Agence spatiale canadienne | Canadian Space Agency

Vérification de la sécurité des systèmes et des données

RAPPORT DE VÉRIFICATION

Projet # 09/10 01-05

Mars 2010

Canada

Table des matières

1.0 Sommaire 1

1.1 Objectif de la vérification 1

1.2 Opinion de vérification 1

1.3 Énoncé d'assurance 1

1.4 Résumé des recommandations 1

2.0 Rapport de vérification 3

2.1 Contexte 3

2.2 Objectifs de la vérification, portée et méthodologie 3

2.3 Constatations, recommandations et réactions de la direction 4

Annexe – Tableau détaillé des constatations, recommandations et réactions de la direction 5

1.0 SOMMAIRE

1.1 OBJECTIF DE LA VÉRIFICATION

La présente vérification avait pour objet d'évaluer dans quelle mesure les processus et procédures en matière de sécurité des données et des systèmes sous la responsabilité de la Gestion de l'Information et de la Technologie de l'Information (GITI) assurent une protection adéquate des données et des systèmes de l'Agence spatiale canadienne (l'Agence).

1.2 OPINION DE VÉRIFICATION

À notre avis, les processus et procédures en matière de sécurité des données et des systèmes sous la responsabilité de la GITI connaissent certains problèmes qui exigent une attention particulière de la part de la direction, mais dont l'enjeu est modéré.

1.3 ÉNONCÉ D'ASSURANCE

À titre de dirigeante principale de la vérification, je suis d'avis que les procédés de vérification appliqués et les éléments probants recueillis sont suffisants et appropriés pour étayer l'opinion formulée dans le présent rapport. Cette opinion est fondée sur une comparaison des conditions qui existaient et des critères de vérification établis au préalable et acceptés par la direction. L'opinion s'applique uniquement à l'entité examinée.

1.4 RÉSUMÉ DES RECOMMANDATIONS

Nous avons noté un certain nombre de bonnes pratiques en matière de sécurité des données et des systèmes sous la responsabilité de la GITI. En effet, l'architecture du périmètre du réseau était bien conçue. Celle-ci permet de bien filtrer le trafic provenant autant de l'interne que de l'Internet. De plus, la stratégie centrale des mécanismes anti-virus est bien conçue.

Par ailleurs, suite à notre examen des processus et procédures en place en matière de sécurité des données et des systèmes sous la responsabilité de la GITI, nous recommandons de :

- Documenter des normes de configurations en fonction des diverses technologies en place;
- Considérer centraliser tous les journaux de systèmes et implanter un outil générant des alertes en fonction d'événements;
- Revoir le processus d'octroi des mots de passe afin que les administrateurs ne connaissent pas les mots de passe initiaux;
- Réviser les listes de détenteurs de carte d'accès aux salles informatiques.

Signature de la Dirigeante principale de la vérification

Original signé par Dominique Breden

Membre de l'équipe de vérification

Pierre Lapointe, associé délégué, Samson Bélair/Deloitte & Touche s.e.n.c.r.l.
David Liberatore, directeur principal, Samson Bélair/Deloitte & Touche s.e.n.c.r.l.
Huy Roan, vérificateur principal, Samson Bélair/Deloitte & Touche s.e.n.c.r.l.
Ndeye Astou Ndao, vérificateur principal, Samson Bélair/Deloitte & Touche s.e.n.c.r.l.
Anne Turski, vérificateur principal, Samson Bélair/Deloitte & Touche s.e.n.c.r.l.
Stephanie Ranno, vérificateur principal, Samson Bélair/Deloitte & Touche s.e.n.c.r.l.

2.0 RAPPORT DE VÉRIFICATION

2.1 CONTEXTE

La mission de l'Agence est d'avancer le développement et l'application des connaissances spatiales pour le mieux-être des Canadiens et de l'humanité. Le mandat est de promouvoir l'exploitation et le développement pacifiques de l'espace, de faire progresser la connaissance de l'espace par la science et de faire en sorte que les Canadiens tirent profit des sciences et technologies spatiales sur les plans tant social qu'économique.

L'Agence compte environ 635 employés dont près de 90 % œuvrent au Centre John H. Chapman, le siège social de l'Agence situé à St-Hubert, Québec. Parmi ces employés, il y a 90 postes qui font partie du secteur de la GITI (79 employés et 11 postes vacants). Des 79 employés, environ 30 sont assignés à la gestion de l'information et le reste à la gestion des TI. Les tâches de ces employés comportent les fonctions TI traditionnelles, soit :

- concevoir et implanter les systèmes de télécommunications, réseaux et systèmes de stockage,
- installer et configurer des postes de travail, applications et base de données, et
- fournir le support technique associé.

L'Agence compte 85 % de ses systèmes d'information qui fonctionnent dans un environnement Windows et 15 % dans un environnement UNIX. Leurs réseaux comptent présentement entre 900 et 1 000 utilisateurs, la plupart étant situés au siège social de l'Agence à St-Hubert, Québec.

La structure organisationnelle de l'Agence tient compte du contexte mondial. De nombreuses activités spatiales sont de plus en plus axées sur les services et sont principalement orientées vers les besoins des utilisateurs finaux et l'intégration des technologies à diverses applications terrestres. L'étendue de la responsabilité du directorat de la GITI inclut la gestion des applications, des données et des technologies entourant les systèmes corporatifs. Il y a environ 60 applications, soit achetées ou développées à l'interne, sous la responsabilité de la GITI.

La raison d'être de la GITI est de comprendre les besoins et conditions et de développer et de mettre en place des politiques, procédures, programmes et activités qui visent à rencontrer ces besoins.

La GITI fait face à différents risques pour atteindre leurs objectifs tels que la quantité et l'étendue des données dont ils sont responsables. En raison de l'importance des données gérées par la GITI, la prise adéquate des copies de sauvegarde et le processus de rétention des données représentent un risque significatif. La sécurité entourant l'accès aux systèmes et aux données représentent aussi un risque significatif.

2.2 OBJECTIFS DE LA VÉRIFICATION, PORTÉE ET MÉTHODOLOGIE

La présente vérification avait pour objet d'évaluer dans quelle mesure les processus et procédures en matière des TI assurent une protection adéquate des données et des systèmes de l'Agence.La

vérification a examiné les processus et activités liés à la sécurité des données et des systèmes sous la gestion de la GITI. De façon plus spécifique, nous avons examiné les sujets présentés ci-dessous :

- Sécurité des données et des systèmes des TI
  - Gestion des demandes d'accès;
  - Sécurité logique (applications, bases de données et systèmes d'exploitation);
  - Classification des actifs TI;
  - Sécurité du périmètre du réseau;
  - Gestion des rustines.

La présente vérification ne vise que les systèmes corporatifs, incluant les applications, les systèmes de gestion de bases de données, systèmes d'exploitation et équipements réseaux sous-jacents, qui sont sous la responsabilité de la GITI, ce qui exclut certains environnements technologiques spécifiques dont ceux des opérations satellitaires et du Centre de contrôle de mission de la Station spatiale internationale. De plus, certains systèmes corporatifs dont SAP ne sont pas gérés par la GITI et ne sont pas couverts par cette vérification. Par conséquent, la vérification a été effectuée principalement à l'Agence située à St-Hubert, Québec.

Les procédés de vérification ont été réalisés de janvier à mars 2010. Les tests que nous avons effectués dans le cadre de ce projet de vérification ont consisté principalement à mener des entrevues avec les différents intervenants, à examiner la documentation existante, à examiner des configurations d'équipements en place et à comparer les procédures et contrôles mis en place par l'Agence aux pratiques de l'industrie ainsi que leur mise en application.

2.3 CONSTATATIONS, RECOMMANDATIONS ET RÉACTIONS DE LA DIRECTION

Le détail des constatations, recommandations et réactions de la direction est présenté dans l'annexe aux pages suivantes.

ANNEXE – TABLEAU DÉTAILLÉ DES CONSTATATIONS, RECOMMANDATIONS ET RÉACTIONS DE LA DIRECTION

RÉF.	CONSTATATIONS	IMPACTS	RECOMMANDATIONS	COMMENTAIRES DE LA DIRECTION / PLAN D'ACTION	ÉCHÉANCIER
1	L'agence utilise des gabarits pour configurer les nouveaux serveurs Windows et les coupe-feux. Cependant, l'Agence ne dispose pas de normes documentées de configuration en matière de technologies pour certaines autres technologies tels que systèmes de gestion de bases de données, systèmes d'exploitation UNIX et Linux, etc. Dans certaines situations, l'Agence suit les pratiques de l'industrie (ex. : Windows et Oracle).	Cette situation augmente le risque d'accès non autorisés aux systèmes de l'Agence. Cette situation augmente aussi le temps consacré à la maintenance des équipements.	L'agence devrait continuer à documenter des normes de configurations en fonction des diverses technologies en place.	Responsable : Dirigeant principal de l'information (DPI) La recommendation des vérificateurs est bien accueillie. L'ASC continuera à documenter les normes de configuration, particulièrement en ce qui concerne les environnements Linux.	Aucune action nécessaire.
2	Bien qu'il y ait une pratique en place, le processus d'accréditation et de certification n'est pas documenté.	Cette situation accroît le risque que des modifications apportées ne soient pas conformes aux intentions de la direction.	L'agence devrait considérer documenter une procédure formelle d'accréditation et de certification.	Responsable : DPI La documentation du processus de certification et d'accréditation est présentement en cours. Un guide et des gabarits sont en développement.	Mars 2011.

RÉF.	CONSTATATIONS	IMPACTS	RECOMMANDATIONS	COMMENTAIRES DE LA DIRECTION / PLAN D'ACTION	ÉCHÉANCIER
3	Les rustines (*patches*) ne sont pas à jour sur les serveurs opérant Linux comme système d'exploitation.	Cette situation augmente le risque d'accès non autorisés aux systèmes. De plus, cette situation augmente aussi le risque de défaillance des systèmes.	Installer les rustines les plus récentes sur les serveurs opérant Linux comme système d'exploitation.	Responsable : DPI Cette situation était due à des complications au niveau des contrats de maintenance de Red Hat entre le fournisseur et TPGSC. La situation a été réglée à la fin de mars 2010 et les rustines appliquées.	Aucune action nécessaire.

RÉF.	CONSTATATIONS	IMPACTS	RECOMMANDATIONS	COMMENTAIRES DE LA DIRECTION / PLAN D'ACTION	ÉCHÉANCIER
4	Les journaux de systèmes (*syslog*) Linux et Oracle ne sont pas centralisés. De plus, les journaux des systèmes d'exploitation Windows et Linux de même que les journaux des coupe-feux ne sont pas analysés sur une base régulière. Ceux-ci ne sont révisés qu'au besoin. Enfin, l'Agence ne dispose pas d'outils de surveillance et de corrélation des journaux Linux et Oracle.	Ces situations augmentent le risque que des accès non autorisés ne soient pas détectés en temps opportun.	• L'Agence pourrait considérer centraliser tous les journaux de systèmes et implanter un outil générant des alertes en fonction d'événements. Cet outil pourrait aussi cumuler des fonctions de corrélation des événements. • Si l'Agence ne retient pas cette option, elle devrait s'assurer de réviser les journaux des divers systèmes sur une base régulière de façon proactive.	Responsable : DPI Connexe au projet 10g, il est déjà prévu d'implanter OEM Grid (Oracle Enterprise Manager), ce qui permettra de consulter les journaux Oracle situés sur différents serveurs à partir d'un seul point central. Pour ce qui est d'un outil de corrélation entre les journaux Linux et Oracle, cette solution sera analysée. Entretemps, les administrateurs de systèmes effectueront un examen régulier des journaux. La TI effectuera une analyse sur la centralisation des journaux des coupe-feux.	31 mars 2011.

RÉF.	CONSTATATIONS	IMPACTS	RECOMMANDATIONS	COMMENTAIRES DE LA DIRECTION / PLAN D'ACTION	ÉCHÉANCIER
5	Nous avons noté que des utilisateurs sont administrateurs de leur poste de travail, ce qui leur permet notamment de désactiver les configurations de l'antivirus et de l'écran de veille sur leur poste de travail.	Cette situation augmente le risque d'accès non autorisés aux systèmes de l'Agence.	Retirer les privilèges d'administrateurs aux utilisateurs pour leur poste de travail.	Responsable : DPI Cette situation était surtout prévalente avec Windows 2000. Avec Vista, les utilisateurs ne se voient accordés que les privilèges dont ils ont besoin pour effectuer leurs tâches. Les exceptions sont rares. Au fur et à mesure que les postes Windows 2000 seront convertis à Vista, la situation se résorbera.	S/O
6	Nous avons été informés que quelques applications ne permettent pas l'envoi d'un mot de passe temporaire lors de la création d'un nouveau compte utilisateur. Par conséquent, les administrateurs créant les comptes utilisateurs connaissent les mots de passe des utilisateurs à la création.	Cette situation nuit à la responsabilisation des actions posées par les comptes utilisateurs.	• Revoir le processus d'octroi des mots de passe afin que les administrateurs ne connaissent pas les mots de passe initiaux. • Considérer migrer ces environnements vers des environnements supportant un meilleur processus de gestion des accès.	Responsable : DPI Les applications développées à l'interne comportent un mot de passe temporaire. Certaines applications achetées à l'externe ne permettent pas d'avoir un mot de passe temporaire. Pour celles qui possèdent cette caractéristique, nous nous assurerons qu'elle est activée.	Aucune action.

RÉF.	CONSTATATIONS	IMPACTS	RECOMMANDATIONS	COMMENTAIRES DE LA DIRECTION / PLAN D'ACTION	ÉCHÉANCIER
7	Nous avons été informés que les administrateurs de bases de données ne sont pas systématiquement informés des mutations de personnel occupant des postes rattachés à des privilèges d'accès dans certaines applications. De ce fait, les privilèges des utilisateurs qui ne sont plus en poste ne sont pas nécessairement retirés.	Cette situation augmente le risque d'accès non autorisés aux systèmes de l'Agence.	Mettre en place un processus de communication entre le service des ressources humaines gérant les mutations de poste et les administrateurs de bases de données.	Responsable : DPI Les communications entre les ressources humaines et les administrateurs de bases de données ne peuvent pas toujours faire état des changements au niveaux des accès. Toutefois, nous nous assurerons de sensibiliser plus les gestionnaires au besoin d'informer la GI/TI des mouvements de personnel et leur impact sur les accès.	Rappel dans un bulletin de la GI/TI – Septembre 2010 et lors de la Journée Branchez-vous à l'information du 17 juin 2010.

RÉF.	CONSTATATIONS	IMPACTS	RECOMMANDATIONS	COMMENTAIRES DE LA DIRECTION / PLAN D'ACTION	ÉCHÉANCIER
8	Nous avons noté qu'un grand nombre de personnes avait accès au laboratoire informatique. Nous avons aussi noté que deux employés de l'Agence possédaient deux cartes d'accès au laboratoire informatique. Enfin, il n'existe pas de procédure de révision des cartes d'accès à l'Agence.	Ces situations augmentent le risque d'accès non autorisé au laboratoire informatique.	• Réviser les listes de détenteurs de cartes d'accès au laboratoire informatique. • Documenter une procédure de révision périodique de la liste de détenteurs de cartes d'accès aux salles informatiques.	Responsable : DPI et Directeur, sécurité et installations (DSI) La salle des serveurs contient une zone (le laboratoire) dont l'accès est plus permissif. Cette zone ne contient que des serveurs de tests. Depuis l'aménagement de la salle des serveurs corporative et le laboratoire en 2006, les vérifications des listes de détenteurs de cartes effectuées (une ou deux fois par année) n'ont jamais démontré d'accès non autorisé. Une procédure de révision périodique des accès aux salles informatiques sera élaborée. Le cas de la personne possédant deux cartes d'accès a été corrigé par le responsable de la Direction, sécurité et installations.	Procédure de révision des accès aux salles sera élaborée (Décembre 2010).