions antimaliciels.

3.6 Application des correctifs et gestion des changements

Dans tous les cas, il faut assurer la maintenance et la tenue à jour de l'infrastructure AD. Cela pourrait comprendre planifier l'application des correctifs, tester Windows et confirmer la compatibilité des correctifs avec les applications du secteur d'activités. Le serveur AD doit être configuré en suivant une stratégie progressive offrant la capacité de faire une restauration selon la disponibilité du matériel de maintenance logicielle de Microsoft, et de limiter les interruptions planifiées. Il sera ainsi possible de prévenir les interruptions de service advenant un problème avec le correctif. Cela permettra également de s'assurer que les restaurations se font sans affecter l'ensemble de l'environnement. De plus, il est nécessaire d'adopter des processus de gestion des changements pour certifier et vérifier que les mises à jour requises sont bien appliquées.

3.7 Continuité des activités

La continuité des activités implique que votre organisation doit avoir mis en place des activités de planification d'urgence pour aider au rétablissement du service d'annuaire en cas de menaces de toute sorte, comme des interruptions de système ou des incidents liés à la cybersécurité. Vous devriez mettre en œuvre la corbeille des services AD pour vous aider à récupérer vos objets AD.

Dans le cadre de vos efforts de continuité des activités, il serait bon d'établir des processus qui permettent la collecte automatisée des données essentielles du système et des sauvegardes de l'information. Veillez à ce que les sauvegardes fassent l'objet de tests périodiques. Ces tests pourraient avoir lieu chaque trimestre ou après un changement important pour valider l'intégrité et l'utilité. Vos données de sauvegarde devraient être isolées du réseau principal. Il convient également d'accorder une attention particulière à la conservation de sauvegardes hors ligne, en plus de toute autre stratégie de sauvegarde déjà en place.

Outre les sauvegardes, votre organisation doit créer, tester et mettre à jour des plans d'intervention en cas d'incident découlant de scénarios de risques qui pourraient survenir dans votre organisation. Vous devriez vous préparer à une reprise à la suite d'incidents liés à la sécurité qui pourraient avoir une incidence sur l'intégrité ou la disponibilité de votre environnement AD. Pour se faire, vous pouvez établir des documents et des procédures de reprise du système pour votre environnement AD, et fournir des exercices de formation ou de simulation aux administratrices et administrateurs de système afin de leur permettre d'élaborer et de valider des plans d'intervention et de reprise.

3.8 Formation des utilisatrices et utilisateurs

Votre organisation doit organiser régulièrement des séances de sensibilisation à la sécurité pour les détentrices et détenteurs de comptes privilégiés et les autres utilisatrices et utilisateurs finaux de système. Votre programme de formation doit être conçu pour offrir une formation continue à l'ensemble des utilisatrices et utilisateurs sur les pratiques exemplaires actuelles en matière de sécurité et pour encourager les changements de comportement ainsi que l'amélioration des pratiques en cybersécurité pour contrer les comportements indésirables et plus à risque. Votre organisation devrait également établir des processus visant à simplifier les exigences de sécurité pour les utilisatrices et utilisateurs finaux, et ce, en tirant profit de séances de formation structurées et de supports visuels.

4 Contenu complémentaire

4.1 Liste des acronymes, des abréviations et des sigles

Abréviation, acronyme ou sigle	Définition
AD	Active Directory
ADFS	Services de fédération AD (*AD Federation Services*)
AMF	Authentification multifacteur
ATO	Autorisation d'exploiter (*Authority to Operate*)
CEI	Center for Internet Security
DHCP	Protocole DHCP (*Dynamic Host Configuration Protocol*)
DISA	Defense Information Systems Agency
DNS	Système de noms de domaine (*Domain Name System*)
GC	Gouvernement du Canada
GIJIA	Gestion de l'identité, des justificatifs d'identité et de l'accès
MHEMR	Méthodologie harmonisée de l'évaluation des menaces et des risques
PDU	Point de défaillance unique
SSO	Authentification unique (*Single Sign-On*)
STI	Sécurité des technologies de l'information
STIG	Guide de mise en œuvre technique de sécurité (*Security Technical Implementation Guide*)
TI	Technologies de l'information

4.2 Glossaire

Terme	Définition
Authentification multifacteur	Mécanisme pouvant ajouter une couche supplémentaire de sécurité aux appareils et aux comptes. L'authentification multifacteur exige une vérification supplémentaire (comme un numéro d'identification personnel [NIP] ou une empreinte digitale) pour accéder aux appareils ou aux comptes. L'authentification à deux facteurs est un type d'authentification multifacteur.
Droit d'accès minimal	Principe selon lequel une personne ne reçoit que l'ensemble des privilèges dont elle a besoin pour accomplir des tâches autorisées. Ce principe limite les dommages pouvant résulter d'une utilisation non autorisée, incorrecte ou accidentelle d'un système d'information.
Niveau d'assurance (*Level of assurance*)	Degré de confiance dans le processus de filtrage utilisé pour établir l'identité d'une personne et les contrôles utilisés pour gérer les justificatifs d'identité qui leur ont été confiés.

4.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) décembre 2014.
2	Centre canadien pour la cybersécurité, *Gestion de l'identité, des justificatifs d'identité et de l'accès* (ITSAP.30.018), août 2022.
3	Centre canadien pour la cybersécurité, *Guide des praticiennes et praticiens visant à sécuriser les services Active Directory au sein du gouvernement du Canada* (ITSP.60.100), date à déterminer.
4	Microsoft, Recommandations de stratégie d'audit pour Microsoft Windows Server, juillet 2021.