Bureau du vérificateur général

V.9. Sécurité des Active Directory

TABLE DES MATIÈRES

1. INTRODUCTION 349

2. PORTÉE DE LA MISSION 351

3. CONSTATATIONS, RECOMMANDATIONS ET PLANS D'ACTION 352

3.1. Active Directory multiples 352

3.2. Analyse de risques relative à l'Active Directory 354

3.3. Fichiers journaux 355

3.4. Logiciel antivirus 357

3.5. Stratégies de mots de passe 359

3.6. Stratégies de verrouillage de comptes 361

3.7. Comptes à privilèges élevés 362

3.8. Normes de configuration des contrôleurs de domaine 364

3.9. Services non essentiels 365

3.10. Correctifs de sécurité des contrôleurs de domaine 368

4. ANNEXE 370

4.1. Glossaire des termes de l'Active Directory 370

V.9. SÉCURITÉ DES ACTIVE DIRECTORY

1. INTRODUCTION

Mise en contexte

À l'instar des grandes municipalités d'Amérique du Nord et d'Europe, les technologies de l'information sont devenues essentielles à la gestion opérationnelle efficace de la Ville de Montréal (la Ville). Les technologies de l'information doivent permettre aux élus, aux employés et au public d'avoir accès à de l'information pertinente lorsqu'ils en ont besoin.

Pour réaliser leurs tâches quotidiennes, la grande majorité des employés de la Ville doivent avoir accès en toute confiance à un système informatique, qu'il s'agisse de leur ordinateur de bureau, d'un ordinateur portable ou d'un poste de travail mobile connecté aux réseaux informatiques de la Ville.

Afin de gérer efficacement ces réseaux et l'accès aux données de ceux-ci, le Service des technologies de l'information (STI) et les divisions de l'informatique des arrondissements ont mis en place des services centralisés d'identification et d'authentification aux réseaux d'ordinateurs et de serveurs utilisant le système d'exploitation Windows. Ces services centralisés sont mis en œuvre par le service d'annuaire Active Directory (AD) de Microsoft.

Active Directory : son rôle et ses fonctions

Depuis que les architectures Windows sont décentralisées, chaque serveur et poste de travail fonctionne de façon indépendante. L'AD de Microsoft est la technologie sous-jacente au sein du système d'exploitation Windows qui fournit un référentiel central, communément appelé service d'annuaire, qui permet une gestion centralisée des utilisateurs et de la sécurité.

L'AD permet de réaliser la gestion des objets sans lien avec la disposition réelle de ceux-ci ou les protocoles réseau employés, fournissant ainsi une gestion des postes et des utilisateurs distants de façon complètement centralisée. L'AD organise l'annuaire en sections afin de s'arrimer aussi bien au développement d'un organisme qui manipule quelques objets qu'à celui qui en manipule des millions.

Plus spécifiquement, l'AD fournit des services centralisés d'identification et d'authentification aux réseaux d'ordinateurs de la Ville utilisant le système Windows. En tant que service d'annuaire, l'AD répertorie tous les éléments du ou des réseaux tels que les comptes des utilisateurs, les postes de travail, les serveurs, les imprimantes, etc. Tous les renseignements et paramètres de l'AD sont enregistrés dans une base de données centralisée propriétaire qui réside sur les contrôleurs de domaine. Tous ces renseignements et paramètres forment la structure de l'AD, qui est en fait une organisation hiérarchisée d'objets.

Un contrôleur de domaine est un serveur qui stocke un duplicata de l'annuaire AD. Il assure la propagation des modifications apportées sur l'annuaire ainsi que l'authentification et l'ouverture des sessions des utilisateurs, en plus des recherches dans l'annuaire. Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Chaque contrôleur de domaine est capable de recevoir ou de dupliquer les modifications de l'ensemble de ses homologues du domaine. Les paramètres de sécurité appliqués au contrôleur de domaine sont primordiaux, car si la sécurité du contrôleur de domaine est compromise, c'est l'ensemble de la sécurité de l'AD qui sera alors compromise.

L'AD est la fondation sur laquelle dépend la sécurité de Windows. On entend par sécurité Windows la sécurité des postes de travail, des utilisateurs, des serveurs, des données et des réseaux fonctionnant sous le système d'exploitation Windows. Si la sécurité de l'AD est compromise, cela conduirait à l'effondrement de toutes les autres mesures de sécurité lui étant liées.

Le point névralgique de la sécurité de l'AD repose sur les paramètres de configuration de l'AD mis en place au moment de son implantation et le maintien de cette configuration au cours du cycle de vie de l'AD. Ces paramètres sont définis dans les stratégies de groupes (ou GPO) qui sont appliquées au démarrage de l'ordinateur et pendant l'ouverture de session de l'utilisateur. Les GPO sont utilisées pour maintenir un niveau de sécurité adéquat des systèmes et des données, mais elles sont aussi utilisées pour diminuer les risques potentiels inhérents aux utilisateurs en restreignant leurs actions (p. ex. verrouillage du panneau de configuration, restriction de l'accès à certains dossiers, désactivation de l'utilisation de certains exécutables, etc.).

Ayant été conçu pour assurer un niveau de performance et de sécurité adéquat, l'AD permet aux administrateurs de système de contrôler les accès et l'utilisation des données et des ressources partagées grâce aux fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès à ces actifs.

2. PORTÉE DE LA MISSION

Notre mission de vérification consistait à évaluer les mécanismes de contrôle mis en place afin d'assurer la sécurité de l'AD.

Les objectifs de notre mission de vérification étaient les suivants :

- Fournir une évaluation de l'efficience et de l'efficacité des contrôles mis en place pour assurer l'implantation et la gestion sécuritaire de l'AD;
- Fournir une évaluation indépendante de la configuration sécuritaire de l'AD.

Notre approche de vérification a été élaborée à la suite de notre analyse de risques afférente à la sécurité de l'AD et au contexte de la Ville. Nous avons défini notre approche ainsi que nos critères de vérification selon les bonnes pratiques de l'industrie. Nous avons développé le programme de vérification en consultant plusieurs publications pertinentes.

Nous avons réalisé nos tests de vérification en présence des administrateurs de l'AD du STI et des administrateurs des AD des arrondissements de l'ex-banlieue. Nous avons procédé par entrevues auprès de ces personnes et nous avons également utilisé les outils d'administration de l'AD de Microsoft.

Plusieurs services d'annuaire AD sont présents au sein de la Ville. À la suite de notre analyse de risques, l'étendue de notre mission de vérification a porté sur sept AD.

Étant donné la nature sensible des AD, nous préférons conserver la liste de ceux-ci confidentielle.

La vérification de la sécurité de l'AD portait sur les mécanismes de contrôle de gestion et de configuration des aspects suivants :

- Gestion de l'AD;
- Sécurité du périmètre de l'AD;
- Sécurité logique des contrôleurs de domaine;
- Paramètres de configuration des domaines et des contrôleurs de domaine;
- Encadrements et procédures de l'AD.

Les éléments suivants ont été exclus de notre vérification :

- Configuration des serveurs qui n'étaient pas des contrôleurs de domaine;
- Configuration des postes de travail;
- Gestion des identités et des accès des utilisateurs;
- Gestion du système de noms de domaine (DNS);
- Sécurité physique des serveurs;
- Gestion de la sécurité applicative;
- Accès aux bases de données;
- Gestion des codes d'accès.

3. CONSTATATIONS, RECOMMANDATIONS ET PLANS D'ACTION

Nous énumérons dans cette section les principales constatations relevées pour l'ensemble des AD. Cependant, à cause de la criticité des AD pour lesquels nous avons constaté des lacunes, nous avons décidé de garder confidentiels le détail et les résultats de nos travaux de vérification pour chacun des AD. Un rapport de vérification spécifique a cependant été remis sous le sceau de la confidentialité aux personnes responsables de chaque AD. Celles-ci ont validé les constatations qui leur étaient spécifiques ainsi que les recommandations proposées.

3.1. ACTIVE DIRECTORY MULTIPLES

3.1.A. Contexte et constatations

CONSTATATION
Nos travaux de vérification nous ont permis de constater qu'il n'y avait pas qu'un seul AD au sein de la Ville.

En effet, les ex-villes de banlieue qui sont devenues des arrondissements au moment des fusions municipales du 1er janvier 2002 ont maintenu leur propre Active Directory qui était déjà implanté bien avant ces fusions.

À cette époque, cette situation était justifiée, d'une part, par le fait que ces arrondissements utilisaient leurs propres applications de gestion et d'opération pour leur municipalité et, d'autre part, parce que le STI ne fournissait pas de telles applications.

Toutefois, depuis ce temps, ce contexte a changé puisque le STI offre maintenant des solutions intégrées qui sont utilisées par l'ensemble des arrondissements (p. ex. SIMON, Ludik) et les applications « orphelines » de ces arrondissements seront obsolètes à brève échéance.

En maintenant plusieurs AD au sein de ses unités d'affaires, la Ville fait face aux risques et aux impacts potentiels suivants :

- Difficultés à maintenir un niveau de sécurité homogène pour l'ensemble des AD. En effet, la sécurité afférente aux AD (non gérés par le STI) pourrait ne pas respecter les exigences de sécurité et d'affaires de la Ville. Advenant des bris de sécurité, l'environnement Windows de l'arrondissement pourrait être compromis, mais également celui de la Ville puisque des relations d'approbation sont présentes entre l'AD de la Ville et certains AD des arrondissements;
- Élaboration et mise en place de plans de relève plus complexes, engendrant par conséquent des coûts plus élevés, car il est nécessaire d'établir des plans d'action pour la continuité des opérations en cas de sinistre pour chacun des AD, au lieu de disposer d'un plan de relève unique si la Ville détenait un seul AD. En conséquence, les opérations des arrondissements pourraient ne pas être relevées en temps opportun en cas de désastre;
- Augmentation des coûts d'infrastructure, incluant les licences des logiciels, afférents à l'augmentation du nombre de contrôleurs de domaine. En effet, chaque AD distinct doit avoir un minimum de deux contrôleurs de domaine pour pouvoir fonctionner convenablement.

3.1.B. Recommandations

Nous estimons qu'un seul Active Directory global devrait exister au sein de la Ville. Nous recommandons à la Direction générale de :

- **réaliser une analyse coûts-bénéfices ainsi qu'une analyse d'impacts afférentes à un Active Directory unique;**
- **faire participer activement les unités d'affaires de l'informatique au sein de l'étude et du projet;**
- **fournir une architecture de capacité et de performance suffisantes. Par exemple, certains liens de télécommunications devront être remplacés afin de disposer de bandes passantes plus conséquentes;**
- **définir formellement des niveaux de services (SLA) avec la clientèle afin que les performances des environnements Windows et le service aux utilisateurs ne soient pas dégradés et qu'ils répondent aux exigences d'affaires.**

3.1.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec l'unité d'affaires concernée. Elle va nous communiquer son plan d'action ultérieurement.

3.2. ANALYSE DE RISQUES RELATIVE À L'ACTIVE DIRECTORY

3.2.A. Contexte et constatations

Une analyse de risques consiste à identifier et à évaluer les facteurs pouvant compromettre le succès des projets ou l'atteinte des objectifs d'affaires. Plus spécifiquement, elle détermine les risques que fait peser une menace en fonction de sa probabilité et de son impact.

L'analyse de risques permet également à l'organisme d'élaborer des mécanismes de contrôle afin de réduire à un niveau acceptable la probabilité que les risques et leurs impacts se concrétisent. Afin de pouvoir identifier l'ensemble des risques auxquels fait face la Ville, cette analyse s'avère un outil essentiel et fondamental.

Une analyse de risques effectuée par la Ville et par les arrondissements relativement à l'AD permettrait à la Ville d'identifier les facteurs pouvant compromettre sa sécurité en matière de confidentialité, d'intégrité ou de disponibilité des données traitées, envoyées et stockées par l'entremise de l'AD. L'analyse de risques est donc la première étape à entreprendre afin d'optimiser la sécurité de l'AD et devrait être réalisée périodiquement par le STI. En effet, les meilleures pratiques suggèrent que cette activité soit faite à l'interne et qu'elle soit documentée. Elle constitue la base pour déterminer les mécanismes de sécurité appropriés dont, entre autres, les paramètres de configuration. De cette analyse de risques découle la manière dont les paramètres de sécurité seront configurés.

CONSTATATION

Bien que certaines analyses de risques soient effectuées globalement par certaines unités d'affaires, les risques spécifiques liés à l'AD ne sont pas pris en compte.

Sans analyse exhaustive des risques relatifs à l'AD de la Ville ou des arrondissements, il s'avère difficile pour les unités d'affaires de mettre en place tous les mécanismes de contrôle requis afin de diminuer l'ensemble des risques liés à l'AD à un niveau acceptable. Si certains risques ne sont pas pris en compte, ils pourraient engendrer des failles de sécurité pouvant être exploitées par des personnes malintentionnées afin de porter atteinte à la sécurité de l'AD, donc aux actifs

informationnels tels que les serveurs et les postes de travail. Ainsi, la confidentialité, l'intégrité et la disponibilité des données ne seraient plus assurées.

3.2.B. Recommandations

Nous recommandons aux unités d'affaires concernées d'intégrer les risques inhérents à l'Active Directory à l'actuel processus récurrent d'analyse de risques des technologies de l'information. Les mécanismes de sécurité de l'Active Directory devront être modifiés en fonction des résultats de cette analyse.

3.2.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.3. FICHIERS JOURNAUX

3.3.A. Contexte et constatations

Un fichier journal est un registre consignant les événements qui se produisent au sein des systèmes et des réseaux de la Ville. Les fichiers journaux sont composés d'entrées de journal; chacune d'entre elles contient des renseignements relatifs à un événement précis qui a eu lieu au sein d'un système ou du réseau. Beaucoup de fichiers journaux contiennent des enregistrements liés à des événements touchant la sécurité informatique. Ces journaux de sécurité peuvent être générés par de nombreuses sources, y compris les systèmes d'exploitation sur les serveurs, les postes de travail, les équipements de réseau, les applications utilisateur et les logiciels de sécurité tels que les logiciels antivirus, les coupe-feu et les systèmes de détection et de prévention d'intrusion.

Le nombre, le volume et la variété des fichiers journaux ont considérablement augmenté au cours des dernières années, ce qui a créé le besoin d'avoir un processus de gestion de ces fichiers journaux qui comprend la production, la transmission, le stockage, l'analyse et l'élimination des données informatiques afférentes aux journaux de sécurité.

La gestion des fichiers journaux est essentielle afin de veiller à ce que les événements de sécurité soient enregistrés avec suffisamment de détails pour une période de temps appropriée. L'analyse des fichiers journaux est essentielle pour détecter les incidents de sécurité, les violations des politiques, les activités frauduleuses ainsi que les problèmes opérationnels.

Les fichiers journaux sont également essentiels au moment de vérifications et d'analyses juricomptables, d'enquêtes internes et pour établir les tendances opérationnelles ainsi que les problèmes à long terme. Ces fichiers journaux peuvent servir de preuves recevables en cour en cas de fraudes ou de malversations dont les auteurs seraient traduits en justice.

Les fichiers journaux doivent en tout temps demeurer exacts et intègres afin d'empêcher qu'ils soient modifiés par des personnes malintentionnées. En effet, les fichiers journaux présents sur les contrôleurs de domaine peuvent être modifiés par des personnes détenant des privilèges d'administrateur de système dont le code d'accès dispose de tous les privilèges (lecture, écriture et suppression). Par conséquent, une personne ayant des droits d'administrateur de système pourrait commettre des gestes illicites et ensuite effacer toute trace de ses gestes dans les fichiers journaux.

CONSTATATION

Nous avons constaté que les événements afférents à l'AD sont enregistrés dans des fichiers journaux. Cependant, ces derniers ne sont pas automatiquement envoyés, en temps réel, sur un serveur dédié où les administrateurs de système y auraient accès en lecture seulement. En conséquence, les personnes disposant des droits d'administrateur de l'AD pourraient effectuer des gestes illicites, intentionnels ou non, et, compte tenu de leurs privilèges élevés, pourraient sans aucune difficulté supprimer les traces de leurs actes dans les fichiers journaux. Ainsi, en cas d'enquête, il serait impossible de retracer les événements et de remonter à l'auteur des faits. De plus, en cas de recours en justice, en l'absence de fichiers journaux intègres, il serait difficile de les présenter en tant que preuves recevables en cour.

CONSTATATION

Nous avons également constaté que les administrateurs de l'AD ne consultent pas les fichiers journaux sur une base continue. Ces journaux sont vérifiés *ad hoc* lorsque des problèmes surviennent. Cependant, compte tenu de la quantité de renseignements présents au sein de ces journaux et en l'absence d'outils automatisés de filtrage des événements systèmes, les administrateurs de système ne disposeraient pas du temps nécessaire pour détecter manuellement des événements suspects survenus dans l'AD. Ils ne pourraient pas être aptes à répondre de manière proactive aux problèmes potentiels et aux bris de sécurité.

3.3.B. Recommandations

Nous recommandons à l'unité d'affaires concernée de :

- **mettre en place les outils nécessaires afin de disposer d'un serveur dédié et centralisé pour la journalisation des événements. L'accès à ce serveur devrait être restreint uniquement en mode consultation pour les administrateurs de système du secteur responsable de la sécurité opérationnelle des technologies de l'information. Tous les droits d'accès privilégiés à ce serveur, par exemple en écriture, modification et suppression, pourraient être octroyés au service de la sécurité de l'information qui n'a pas la responsabilité de gérer la sécurité tactique et opérationnelle de l'environnement de l'AD. Cette mesure assurerait une séparation adéquate des tâches;**
- **réviser régulièrement les fichiers journaux afin d'être en mesure de détecter promptement les problèmes et les anomalies.**

3.3.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec l'unité d'affaires concernée. Elle va nous communiquer son plan d'action ultérieurement.

3.4. LOGICIEL ANTIVIRUS

3.4.A. Contexte et constatations

Les contrôleurs de domaine constituent le cerveau et la moelle épinière de l'AD. En ne les protégeant pas adéquatement contre les logiciels malveillants, ils pourraient être victimes d'un virus informatique.

Un logiciel antivirus, communément appelé antivirus, est une application permettant de détecter, de neutraliser et d'éradiquer les logiciels malveillants (p. ex. virus, chevaux de Troie, vers). Les logiciels malveillants, ou maliciels, sont créés et propagés sur Internet dans le but de compromettre la sécurité et le fonctionnement des systèmes informatiques.

Les antivirus disposent en général de deux modes de fonctionnement. Le premier consiste à vérifier en temps réel les nouveaux fichiers et les courriels. Le second consiste à effectuer un examen complet *ad hoc* de l'ensemble des données présentes sur l'ordinateur (qu'elles soient sur le disque dur, sur un support amovible ou dans la mémoire).

Afin de détecter les logiciels malveillants, l'antivirus utilise un fichier de signatures (contenant les signatures virales des maliciels) et effectue un appariement de ces signatures virales avec les données de l'ordinateur.

Pour qu'un antivirus soit efficace, il est primordial que le fichier de signatures soit maintenu à jour afin qu'il soit apte à détecter promptement les logiciels malicieux. Un antivirus avec un fichier de signatures obsolète revient à ne pas avoir d'antivirus puisqu'il ne pourra pas déceler les virus les plus récents.

L'antivirus génère également des rapports et des alertes afin que les administrateurs de système puissent être avisés en temps opportun des infections détectées ou potentielles. Il est nécessaire que les infections soient traitées le plus rapidement possible afin d'éviter la propagation des maliciels sur tous les postes de travail et les serveurs des environnements Windows. À cet effet, les saines pratiques de sécurité recommandent que les alertes soient envoyées en temps réel aux boîtes de courriels ou aux téléavertisseurs des administrateurs et que ceux-ci consultent régulièrement les rapports.

CONSTATATION

Pour deux des sept AD qui comportent un total de six contrôleurs de domaine, nous avons constaté :

- **que quatre contrôleurs de domaine ne disposaient pas d'un logiciel antivirus;**
- **qu'un contrôleur de domaine avait un antivirus, mais que celui-ci était désactivé;**
- **que pour le dernier contrôleur de domaine, l'antivirus n'avait pas son fichier de signatures à jour.**

Advenant une infection par un virus, ce n'est pas seulement les contrôleurs de domaine qui seront compromis, mais l'ensemble des ressources de l'AD, telles que les postes de travail et les autres serveurs. Dans une telle situation, une attaque virale aurait également une portée de plus grande ampleur. Il est reconnu que le niveau d'infection et les dommages afférents sont directement liés à la rapidité d'intervention et d'éradication des maliciels.

3.4.B. Recommandations

Nous recommandons aux unités d'affaires concernées :

- **de s'assurer que tous les contrôleurs de domaine ont un antivirus dont les fichiers de signatures sont mis à jour régulièrement;**

- **de mettre en place un processus formel et récurrent (idéalement quotidien) de révision des rapports des logiciels antivirus.**

3.4.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.5. STRATÉGIES DE MOTS DE PASSE

3.5.A. Contexte et constatations

Les stratégies de mots de passe permettent d'exiger des utilisateurs le choix de mots de passe robustes. Ces stratégies utilisent plusieurs paramètres de sécurité dont, entre autres, la longueur du mot de passe, sa complexité, son délai d'expiration et l'historique des derniers mots de passe utilisés.

Une des stratégies oblige l'utilisateur à changer son mot de passe régulièrement. Généralement, plus la période entre les changements est courte, plus le niveau de sécurité est rehaussé. Quant à la longueur du mot de passe, plus il est long, plus le niveau de sécurité est étanche.

Le STI a défini la procédure intitulée *Standard sur les clefs d'accès aux ressources informationnelles,* qui stipule les exigences des mots passe telles que le délai d'expiration, la longueur minimale et l'historique.

Dans la procédure intitulée *Standard sur les clefs d'accès aux ressources informationnelles* du STI, les exigences mentionnées à la rubrique 3.2 « Mots de passe » sont les suivantes :

- Utilisateur régulier :
  - Délai d'expiration : 90 jours,
  - Longueur des mots de passe : huit caractères minimum,
  - Historique : six derniers mots de passe;
- Administrateur :
  - Délai d'expiration : non spécifié donc le même que celui d'un utilisateur régulier,
  - Longueur des mots de passe : huit caractères minimum,
  - Composition des mots de passe : doivent être formés au minimum d'une lettre majuscule, d'une lettre minuscule, d'un chiffre et d'un caractère spécial,
  - Historique : non spécifié donc le même que celui d'un utilisateur régulier.

Ces standards, qui découlent de la politique de sécurité de l'information de la Ville, s'appliquent à l'ensemble des unités administratives, y compris les 19 arrondissements. Ils sont essentiels, car ils assurent un niveau de sécurité constant d'un contrôleur de domaine à un autre et, par conséquent, des AD.

Nous avons comparé le standard de la Ville, qui est de 90 jours, aux meilleures pratiques proposées par Microsoft qui recommande un délai de 30 à 90 jours. Il est à noter qu'au moment de la réalisation de nos tests en octobre 2010, le standard de la Ville pour le délai d'expiration de n'importe quel mot de passe était fixé à 30 jours. Le 28 janvier 2011, le STI a augmenté le délai d'expiration du mot de passe Windows à 90 jours de même que celui des mots de passe pour accéder à Internet, à l'application SIMON et à l'ordinateur central IBM. Bien que le délai fixé à 90 jours respecte les bonnes pratiques, il atteint la limite du niveau de sécurité minimal.

La longueur et la complexité des mots de passe sont deux composantes ajoutant à la sécurité du réseau. À titre d'exemple, si nous comptons les 26 lettres de l'alphabet et y ajoutons les 10 chiffres (0 à 9), un mot de passe d'une longueur de six caractères génère 2,1 milliards de possibilités (36 à la puissance 6), et un mot de passe de huit caractères, 2,8 billions de possibilités (36 à la puissance 8). De nos jours, en considérant le nombre d'outils de décryptage de mots de passe accessibles sur Internet, leur développement et leur amélioration constante par des pirates informatiques, il est plus important que jamais d'utiliser un mot de passe complexe qui dépasse les simples mots du dictionnaire ou les combinaisons rudimentaires de chiffres (p. ex. 11111111).

Quant à l'historique des mots de passe, ce paramètre permet à l'AD d'en mémoriser un certain nombre afin que les utilisateurs et les administrateurs de l'AD ne puissent pas, au cours du changement d'un mot de passe, réutiliser le même ou un déjà utilisé antérieurement.

CONSTATATION

Nous avons constaté les faiblesses suivantes :

- **Délai d'expiration : pour un AD sur sept, les mots de passe n'ont aucun délai d'expiration, c'est-à-dire qu'un utilisateur n'est pas forcé par le système de changer son mot de passe; il peut garder le même indéfiniment;**
- **Longueur minimale : pour cinq AD sur sept, la longueur minimale des mots de passe est inférieure au minimum requis par les standards de la Ville;**
- **Complexité : pour cinq AD sur sept, la complexité des mots de passe n'était pas activée.**

Avec des stratégies de mots de passe inadéquates, les mots de passe des utilisateurs et des administrateurs de système pourraient être facilement découverts, car il a été prouvé que la robustesse d'un mot de passe est directement proportionnelle à la fréquence du délai d'expiration, à la longueur minimale ainsi qu'à sa complexité. Advenant que des personnes malintentionnées réussissent à découvrir des mots de passe afférents à des comptes à privilèges élevés, la sécurité des contrôleurs de domaine et des actifs gérés par les AD serait compromise.

3.5.B. Recommandations

Nous recommandons aux unités d'affaires concernées de paramétrer le délai d'expiration, la longueur minimale et la complexité des mots de passe de manière à respecter les exigences du standard de la Ville.

3.5.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.6. STRATÉGIES DE VERROUILLAGE DE COMPTES

3.6.A. Contexte et constatations

Les stratégies de verrouillage de comptes sont utilisées pour tout type de compte, aussi bien pour les administrateurs que pour les utilisateurs réguliers, et déterminent principalement la durée pendant laquelle un compte est inaccessible à la suite de tentatives d'accès infructueuses. Nous avons examiné la valeur des trois paramètres suivants en tenant compte des normes édictées dans le standard de la Ville (établi par le STI) :

- « Durée de verrouillage de comptes » : ce paramètre de sécurité détermine le nombre de minutes durant lequel un compte reste verrouillé avant d'être déverrouillé automatiquement. Le standard est fixé à 15 minutes;
- « Seuil de verrouillage de comptes » : ce paramètre de sécurité définit le seuil du nombre de tentatives d'ouverture de session infructueuses avant de provoquer le verrouillage d'un compte d'utilisateur. Un compte verrouillé ne peut être réutilisé qu'au moment de sa réinitialisation par un administrateur ou à l'expiration de la durée de verrouillage du compte. Le standard suggère que le compte se verrouille après trois tentatives infructueuses;
- « Réinitialiser le compteur de verrouillage du compte après » : ce paramètre de sécurité détermine le nombre de minutes qui doivent s'écouler après une tentative d'ouverture de

session infructueuse pour que le compteur de tentatives d'ouverture de session infructueuses soit remis à zéro. Le standard est fixé à 15 minutes.

CONSTATATION
Pour deux des sept AD, nous avons constaté que le verrouillage de comptes avait été désactivé.

Cette situation permet à une personne non autorisée équipée d'outils spécialisés d'effectuer un nombre illimité de tentatives d'intrusion sur les contrôleurs de domaine. En cas de réussite, la sécurité des contrôleurs de domaine et des actifs gérés par les AD serait compromise.

CONSTATATION
De plus, pour un AD, la valeur du paramètre de verrouillage a été fixée à huit, alors que pour deux AD la valeur du paramètre a été fixée à cinq. Dans ces trois cas, la valeur fixée dépasse le standard de la Ville qui est de trois.

3.6.B. Recommandations

Nous recommandons aux unités d'affaires concernées de définir les stratégies de verrouillage de comptes selon les standards de la Ville.

3.6.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.7. COMPTES À PRIVILÈGES ÉLEVÉS

3.7.A. Contexte et constatations

Une personne qui possède un compte à privilèges élevés pourrait obtenir des droits illimités à l'AD, incluant les contrôleurs de domaine et les postes de travail. Ces comptes sont octroyés aux personnes sur la base des qualifications nécessaires qu'elles possèdent dans l'environnement Windows, de leurs compétences en sécurité informatique et de leur expertise en architecture réseau. Ces personnes doivent être dignes de confiance. De plus, les tâches des personnes détenant un compte à privilèges élevés ne doivent pas être incompatibles avec d'autres fonctions que la personne occupe afin de respecter le principe fondamental d'une bonne séparation des tâches.

Les privilèges élevés comprennent, entre autres, les accès aux journaux d'événements et aux journaux d'audit. Un individu qui s'approprie des droits élevés dans le but de commettre des actes illicites pourrait ainsi procéder à l'effacement de ses traces dans les fichiers journaux.

CONSTATATION

Pour six des sept AD, nous avons constaté la présence d'un grand nombre de comptes à privilèges élevés qui ne sont pas justifiés par des besoins d'affaires. Cette situation pourrait signifier que ces comptes sont inutilisés ou qu'ils ont été octroyés à des personnes sans véritable justification, ce qui augmente considérablement la possibilité d'utilisation non autorisée de privilèges élevés.

CONSTATATION

Pour un AD, nous avons noté que des comptes à privilèges élevés étaient associés à des groupes qui ne devraient pas disposer de privilèges importants : comptes associés à des consultants et à des stagiaires, des « comptes pour tests » et des comptes dits « génériques ». Pour ces derniers, le principal danger est que les mots de passe peuvent circuler parmi plusieurs employés. Si plusieurs individus utilisent les comptes génériques, il serait difficile de déterminer l'imputabilité des actions inscrites dans les journaux d'événements ou d'audit.

CONSTATATION

Pour cinq des huit AD vérifiés, nous avons constaté la présence de comptes ayant le libellé « Administrateur » ou « Administrator ». Ces derniers représentent des proies évidentes pour des tentatives d'intrusion et de contrôle complet de l'AD. Normalement, un compte avec un nom générique et facilement identifiable doit être renommé ou on doit lui enlever ses droits. Ainsi, une personne malveillante pourrait prendre le contrôle total de l'AD et compromettre la sécurité des données, des serveurs et des postes de travail.

La présence d'un trop grand nombre de comptes à privilèges élevés qui ne sont pas justifiés par des besoins d'affaires augmente considérablement les probabilités qu'une personne malintentionnée utilise l'un de ces comptes pour prendre le contrôle de l'AD afin de commettre des actes frauduleux. Advenant de telles actions, la sécurité des actifs, au chapitre de la confidentialité, de l'intégrité et de la disponibilité, ne pourrait plus être assurée.

3.7.B. Recommandations

Nous recommandons aux unités d'affaires concernées de :

- **réduire le nombre de comptes à privilèges élevés afin qu'ils ne soient octroyés qu'à des personnes légitimes;**
- **retirer les privilèges élevés aux types de comptes suivants :**
  - **consultants,**
  - **stagiaires,**
  - **comptes pour tests,**
  - **comptes génériques;**
- **renommer les comptes « Administrateur » et « Administrator » autrement.**

3.7.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.8. NORMES DE CONFIGURATION DES CONTRÔLEURS DE DOMAINE

3.8.A. Contexte et constatations

Les normes de configuration des contrôleurs de domaine sont des guides techniques qui précisent les valeurs de l'ensemble des paramètres de configuration à appliquer au moment de l'installation des serveurs. Ces paramètres de configuration découlent directement des directives et des procédures de sécurité. Ainsi, l'administrateur de système sait exactement, au moment de l'installation du système d'exploitation, quelle valeur accorder à chaque paramètre de configuration pour que les contrôleurs de domaine soient conformes aux exigences de sécurité de la Ville.

De plus, ces normes sont nécessaires afin d'avoir un niveau de sécurité homogène, puisque tous les contrôleurs de domaine seront configurés uniformément, réduisant ainsi les risques qu'un contrôleur de domaine dispose d'une configuration moins sécuritaire.

CONSTATATION

Dans certains cas, les procédures d'installation et de configuration des contrôleurs de domaine sont documentées, mais n'ont jamais été mises à jour depuis. Dans d'autres cas, nous avons constaté l'absence de normes ou de guide de configuration des contrôleurs de domaine. Les serveurs sont configurés selon les connaissances des administrateurs de système.

3.8.B. Recommandations

En l'absence de mise à jour des procédures d'installation, les paramètres de configuration pourraient ne pas refléter les exigences de sécurité de la Ville. Ainsi, les nouveaux contrôleurs de domaine pourraient être installés avec des paramètres de configuration inadéquats, les rendant potentiellement vulnérables à un bris de sécurité. Nous recommandons aux unités d'affaires concernées de développer ou de mettre à jour les procédures d'installation des contrôleurs de domaine.

3.8.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.9. SERVICES NON ESSENTIELS

3.9.A. Contexte et constatations

Un « service » est un type d'application qui s'exécute en arrière-plan au sein du système d'exploitation. Les services ne sont pas utilisés directement par les utilisateurs, mais ils fournissent des fonctionnalités essentielles pour les serveurs Internet, les serveurs de courrier électronique ou les serveurs de bases de données. Les services sont généralement de « longue durée », c'est-à-dire qu'ils s'exécutent au démarrage du système et ne s'arrêtent qu'à la fermeture de l'ordinateur.

Selon les pratiques recommandées par l'industrie, seuls les services nécessaires et essentiels doivent être activés sur les contrôleurs de domaine. Cette mesure s'explique, d'une part, par le fait que certains services amènent des risques de sécurité qui seront d'autant plus élevés si le serveur est de type contrôleur de domaine et, d'autre part, du fait que chaque service s'accapare les ressources du système, ce qui pourrait engendrer des problèmes de performance et, par conséquent, une détérioration de la disponibilité de ce dernier. De plus, en appliquant le principe de ne garder que les services strictement nécessaires au bon fonctionnement des contrôleurs de

domaine, cela réduit d'autant les possibilités offertes aux individus malintentionnés d'obtenir des accès non autorisés par le biais de ces services.

Les paramètres de configuration pour l'activation (ou le démarrage) des services peuvent prendre les valeurs suivantes :

- « Automatique » : le service est démarré automatiquement au moment de l'ouverture de l'ordinateur;
- « Manuel » : le service peut être démarré manuellement soit par l'administrateur de système, soit par un autre service qui en dépend;
- « Désactivé » : le service n'est pas démarré.

Compte tenu de ces paramètres, tous les services qui ne sont pas essentiels au fonctionnement des serveurs contrôleurs de domaine doivent être configurés avec le paramètre « désactivé ». Ainsi, ces services ne peuvent pas être activés sans l'intervention d'un administrateur de système.

Afin de nous assurer que seuls les services essentiels étaient activés sur les serveurs de contrôleurs de domaine des unités d'affaires auditées, nous avons obtenu, pour chacun de ces serveurs, la liste des services incluant leurs paramètres de configuration.

CONSTATATION

Nous avons constaté que, pour l'ensemble des unités d'affaires vérifiées, plusieurs services non essentiels n'étaient pas désactivés. Par exemple, nous avons remarqué, pour certaines unités d'affaires, que les services suivants n'étaient pas désactivés :

- ***IIS Admin Service*** **: ce service permet au serveur de gérer les services Internet (p. ex. serveur Web). À l'aide de ce service, des personnes non autorisées pourraient prendre le contrôle total du système à cause des nombreuses failles de sécurité des sites Internet. De plus, il est vivement déconseillé qu'un serveur Internet coexiste sur le même serveur qu'un contrôleur de domaine. Advenant une intrusion sur le site Internet, ce n'est pas seulement le serveur Internet qui serait compromis, mais l'ensemble de l'AD et de ses ressources;**
- ***Indexing Service*** **: ce service permet d'indexer le contenu et les propriétés des fichiers sur les ordinateurs locaux ou distants. En conséquence, une personne malintentionnée pourrait avoir des accès non autorisés aux données présentes dans ces fichiers et compromettrait donc la confidentialité et l'intégrité de ces données;**
- ***Special Administrator Console Helper*** **: ce service permet d'effectuer des commandes d'administration de systèmes à distance. Par conséquent, une personne malintentionnée pourrait exploiter ce service et prendre le contrôle du système, ce qui pourrait compromettre la sécurité des contrôleurs de domaine et de l'AD;**
- ***Application Management*** **: ce service fournit des fonctionnalités d'installation de logiciel (assignation, publication et suppression). Des personnes malintentionnées pourraient utiliser ce service pour installer des logiciels malveillants ou, tout simplement, pour supprimer des applications essentielles des postes des utilisateurs, ce qui pourrait entraîner une perte de disponibilité des systèmes;**
- ***Distributed Link Tracking Client*** **: ce service permet aux programmes clients de retracer les fichiers qui ont été déplacés au sein du système ou d'un autre ordinateur. Par l'intermédiaire de ce service, des personnes malintentionnées pourraient avoir accès à de l'information confidentielle afférente à certaines applications (p. ex. dossier d'employé, peu importe où il se trouve sur le système) et ainsi compromettre la confidentialité des données;**
- ***Portable Media Serial Number Service*** **: ce service permet de récupérer le numéro de série de n'importe quel lecteur multimédia portatif branché à l'ordinateur. À l'aide de ce service, des personnes malintentionnées pourraient télécharger du contenu protégé sur le périphérique et ainsi compromettre la confidentialité des données.**

La valeur du paramètre de démarrage des services non essentiels n'étant pas adéquatement configurée, le risque d'une attaque sur les serveurs s'en trouve accru, ce qui permettrait à des personnes malintentionnées d'obtenir des accès privilégiés, tels des droits d'administrateur, et de prendre le contrôle de l'ensemble du serveur.

Dans un tel cas, non seulement la sécurité des contrôleurs de domaine serait compromise, mais l'ensemble de la sécurité de l'AD le serait tout autant. En conséquence, la confidentialité, l'intégrité et la disponibilité des données et des ressources ne seraient plus assurées.

3.9.B. Recommandations

Afin d'augmenter le niveau de sécurité logique des serveurs contrôleurs de domaine, nous recommandons aux unités d'affaires concernées d'activer uniquement les services essentiels liés aux besoins de la Ville et de désactiver les services non essentiels.

3.9.C. Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec les unités d'affaires concernées. Elles vont nous communiquer leur plan d'action ultérieurement.

3.10. CORRECTIFS DE SÉCURITÉ DES CONTRÔLEURS DE DOMAINE

3.10.A.Contexte et constatations

Une faille de sécurité informatique est une vulnérabilité au sein d'un système d'information qui permet à une personne malintentionnée de l'exploiter et de menacer la sécurité du système d'exploitation.

En exploitant ces vulnérabilités, les individus malintentionnés peuvent aller jusqu'à prendre le contrôle des serveurs et des postes de travail. Les failles de sécurité sont généralement colmatées très rapidement par les fournisseurs de logiciels à l'aide d'un correctif de sécurité. Cependant, si les correctifs ne sont pas appliqués régulièrement sur les serveurs, ces derniers restent vulnérables non seulement aux failles récentes, mais également aux anciennes failles.

Concernant l'AD, Microsoft corrige ces vulnérabilités logicielles au fur et à mesure de leur découverte au moyen de correctifs de sécurité appelés « Service Pack » ou « Hotfix ». C'est pourquoi il est important de maintenir les contrôleurs de domaine à jour avec les correctifs fournis par Microsoft, d'autant plus que les procédures d'exploitation des vulnérabilités sont souvent documentées et rendues accessibles au public sur Internet.

L'installation des correctifs de sécurité permet aux administrateurs de système de restreindre les possibilités d'attaques de la part d'individus malveillants.

CONSTATATION

Nous avons constaté pour un AD d'une unité d'affaires vérifiée que les trois contrôleurs de domaine n'avaient pas été mis à jour depuis juin 2010. Cela signifie que ces contrôleurs de domaine sont vulnérables à des attaques utilisant les failles découvertes depuis juin 2010.

Advenant de telles attaques, des personnes non autorisées pourraient obtenir des accès de type « administrateur » et prendre le contrôle de l'AD et de ses ressources (p. ex. poste de travail, serveur de fichiers, données).

3.10.B.Recommandations

Nous recommandons à l'unité d'affaires concernée de mettre en place un processus formel de mise à jour des correctifs de sécurité sur ses serveurs. Ce processus devra inclure des tests d'installation des correctifs en environnement de test ou de développement afin de s'assurer que les correctifs qui seront installés en production ne pourront pas causer de problèmes à la suite d'incompatibilités avec certaines applications.

3.10.C.Plan d'action de l'unité d'affaires concernée

Nos recommandations ont été validées avec l'unité d'affaires concernée. Elle va nous communiquer son plan d'action ultérieurement.

4. ANNEXE

4.1. GLOSSAIRE DES TERMES DE L'ACTIVE DIRECTORY

Cette annexe présente, par ordre alphabétique, la définition des termes afférents à l'AD.

CONTRÔLEUR DE DOMAINE :

Un contrôleur de domaine est un serveur qui stocke un duplicata de l'annuaire AD. Il assure la propagation des modifications apportées sur l'annuaire. Il assure également l'authentification et l'ouverture des sessions des utilisateurs ainsi que les recherches dans l'annuaire. Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Chaque contrôleur de domaine est capable de recevoir ou de dupliquer les modifications de l'ensemble de ses homologues du domaine. Les paramètres de sécurité appliqués au contrôleur de domaine sont primordiaux, car si la sécurité du contrôleur de domaine est compromise, c'est l'ensemble de la sécurité de l'AD qui sera alors compromise.

DOMAINE :

Un domaine est l'unité de base de la structure de l'AD. C'est un ensemble d'ordinateurs ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine a un nom unique sur le réseau. Le domaine sert de limite de sécurité en restreignant les droits d'un administrateur ou de tout autre utilisateur avec pouvoir, uniquement aux ressources de ce domaine.

RELATION D'APPROBATION (*TRUST*) :

Une relation d'approbation permet aux utilisateurs d'un AD d'accéder aux ressources d'un autre AD.