Gestion du système Artemis

Service de sécurité incendie de Montréal
Service des technologies de l'information

3.7.

Le 1er mars 2023

Rapport annuel 2022
Bureau du vérificateur général
de la Ville de Montréal

Gestion du système Artemis

Mise en contexte

Pour répondre continuellement aux appels et à l'instar des corps de sapeurs-pompiers de plusieurs grandes villes canadiennes, le Centre de communication en sécurité incendie (CCSI) du Service de sécurité incendie de Montréal (SIM) utilise un système informatique de répartition des appels appelé Artemis depuis novembre 2007. Le SIM, qui compte 67 casernes, est l'unique corps de ce genre dans toute l'agglomération de Montréal à assurer la sécurité de la population montréalaise.

Ainsi, il est crucial pour lutter efficacement contre les incendies et répondre aux appels, que le SIM, plus précisément le CCSI, puisse s'appuyer sur un système performant avec une haute disponibilité visant à distribuer les appels entrants parmi les 2 739 membres du personnel du service. En 2022, ceux-ci ont pris en charge 118 916 interventions d'urgence incendie et à titre de premiers répondants dans la Ville de Montréal (la Ville).

Objectif de l'audit

Déterminer si les mécanismes de contrôle en place permettent une saine gestion ainsi qu'une haute disponibilité du système Artemis du SIM.

Résultats

Globalement, nous concluons que la Ville a mis en place plusieurs mécanismes de contrôle assurant une saine gestion du système Artemis. En effet, la définition des rôles et responsabilités, le processus de gestion des correctifs et des mises à jour, la surveillance des niveaux de services, les ressources humaines spécialisées, les comptes à haut privilèges et le plan de relève informatique sont adéquats.

Cependant, certains éléments nécessitent des améliorations, dont les paramètres d'authentification d'Artemis, la procédure sur la gestion des accès logiques à hauts privilèges, la documentation fonctionnelle de l'environnement du système d'Artemis et les mécanismes d'alertes automatisées pour les incidents.

Principaux constats

Gouvernance

→ Les rôles et responsabilités des parties prenantes à la gouvernance et la gestion du système Artemis sont documentés.

Gestion des accès logiques

→ Aucun compte obsolète à hauts privilèges n'est présent dans Artémis.

→ Le standard de la Ville sur la gestion des accès logiques qui décrit les exigences sur les paramètres d'authentification n'est pas appliqué à Artemis 2.6.

→ Il n'existe pas de procédure de gestion des accès logiques à hauts privilèges pour Artemis, Smartemis et Artemis Web.

Gestion des correctifs et des mises à jour

→ L'implantation de la nouvelle version d'Artemis a été réalisée selon les meilleures pratiques. Cependant, ce processus n'est pas documenté dans une procédure.

Gestion des incidents

→ La procédure de gestion des incidents d'Artemis respecte les saines pratiques.

→ Aucun mécanisme d'alertes automatisées n'est en place dans l'environnement Artemis. Cependant, le personnel du CCSI, étant présent en tout temps, détecterait en temps réel tout problème.

Surveillance

→ Des niveaux de services avec le fournisseur intégrateur sont définis et suivis lors des rencontres du comité de pilotage.

Ressources spécialisées

→ Le SIM et le Service des technologies de l'information (STI) comptent un nombre suffisant de ressources humaines spécialisées en soutien au maintien en conditions opérationnelles du système Artemis.

Documentation fonctionnelle

→ La documentation fonctionnelle d'Artemis n'est pas systématiquement mise à jour à chaque changement de son environnement.

Relève informatique

→ Un plan de relève informatique adéquat a été développé et fait l'objet de tests annuels.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées aux pages suivantes.

Liste des sigles

Artemis
Système Artemis

CAC
Comité d'approbation des changements

CCSI
Centre de communication en sécurité incendie

CDS
Centre de service TI

DDC
Demande de changement

DSP
Division Sécurité publique

GPRAO
Solution Artemis de dépannage

la Ville
la Ville de Montréal

MOP
Manuel d'organisation de projet

RACI
Réalisateur, Approbateur, Consulté et Informé

RAO
Répartition automatisée par ordinateur

SGI
Système de gestion des interventions

SIM
Service de sécurité incendie de Montréal

SSDO
Système de suivi des données opérationnelles

STI
Service des technologies de l'information

Table des matières

1. Contexte **271**

1.1. Description du système Artemis 272

2. Objectif de l'audit, critères d'évaluation et portée des travaux **275**

2.1. Objectif de l'audit 275

2.2. Critères d'évaluation 275

2.3. Portée des travaux 277

3. Résultats de l'audit **278**

3.1. Gouvernance 278

3.2. Gestion des accès logiques 279

3.2.1. Paramètres d'authentification 279

3.2.2. Procédure de gestion des accès logiques à hauts privilèges 282

3.3. Gestion des correctifs et des mises à jour 284

3.4. Gestion des incidents 286

3.5. Surveillance 288

3.6. Ressources spécialisées 289

3.7. Documentation fonctionnelle 290

3.8. Relève informatique 291

4. Conclusion **293**

1. Contexte

Le service 9-1-1 a débuté officiellement ses opérations à Montréal le 1er décembre 1985. Avec l'arrivée des téléphones mobiles, ce service a évolué pour pouvoir recevoir tous les appels des téléphones filaires et des téléphones intelligents. En parallèle, le Centre de communication en sécurité incendie (CCSI) du Service de sécurité incendie de Montréal (SIM) effectuait la répartition des appels et faisait face à une augmentation importante de leur nombre. En 2002, à la suite des fusions municipales, le SIM décida de remplacer son système de répartition devenu obsolète.

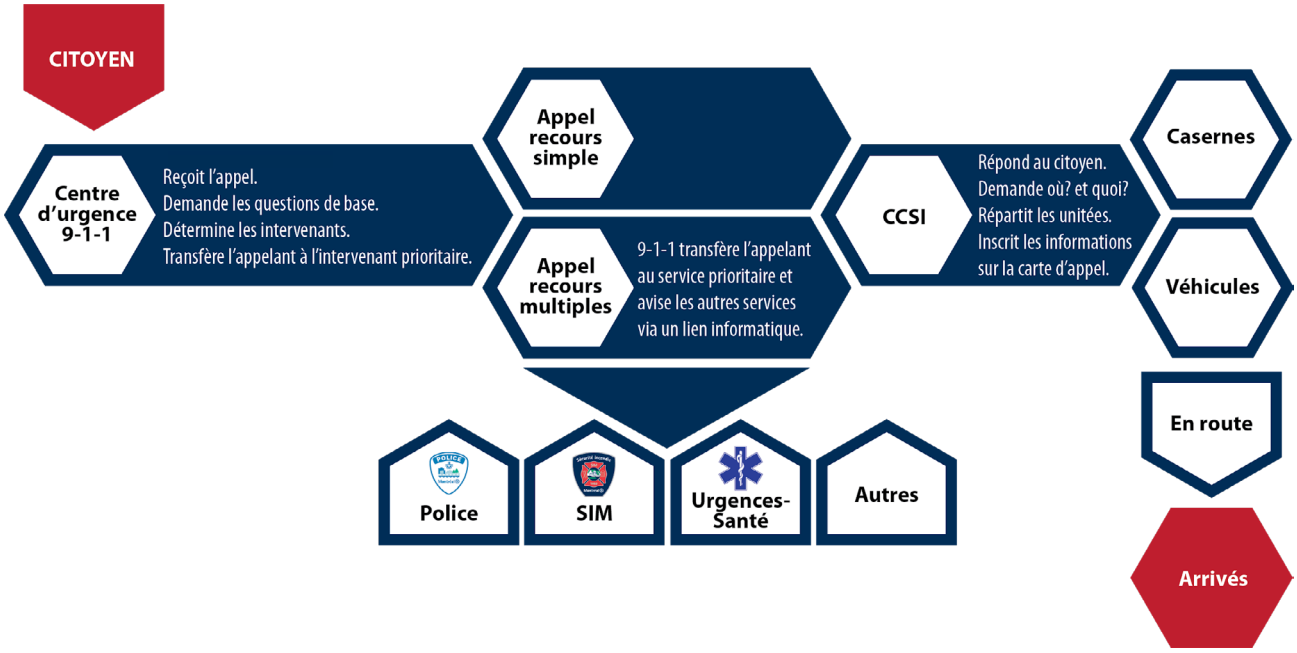
À l'instar des corps de sapeurs-pompiers de plusieurs grandes villes canadiennes, le SIM utilise un système informatique de répartition des appels – soit un système de répartition automatisée par ordinateur (RAO) – communément appelé Artemis depuis novembre 2007. La même année, le SIM a commencé à offrir des soins préhospitaliers d'urgence en tant que premier répondant lors des appels urgents en provenance du 911[1]. Le SIM, qui compte 67 casernes, est l'unique corps de ce genre dans toute l'agglomération de Montréal à assurer la sécurité des Montréalaises et Montréalais.

Ainsi, il est crucial pour lutter efficacement contre les incendies et répondre aux appels, que le SIM, plus précisément le CCSI, puisse s'appuyer sur un système performant avec une haute disponibilité visant à distribuer les appels entrants parmi les 2 739 membres du personnel du service. En 2022, ceux-ci ont pris en charge 118 916 interventions d'urgence incendie et à titre de premiers répondants dans la Ville de Montréal (la Ville).

1 « SIM - Rapport des activités 2021 », page 21.

1.1. Description du système Artemis

Voici le schéma des appels au 911 et du RAO - Artemis du CCSI :



Source : Présentation de la division du CCSI intitulée « Module 1 – Présentation du CCSI aux recrues ».

Artemis est le système RAO du SIM, édité historiquement par un fournisseur de solutions. Ce système traite les appels en provenance des centres d'urgence. Il permet aux agentes et agents du CCSI de coordonner les interventions menées sur le terrain et de dépêcher les ressources à la grandeur du territoire de l'île de Montréal. Comme chaque seconde compte lors des interventions du SIM, l'utilisation d'Artemis permet d'en réduire les délais et d'optimiser les opérations.

Le système Artemis est composé de plusieurs applications reliées à celui-ci permettant aux intervenantes et intervenants du SIM de gérer du début à la fin les urgences :

- **Artemis version 2.6 (Artemis 2.6)** : ce système constitue le module principal utilisé par le CCSI à travers les ordinateurs des centres de répartition, dans le centre principal et le centre de relève. Il communique avec les modules Artemis mobile et Artemis caserne, ainsi qu'avec Smartemis et Artemis Web.

  Celui-ci comporte, notamment, les fonctionnalités de prise d'appel et de traitement de l'appel, de gestion des interventions et des véhicules, de relocalisation[2], de réassignation des véhicules, de gestion de la cartographie Artemis maps et d'envoi de commentaires ou de consignes.

2 Relocalisation : consiste à redistribuer les véhicules en fonction des appels reçus pour assurer une couverture optimale du territoire.

- **Artemis maps** : cette composante cartographique d'Artemis est utilisée par le CCSI pour planifier, superviser les interventions et permettre aux pompières et pompiers dans les véhicules et casernes de disposer d'une visualisation détaillée du secteur d'intervention.
- **Artemis mobile** : ce module d'Artemis est installé sur les ordinateurs véhiculaires des camions d'urgence qui communique avec Artemis 2.6. Il fournit des informations dans des cartes pour déterminer, entre autres, le meilleur chemin de déplacement en fonction des fermetures de rues. Il permet aux pompières et pompiers d'enregistrer, en temps réel, leur statut concernant l'appel en cours. De plus, il présente des informations clés liées aux lieux d'interventions telles que les matières dangereuses et l'état de la construction.
- **Artemis caserne** : ce module d'Artemis est installé sur les ordinateurs des postes de garde des casernes, chacun connecté à une imprimante, pour la réception et l'acquittement des ordres de mission pour les demandes des interventions. Il fournit les informations nécessaires aux pompières et pompiers pour les interventions assignées. Cela permet de déterminer les ressources requises (nombre et type de camions, nombre de pompiers et autres).
- **Smartemis** : cette application comporte quatre fonctions :

  1. Notifications : recevoir en temps réel les notifications d'intervention dès leur répartition;
  2. Synoptique des interventions : visualisation des détails des interventions;
  3. Synoptique des véhicules : visualisation en temps réel des véhicules et leur statut;
  4. Navigation : comment se rendre vers les lieux d'interventions.

  Smartemis est utilisée par la direction du SIM ainsi que les pompières et pompiers selon leur profil d'accès.
- **Artemis Web** : cette application permet d'accéder aux données opérationnelles d'Artemis en dehors des postes utilisateurs (le CCSI, le centre de relève et les casernes) dédiés et à certaines fonctions (p. ex. : les synoptiques des interventions, les synoptiques des véhicules, les historiques des interventions et le chronogramme de l'intervention) depuis un navigateur Internet. Elle est accessible à tout le personnel du SIM avec des restrictions selon leur profil d'accès logique.
- **Solution Artemis de dépannage (GPRAO)** : c'est la solution Artemis installée sur un poste autonome (portable) pour opérer en mode déconnecté / local en cas de panne du réseau localisé dans le CCSI.
- **Système de suivi des données opérationnelles (SSDO)** : ce système permet la saisie et la compilation des données opérationnelles des interventions du SIM. La base de données (BD) contient les données en provenance d'Artemis automatiquement retranscrites dans les champs du SSDO. C'est un mécanisme de conciliation des données provenant du RAO, des actions posées et des faits consignés sur les lieux des interventions. Pour fin d'approbation, les gestionnaires du SIM signent les interventions avec l'interface de cette BD.

  Ces principales fonctions du système sont l'identification des causes d'incendie, la saisie des données sur les actions posées, la constatation des faits sur les lieux des interventions et la production des rapports pour le ministère de la Sécurité publique.

À la Ville, la gestion du système Artemis est assurée par deux unités d'affaires de la Ville et deux fournisseurs :

- Le SIM :
  - Le Centre de services – planification stratégique et opérationnelle du SIM effectue du support dans la gestion des accès logiques à Smartemis et Artemis Web le temps du transfert à la Division de la planification opérationnelle du CCSI;
  - Le Centre de services – intervention composé notamment du CCSI du SIM réalise le support aux utilisatrices et utilisateurs et communique leurs besoins d'affaires à la Division Sécurité publique (DSP) du STI;
- Le STI :
  - La Division solutions d'affaires – systèmes corporatifs de la DSP de la Direction Sécurité publique et justice du Service des technologies de l'information (STI) est responsable des aspects liés aux infrastructures technologiques et fournit du soutien aux opérations et aux projets d'évolution de l'environnement d'Artemis. Celle-ci travaille étroitement avec le fournisseur intégrateur, responsable de l'impartition de l'environnement Artemis;
- Le fournisseur intégrateur est responsable de la maintenance – l'exploitation et l'évolution – de l'environnement d'Artemis. Il travaille avec le fournisseur de la solution Artemis;
- Le fournisseur de la solution Artemis (fournisseur de solutions) a développé la solution Artemis et il est l'ultime responsable de faire évoluer ce système selon les besoins du SIM.

2. Objectif de l'audit, critères d'évaluation et portée des travaux

2.1. Objectif de l'audit

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit de performance portant sur la Gestion du système Artemis du SIM. Nous avons réalisé cette mission conformément à la *Norme canadienne de missions de certification* (NCMC) 3001 du *Manuel de CPA Canada – Certification.*

Cet audit avait pour objectif de déterminer si les mécanismes de contrôle, mis en place pour la Gestion du système Artemis, permettent une saine gestion ainsi qu'une haute disponibilité du système Artemis du SIM.

2.2. Critères d'évaluation

Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances, soit :

1. Gouvernance

Les rôles et responsabilités liés à la gouvernance et à la gestion du système sont documentés, complets, approuvés, à jour et formellement diffusés auprès des parties prenantes et mis en application par ces dernières.

2. Gestion des accès logiques

Un encadrement sur les paramètres d'authentification est défini et appliqué de façon appropriée à Artemis.

Une procédure de gestion des accès logiques (création, modification, révocation, révision, suppression et surveillance des droits d'accès privilégiés) a été développée et est connue et suivie par les parties prenantes à cette gestion.

3. Gestion des correctifs et des mises à jour

Un processus formel de gestion des correctifs et des mises à jour a été défini et est appliqué de façon appropriée.

Un suivi formel et régulier est réalisé avec l'ensemble des parties prenantes à la gestion des correctifs et des mises à jour et les actions appropriées sont appliquées.

4. Gestion des incidents

Une procédure de gestion des incidents a été développée, approuvée, diffusée aux parties prenantes et appliquée par celles-ci ainsi que révisée selon la fréquence prédéfinie.

5. Surveillance

Une surveillance adéquate est effectuée par le fournisseur incluant la définition des niveaux de services et une reddition de comptes à cet égard, ainsi qu'une journalisation d'événements de sécurité prédéfinis qui fait l'objet d'un suivi sur une base régulière.

6. Ressources spécialisées

Des ressources spécialisées en répartition des appels sont en nombre suffisant dans l'ensemble des parties prenantes à la gestion d'Artemis.

Un plan de relève de ressources humaines ainsi qu'un programme de formation sur Artemis sont en place.

7. Documentation fonctionnelle

De la documentation technique couvrant la configuration, l'utilisation et l'environnement a été développée par les parties prenantes à la gestion de ces systèmes (c'est-à-dire le STI, le SIM et le fournisseur intégrateur).

Ces documents sont à jour, approuvés, connus et utilisés par l'ensemble des parties prenantes.

8. Relève informatique

Une relève informatique a été mise en place dont son plan de relève fait l'objet d'un test annuel et, le cas échéant, des plans d'action sont définis et appliqués selon les résultats de ce test.

La responsabilité de la vérificatrice générale de la Ville consiste à fournir une conclusion sur l'objectif de l'audit. Pour ce faire, nous avons recueilli des éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable.

La vérificatrice générale de la Ville applique la Norme canadienne de gestion de la qualité 1, *Gestion de la qualité par les cabinets qui réalisent des audits ou des examens d'états financiers, ou d'autres missions de certification ou de services connexes.* Cette norme exige de la vérificatrice générale de la Ville qu'elle conçoive, mette en place et fasse fonctionner un système de gestion de la qualité qui comprend des politiques et des procédures en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. Au cours de ses travaux, la vérificatrice générale de la Ville s'est conformée aux règles sur l'indépendance et aux autres règles de déontologie du Code de déontologie des comptables professionnels agréés du Québec, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Nos travaux d'audit ont porté sur la période s'échelonnant d'octobre 2021 à décembre 2022. Ils ont consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'au 1er mars 2023.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein de l'unité d'affaires auditée. Par la suite, le rapport final a été transmis à la direction des unités d'affaires concernées ainsi qu'à la Direction générale de la Ville.

2.3. Portée des travaux

Nos travaux d'audit ont porté sur l'environnement d'Artemis comportant :

- Artemis 2.6;
- Artemis Maps;
- Artemis mobile;
- Artemis caserne;
- Smartemis;
- Artemis Web;
- Solution Artemis de dépannage (GPRAO);
- Système de suivis des données opérationnelles (SSDO).

3. Résultats de l'audit

3.1. Gouvernance

Une saine gouvernance d'Artemis consiste à définir avant tout les rôles et responsabilités des différentes parties prenantes impliquées dans sa gestion. Cela se formalise dans une matrice de responsabilités de type RACI (Réalisateur, Approbateur, Consulté et Informé).

Les parties prenantes à la gouvernance et à la gestion d'Artemis sont le STI, le SIM ainsi que le fournisseur intégrateur en collaboration avec le fournisseur de la solution.

Nous avons constaté que la gouvernance et la gestion d'Artemis sont basées sur un modèle de gouvernance du projet – Système de gestion des interventions (SGI), exploitation et évolution depuis sa première ébauche en 2007. Ainsi, ce modèle est constitué en premier lieu d'un comité de suivi de contrat qui se réunit au besoin selon les enjeux et problèmes en cours. En second lieu se trouve le comité de pilotage du SGI dont les rencontres ont lieu toutes les deux semaines. Ce comité effectue le suivi des incidents et des problèmes, de l'avancement des demandes de changements et rend compte des diverses actions attribuées aux parties prenantes présentes dans l'un ou l'autre des comités.

Nous avons noté que des rôles et responsabilités sont définis dans les documents suivants :

- Le *Manuel d'organisation de projet* (MOP) aux sections *Rôles et responsabilités* et *Gouvernance* ainsi qu'à l'*Annexe A tableau des responsabilités contractuelles.* C'est l'ultime référence pour les parties prenantes;
- Le dossier d'exploitation Artemis 2.4 liste aussi des rôles et responsabilités dans le tableau de responsabilité par composante;
- Les activités journalières d'exploitation et d'évolution du SGI, communément appelées maintenance, incombent au fournisseur intégrateur. Une entente contractuelle est en vigueur à cet effet;
- Le RACI sur le projet de mise à niveau et modernisation d'Artemis 2.4 daté du 31 octobre 2016 cite les rôles et responsabilités sur les étapes dudit projet.

Ces documents ne sont pas à jour, car la version utilisée actuellement est Artemis 2.6 et non Artemis 2.4. Cependant, ce changement de version est récent (septembre 2022) et ne comporte que des changements mineurs. Des transferts de responsabilités au STI – p. ex. le support niveau 1[3] – ne sont pas reflétés ni les changements organisationnels vécus. Une demande de révision du MOP a été entamée auprès du fournisseur intégrateur à cet effet.

Nous considérons que les éléments listés ci-dessus correspondent à une matrice de responsabilités pour Artemis, particulièrement dans le cadre d'un projet imparti au fournisseur intégrateur avec la collaboration du fournisseur de la solution même. Aucune recommandation n'est requise puisque la documentation fonctionnelle est en cours.

---

[3] Le support niveau 1 correspond au centre de services TI qui répond aux appels des utilisateurs et les achemine aux bonnes équipes internes ou externes.

3.2. Gestion des accès logiques

La gestion des accès logiques comporte deux volets, soit les paramètres d'authentification et la procédure de gestion des accès logiques aux systèmes informatiques.

3.2.1. Paramètres d'authentification

Les paramètres d'authentification permettent d'encadrer formellement les identifiants (code usager et mot de passe) utilisés pour se connecter aux systèmes informatiques. Pour ce faire, il est requis de définir un encadrement sur l'authentification et de l'appliquer de façon appropriée dans les systèmes informatiques. Ces paramètres d'authentification portent sur l'utilisation d'un code usager et la stratégie de mots de passe. C'est-à-dire la longueur minimale, la complexité, la période de validité et l'historique des mots de passe ainsi que le nombre de tentatives infructueuses, la durée du verrouillage des comptes et autres.

Nous avons constaté les éléments suivants :

Artemis 2.6 et son sous-menu Artemis maps

Les utilisateurs d'Artemis avec un accès en écriture à Artemis ne peuvent se connecter qu'à partir de leur poste de travail situé dans les locaux du CCSI sous la surveillance d'un superviseur.

L'authentification à Artemis 2.6, et à son sous-menu Artemis maps, s'effectue avec des identifiants dont le format du compte usager varie selon sa fonction. L'équipe du CCSI utilise des comptes personnels qui peuvent être réassignés après des départs.

Un fichier externe est utilisé par le SIM pour contrôler l'utilisation de ces comptes. Ceux-ci sont associés à une utilisatrice ou un utilisateur via leur matricule. La méthode d'authentification implantée dans Artemis 2.6 n'est pas munie des fonctionnalités – la longueur, la complexité ainsi que l'historique des mots de passe – permettant de se conformer aux encadrements de gestion des accès établis par la Ville (la Directive sur la gestion des accès logiques ainsi que le Standard sur la gestion des accès logiques datés respectivement de juillet 2020 et janvier 2021).

Une mauvaise configuration des paramètres d'authentification pourrait permettre à des personnes malintentionnées d'obtenir des accès non autorisés à Artemis et à ses composantes.

RECOMMANDATION 3.2.1.A.

Nous recommandons à la Division Sécurité publique de la Direction Sécurité publique et justice du Service des technologies de l'information et au Service de sécurité incendie de Montréal, avec la collaboration du fournisseur intégrateur, d'analyser les options envisageables afin d'augmenter la robustesse des paramètres d'authentification d'Artemis 2.6 selon le Standard de gestion des accès logiques.

Artemis mobile et Artemis caserne

Aucune authentification humaine n'est requise pour accéder à Artemis mobile et à Artemis caserne. Leur authentification à Artemis 2.6 est exécutée de façon automatique à travers un script (utilisant l'adresse IP et la localisation physique de la machine – poste de travail ou ordinateur véhiculaire – dans une caserne ou un véhicule). Ces systèmes n'octroient aucun accès privilégié. Ces postes sont utilisés pour fournir aux pompières et pompiers des informations d'interventions en temps réel afin de répondre efficacement aux appels des citoyennes et citoyens assignés. Ils doivent être actifs 24 heures sur 24 et 7 jours sur 7.

Aucune recommandation n'est nécessaire.

Smartemis et Artemis Web

L'authentification à l'application mobile Smartemis, du même fournisseur de solution qu'Artemis, est effectuée uniquement lors de son installation dans le téléphone intelligent. Il est requis de fournir le numéro de matricule, le code U et le numéro de téléphone. Une fois Smartemis installée, elle n'exige plus d'informations d'authentification à l'utilisatrice ou l'utilisateur. Exceptionnellement, les six gestionnaires peuvent ajouter un autre dispositif dans l'utilisation de Smartemis.

L'authentification à Artemis Web s'effectue avec le code U, pour les gestionnaires, et avec le numéro de matricule de l'employé, pour les équipes opérationnelles et les pompières et les pompiers ainsi que le mot de passe d'Artemis 2.6. L'option d'installer un annuaire pour Artemis Web dans l'extranet[4] n'a pas été déployée suivant les discussions entre les parties prenantes.

Les utilisatrices et utilisateurs de Smartemis et d'Artemis Web (accessible de l'intranet Ville seulement) consultent des informations issues d'Artemis 2.6. Aucune transaction ni mise à jour des informations n'est permise ni possible. Ces deux systèmes utilisent l'authentification d'Artemis 2.6. Le mot de passe est normalement le numéro de matricule. Le SIM privilégie la haute disponibilité et la simplicité d'accès.

Nous jugeons que l'authentification à Smartemis et Artemis Web est adéquate. Aucune recommandation n'est requise.

---

4 L'extranet est un réseau privé contrôlé entre partenaires tandis que l'intranet d'une organisation est accessible uniquement aux employés.

GPRAO (solution Artemis de dépannage)

GPRAO est une solution Artemis de dépannage, accessible en mode multi-utilisateur et sur un poste autonome. La version multi-utilisateur est utilisée lorsque les serveurs d'Artemis tombent en panne. Cette solution n'offre pas de communication avec les casernes. Depuis novembre 2022, lors du retour à la situation normale (c'est-à-dire à la fin d'une panne), les données de GPRAO sont synchronisées automatiquement avec le SSDO.

Le GPRAO, en mode multi-utilisateur et en mode autonome, ne requiert ni un compte usager ni un mot de passe. Le mode multi-utilisateur requiert la saisie du numéro de poste.

Le poste autonome GPRAO est dans un local sécurisé accessible uniquement par le personnel du CCSI.

Aucune recommandation n'est requise.

Système de suivi des données opérationnelles (SSDO)

Créée en 2001, SSDO est une application de création de rapports qui reprend toutes les données associées à une intervention et les classe sous forme de registre consultable. Deux formats de rapport sont associés à une intervention : celui consulté par le personnel répartiteur et celui à remplir par les pompières et pompiers. Toutes les 10 secondes, SSDO reçoit les interventions d'Artemis.

SSDO est uniquement accessible depuis un poste de travail de la Ville à l'interne ou à travers le VPN[5], et ce, à partir de l'Intranet du SIM. L'authentification à la BD SSDO s'effectue avec le mot de passe – selon la politique de mots de passe de la Ville – combiné avec le code U, pour les gestionnaires, et avec le numéro de matricule de l'employé, pour les équipes opérationnelles et les pompières et les pompiers.

Aucun des paramètres d'authentification – longueur, complexité et historique des mots de passe – de cette politique de mots de passe n'est conforme au Standard sur la gestion des accès logiques de la Ville. Cependant, les paramètres pourraient être changés à la demande du SIM pour s'y conformer. Aucune modification n'a été réalisée pour en faciliter l'accès aux pompiers.

Des paramètres d'authentification non robustes pourraient permettre à des ressources non autorisées d'accéder aux rapports.

RECOMMANDATION 3.2.1.B.

Nous recommandons à la Division Sécurité publique de la Direction Sécurité publique et justice du Service des technologies de l'information, et au Service de sécurité incendie de Montréal d'analyser la pertinence d'augmenter la robustesse des paramètres d'authentification du Système de suivi des données opérationnelles.

---

5 Le VPN est un réseau privé virtuel qui permet de relier deux ordinateurs distants par une seule et même connexion privée, ou tunnel, tout en utilisant une infrastructure réseau de plus grande taille, comme Internet ou un réseau étendu. Une fois activé, un VPN fait office de connexion directe à un réseau privé.

3.2.2. Procédure de gestion des accès logiques à hauts privilèges

Une procédure de gestion des accès logiques détaille la marche à suivre pour la création, la modification, la révocation, la révision, la suppression de comptes et la surveillance des droits d'accès logiques, plus particulièrement les accès privilégiés. En effet, les accès à hauts privilèges sont octroyés notamment à des administrateurs de systèmes et à des ressources autorisées nécessitant des accès plus étendus aux données pour l'exécution de leurs tâches.

Cette procédure devrait couvrir notamment les éléments suivants :

- L'utilisation limitée et restreinte des accès privilégiés aux ressources autorisées;
- L'approbation formelle de toutes demandes d'utilisation d'un compte avec des accès privilégiés;
- La suppression des comptes usagers inutilisés suspendus pour une certaine période;
- La révision régulière des droits d'accès associés aux comptes;
- La surveillance des comptes à hauts privilèges.

Nous avons constaté que le Standard de gestion des accès logiques de janvier 2021 comporte des exigences spécifiques pour les comptes à hauts privilèges. Ces exigences devraient se retrouver détaillées dans une procédure de gestion des accès logiques fournissant les étapes à suivre lors de la création, la modification, la révocation, la révision, la suppression et la surveillance des droits d'accès logiques pour ce type de comptes.

Nous avons constaté les éléments suivants :

Artemis 2.6 et son sous-menu Artemis maps

Aucune procédure de gestion des accès logiques privilégiés à Artemis n'a été développée, approuvée et diffusée aux parties prenantes conformément au Standard de gestion des accès logiques de janvier 2021.

Seules la création des utilisateurs et l'association des profils aux utilisateurs sont décrites dans le document « Formation aux administrateurs » du fournisseur de la solution.

Deux entités distinctes ont des accès privilégiés, soit le fournisseur intégrateur qui assure le support et la maintenance d'Artemis et certains membres du personnel du SIM. Depuis le printemps 2021, à la demande de la gestionnaire en chef de la Division Centre de communication d'urgence, le fournisseur intégrateur traite et ferme toutes les demandes d'accès logiques.

Toutefois, des processus de gestion des accès logiques pour la création et la modification des accès privilégiés sont en place. Contrairement à la règle générale, les comptes usagers sont désactivés et les droits d'accès demeurent associés aux comptes après leur départ. Par conséquent, aucune révocation des droits d'accès ni de suppression de compte ne sont réalisées. De plus, aucune révision ni surveillance des droits d'accès ne sont effectuées.

Jusqu'au départ de l'ancienne gestionnaire en avril 2022, les demandes d'accès logiques à hauts privilèges étaient traitées directement dans le système. Nous n'avons pas obtenu de documents probants à cet effet. Un formulaire de création a été implanté en novembre 2022

par le fournisseur intégrateur lors de nos travaux.

En l'absence de demandes de création, de modification et de révocation des accès logiques privilégiés au système Artemis, aucun test d'efficacité n'a été réalisé pour la période d'octobre 2021 à septembre 2022. Par contre, nous avons constaté qu'aucun compte obsolète n'était présent dans les listes d'utilisateurs privilégiés à Artemis 2.6.

L'absence d'une procédure de gestion des accès logiques à hauts privilèges pourrait occasionner une mauvaise gestion de ce type d'accès allant jusqu'à l'attribution d'accès non autorisés à Artemis 2.6 et ses données.

RECOMMANDATION 3.2.2.A.

Nous recommandons à la Division Sécurité publique de la Direction Sécurité publique et justice du Service des technologies de l'information, et au Service de sécurité incendie de Montréal, avec la collaboration du fournisseur intégrateur, de développer, d'approuver et de diffuser une procédure de gestion des accès logiques privilégiés applicable au système Artemis 2.6.

Artemis mobile et Artemis caserne

Lorsqu'une caserne et un véhicule sont intégrés à Artemis 2.6, les ordinateurs sont configurés avec des scripts pour effectuer une connexion automatique par le fournisseur intégrateur. Ainsi, aucune gestion des accès logiques privilégiés ne s'applique à Artemis mobile et Artemis caserne.

Aucune recommandation n'est requise.

Smartemis et Artemis Web

Le fournisseur intégrateur traite et ferme les demandes de gestion des accès logiques à Smartemis et Artemis Web du SIM. Les accès privilégiés sont uniquement octroyés à six ressources du SIM, au fournisseur intégrateur et au fournisseur de la solution Artemis 2.6.

Aucune procédure de gestion des accès logiques privilégiés à Smartemis et Artemis Web n'a été développée, approuvée et diffusée aux parties prenantes conformément au Standard de gestion des accès logiques de janvier 2021.

Toutefois, dans l'ensemble, les processus appliqués sont adéquats. Un formulaire Google est utilisé pour l'approbation des demandes d'accès à Smartemis sur un téléphone personnel.

En l'absence de demandes de création, de modification et de révocation des accès privilégiés à Smartemis et à Artemis Web, aucun test d'efficacité n'a été réalisé pour la période d'octobre 2021 à septembre 2022. Par contre, nous avons constaté qu'aucun compte obsolète n'était présent dans les listes d'utilisateurs privilégiés à ces deux systèmes.

L'absence d'une procédure de gestion des accès logiques à hauts privilèges pourrait occasionner une mauvaise gestion de ce type d'accès, allant jusqu'à l'attribution d'accès non autorisés aux données d'Artemis 2.6 accessibles à travers les systèmes Smartemis et Artemis Web.

RECOMMANDATION 3.2.2.B.

Nous recommandons à la Division Sécurité publique de la Direction Sécurité publique et justice du Service des technologies de l'information, et au Service de sécurité incendie de Montréal, avec la collaboration du fournisseur intégrateur, de développer, d'approuver et de diffuser une procédure de gestion des accès logiques privilégiés applicable à Smartemis et Artemis Web.

GPRAO (mode multi-utilisateur et poste autonome)

Cette application ne requiert ni de compte usager ni de mot de passe et fonctionne uniquement avec un compte administrateur système. Ainsi, aucune gestion des accès logiques privilégiés ne s'applique à celle-ci.

Aucune recommandation n'est requise.

SSDO (Système de suivi des données opérationnelles)

Les processus de création, de modification et de révocation des droits d'accès passent par l'utilisation de l'outil de gestion des services TI pour l'ouverture et la fermeture d'une demande d'accès à SSDO. Aucune procédure formelle de gestion des accès logiques n'a été développée par l'équipe de la DSP de la Direction Sécurité publique et justice du STI responsable de SSDO. Cependant, outre les huit spécialistes pour SSDO du STI, deux gestionnaires du SIM ont des droits d'accès privilégiés (accès à tous les écrans et aux rapports SSDO).

Cette division utilise une application de pilotage pour réaliser cette gestion des accès logiques. Une équipe de cinq personnes traite ces demandes d'accès à SSDO pour le SIM. Les processus de création et de modification sont adéquats. Cependant, lors d'un départ, le SIM ne crée pas de demande de révocation des droits d'accès et le compte demeure donc actif.

Une seule demande de création des accès privilégiés à SSDO a été réalisée pour la période d'octobre 2021 à septembre 2022, respectant les saines pratiques. Aucune demande de modification ou de révocation des accès privilégiés à SSDO n'a été réalisée dans cette période. Nous avons constaté qu'aucun compte obsolète n'était présent dans les listes d'utilisateurs privilégiés à ce système.

Le nombre d'utilisateurs étant restreint, les impacts de l'absence d'une procédure de gestion des accès logiques privilégiés à SSDO sont faibles. Par conséquent, aucune recommandation n'est requise.

3.3. Gestion des correctifs et des mises à jour

Les mises à jour d'un système RAO comme Artemis sont complexes, car il doit toujours être disponible. Ainsi, il faut éviter des changements qui auraient des impacts significatifs sur les opérations du SIM. Chaque seconde dans ce service est précieuse. Il est crucial de maintenir Artemis le plus stable possible.

Le fournisseur intégrateur est responsable de l'évolution d'Artemis pour la Ville, avec la

collaboration du fournisseur de solution.

Nous avons constaté que le processus de gestion des correctifs et des mises à jour mis en place depuis plusieurs années est connu et utilisé par les parties prenantes concernées.

Nous avons été informés des éléments suivants de ce processus :

- Il couvre les correctifs et les mises à jour suivant un incident, une anomalie sur Artemis ou une Demande de changement (DDC). Le fournisseur intégrateur le prend en charge et travaille avec le fournisseur de la solution pour développer un correctif en suivant son processus de certification. Des tests ont lieu du côté du fournisseur dans l'environnement de laboratoire, avec sa grille de tests, et le SIM effectue des tests opérationnels dans son environnement de formation dans le but de donner son accord pour l'implantation finale. Dans le cas contraire, les défaillances soulevées par le SIM sont transmises au fournisseur intégrateur et ce dernier les renvoie au fournisseur de la solution jusqu'à l'acceptation finale du SIM;
- La planification du déploiement d'un correctif prend en compte s'il est urgent ou non. Le STI, après avoir reçu la grille de tests du SIM, rédige un rapport d'acceptation dûment documenté pour approbation par le comité de pilotage du SGI et une plage horaire est déterminée. Le STI remplit la fiche du Comité d'approbation des changements (CAC) avec la documentation requise par celui-ci. Le STI présente au CAC le type d'intervention, son impact et la procédure de retour en arrière. Une fois son autorisation obtenue, il en informe le SIM par courriel. La date de déploiement est déterminée selon le calendrier de changements autorisé par le CAC pour assurer la disponibilité des équipes essentielles à Artemis. Une communication du déploiement planifié est effectuée auprès des équipes du STI visées ainsi qu'aux chefs de section du SIM;
- Lors du déploiement des mises à jour et des correctifs, les actions nécessaires sont effectuées pour que celui-ci se réalise sans affecter la production. Ensuite, le fournisseur intégrateur communique avec le SIM. Les parties prenantes vérifient le bon fonctionnement du système Artemis, car des problèmes non reliés aux correctifs pourraient subvenir. S'il s'avère que cette situation se présente, le STI les documente pour qu'ils soient corrigés par le fournisseur intégrateur;
- Tous les correctifs et mises à jour sont discutés et suivis lors des rencontres aux deux semaines du comité de pilotage.

Nous avons constaté que ce processus de gestion des correctifs et des mises à jour d'Artemis a été respecté et appliqué entièrement lors de l'implantation d'Artemis 2.6. Il comportait deux correctifs, une évolution et aucune DDC. De plus, ce processus respecte les saines pratiques en matière de documentation, d'évaluation de l'impact, de priorisation et d'autorisation, du suivi, du contrôle de qualité et de fermeture.

Bien que tout ceci soit en place, ce n'est pas consigné par écrit dans une procédure formelle de gestion des correctifs et des mises à jour d'Artemis, chaque étape est documentée dans un livrable approprié.

L'absence d'une procédure de gestion des correctifs et des mises à jour d'Artemis pourrait occasionner des écarts dans l'application des étapes à suivre pour ce système critique.

RECOMMANDATION 3.3.A.

Nous recommandons à la Division Sécurité publique de la Direction Sécurité publique et justice du Service des technologies de l'information, et au Service de sécurité incendie de Montréal, avec la collaboration du fournisseur intégrateur, de développer, d'approuver et de diffuser une procédure de gestion des correctifs et des mises à jour.

3.4. Gestion des incidents

Un incident est un événement non planifié pouvant causer une interruption ou une dégradation de service. Ainsi, une saine gestion des incidents vise à rétablir le service le plus rapidement possible de concordance avec les niveaux de services définis contractuellement.

Nous avons constaté que le processus de gestion des incidents d'Artemis est constitué d'une documentation développée par le STI, avec la collaboration du SIM, et par le fournisseur intégrateur accessible à toutes ces parties prenantes. Elle se détaille comme suit :

- « Arbre de décision – Système de gestion des interventions (SGI) et Artemis (SIM) V02.2 » : ce document est utilisé pour transférer l'incident à l'équipe la plus appropriée;
- « Documents de connaissance sur le SGI et Artemis » : ils décrivent comment créer un incident et le fonctionnement du support d'Artemis du CDS auprès du fournisseur intégrateur ainsi que les groupes de support.

Ces procédures de gestion des incidents applicables à Artemis se trouvent dans l'outil de gestion des services TI.

Nous avons été informés que la gestion des incidents incombe en premier lieu au fournisseur intégrateur. Après la saisie des incidents par le Centre de service TI (CDS), celui-ci traite tous les incidents et les ferme dans l'outil de gestion des services TI. Ainsi, la procédure de gestion des incidents du fournisseur est régie par l'entente contractuelle avec la Ville.

Lors de la tenue du comité de pilotage du SGI aux deux semaines, les parties prenantes liées au SGI (c'est-à-dire, au minimum, le chef de projet du fournisseur intégrateur, une ressource du STI, une ressource des opérations du SIM et une ressource du CCSI avec, au besoin, d'autres participants) effectuent le suivi des incidents, dont les incidents majeurs et les problèmes vécus par les utilisatrices et utilisateurs.

Nous avons sélectionné aléatoirement, à partir de la liste d'incidents obtenue du STI, 14 incidents sur les 135 incidents de priorité[6] critique, élevée et modérée ainsi qu'un incident sur les 11 incidents de priorité faible survenus au cours de la période du 1er octobre 2021 au 30 septembre 2022. Cette liste comportait un seul incident de priorité critique et 127 de priorité élevée. Notre échantillon d'incidents se détaille comme suit :

- 1 incident de priorité critique;
- 12 incidents de priorité élevée;
- 1 incident de priorité modérée;
- 1 incident de priorité faible.

Dans l'application de la procédure de gestion des incidents, nous avons constaté :

Aucun mécanisme d'alertes automatisées n'est en place pour le signalement d'un incident causé par un problème applicatif dans l'environnement Artemis. Cependant, le personnel du CCSI étant présent 24 heures par jour, 7 jours par semaine et 365 jours par année, détecterait en temps réel ces problèmes.

Le cheminement d'une alerte d'un incident se déroule comme suit : un appel est fait par le CCSI vers le CDS qui le transfère au fournisseur intégrateur pour le soutien. Tous les incidents nécessitent l'intervention de ce fournisseur. Une équipe de 7 personnes du CDS est dédiée au support du SIM.

Le processus de gestion des incidents au CDS respecte les saines pratiques en ce qui concerne la documentation, la classification et la priorisation, la catégorisation jusqu'à la résolution et la fermeture de l'incident. Tout appel du quartier général au CDS est toujours jugé urgent. Un processus d'escalade d'un incident majeur a été implanté pour Artemis. L'équipe du CDS dédié au SIM et le chef des incidents majeurs prennent en charge l'incident. Cette pratique vise à coordonner le travail avec les parties prenantes requises. Autrement, le SIM communique directement avec le STI afin de maintenir les gestionnaires informés de la panne et de son évolution.

Comme le fournisseur intégrateur n'a pas de mécanismes d'alertes automatisées permettant de détecter en temps réel une panne, il dépend des appels du SIM en premier lieu.

L'absence de mécanismes d'alertes automatisées dans Artemis pourrait accroître les délais de prise en charge d'un incident critique.

RECOMMANDATION 3.4.A.

Nous recommandons au Service des technologies de l'information et au Service de sécurité incendie de Montréal, avec la collaboration du fournisseur intégrateur, d'analyser la pertinence d'implanter des alertes automatisées en temps réel en cas de panne du système Artemis.

6 La priorité de l'incident est la conjonction de l'impact et de l'urgence. La priorité va permettre d'identifier l'importance relative des incidents les uns par rapport aux autres, et d'affecter les ressources en conséquence.

3.5. Surveillance

La surveillance active s'effectue avec un outil permettant de voir en temps réel les activités ou les transactions en cours sur un système informatique. La journalisation des événements de sécurité (c'est-à-dire la surveillance passive) vise à conserver une trace – qui fait quoi et quand – en tout temps dans un système informatique. Cela s'applique spécialement pour les comptes usagers avec des privilèges élevés (« super users »).

Nous avons constaté que des niveaux de services sont définis dans le MOP pour l'exploitation et l'évolution d'Artemis. Un des niveaux de service toujours sous la responsabilité du fournisseur est le suivant :

- Taux de disponibilité du RAO (Artemis) = (le temps de la période – le temps de panne – le temps de maintenance) / par le temps de la période. Ce critère de qualité des services de maintenance du fournisseur doit atteindre le seuil de 99.5 % (selon les informations obtenues pour 2022, aucune panne n'est advenue). Dans le cas contraire, une analyse sera déclenchée pour trouver la cause et définir les actions correctives qui s'imposent.

Le fournisseur de service réalise la surveillance qui lui incombe pour le volet applicatif. Il utilise un outil pour surveiller les serveurs Artemis et les bases de données ainsi que pour vérifier l'état de la connexion. Aucune alerte automatisée n'a été déployée de leur côté.

Le fournisseur a aussi un outil de surveillance opérationnelle des interfaces à Artemis (GPRAO, SSDO, bornes-fontaines). Pour leur part, le STI utilise des outils de surveillance pour l'infrastructure sous-jacente à Artemis qui permettent de s'assurer du bon état des serveurs et du réseau.

Également, le SIM a un outil de surveillance opérationnelle en ce qui a trait à la synchronisation du GPRAO. De plus, comme le service est offert 24 heures par jour, 7 jours par semaine et 365 jours par année, l'équipe du CCSI détecte, en temps réel, toute panne ou tout problème de performance d'Artemis.

Nous avons noté que le suivi des niveaux de service ainsi que l'annonce de toute future intervention du STI pouvant avoir un impact sur l'environnement Artemis sont réalisés lors des rencontres du comité de pilotage. Le tout étant coordonné en collaboration avec les ressources du STI, du SIM et du fournisseur de service.

Reddition de comptes

Nous avons constaté que des tableaux de bord sont créés par le fournisseur comme convenu, et ce, sur les niveaux de service définis dans l'entente de service. Pour donner suite à la prise en charge par la Ville du guichet unique, des infrastructures et du réseau pour le SGI, le SIM a demandé une refonte du tableau de bord du SGI. Ce tableau a été revu afin de porter uniquement sur le niveau de service du temps en service, temps d'indisponibilité et le pourcentage de disponibilité du SGI incluant l'environnement d'Artemis.

Nous avons été informés que le tableau de bord n'a pas été envoyé systématiquement chaque mois aux destinataires du STI et du SIM en 2022. La liste des destinataires est en révision. Le STI a fait des demandes ponctuelles pour analyser la pertinence des métriques, le temps de maintenance et des pannes avant la remise en place du tableau de bord mensuel. De plus,

lors du comité de pilotage, toutes les parties prenantes à la gestion des incidents revoient le tableau de bord du mois en cours comportant le récapitulatif depuis le début de l'année.

Compte tenu de ces éléments, aucune recommandation n'est nécessaire.

3.6. Ressources spécialisées

Artemis provient d'un fournisseur de solutions spécialisé en système de répartition des appels automatisé par ordinateur. Un fournisseur distinct exécute la fonction d'intégrateur et de responsable de l'évolution et de l'exploitation de l'environnement Artemis selon l'entente de service conclue avec la Ville. C'est surtout lui qui possède toute la connaissance pointue de cet environnement. Lors d'un changement majeur et même mineur, le fournisseur intégrateur travaille conjointement avec le fournisseur de la solution Artemis ainsi que le STI et le SIM.

Nous avons constaté les éléments suivants :

Service des technologies de l'information (STI)

Au sein de la Division Solutions d'affaires – systèmes corporatifs de la DSP, personne n'est spécialisée au système Artemis. C'est le fournisseur intégrateur qui est l'expert dans ce domaine avec une équipe dédiée pour la Ville. Cependant, cette division du STI soutient le fournisseur dans la gestion de cet environnement et travaille avec un concept de collaboration et de priorité des tâches.

Aucune ressource n'est disponible en tout temps pour répondre aux appels du SIM. Le but est d'accompagner le SIM pour servir d'interface auprès du fournisseur intégrateur. Les 13 ressources de cette équipe – 3 en lien direct avec Artemis et 11 disponibles sur demande selon le besoin – ainsi que les 11 ressources en soutien des autres équipes du STI (p. ex. un chargé de projet, un administrateur, un analyste TI, un chargé d'opération) représentent un nombre suffisant de ressources spécialisées en soutien aux opérations et projets touchant l'environnement d'Artemis.

Aucune recommandation n'est nécessaire.

Service des incendies de Montréal

Le Centre de communication du service incendie du SIM est constitué d'une soixantaine de ressources dont trois ont des accès administrateurs à Artemis et effectuent le lien entre ce centre, le fournisseur intégrateur ainsi que le DSP du STI. Cette équipe composée principalement de préposés (c'est-à-dire répartiteurs et opérateurs radio), d'une préposée principale pour le traçage des types de camions et des types d'interventions, ainsi que de gestionnaires superviseurs et d'une cheffe de division sont majoritairement des utilisatrices et utilisateurs finaux d'Artemis.

Une réorganisation a eu lieu au SIM en août 2022. En fonction de celle-ci, le SIM doit revoir la constitution de ses équipes, dont les besoins réels de ressources en soutien à l'utilisation d'Artemis. La formation sur Artemis découle principalement de la documentation en provenance du fournisseur ainsi que des documents internes développés pour les préposés.

Nous jugeons que le nombre de ressources spécialisées en soutien est adéquat. Aucune recommandation n'est nécessaire.

3.7. Documentation fonctionnelle

L'environnement d'Artemis est composé de plusieurs composantes et modules interreliés. Une documentation fonctionnelle à jour permet d'assurer un support, une exploitation et évolution de l'environnement ainsi qu'un transfert de connaissances aux ressources spécialisées.

La documentation technique a été développée principalement par le fournisseur de la solution Artemis ainsi que par l'intégrateur pour la Ville. Ce dernier traite tout changement technique relié à Artemis et est responsable de leur documentation. Le SIM, pour sa part, a développé de la documentation de formation pour ses préposés accessible dans Artemis. Depuis 2017, la configuration d'Artemis est sous la responsabilité de l'intégrateur.

Nous avons constaté que d'autres documents ont été développés et approuvés avec la collaboration de l'ensemble des parties prenantes, notamment :

- Dossier d'exploitation Artemis 2.4 (RUN BOOK) daté du 26 août 2020 : ce document porte sur le projet de mise à niveau et de modernisation des systèmes de répartition des interventions d'urgence Artemis 2.4. Il définit les méthodes d'exploitation du projet et vise à soutenir le maintien des activités ainsi que de définir les opérations usuelles à effectuer sur le système. De plus, il contient, notamment, une description technique, plusieurs schémas dont un schéma réseautique de l'environnement Artemis ainsi qu'un diagramme de flux de données d'applications Artemis 2.4 sans Smartemis et Artemis Web. Ces derniers sont en production depuis octobre 2020;
- MOP daté du 10 février 2020 : ce document est considéré comme l'ultime référence pour toutes les parties prenantes. Il couvre l'organisation de projet pour l'exploitation et l'évolution du SGI dont l'environnement d'Artemis fait partie intégrante. Cette version du document devrait constituer une mise à jour annuelle pour refléter les divers changements entendus entre le fournisseur de service et la Ville. Celle-ci porte sur la mise en service le 14 novembre 2018 d'Artemis version 2.4, d'Artemis Maps et d'une nouvelle architecture de serveurs virtuels.

L'ensemble de cette documentation existante porte sur la version d'Artemis 2.4. Depuis, ce système est passé à la version 2.5 le 8 octobre 2020 et tout récemment à la version 2.6 le 7 septembre 2022.

Nous avons été informés qu'une démarche a été entamée avec le fournisseur de service en septembre 2022 pour réaliser la revue annuelle du MOP en raison de l'implantation d'Artemis 2.6. Le dossier d'exploitation Artemis 2.4 est un document plus complexe à mettre à jour.

Une documentation fonctionnelle non complète et non à jour du système Artemis pourrait affecter le processus d'ajout de fonctionnalités, l'analyse de la cause profonde d'un problème ainsi que la qualité du service offert.

RECOMMANDATION 3.7.A.

Nous recommandons au Service des technologies de l'information et au Service de sécurité incendie de Montréal, avec la collaboration du fournisseur intégrateur, de réviser et mettre à jour les documents techniques, notamment, le Manuel d'organisation de projet et le dossier d'exploitation du système Artemis.

3.8. Relève informatique

Pour le fonctionnement d'Artemis, il y a des procédures à maîtriser et des méthodes variées pour toujours assurer la disponibilité du service en tout temps. La relève informatique vise justement à assurer cette disponibilité. Pour ce faire, il est primordial d'avoir un plan de relève informatique complet et à jour, un environnement de relève reproduisant l'environnement de production et d'effectuer des tests de relève annuels. Ces derniers permettent de soulever tous les problèmes et d'y remédier avec des plans d'action, d'améliorer la performance et de mettre à jour l'environnement de relève.

Plan de relève informatique

Nous avons constaté qu'un plan de relève informatique a été développé, couvrant l'environnement d'Artemis et toutes les composantes du SGI du SIM. Cela a été réalisé avec la collaboration de l'ensemble des parties prenantes concernées par cette relève, soit le fournisseur intégrateur, les différentes équipes du STI et le SIM. L'objectif est de documenter la relève du SGI du SIM suite à une interruption due à un incident majeur.

Nous avons constaté dans le MOP que le fournisseur est responsable de fournir la documentation pour les procédures de relève de l'environnement d'Artemis sous sa responsabilité. Lors d'une relève du SGI en cas de désastre, l'équipe de soutien du fournisseur exécute alors ces procédures de relève prévues et documentées.

Nous avons été informés que le « Plan de relève Service de Répartition » SIM est en cours de révision et de mise à jour suivant les changements sur la téléphonie d'octobre 2022. D'autres changements sont à prévoir sur le système de caserne en 2023. L'implantation d'Artemis 2.6 le 7 septembre 2022 constitue des évolutions mineures sans impact sur le PRI. Nous avons constaté qu'il comporte toutes les informations sur la partie informatique et sur la partie télécommunication attendues d'un tel plan. De plus, ce plan est mis à jour annuellement et à chaque changement important des composantes de l'environnement informatique. Il fait l'objet d'une approbation par les directions visées du STI et du SIM. Sa diffusion est effectuée à travers une plate-forme interne accessible seulement aux ressources autorisées des diverses équipes internes du STI, du SIM et du fournisseur.

Nous avons été informés que peu importe l'incident majeur concernant le volet informatique du SGI du SIM, la bascule vers le site secondaire fait essentiellement intervenir l'équipe du fournisseur intégrateur pour l'activation du système Artemis. En ce qui concerne les infrastructures redondantes, la bascule est automatique.

Environnement de relève informatique du système Artemis

Nous avons constaté qu'un environnement de relève informatique d'Artemis a été déployé dans deux salles de traitement des données situées dans deux sites distincts éloignés. La télécommunication dispose d'une redondance avec deux opérateurs publics distincts. Finalement, le système informatisé de gestion d'appels d'urgence (consoles téléphoniques) permettant au CCSI de traiter les appels d'urgence et administratifs est en redondance active.

Test du plan de relève

Nous avons constaté que le plan de relève fait l'objet d'un test annuel et qu'il est également utilisé lors des changements importants planifiés. Un post-mortem est produit lors d'enjeux ou de problèmes et des plans d'action sont définis pour rectifier la situation. Or, le dernier test annuel de 2021 n'a soulevé aucun problème.

Nous jugeons que la relève informatique est adéquate. Aucune recommandation n'est nécessaire.

4. Conclusion

Globalement, nous concluons que la Ville de Montréal (la Ville) a mis en place les mécanismes de contrôle assurant une saine gestion du système Artemis.

En effet :

- les rôles et responsabilités des parties prenantes à la gouvernance et la gestion d'Artemis sont documentés;
- le processus appliqué lors de l'implantation de la nouvelle version d'Artemis a respecté, à chaque étape, les saines pratiques de gestion des correctifs et des mises à jour;
- la surveillance des niveaux de services rendus par le fournisseur intégrateur s'effectue au comité de pilotage;
- les ressources humaines spécialisées en soutien à Artemis sont en nombre suffisant;
- aucun compte utilisateur obsolète avec de hauts privilèges n'est présent dans Artemis et ses composantes;
- un plan de relève informatique adéquat de l'environnement Artemis est testé régulièrement.

Cependant, certains éléments nécessitent des améliorations :

- Les paramètres d'authentification d'Artemis 2.6 ne respectent pas le standard de gestion des accès logiques de la Ville. Par contre, tout accès en écriture sur Artemis n'est permis qu'à partir d'un poste de travail installé dans les locaux du Centre de communication en sécurité incendie (CCSI) du Service de sécurité incendie de Montréal (SIM) sous la surveillance d'un superviseur;
- La procédure sur la gestion des accès logiques à hauts privilèges d'Artemis 2.6, de Smartemis ainsi que d'Artemis Web n'est pas documentée;
- La procédure de gestion des correctifs et des mises à jour en production d'Artemis n'est pas documentée;
- Le maintien à jour de la documentation fonctionnelle de l'environnement d'Artemis ne se fait pas systématiquement à chaque changement. Néanmoins, Artemis 2.6, implantée en septembre 2022, diffère peu de la version 2.5;
- Aucun mécanisme d'alertes automatisées n'est en place pour le signalement d'un incident dans l'environnement Artemis. Cependant, le personnel du CCSI, étant présent en tout temps, détecterait en temps réel tout problème de production.

Plus précisément, voici les détails selon les critères d'évaluation suivants :

Gouvernance

Les rôles et responsabilités des parties prenantes à la gouvernance et à la gestion d'Artemis sont documentés, notamment dans le Manuel d'organisation de projet (MOP) et le dossier d'exploitation Artemis 2.4. Également, un RACI (Réalisateur, Approbateur, Consulté et Informé) sur le projet de mise à niveau et de modernisation d'Artemis 2.4 a été défini en octobre 2016. Ces documents ne sont pas à jour, car la version en production depuis septembre 2022 est Artemis 2.6. Cependant, une demande de révision à cet effet est en cours.

Gestion des accès logiques

Le standard de la Ville sur la gestion des accès logiques de janvier 2021 précise les exigences sur les paramètres d'authentification et respecte les saines pratiques. Cependant, ces paramètres ne sont pas appliqués dans le système Artemis 2.6 ni dans le Système de suivi des données opérationnelles (SSDO).

Aucune procédure de gestion des accès logiques privilégiés à Artemis, à Smartemis ainsi qu'à Artemis Web n'a été développée, approuvée et diffusée auprès des parties prenantes, ce qui pourrait engendrer des accès non autorisés. Toutefois, dans l'ensemble, les processus informels de gestion des accès logiques privilégiés en place sont adéquats pour Smartemis et Artemis Web. Ceux de création et de modification des accès privilégiés à Artemis sont adéquats également.

Critère d'évaluation – Gestion des correctifs et des mises à jour

Un processus de gestion des correctifs et des mises à jour d'Artemis a été défini et appliqué de façon appropriée lors de l'implantation d'Artemis 2.6. De plus, ce processus respecte les saines pratiques en matière de documentation, d'évaluation de l'impact, de priorisation et d'autorisation, du suivi, du contrôle de qualité et de fermeture. Néanmoins, ce processus ne se trouve pas dans une procédure de gestion des correctifs et des mises à jour d'Artemis. Cette absence de procédure pourrait occasionner des écarts dans l'application des étapes à suivre pour ce système critique.

Critère d'évaluation – Gestion des incidents

Une procédure de gestion des incidents d'Artemis a été développée, approuvée et diffusée aux parties prenantes. De plus, le processus de gestion des incidents respecte les saines pratiques en matière de documentation, de classification et de priorisation, de catégorisation, de résolution et de fermeture de l'incident. Comme le fournisseur intégrateur n'a pas de mécanismes d'alertes automatisées permettant de détecter en temps réel une panne, il dépend des appels du personnel du CCSI présent en tout temps. L'absence de mécanismes d'alertes automatisées dans Artemis pourrait accroître les délais de prise en charge d'un incident critique.

Critère d'évaluation – Surveillance

Des niveaux de services avec le fournisseur intégrateur et de service sont définis dans le MOP pour l'exploitation et l'évolution. Ce fournisseur réalise la surveillance pour le volet applicatif. Le suivi des niveaux de services s'effectue lors des rencontres du comité de pilotage. Une reddition de comptes est effectuée auprès des parties prenantes.

Critère d'évaluation – Ressources spécialisées

En plus du fournisseur intégrateur, les parties prenantes internes liées à la gestion d'Artemis comptent toutes un nombre suffisant de ressources spécialisées en soutien aux opérations et projets touchant l'environnement d'Artemis ainsi qu'en soutien à son utilisation.

Critère d'évaluation – Documentation fonctionnelle

La documentation existante développée et approuvée par l'ensemble des parties prenantes à sa gestion n'est pas revue et maintenue à jour. Elle couvre une version antérieure comportant peu de différences par rapport à Artemis 2.6 en production. Une documentation fonctionnelle non complète et non à jour d'Artemis pourrait affecter l'analyse de la cause profonde d'un problème.

Critère d'évaluation – Relève informatique

Un plan de relève informatique adéquat a été développé couvrant l'environnement d'Artemis et toutes les composantes du Système de gestion des interventions (SGI) du SIM. Le plan de relève fait l'objet d'un test annuel.