Pleins Feux
sur la sécurité des technologies de l'information

FONDATION CANADIENNE POUR L'AUDIT ET LA RESPONSABILISATION

UNE PUBLICATION DE

VIGIE AUDIT

À propos de la Fondation canadienne pour l'audit et la responsabilisation

La Fondation canadienne pour l'audit et la responsabilisation se consacre à la recherche et à l'éducation. Notre mission consiste à renforcer l'audit de performance, la surveillance et la reddition de comptes dans le secteur public, tant au Canada qu'à l'étranger. Nous contribuons au développement des capacités des bureaux d'audit législatif, des organes de surveillance, des ministères et des sociétés d'État en élaborant et en mettant en œuvre ce qui suit :

- des ateliers de formation et des possibilités d'apprentissage;
- des méthodes, des guides et des trousses à outils;
- des recherches appliquées et avancées;
- des rencontres pour la diffusion de l'information et des initiatives de développement communautaire.

Rendez-vous sur www.caaf-fcar.ca pour en savoir plus sur nos produits et services.

Pleins feux sur la sécurité des technologies de l'information

Publié par :

Fondation canadienne pour l'audit et la responsabilisation
100-1505, avenue Laperrière
Ottawa (Ontario) CANADA
K1Z 7T1

Tél : 613-241-6713
info@caaf-fcar.ca
www.caaf-fcar.ca

ISBN : 978-1-7752844-0-6
Cette publication est aussi disponible en anglais sous le titre :
Focus On Information Technology Security

Table des matières

Introduction

La série *Pleins feux* de Vigie Audit

La série *Pleins feux* de Vigie Audit est un produit d'information sur l'audit de performance qui vise à aider les auditeurs de performance à gagner du temps et à réaliser plus rapidement leurs travaux de planification et d'examen.

Cette série s'adresse aux professionnels suivants :

- les auditeurs préparant un plan stratégique d'audit;
- les auditeurs participant à la phase de planification d'un nouvel audit de performance;
- les directeurs d'audit ayant des responsabilités permanentes à l'égard d'une entité ou d'un thème donné.

Chaque numéro de la série *Pleins feux* couvre un thème général susceptible de présenter un intérêt pour la plupart des auditeurs de performance, qu'ils exercent à l'échelon municipal, provincial ou fédéral.

Chaque numéro contient :

- une brève introduction sur le thème traité et son importance;
- une liste de ressources documentaires et de rapports d'audit pertinents qui ont été publiés sur ce thème au cours des cinq dernières années et compilés dans la Base de données de Vigie Audit;
- un résumé de chaque audit pertinent contenant notamment des renseignements sur les objectifs, l'étendue, les critères, les constatations et les recommandations de l'audit;
- une analyse des principaux domaines couverts par les audits pertinents au cours des cinq dernières années;
- des hyperliens vers les ressources documentaires et les rapports d'audit complets mentionnés dans le numéro.

Ce numéro contient aussi un glossaire qui fournit la définition de plusieurs termes techniques du domaine des technologies de l'information.

Nous prévoyons publier d'autres numéros de la série *Pleins feux*. N'hésitez pas à communiquer avec nous à info@caaf-fcar.ca pour nous suggérer de futurs thèmes.

Retour à la table des matières

La sécurité des technologies de l'information – Pourquoi cette question est importante

Les technologies de l'information (TI) sont omniprésentes au XXIe siècle. En quelques années à peine, les téléphones intelligents, les tablettes et divers appareils connectés se sont intégrés à notre quotidien. L'innovation technologique connaît une accélération constante et donne lieu à l'émergence d'idées qui paraissent encore « futuristes », comme les véhicules autonomes, mais qui semblent en voie de se concrétiser dans un avenir prochain.

Ce foisonnement de nouvelles technologies procure certes aux populations de la planète de nombreux et importants avantages et des occasions à saisir. Il s'accompagne cependant de nouveaux risques qu'il faut gérer avec beaucoup d'attention. Les virus informatiques, les logiciels de rançon (qu'on appelle aussi, rançongiciels, logiciels rançonneurs et logiciels d'extorsion), l'hameçonnage, le piratage informatique et l'usurpation d'identité (ou vol d'identité) sont des exemples de technologies de l'information exploitées à des fins malveillantes, qui entraînent souvent de désastreuses et coûteuses conséquences. Pratiquement pas un mois ne passe sans que les médias d'information ne fassent état d'un nouvel incident de piratage informatique visant une grande société, qui aura permis à des cyberpirates de s'emparer des données confidentielles de milliers, voire de millions, de personnes. Les auteurs de ces actes peuvent être aussi bien des adolescents à la recherche de sensations fortes, que des cyberactivistes, des membres du crime organisé, des terroristes ou encore des cyberacteurs malveillants.

L'usage malveillant des technologies de l'information peut avoir des conséquences qui transcendent largement le vol de renseignements confidentiels. Les organismes gouvernementaux ou du secteur public ne sont pas à l'abri de ces risques. À titre d'exemples récents, des cyberpirates ont réussi à mettre la main sur plus de 20 millions de dossiers du personnel au Office of Personnel Management (Office de l'administration du personnel) des États-Unis, alors que dans un autre cas, ils ont supprimé toutes les données des systèmes de TI de la société pétrolière nationale d'Arabie saoudite. Au Royaume-Uni, d'autres cyberpirates ont détourné et « pris en otage » les systèmes de TI de plusieurs hôpitaux au moyen d'un logiciel de rançon, obligeant ainsi plusieurs hôpitaux à annuler les rendez-vous non urgents.

Par ailleurs, comme les infrastructures industrielles publiques et les infrastructures de transport en commun sont de plus en plus connectées à des réseaux d'entreprise et à Internet, ces infrastructures sont par le fait même exposées à des cyberattaques qui peuvent entraîner des dommages physiques et perturber des services importants. À titre d'exemples au cours des années récentes, des cyberpirates ont réussi à interrompre temporairement la production d'électricité dans certaines régions de l'Ukraine ou encore à endommager une aciérie en Allemagne et des pièces d'équipement du programme nucléaire en Iran.

À vrai dire, tout dispositif connecté, qu'il s'agisse d'un simple téléphone intelligent, d'un véhicule autonome ou d'un système de contrôle industriel, est exposé, dans une certaine mesure, au risque de subir un acte de piratage informatique, sous une forme ou une autre. À mesure que le temps passe, le nombre et les types de dispositifs connectés connaissent une croissance rapide, tout comme le nombre de pirates informatiques et leur aptitude à déceler et exploiter les faiblesses des systèmes de TI.

Dans un tel contexte, les organismes du secteur public ont un devoir d'extrême vigilance. Ils doivent veiller à mettre en œuvre les bonnes pratiques les plus récentes en matière de gestion des risques associés aux TI, de manière à protéger leurs actifs de technologie de l'information contre un accès non autorisé, et de manière à prévenir l'utilisation, le dévoilement, la perturbation, la modification, l'examen ou la destruction de l'information qui s'y trouve.

Uniquement s'ils gèrent de manière efficace les risques liés à la sécurité des TI les organismes du secteur public seront-ils en mesure de :

- protéger la confidentialité, l'intégrité et l'accessibilité de l'information qu'ils ont en leur possession;
- protéger contre les cyberattaques les infrastructures publiques essentielles, comme les installations de production de l'électricité et les réseaux de transport en commun;
- garantir la continuité des activités et l'accessibilité des services aux citoyens.

Les auditeurs internes et les auditeurs législatifs peuvent les uns et les autres soutenir les organismes du secteur public et les aider à atteindre ces objectifs en leur donnant une assurance indépendante qui leur permettra de déterminer s'ils gèrent adéquatement les risques liés à la sécurité des technologies de l'information et en formulant des recommandations pour améliorer les domaines présentant des faiblesses.

Retour à la table des matières

Aperçu des audits sur la sécurité des technologies de l'information de 2013 à 2017

En consultant la Base de données de Vigie Audit, nous avons recherché les audits portant sur la sécurité des technologies de l'information qui ont été réalisés depuis 2013. Nous avons recensé plus de 30 rapports d'audit préparés par 17 bureaux d'audit. Dans le présent numéro de *Pleins feux*, nous avons retenu 16 de ces rapports d'audit pour une analyse plus détaillée.

Voir la liste des audits sur la sécurité des TI qui ont été sélectionnés

Nous avons aussi répertorié deux guides, en anglais seulement (voir les deux hyperliens ci-dessous), portant sur les contrôles liés aux TI, publiés respectivement par le Victorian Auditor-General's Office, qui est le bureau du vérificateur général de l'État de Victoria en Australie, et par l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI), dans le contexte de l'Initiative de développement de l'INTOSAI (IDI).

- Information and Communication Technology Controls Guide (2016)
- IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

Nous avons analysé l'étendue des audits sélectionnés et avons dressé la liste des sous-thèmes abordés dans le contexte de ces travaux d'audit. Nous avons ensuite établi une correspondance entre le contenu de chacun des rapports d'audit retenus et cette liste de sous-thèmes. Les résultats de cette analyse sont présentés à la section intitulée Principaux domaines d'audit.

De plus, la définition de certains termes techniques est présentée dans le glossaire qui se trouve à la fin du document.

Pour des raisons de sécurité, les auditeurs généraux doivent parfois s'abstenir de rendre public les constatations et les recommandations liées à leurs travaux d'audit sur la sécurité des TI, ou n'en présenter que des résultats agrégés. Pour cette raison, nous ne sommes pas en mesure de présenter dans le présent numéro de *Pleins feux* l'intégralité des constatations et des recommandations. L'information présentée dans le présent numéro a été colligée à partir de documents accessibles au public.

Retour à la table des matières

Liste des audits sélectionnés portant sur la sécurité des technologies de l'information

#	**Bureau d'audit**	**Titre du rapport** (cliquer sur le titre pour accéder au résumé)	**Date de publication**
1	Vérificateur général de la Ville de Québec	Gouvernance de la sécurité de l'information	2017
2	Bureau du vérificateur général de la Colombie-Britannique	Un audit indépendant des contrôles de cybersécurité du Centre régional de gestion de la circulation routière	2017
3	Bureau du vérificateur général de Ontario	Société indépendante d'exploitation du réseau d'électricité — Surveillance du marché et cybersécurité	2017
4	Bureau du vérificateur général de l'Alberta	La sécurité des technologies de l'information des systèmes de contrôle industriels de l'industrie pétrolière et gazière de l'Alberta	2016
5	Bureau du vérificateur général de l'État de Victoria (Australie)	La sécurité des systèmes de contrôle des infrastructures critiques pour les trains	2016
6	Vérificateur provincial de la Saskatchewan	Services centraux — Les exigences de sécurité à l'égard des applications Web	2016
7	Vérificateur provincial de la Saskatchewan	Services centraux — La sécurité du centre de données	2016
8	Bureau du vérificateur général d'Australie-Occidentale	Les logiciels malveillants dans les systèmes du gouvernement de l'État d'Australie-Occidentale	2016
9	Bureau du vérificateur général d'Australie-Méridionale	La gestion de la sécurité des systèmes d'information	2016
10	Vérificateur provincial de la Saskatchewan	SaskPower — La gestion des risques liés aux cyberincidents	2015

#	**Bureau d'audit**	**Titre du rapport** (cliquer sur le titre pour accéder au résumé)	**Date de publication**
11	Bureau du vérificateur général du Manitoba	Manitoba Hydro — La gestion des cyberrisques liés aux systèmes de contrôle industriels	2014
12	Vérificateur général de la Ville de Montréal	Sécurité des réseaux sans fil	2014
13	Bureau du vérificateur général d'Australie	Les cyberattaques : Sécuriser les systèmes de TIC	2014
14	Bureau du vérificateur général de l'État de Victoria (Australie)	Le cadre de gestion de la sécurité de l'information à l'échelle de l'ensemble du gouvernement de l'État de Victoria	2013
15	Bureau du vérificateur général du Manitoba	Les pratiques de gestion de la sécurité des technologies de l'information	2013
16	Bureau du vérificateur général de la Colombie-Britannique	Assurer la sécurité du système JUSTIN : Audit sur l'accès et la sécurité au ministère de la Justice	2013

Retour à la table des matières

Principaux domaines d'audit

Dans le cadre de notre examen des audits que nous avons retenus, nous avons recensé environ 20 domaines d'audit (ou sous-thèmes) qui peuvent s'inscrire dans l'étendue d'un audit de performance sur la sécurité des technologies de l'information (TI). Nous avons dressé la liste des 10 sous-thèmes sur lesquels l'accent a été mis le plus fortement (voir l'encadré) et nous avons établi une correspondance entre le contenu de chacun des rapports d'audit retenus et cette liste de sous-thèmes. Le résultat de cette analyse est présenté au **tableau 1**. Le tableau comprend un hyperlien pour chaque audit, qui mène au résumé d'audit correspondant que nous avons préparé. Par ailleurs, chaque résumé comprend un hyperlien qui permet d'accéder au rapport d'audit intégral publié en ligne.

Sous-thèmes répertoriés dans les audits retenus (ordre alphabétique)

- Accès logique
- Applications Web
- Continuité des activités
- Correctifs informatiques
- Évaluation des vulnérabilités
- Formation de sensibilisation à la sécurité
- Gouvernance
- Listes blanches d'applications
- Logiciels malveillants
- Réseaux

Les 10 sous-thèmes retenus sont tous pertinents pour les auditeurs désireux de mener un audit de la sécurité des TI. Les renseignements qui suivent expliquent brièvement pourquoi chacun des sous-thèmes peut constituer un élément important à prendre en compte au moment de la planification d'un audit; certains éléments précis à examiner sont aussi mentionnés.

Accès logique. Les organismes du secteur public possèdent souvent des systèmes de TI et des bases de données qui stockent des renseignements personnels de nature sensible sur un grand nombre de citoyens. Si elles se retrouvaient entre les mains d'acteurs malintentionnés, ces données pourraient servir à des fins malveillantes. Des contrôles rigoureux peuvent donc faire en sorte que seul le personnel autorisé ait accès à ces données.

Les organismes publics devraient mettre en œuvre des mesures de protection d'accès logique (comme les droits d'accès et les niveaux d'autorisation définis, et l'emploi d'identificateurs d'utilisateur et de mots passe) pour empêcher l'accès non autorisé aux systèmes de TI et aux bases de données par des intervenants externes qui cherchent à exploiter les failles d'Internet ou des intervenants internes qui cherchent à faire mauvais usage de la confiance qui leur est accordée.

Tableau 1 – Étendue de l'audit pour chacun des 16 audits retenus

	Accès logique	Applications Web	Continuité des activités	Correctifs informatiques	Évaluation des vulnérabilités	Gouvernance	Listes blanches d'applications	Logiciels malveillants	Réseaux	Sensibilisation à la sécurité
1. Vérificateur général de la ville de Québec			✓		✓	✓				✓
2. Bureau du vérificateur général de la Colombie-Britannique	✓				✓					
3. Bureau du vérificateur général de l'Ontario	✓				✓	✓				
4. Bureau du vérificateur général de l'Alberta						✓				
5. Bureau du vérificateur général de l'État de Victoria (Australie)			✓		✓	✓				
6. Vérificateur provincial de la Saskatchewan		✓								
7. Vérificateur provincial de la Saskatchewan	✓		✓			✓			✓	
8. Bureau du vérificateur général d'Australie-Occidentale								✓		✓
9. Bureau du vérificateur général de l'Australie-Méridionale	✓			✓			✓			
10. Vérificateur provincial de la Saskatchewan	✓		✓		✓	✓				
11. Bureau du vérificateur général du Manitoba						✓				✓

	Accès logique	Applications Web	Continuité des activités	Correctifs informatiques	Évaluation des vulnérabilités	Gouvernance	Listes blanches d'applications	Logiciels malveillants	Réseaux	Sensibilisation à la sécurité
12. Vérificateur général de la ville de Montréal									✓	
13. Bureau du vérificateur général de l'Australie	✓			✓		✓	✓			
14. Bureau du vérificateur général de l'État de Victoria (Australie)						✓				✓
15. Bureau du vérificateur général du Manitoba						✓				✓
16. Bureau du vérificateur général de la Colombie-Britannique	✓					✓				

Applications Web. Les applications Web sont des programmes informatiques qui sont intégrés à des sites Web et qui aident au fonctionnement des sites Web. Les organismes du secteur public mettent souvent au point des applications Web qui permettent aux citoyens d'accéder à certains services gouvernementaux. Quand elles sont mal conçues, les applications Web peuvent présenter certaines faiblesses que les pirates informatiques chercheront à exploiter pour accéder à des renseignements de nature sensible (comme les dates de naissance ou les numéros de cartes de crédit) qui sont stockés sur un réseau ou pendant le traitement de ces renseignements par l'intermédiaire de l'application Web.

Pour se prémunir contre les atteintes à la sécurité, les organisations devraient adopter un système de sécurité multicouches qui permet de maintenir la sécurité même quand une couche subit une atteinte. Les pare-feu, les protocoles de codage sécurisé et les contrôles d'accès logiques sont au nombre des mesures que l'on peut mettre en place pour sécuriser les applications Web.

Continuité des activités. Les cyberattaques et les atteintes à la sécurité des données peuvent perturber de façon considérable une organisation et même l'empêcher de procurer des services essentiels à la population. Une cyberattaque peut avoir pour conséquence d'entraîner des pertes de données, des renseignements personnels ou financiers compromis, des temps d'arrêt imprévus en raison de pannes, et d'autres difficultés.

Pour atténuer les conséquences d'une cyberattaque, les organisations devraient intégrer des mesures de protection des TI dans leur plan de continuité des activités. Ce plan devrait comporter, entre autres choses, des renseignements sur les processus de sauvegarde et de récupération de données.

Correctifs informatiques. Les pirates informatiques cherchent constamment à détecter les failles dans les logiciels et dans les systèmes de TI qui leur permettraient d'accéder de manière non autorisée à des données sensibles. Parallèlement, les spécialistes des TI s'emploient constamment à mettre au point des solutions ou correctifs informatiques, pour résoudre des problèmes qui ont été détectés dans les logiciels et les systèmes de TI. Les organismes qui n'installent pas en temps opportun ces correctifs exposent inutilement leurs systèmes de TI à des cyberattaques.

Pour faire en sorte que tous les correctifs informatiques nécessaires soient installés en temps opportun, les organismes devraient consigner dans des documents des politiques et des processus qui permettent de déterminer les exigences à l'égard de l'installation des correctifs pour les postes de travail et les serveurs, et de les mettre en application. Ils devraient aussi évaluer de manière périodique les niveaux de conformité aux exigences à l'égard de l'installation des correctifs.

Évaluation des vulnérabilités. Une organisation peut réduire la vulnérabilité de ses systèmes de TI et la probabilité d'une cyberattaque réussie en veillant à se doter d'un processus visant à détecter de façon continue, à classifier et à prioriser les vulnérabilités de ses systèmes de TI, ainsi qu'à prévoir des mesures d'intervention rapide pour s'attaquer aux questions prioritaires.

Il existe une diversité d'outils et de méthodes pour effectuer une évaluation des réseaux, des applications et des bases de données. Certains de ces outils sont automatisés et peuvent aider les organisations à mener périodiquement des évaluations normalisées.

Formation de sensibilisation à la sécurité. Même un organisme qui possède de bons systèmes de TI et une bonne équipe de spécialistes des TI continuera d'être exposé au risque si ses employés, qui utilisent une diversité d'applications de TI chaque jour, ne connaissent pas les politiques internes en matière de TI et ne sont pas en mesure de discerner les comportements qui exposent à des risques les TI de l'organisme. C'est pourquoi, il est essentiel de donner une formation de sensibilisation à tout le personnel qui utilise de l'équipement de TI et cet aspect devrait faire partie d'une stratégie efficace en matière de sécurité des TI.

Gouvernance. La gouvernance en matière de sécurité des TI, ce sont les systèmes et pratiques qui permettent à une organisation de diriger et de contrôler la sécurité des TI. Elle consiste essentiellement à ce qui suit :

- définir les rôles et responsabilités;
- établir les politiques;
- donner les orientations stratégiques;
- veiller à assurer une bonne gestion des risques;

- examiner le rendement;
- surveiller la conformité aux politiques et aux règles.

Listes blanches d'applications. Les listes blanches d'applications sont un moyen de contrôle qui permet de protéger contre l'installation ou l'utilisation d'applications dans un système. Le recours à une liste blanche d'applications peut être un mécanisme efficace pour prévenir l'éventualité que des systèmes de TI soient compromis en raison de l'exécution d'un programme malveillant.

Pour que le recours aux listes blanches d'applications soit efficace, il faut : (1) définir dans une politique les types d'applications que les utilisateurs sont autorisés à exploiter sur leurs appareils dans le cadre de leurs fonctions; (2) établir une liste détaillée des applications qui sont autorisées; (3) s'assurer que la mise en œuvre technique de la liste blanche est conforme à l'intention sous-jacente de la politique.

Logiciels malveillants. L'expression « logiciel malveillant » (aussi appelé « maliciel ») désigne tout programme informatique nuisible qui permet de « voler » les renseignements d'un utilisateur (comme les noms d'utilisateur et les mots de passe, les numéros de cartes de crédit, ou des fichiers ou documents), ou encore qui permet à un pirate informatique de prendre le contrôle à distance d'un ordinateur et d'accéder aux réseaux auxquels il est connecté. Un ordinateur peut être infecté par un logiciel malveillant quand l'utilisateur télécharge un fichier infecté, quand il ouvre un fichier joint à un message d'hameçonnage ou quand il utilise une clé USB infectée.

Une protection efficace contre les logiciels malveillants comprend les versions maintenues à jour des logiciels antivirus et des systèmes d'exploitation, une surveillance adéquate des systèmes de TI, ainsi que la formation de sensibilisation des fonctionnaires.

Réseaux. Les travailleurs au sein des organismes gouvernementaux sont connectés à des réseaux informatiques qui leur permettent d'échanger et de stocker des renseignements de nature sensible. Si ces réseaux ne sont pas protégés adéquatement, ils peuvent être vulnérables aux atteintes à la sécurité et permettre alors à des utilisateurs non autorisés d'accéder aux renseignements qui y sont stockés.

Pour prévenir de telles atteintes à la cybersécurité, il faut veiller à ce que la configuration réseau de tous les appareils avec fils et sans fil qui permettent d'accéder au réseau soit faite et maintenue de façon appropriée. Cela comprend notamment l'emploi de logiciels de chiffrement (cryptage), l'installation et la mise à jour de logiciels antivirus, et la configuration appropriée des pare-feu, des routeurs et des imprimantes.

Retour à la table des matières

Annexe 1
Résumés des audits

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Gouvernance de la sécurité de l'information

Date de publication : 2017

Bureau d'audit : Vérificateur général de la Ville de Québec

Hyperlien pour accéder au rapport integral :

https://www.ville.quebec.qc.ca/publications/docs_ville/VG_Rapport2016.pdf

Organisme audité

- Direction de la Ville de Québec

Objectif de l'audit

- Déterminer si la Direction de la Ville voit à la mise en place des assises nécessaires à une saine gouvernance et à la gestion de la sécurité de l'information et en surveille le fonctionnement.

Critères d'audit

- Les attentes de la Direction à l'égard de la sécurité de l'information sont définies et communiquées à l'ensemble des acteurs concernés. Ces attentes traitent notamment des éléments suivants :
  - principes de sécurité à respecter;
  - rôles et responsabilités des divers acteurs;
  - surveillance prévue de l'application des principes.
- La Direction voit à ce que les actifs informationnels soient catégorisés selon leur degré de criticité (disponibilité, intégrité et confidentialité) et que les responsabilités des détenteurs désignés soient clairement définies et communiquées.
- La Direction voit à ce que les risques liés à la sécurité de l'information lors de sa collecte, de son traitement, de son stockage et de sa destruction soient recensés et analysés et qu'ils servent à prioriser les actions et les investissements en la matière.
- La Direction voit à la mise en place d'un système de gestion de la sécurité de l'information et s'assure que les ressources humaines, matérielles et financières nécessaires à son fonctionnement y sont affectées.
- La Direction voit à ce que les processus et les dispositifs de sécurité appropriés soient mis en place.
- La Direction voit à ce qu'un plan de sensibilisation et de formation soit élaboré pour sensibiliser tous les acteurs concernés à la sécurité de l'information et pour doter les personnes qui assument des responsabilités en matière de sécurité de connaissances qui leur sont nécessaires.

- La Direction exerce la surveillance nécessaire à une gouvernance diligente de la sécurité de l'information, notamment au regard :
    - du fonctionnement des processus en place;
    - de la couverture des risques;
    - de l'efficacité des mesures de sécurité.

Principales constatations de l'audit

- La Direction de la Ville n'a pas mis en place toutes les assises nécessaires à une gestion appropriée de la sécurité de l'information et elle n'effectue pas une surveillance suffisante de leur fonctionnement. Plusieurs processus et dispositifs de sécurité de l'information ont été installés sur la base d'initiatives sectorielles, mais sans une perspective globale. La gouvernance exercée par la Ville ne favorise donc pas la mise en œuvre de tous les moyens nécessaires pour assurer la sécurité de l'information en fonction de ses besoins.
- Les responsables de la sécurité de l'information ne disposent pas des assises nécessaires pour assumer pleinement les responsabilités qui leur sont confiées. Ils ne peuvent s'appuyer sur un cadre de gestion intégrée des risques.
- En raison d'une gestion partielle des risques liés à la sécurité de l'information, il est possible que des risques importants ne soient pas détectés et qu'ils ne soient pas pris en charge selon leur importance.
- L'audit a relevé des problèmes en ce qui a trait à la désignation des détenteurs :
    - aucun détenteur n'a été désigné pour 105 des 522 systèmes d'information (20 %), dont ceux relatifs à 5 systèmes critiques;
    - les tests effectués sur les systèmes d'information d'un secteur d'activité de la Ville révèlent un problème dans 42 % des cas.
- L'analyse du plan d'action pour la sécurité de l'information de mars 2014 a fait ressortir les lacunes suivantes :
    - il comporte beaucoup d'actions générales sans fixer de priorités à court terme;
    - il ne fait pas le lien avec les risques encourus;
    - il ne prévoit pas de mécanisme d'arrimage de la planification avec les diverses initiatives de la Ville susceptibles d'avoir une incidence sur la sécurité de l'information;
    - il ne précise pas les responsables de la mise en œuvre des activités, pas plus que les efforts prévus pour les réaliser.
- La Direction n'a pas déployé suffisamment d'efforts pour orienter et soutenir la mise en œuvre des mesures de sécurité. Elle reçoit d'ailleurs peu d'information sur la nature, le fonctionnement et l'efficacité de ces mesures.
- Les principaux problèmes décelés à l'égard de la gestion des incidents sont les suivants :
    - les procédures pour réagir aux incidents sont dispersées et peu élaborées, notamment en ce qui a trait aux rôles et responsabilités, et elles n'intègrent pas toutes les sources possibles de déclaration des incidents;
    - les incidents liés à la sécurité de l'information sont classés sous des rubriques trop générales, ou mal classés, et peu d'informations sont consignées sur leur nature;

  - les utilisateurs ne sont pas sensibilisés au fait qu'ils doivent signaler les incidents et les failles de sécurité de l'information;
  - il n'y a pas d'analyse des incidents dans une perspective d'amélioration continue des dispositifs de sécurité.
- Au cours des dernières années, la Ville de Québec a mené quelques actions de sensibilisation à la sécurité de l'information, mais dans l'ensemble, elle a déployé peu d'efforts pour instaurer une culture à cet égard.
- La Ville n'a pas élaboré un plan de sensibilisation à la sécurité de l'information, basé sur une analyse rigoureuse des besoins et adopté à un niveau hiérarchique suffisamment élevé, pour en assurer la mise en œuvre dans l'ensemble de l'organisation.
- Au cours des trois dernières années, très peu d'activités organisationnelles de formation ont été ciblées et suivies en matière de sécurité de l'information.
- On ne précise pas les responsabilités d'acteurs essentiels au regard de la sécurité de l'information, tels que la Direction générale, les détenteurs, les gestionnaires et le responsable de la sécurité de l'information numérique. Parmi les cinq politiques encadrant la sécurité de l'information :
  - une seule fait référence aux responsabilités de la Direction générale et celles-ci ne sont pas explicites;
  - aucune n'attribue de responsabilités aux détenteurs (seule la directive les décrit);
  - seulement trois mentionnent les responsabilités confiées aux gestionnaires.
- La Direction n'exerce pas une surveillance adéquate de la sécurité de l'information. D'abord, elle n'a pas défini ses besoins de surveillance ni d'indicateurs de gestion pour mesurer la performance en matière de sécurité de l'information. Dans les faits, très peu d'informations de gestion lui sont transmises.

Recommandations de l'audit

- La Direction générale devrait renforcer la gouvernance exercée sur la sécurité de l'information en :
  - adoptant une politique globale de la sécurité de l'information afin de :
    - préciser ses attentes en la matière ainsi que les responsabilités des acteurs sollicités,
    - prévoir des mécanismes de coordination pour assurer une prise en charge cohérente de tous les aspects de la sécurité;
  - exerçant une surveillance diligente du fonctionnement et de l'efficacité de l'ensemble des composantes de sécurité de l'information, de même qu'un suivi des risques résiduels.
- Le Service des technologies de l'information (STI) devrait soutenir la Direction de la Ville en suggérant des orientations en vue de mettre en place les assises nécessaires à l'exercice d'une gouvernance appropriée de la sécurité de l'information, soit :
  - pour la catégorisation de l'information et la désignation de détenteurs :
    - l'attribution de responsabilités claires à cet égard et le renforcement de l'imputabilité des détenteurs désignés,
    - l'adoption de règles pour assurer une catégorisation de qualité et son utilisation en vue de protéger adéquatement l'information numérique;

- pour la gestion des risques :
  - l'intégration de la sécurité de l'information à la gestion des risques de la Ville;
- pour le système de gestion de la sécurité de l'information numérique :
  - l'élaboration d'un plan de mise en œuvre de la sécurité de l'information qui est basé sur une évaluation des risques et qui indique pour chaque activité le responsable, les efforts prévus et l'échéance,
  - la collecte et l'analyse de l'information nécessaire pour assurer la gestion de la sécurité de l'information et en rendre compte;
- pour la sensibilisation et la formation des utilisateurs et responsables :
  - l'établissement et la priorisation des besoins en matière de sensibilisation et de formation en sécurité de l'information,
  - l'élaboration d'un plan de sensibilisation du personnel qui précise les activités prévues, les clientèles ciblées et l'échéancier, de même que les responsabilités et les ressources nécessaires pour le mettre en œuvre.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Un audit indépendant des contrôles de cybersécurité du Centre régional de la circulation routière

Date de publication : 2017

Bureau d'audit : Bureau du vérificateur général de la Colombie-Britannique

Hyperlien pour accéder au rapport integral :

http://www.bcauditor.com/pubs/2017/independent-audit-regional-transportation-management-centres-cybersecurity-controls (en anglais)

Organisme audité

- Ministère des Transports et de l'Infrastructure de la Colombie-Britannique — Centre régional de gestion de la circulation routière (RTMC) (Ministry of Transportation and Infrastructure – Regional Transportation Management Centre (RTMC))

Objectif de l'audit

- Déterminer si le ministère des Transports et de l'Infrastructure a établi des contrôles de cybersécurité qui sont appropriés en vue de protéger ses systèmes de gestion de la circulation routière.

Critères d'audit

- Le Ministère maintient et gère un inventaire d'appareils et de logiciels autorisés et non autorisés.
- Le Ministère établit et gère les configurations de sécurité du matériel et des logiciels dans le cas de tous les appareils.
- Le Ministère valide de manière continue les systèmes par la voie d'évaluations de la vulnérabilité et l'application de mesures correctives.
- Le Ministère contrôle et gère l'utilisation des privilèges d'administrateur.

Principales constatations de l'audit

- Les contrôles de sécurité au Centre régional de gestion de la circulation routière au sein du Ministère, n'étaient pas suffisamment vigoureux pour assurer une protection adéquate contre les menaces à la cybersécurité des systèmes. Les systèmes étaient donc exposés aux risques de cyberattaques de sources tant internes qu'externes.
- Le Ministère n'avait pas mis à jour et maintenu un inventaire exhaustif des appareils et des logiciels autorisés et non autorisés.

- Le Ministère n'était pas en mesure de détecter les activités qui se déroulaient sur son réseau et d'en rendre compte.
- Le Ministère n'avait pas établi de normes à l'égard de la configuration de base pour tous ses systèmes.
- Un système de gestion des configurations n'avait pas été mis en place pour assurer la gestion et la mise à jour continues des paramètres de la configuration de base des systèmes critiques, et surveiller les paramètres en vue de détecter les changements de configuration.
- Le Ministère avait mené une analyse des vulnérabilités au moment de la mise sur pied du RTMC, mais n'avait pas établi de processus continu d'évaluation des vulnérabilités et d'application de mesures correctives.
- Le Ministère n'avait pas mis en place des contrôles appropriés pour les comptes d'administrateur de système.

Recommandations de l'audit

- Le ministère des Transports et de l'Infrastructure devrait mener des évaluations du risque portant sur l'environnement opérationnel du RTMC et veiller à la mise en œuvre des contrôles de sécurité qui s'imposent.
- Le ministère des Transports et de l'Infrastructure devrait maintenir un inventaire de tous les composants de système (matériel et logiciels) autorisés pour accéder aux réseaux du RTMC, et mettre en œuvre des mécanismes permettant de détecter tout composant inconnu dans le réseau.
- Le ministère des Transports et de l'Infrastructure devrait établir des configurations de base pour tous les composants de système du RTMC, et veiller à en maintenir la sécurité.
- Le ministère des Transports et de l'Infrastructure devrait, de manière continue, mener des évaluations des vulnérabilités et appliquer les mesures correctives nécessaires, pour les systèmes du RTMC.
- Le ministère des Transports et de l'Infrastructure devrait assurer un contrôle approprié de l'utilisation des comptes d'administrateur de système qui s'applique aux systèmes du RTMC.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Société indépendante d'exploitation du réseau d'électricité – Surveillance du marché et cybersécurité

Date de publication : 2017

Bureau d'audit : Bureau du vérificateur général de l'Ontario

Hyperlien pour accéder au rapport integral :

http://www.auditor.on.ca/fr/content-fr/annualreports/arreports/fr17/v1_306fr17.pdf

Organisme audité

- Société indépendante d'exploitation du réseau d'électricité (IESO)

Objectif de l'audit

- Déterminer si la Société indépendante d'exploitation du réseau d'électricité (la SIERE) avait mis en place des systèmes et des processus efficaces pour s'assurer
  - que la surveillance des participants au marché de l'électricité est suffisante et que les participants au marché mènent leurs activités conformément aux règles du marché;
  - que les biens et les infrastructures de TI essentiels sont protégés de sorte que la fiabilité du réseau électrique soit maintenue.

Sélection de critères d'audit

- Des méthodes, contrôles et processus adéquats sont en place pour détecter les attaques à la sécurité, les menaces, les lacunes et les vulnérabilités et pour évaluer leurs répercussions sur la posture de sécurité de la SIERE, tout en contribuant aux objectifs clés des programmes.

Principales constatations de l'audit

- La SIERE ne compte aucun cadre supérieur chargé expressément de la cybersécurité. La personne qui assume les responsabilités les plus importantes en matière de cybersécurité n'a pas le pouvoir de prendre les décisions requises pour s'assurer que la SIERE a mis en place des mesures de protection suffisantes.
- Le nombre d'employés affectés à la cybersécurité est inférieur au nombre recommandé. Au moment de l'audit, la SIERE ne comptait quatre employés affectés à la cybersécurité, un nombre qui n'a pas augmenté au cours de la dernière décennie. Deux experts-conseils externes qui ont effectué des

examens distincts de l'environnement informatiques de la SIERE en 2015 et en 2016 ont recommandé que la SIERE affecte au moins sept employés à la cybersécurité.

- La SIERE ne possède pas un service de cybersécurité independent assorti de fonctions et de responsabilités clairement définies. Il revient aux gestionnaires des projets de TI de décider s'il convient de demander au personnel chargé de la cybersécurité de participer à la planification des projets et à quel moment il convient de le faire. Dans un certain nombre de cas, les gestionnaires de projets ont sollicité la participation du personnel chargé de la cybersécurité seulement aux dernières étapes des projets.
- Les systèmes de cybersécurité de la SIERE ne surveillent pas les activités en temps réel des utilisateurs privilégiés de sorte que des alertes soient déclenchées de manière proactive en cas de comportement inhabituel. Par ailleurs, le système de cybersécurité de la SIERE ne peut soutenir une analyse et une enquête en temps réel concernant certains types d'intrusions.
- L'équipe de la cybersécurité n'examine pas les contrats et n'évalue pas continuellement le risque que posent les fournisseurs pour la sécurité.
- Les bandes sur lesquelles sont stockées les données de sauvegarde ne sont pas chiffrées. Par ailleurs, certaines bandes de sauvegarde sont conservées sur place.

Sélection de recommandations de l'audit

- Pour renforcer sa gouvernance en matière de cybersécurité, la SIERE devrait créer un poste de cadre supérieur de la cybersécurité et établir un processus officiel de reddition de compte aux membres de sa haute direction et à son conseil d'administration.
- Pour que des ressources en cybersécurité suffisantes soient en place afin de réagir aux cyberattaques, la SIERE devrait porter le nombre d'employés affectés à la cybersécurité au niveau recommandé de sept employés ou embaucher un fournisseur externe de services de sécurité qui se tient prêt à intervenir.
- Pour réduire les risques associés à la cybersécurité et prévenir d'éventuels remaniements onéreux de projet de TI, les services de TI de la SIERE devraient faire en sorte que le personnel chargé de la cybersécurité intervienne aux premières étapes de tous les projets de TI pouvant entraîner des risques pour la cybersécurité.
- Pour réduire les risques en matière de cybersécurité auxquels la SIERE est exposée, celle-ci devrait faire l'acquisition d'une technologie qui prévient et détecte les intrusions donnant accès à des renseignements confidentiels, et qui surveille en temps réel l'accès aux renseignements confidentiels par le personnel.
- Pour réduire les risques en matière de cybersécurité, la SIERE devrait :
    - établir une politique de cybersécurité visant les fournisseurs externes;
    - s'assurer que l'équipe de la cybersécurité procède à une évaluation régulière des risques en matière de sécurité auxquels la SIERE est exposée en raison des fournisseurs externes.

- Pour que les bandes de sauvegarde soient protégées adéquatement et accessibles en fonction des besoins, la SIERE devrait :
    - chiffrer de manière appropriée toutes les bandes de sauvegarde;
    - conserver les bandes de sauvegarde dans un lieu sécurisé à l'extérieur de ses locaux.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

La sécurité des technologies de l'information des systèmes de contrôle industriels de l'industrie pétrolière et gazifère de l'Alberta

Date de publication : 2016

Bureau d'audit : Bureau du vérificateur général de l'Alberta

Hyperlien pour accéder au rapport integral :

https://www.oag.ab.ca/webfiles/reports/OAGFeb2016Report.pdf (en anglais)

Organismes audités

- Ministère de l'Énergie (Department of Energy)
- Organisme de réglementation de l'énergie de l'Alberta (Alberta Energy Regulator)
- Ministère de la Justice et du Solliciteur général (Department of Justice and Solicitor General)

Objectif de l'audit

- Déterminer si le ministère de l'Énergie et l'organisme de réglementation de l'énergie de l'Alberta (AER) comprennent les risques associés au manque de sécurité des systèmes de contrôle industriels et déterminer quel rôle, quel qu'il soit, ces organismes devraient-ils jouer pour veiller à atténuer ces risques de manière adéquate.

Critères d'audit

- Le ministère de l'Énergie et l'organisme de réglementation de l'énergie de l'Alberta comprennent si les Albertains sont exposés à des menaces, à des risques et à des conséquences, en raison du manque de sécurité des systèmes de contrôle industriels.

Principales constatations de l'audit

- Le ministère de l'Énergie et l'organisme de réglementation de l'énergie de l'Alberta n'avaient pas évalué les risques liés à la sécurité des technologies de l'information des systèmes de contrôle industriels de l'infrastructure pétrolière et gazière de l'Alberta. Le Ministère estimait qu'il n'était de son ressort de déterminer si les risques liés aux systèmes de contrôle industriels et auxquels est exposée l'infrastructure pétrolière et gazière régie par la province, devaient faire l'objet d'une évaluation. L'AER avait affirmé que, à ce moment-là, aucun rôle ne lui était dévolu à l'égard de l'évaluation des risques liés aux normes de sécurité des systèmes de contrôle industriels ou des technologies de l'information de l'industrie pétrolière et gazière de l'Alberta.

- Le ministère de la Justice et du Solliciteur général recueillait des renseignements de sécurité pour déterminer les menaces liées à la sécurité des infrastructures critiques de l'Alberta. Le Ministère estimait que la menace de cyberattaques contre l'industrie pétrolière et gazière de l'Alberta était faible, mais n'avait évalué ni les risques ni les conséquences dans l'éventualité d'une attaque réussie contre l'infrastructure pétrolière et gazière de l'Alberta.
- L'équipe d'audit n'a pas été en mesure d'obtenir de documents de la part d'une entité provinciale, quelle qu'elle soit, indiquant qu'une évaluation des risques et conséquences éventuels d'une cyberattaque, exploitant les failles de sécurité des systèmes de contrôle industriels, avait été menée.

Recommandations de l'audit

- Le ministère de l'Énergie et l'organisme de réglementation de l'énergie de l'Alberta devraient travailler de concert en vue de déterminer s'il serait avantageux pour l'Alberta de mener une évaluation plus poussée des menaces, risques et conséquences auxquels sont exposés les systèmes de contrôle industriels de l'infrastructure pétrolière et gazière régie par la province.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

La sécurité des systèmes de contrôle des infrastructures critiques pour les trains

Date de publication : 2016

Bureau d'audit : Bureau du vérificateur général de l'État de Victoria (Australie)

Hyperlien pour accéder au rapport integral :

https://www.audit.vic.gov.au/sites/default/files/20161109-Security-ICS.pdf (en anglais)

Organismes audités

- Ministère du Développement économique, des Emplois, du Transport et des Ressources (Department of Economic Development, Jobs, Transport and Resources)
- Administration du transport public de l'État de Victoria (Public Transport Victoria (PTV))
- Metro Trains Melbourne
- V/Line Proprietary Limited
- Victorian Rail Track
- Gestion des urgences de l'État de Victoria (Emergency Management Victoria)

Objectif de l'audit

- Évaluer si les risques liés à la sécurité des systèmes de contrôle des infrastructures critiques qui permettent d'exploiter et de contrôler les services ferroviaires sont gérés de manière efficace.

Critères d'audit

- Des niveaux de gouvernance appropriés ont été établis à l'égard des systèmes de contrôle.
- Les processus et contrôles en vue de déterminer, de prévenir et de détecter les événements liés à la sécurité des systèmes de contrôle et d'y donner suite, sont efficaces.
- Les moyens envisagés en vue de la reprise après catastrophe et de la continuité des activités sont efficaces et les moyens d'intervention ont été établis.
- Les régies ou sociétés de transport ont mis en œuvre les recommandations que formulées dans le rapport d'audit de 2010, intitulé Security of Infrastructure Control Systems for Water and Transport [La sécurité des systèmes de contrôle des infrastructures pour l'eau et les transports].

Principales constatations de l'audit

- L'Administration du transport public de l'État de Victoria n'avait pas encore élaboré de stratégie de cybersécurité pour les systèmes de contrôle.
- La Direction des systèmes et des services d'information ayant été démantelée, il n'était pas clair à qui il revenait de gérer et de soutenir les systèmes de contrôle, et les activités et projets visant les systèmes de contrôle entrepris par les exploitants de train n'étaient pas coordonnés.
- Il y avait un manque de compréhension quant à la propriété des actifs des systèmes de contrôle et quant à la responsabilité à l'égard de ces actifs. Dans certains cas, PTV, les exploitants de train et Victorian Rail Track n'étaient pas en mesure d'indiquer clairement lequel de ces organismes possédait tel ou tel système de contrôle et quel organisme en était responsable. Cette situation a eu pour conséquences d'entraîner parfois certains chevauchements d'activités, parfois certaines omissions, notamment :
    - PTV et les exploitants de train avaient doublonné leurs efforts pour établir des cadres, des politiques et des procédures;
    - les exploitants de train avaient doublonné les ressources de soutien du génie et de la maintenance;
    - la gestion de la sécurité des systèmes de contrôle était limitée.
- L'équipe d'audit a examiné les ententes entre PTV et les exploitants de train et a constaté que la sécurité des systèmes de contrôle ne faisait pas partie des exigences. Par conséquent, les exploitants de train n'étaient pas tenus de mettre en œuvre ou de respecter des normes minimales de sécurité pour les systèmes de contrôle.
- Le manque de clarté quant à savoir quel organisme possédait tels systèmes de contrôle et quel organisme en était responsable avait fait en sorte que le financement de la maintenance et des mises à niveau des systèmes de contrôle n'avait pas été considéré comme étant prioritaire.
- Avant l'audit, PTV n'avait pas élaboré de politiques ni communiqué de lignes directrices aux exploitants de train. Les exploitants avaient alors doublonné les efforts en amorçant de manière indépendante l'élaboration de cadres, de politiques et de procédures de sécurité, qui en étaient à diverses étapes d'avancement au moment de l'audit.
- Le conseil d'administration de PTV exerçait une surveillance limitée des vulnérabilités, menaces et risques auxquels les systèmes de contrôle étaient exposés. Les travaux d'audit ont permis d'en arriver notamment aux constatations suivantes :
    - très peu d'éléments probants indiquaient que des rapports sur les questions de cybersécurité étaient communiqués au conseil d'administration — à une seule occasion seulement, PTV avait présenté au conseil d'administration un rapport de haut niveau sur la cybersécurité, en avril 2016;
    - la participation du conseil d'administration à la gestion des questions de cybersécurité liées aux systèmes de contrôle était limitée.
- La responsabilité pour donner des orientations ou un soutien en matière de cybersécurité des systèmes de contrôle n'était pas établie clairement au sein des cadres supérieurs de PTV.

- Les exploitants de train et PTV devraient jouer un rôle plus actif pour entreprendre des audits sur la sécurité des systèmes de contrôle. Depuis la mise sur pied de PTV, cet organisme n'avait mené qu'un audit, en janvier 2016, lequel visait à évaluer le cadre de sécurité des systèmes de contrôle, à la fois de PTV et des exploitants de train. Les exploitants devraient mettre en œuvre des programmes en vue de mener périodiquement des évaluations des vulnérabilités et des tests pour évaluer la sécurité de leurs systèmes de contrôle.
- Les cadres de sécurité établis par les exploitants de train ne protègeaient pas adéquatements les systèmes de contrôle qui permettent d'exploiter les services ferroviaires. Les contrôles de sécurité qui servaient à déterminer, prévenir et détecter les cybermenaces et à y donner suite, n'étaient pas en mesure d'empêcher l'accès non autorisé aux systèmes de contrôle des exploitants.
- De graves vulnérabilités en matière de sécurité des systèmes de contrôle avaient été détectées et celles-ci pouvaient exposer les systèmes à des cybermenaces.

Sélection de recommandations de l'audit

L'Administration du transport public de l'État de Victoria (Public Transport Victoria) devrait :

- Officialiser les dispositions convenues avec les exploitants de train en matière de gouvernance et déterminer les responsabilités à l'égard de la cybersécurité des systèmes de contrôle.
- Élaborer une stratégie sur la cybersécurité des systèmes de contrôle qui établit :
    - le niveau de sécurité qui doit s'appliquer;
    - les dispositions en matière de gouvernance en vue de garantir une surveillance adéquate.
- Établir les dispositions en matière de financement de la mise à niveau, du renouvellement et de la mise à jour des systèmes de contrôle comme faisant partie de la renégociation des contrats de franchise et des ententes de services.
- Recruter et embaucher une équipe de professionnels possédant les compétences et l'expérience voulues, et dont la mission sera de conseiller les exploitants de train en matière de gestion de la sécurité, des risques et de la continuité des activités.
- Conseiller les exploitants de train sur la façon de mettre en œuvre des systèmes appropriés de gestion des risques qui permettent de déterminer, mesurer et surveiller les risques auxquels les systèmes de contrôle sont exposés, par les voies suivantes :
    - la création d'un registre des risques;
    - la réalisation d'une analyse de risques des vulnérabilités discernées en matière de sécurité, pour déterminer si des mesures immédiates s'imposent comme la mise en place de contrôles de sécurité ou de solutions techniques.
- Conseiller les exploitants de train sur la façon de mettre en œuvre des systèmes appropriés de gestion de la conformité comportant les éléments suivants :
    - des processus pour surveiller, mesurer et évaluer le rendement des contrôles de sécurité et en faire rapport;
    - des programmes d'audit interne en vue de mener périodiquement des évaluations des vulnérabilités ou des tests de sécurité ayant pour but de valider la sécurité des systèmes de contrôle des exploitants de train.

- Établir un cadre de contrôles de sécurité visant à déterminer, détecter et prévenir les cybermenaces et à y donner suite, comportant les éléments suivants :
    - un énoncé clair des exigences minimales et des principaux indicateurs de rendement;
    - un énoncé des exigences en matière de surveillance et de déclaration des incidents de sécurité;
    - un calendrier des audits prévus;
    - l'obligation de donner une formation au personnel en matière de sécurité des systèmes de contrôle.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Services centraux – Les exigences de sécurité à l'égard des applications Web

Date de publication : 2016

Bureau d'audit : Vérificateur provincial de la Saskatchewan

Hyperlien pour accéder au rapport integral :

https://auditor.sk.ca/pub/publications/public_reports/2016/Volume_1/06_Central Services_Web Security.pdf (en anglais)

Organisme audité

- Ministry of Central Services Ministère des Services centraux

Objectif de l'audit

- Évaluer si le ministère des Services centraux avait établi des exigences de sécurité qui étaient conformes aux meilleures pratiques pour l'élaboration et l'exploitation des applications Web des ministères.

Critères d'audit

- Les critères et sous-critères de l'audit sont énoncés dans la figure 3 du rapport d'audit.

Principales constatations de l'audit

- Nous avons constaté que le ministère des Services centraux (Services centraux/le Ministère) ne disposait pas de renseignements complets sur la nature et l'étendue des applications Web que le Ministère hébergeait au nom des autres ministères. En décembre 2015, la liste d'applications Web que le Ministère avait en sa possession ne recensait pas toutes les applications Web des ministères hébergées par Services centraux et qui étaient assujetties à la politique sur la sécurité du Ministère, et ne comprenait pas tous les détails importants à propos des applications Web (p. ex. la classification des risques, la version des logiciels, les serveurs sur lesquels les applications fonctionnaient).
- En décembre 2015, la politique sur la sécurité de Services centraux comportait peu de procédures ou d'orientations pour aider le personnel des ministères, y compris ses propres employés, à interpréter et à mettre en œuvre les sections de sa politique sur la sécurité portant expressément sur les applications Web.
- De façon générale, même si la politique sur la sécurité de Services centraux comportait des exigences de sécurité, le Ministère n'avait pas établi de procédures ni d'orientations de soutien dans plusieurs domaines importants liés à la sécurité des TI ayant trait aux applications Web.

- Services centraux comptait revoir sa politique sur la sécurité au moins à tous les deux ans. Le Ministère n'avait toutefois pas établi le moment et la fréquence où il prévoyait mettre à jour ses procédures et lignes directrices.
- Services centraux n'avait pas établi de procédures pour faire en sorte que les développeurs Web aient accès à des indications écrites à jour à propos de l'évolution des faiblesses de sécurité signalées par l'industrie, de manière à ce qu'ils puissent en tenir compte lors de l'élaboration de nouvelles applications Web.
- Services centraux n'effectuait pas de tests systématiques ou réguliers pour vérifier les vulnérabilités des applications Web, et n'obligeait pas non plus les ministères à le faire. Services centraux n'effectuait de tels tests ou n'externalisait cette tâche qu'à la demande expresse des ministères intéressés. Plutôt que d'adopter une approche proactive en testant de manière systématique les applications Web des ministères pour veiller à ce que les éléments de sécurité liés à leurs vulnérabilité soient adéquats, Services centraux avait adopté une approche réactive.
- Des tests effectués sur 18 sites Web avaient permis de détecter plus de 1 400 vulnérabilités. L'un des sites Web présentait plus de 100 vulnérabilités à risque élevé; dans l'ensemble, 22 % des vulnérabilités recensées étaient classées comme étant à risque moyen ou élevé. Parmi les 18 sites Web testés, 10 d'entre eux présentaient une faiblesse très connue à risque élevé. Les faiblesses recensées étaient présentes et répandues dans les divers ministères; on avait pu en établir la présence dans 17 des 18 sites Web testés. La sécurité de la plupart des sites Web testés était insuffisante.

Recommandations de l'audit

- Le ministère des Services centraux devrait consigner en dossier les renseignements importants à propos de toutes les applications Web des ministères qui sont assujetties à sa politique sur la sécurité.
- Le ministère des Services centraux devrait élaborer et maintenir des procédures et lignes directrices complètes pour soutenir l'élaboration et l'exploitation d'applications Web dont la sécurité est protégée.
- Le ministère des Services centraux devrait exiger une analyse systématique et régulière des vulnérabilités des applications Web pour en vérifier la conformité à la politique sur la sécurité du Ministère.
- Le ministère des Services centraux devrait collaborer avec les ministères en vue de trouver des solutions à l'égard des vulnérabilités présentant un risque élevé des applications Web.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Services centraux – La sécurité des centres de données

Date de publication : 2016

Bureau d'audit : Vérificateur provincial de la Saskatchewan

Hyperlien pour accéder au rapport integral :

https://auditor.sk.ca/pub/publications/public_reports/2016/Volume_1/05_Central Services Data Centre Security.pdf (en anglais)

Organisme audité

- Ministère des Services centraux

Objectif de l'audit

- Évaluer si le ministère des Services centraux avait établi des processus efficaces pour protéger la sécurité du centre de données. (L'audit n'a pas évalué l'efficacité des contrôles de sécurité visant expressément les applications client.)

Critères d'audit

- Les critères et sous-critères de l'audit sont énoncés dans la figure 3 du rapport d'audit.

Principales constatations de l'audit

- Le ministère des Services centraux (Services centraux/le Ministère) continuait de détenir insuffisamment d'information de la part des clients à propos de la classification (p. ex., le niveau de sensibilité) des données qui étaient hébergées sur les serveurs installés au centre de données. Services centraux a besoin de cette information pour être en mesure de collaborer avec ses clients en vue de déterminer le niveau de sécurité qui convient aux données dont il est question (notamment mettre en place des contrôles de sécurité plus stricts pour les renseignements confidentiels comme les numéros d'assurance sociale).
- En décembre 2015, Services centraux n'avait pas terminé la collecte des renseignements indiquant quelles données client étaient hébergées sur quels serveurs. Le Ministère n'avait pas non plus désigné des parties distinctes du réseau pour permettre de différencier les contrôles de sécurité selon la classification des données.
- Services centraux utilisaient des pare-feu pour aider à protéger son centre de données contre les pirates informatiques. Services centraux avait installé les pare-feu du centre de données à des

endroits appropriés et surveillait les événements de sécurité signalés. Toutefois, les pare-feu (tant au centre de données qu'aux sites client) n'étaient pas configurés correctement. Par exemple, les règles de pare-feu ne restreignaient pas suffisamment l'accès au centre de données en raison du fait que Services centraux n'avait pas suffisamment défini les règles de pare-feu que son fournisseur de services devaient respecter.

- Par ailleurs, les pare-feu aux sites client ainsi que les périphériques du réseau (p. ex., les systèmes de commutation) ne recevaient pas les mises à jour de logiciel, ou ne faisaient plus l'objet d'un soutien technique du fournisseur. Par conséquent, les correctifs informatiques qui auraient dû être installés pour parer aux vulnérabilités connues des pare-feu et des périphériques n'avaient pas été installés, et ce, depuis 2013 dans le cas des pare-feu client.
- En décembre 2015, Services centraux avait constaté que plus de 100 des 1 000 serveurs gérés par le Ministère au nom de ces clients, utilisaient des versions des logiciels de base [c.-à-d. les logiciels d'exploitation] ne faisant plus l'objet d'un soutien technique du fournisseur. Services centraux avait collaboré avec certains clients en 2015 pour mettre à niveau les serveurs et les bases de données avec des versions faisant l'objet d'un soutien technique de la part du fournisseur de produit. Cependant, en décembre 2015, les clients n'avaient pas tous produit la documentation confirmant leur acceptation du risque lié aux composants ne faisant plus l'objet d'un soutien technique du fournisseur.
- Même si le fournisseur de services en charge du centre de données de Services centraux effectuait la mise à jour de la plupart des serveurs au minimum à tous les trois mois, l'équipe d'audit avait constaté que l'installation des correctifs informatiques n'était pas complète pour toutes les vulnérabilités connues. Certaines mises à jour (dont un certain nombre étaient associées à des mises à jour qui avaient été offertes en 2012) n'avaient pas été installées dans les 10 serveurs testés par l'équipe d'audit. Services centraux n'avait pas demandé à son personnel ni au fournisseur de services d'effectuer ces mises à jour. Par ailleurs, le Ministère n'avait pas présenté d'analyse de risque étayée par des documents pour justifier le fait que ces serveurs n'avaient pas besoin des mises à jour manquantes.
- Tout comme par les années antérieures, Services centraux n'avait pas en main un plan complet et mis à l'essai, de reprise après catastrophe pour le centre de données. Par conséquent, certains clients de Services centraux possédant des systèmes client essentiels étaient dépourvus d'un plan de reprise après catastrophe. Quelques-uns des clients de Services centraux avaient signé, avec d'autres fournisseurs de services, des ententes séparées de reprise après catastrophe, pour la restauration de données et de systèmes essentiels désignés, en cas de catastrophe. Cependant, la mise en place de plusieurs ententes de reprise en cas de catastrophe ne constitue pas une approche efficace d'entreprise pour prévoir la reprise des activités du centre de données en cas de catastrophe.
- En décembre 2015, Services centraux employait des méthodes plus sécuritaires pour l'accès aux systèmes et aux données. Les comptes de réseau étaient conformes aux normes relatives aux mots de passe.

Recommandations de l'audit

- Le présent audit visait à vérifier les progrès réalisés à l'égard de la mise en œuvre de recommandations d'audit formulées antérieurement (en 2012). Deux de ces recommandations n'avaient pas été mises en œuvre intégralement, et étaient toujours valables après l'audit de suivi :
    - le ministère des Services centraux devrait configurer correctement et maintenir à jour ses serveurs et l'équipement de son réseau pour les protéger contre les menaces à la sécurité;
    - le ministère des Services centraux devrait se doter d'un plan de reprise après catastrophe pour le centre de données et les systèmes client.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Les logiciels malveillants dans les systèmes du gouvernement de l'État d'Australie-Occidentale

Date de publication : 2016

Bureau d'audit : Bureau du vérificateur général d'Australie-Occidentale

Hyperlien pour accéder au rapport integral :

https://audit.wa.gov.au/wp-content/uploads/2016/12/report2016_28-Malware.pdf (en anglais)

Organismes audités

- Ministère de l'Agriculture et de l'Alimentaire (Department of Agriculture and Food)
- Ministère du Procureur général (Department of the Attorney General)
- Routes principales de l'Australie-Occidentale (Main Roads Western Australia)
- Ministère des Mines et du Pétrole (Department of Mines and Petroleum)
- Ministère du Premier ministre et du Cabinet (Department of the Premier and Cabinet)
- Ministère des Transports (Department of Transport)

Objectif de l'audit

- Déterminer si les organismes gouvernementaux sélectionnés ont mis en place des contrôles efficaces pour prévenir, détecter et contrer les menaces liées aux logiciels malveillants qui infectent leurs systèmes informatiques.

Critères d'audit

- Les organismes ont mis en œuvre des contrôles pour prévenir, détecter et contrer les menaces liées aux logiciels malveillants.
- Les contrôles mis en place permettent de gérer efficacement les menaces liées aux logiciels malveillants.

Principales constatations de l'audit

- L'audit a permis de détecter des communications associées à des logiciels malveillants sur tous les réseaux qui ont été testés dans le cadre des travaux d'audit. Cela comprenait des tentatives d'attaque en provenance de pages Web malveillantes, le téléchargement de fichiers de logiciels malveillants et des communications actives entre des logiciels malveillants et Internet. Le volume élevé d'attaques montrait qu'il s'agissait d'une menace structurée et ciblée en vue de déjouer les contrôles de sécurité, et mettait en évidence la nécessité que les organismes comprennent les menaces dont il était question et corrigent toute faille dans leurs contrôles de sécurité.

- Deux organismes présentaient des signes persistants d'infection par des logiciels malveillants qui avaient déjoué leurs contrôles de sécurité. Un organisme présentait une seule infection qui était demeurée active pendant les 12 jours de la période étudiée. Un autre organisme présentait plus de cinq infections qui étaient demeurées actives pendant environ deux jours, et au moins un de ses ordinateurs avait été réinfecté au cours de la période d'évaluation. Ces infections actives avaient exposé les réseaux, systèmes et données des organismes concernés, à des risques.
- Les défaillances des contrôles de TI étaient toujours monnaie courante. Les tests effectués avaient montré que tous les organismes en question présentaient des défaillances des contrôles ou des contrôles manquants. Parmi les problèmes répandus, plusieurs étaient liés au fait que des correctifs de sécurité n'avaient pas été installés ou que les systèmes d'exploitation étaient périmés. On avait aussi relevé des problèmes concernant la gestion des logiciels antivirus, l'attribution de droits d'accès et la conception des réseaux.
- Des professionnels compétents étaient tenus de surveiller l'environnement des TI et de déterminer les enjeux de manière proactive. Tous les organismes sélectionnés aux fins de l'audit comptaient des employés du secteur des TI dont le rôle était lié à la sécurité de l'information. Certains organismes plus chanceux comptaient plus d'un tel employé, mais dans la plupart des cas, l'organisme ne devait s'en remettre qu'à un seul d'entre eux, sur lequel reposaient tant les réussites que les défaillances.
- La plupart des organismes n'avaient pas donné une formation de sensibilisation adéquate à leur personnel.
- Le gouvernement de l'État d'Australie-Occidentale était dépourvu d'une stratégie coordonnée pour parer aux cyberattaques, y compris les logiciels malveillants.
- Au moment de l'audit, aucune politique et aucun cadre en matière de sécurité n'avait été établi à l'échelle de l'ensemble du gouvernement pour orienter les organismes quant à la manière de mettre en œuvre un programme de sécurité qui donne les résultats voulus.
- Par ailleurs, les organismes n'étaient pas tenus de déclarer les incidents liés aux logiciels malveillants et de les signaler à un organisme central. Aucune entité n'était en mesure de présenter à l'équipe d'audit un état général de la situation quant à l'ampleur ou à la nature des menaces liées aux logiciels malveillants, auxquelles les organismes étaient exposés.

Recommandations de l'audit

- Les organismes visés par l'audit devraient :
    - évaluer le risque posé par les menaces liées aux logiciels malveillants qui ont été observées au cours des travaux d'audit;
    - améliorer chacun des contrôles qui s'est révélé inefficace;
    - envisager l'ajout de contrôles qui pourraient mieux protéger la sécurité de leurs réseaux, systèmes et données contre les logiciels malveillants.
- Le secteur public, par l'intermédiaire du Bureau du dirigeant principal de l'information du gouvernement de l'État d'Australie-Occidentale (Office of the Government Chief Information Officer), devrait :

- examiner des méthodes en vue d'encourager la collaboration ainsi que la mise en commun, entre les organismes, d'information et de ressources;
- recueillir de l'information qui permettrait de bien comprendre la menace que représentent les logiciels malveillants et d'autres cybermenaces pour le secteur public.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

La gestion de la sécurité des systèmes d'information

Date de publication : 2016

Bureau d'audit : Bureau du vérificateur général d'Australie-Méridionale

Hyperlien pour accéder au rapport integral :

https://www.audit.sa.gov.au/LinkClick.aspx?fileticket=VVFWud381CQ%3d&tabid=369&portalid=0&mid=970&forcedownload=true (en anglais)

Organismes audités

- Ministère de l'Éducation et du Développement de l'enfant (Department for Education and Child Development)
- Administration du renouveau urbain (Urban Renewal Authority (Renewal SA))
- Commission des services d'incendie et d'urgence d'Australie-Méridionale (SAFECOM) (South Australian Fire and Emergency Services Commission (SAFECOM))
- Administration des tribunaux (Court Administration Authority (CAA))
- Ministère de la Planification, du Transport et de l'Infrastructure (Department of Planning, Transport and Infrastructure (DPTI))
- Curateur public (Public Trustee)
- Ministère de l'Environnement, de l'Eau et des Ressources naturelles (Department for Environment, Water and Natural Resources (DEWNR))
- Société de l'eau d'Australie-Méridionale (South Australian Water Corporation (SA Water))
- Ministère du Procureur général (Attorney-General's Department (AGD))
- Ministère du Premier ministre et du Cabinet (Department of the Premier and Cabinet (DPC))

Objectif de l'audit

- Déterminer si les organismes gèrent de manière efficace les aspects suivants de la sécurité de l'information :
    - les anciens systèmes d'exploitation des serveurs;
    - les correctifs informatiques (pour les systèmes d'exploitation et des bases de données sélectionnées);
    - l'accès des utilisateurs privilégiés;
    - les appareils mobiles;
    - les listes blanches d'applications.

Critères d'audit

- Les critères d'audit n'ont pas été rendus publics.

Principales constatations de l'audit

- Huit des dix organismes audités exploitaient d'anciens serveurs qui ne faisaient plus l'objet d'un soutien technique du fournisseur. Au total 233 anciens serveurs répartis dans les 10 organismes étaient en exploitation (13 % de tous les serveurs exploités par les organismes).
- Tous les organismes s'employaient à mettre hors service les anciens serveurs. Cependant, le degré d'exposition au risque et la portée des contrôles d'atténuation mis en application pour protéger ces serveurs variaient d'un organisme à un autre. Plusieurs organismes n'avaient pas mis en œuvre des contrôles d'atténuation suffisants pendant la période de transition.
- La plupart des organismes audités avaient établi des politiques et des procédures pour gérer le processus d'installation des correctifs informatiques. Cependant, les correctifs de mise à jour de sécurité destinés aux systèmes d'exploitation ou aux bases de données n'avaient pas été installés sur certains serveurs de trois des quatre organismes qui ont fait l'objet d'une vérification. En outre :
    - les correctifs informatiques d'un système d'exploitation, d'une base de données ainsi que d'une application qui constituaient un élément principal du système d'information d'un des organismes n'avaient pas été installés;
    - les politiques et procédures de gestion des correctifs et de gestion des changements de deux des organismes présentaient des lacunes;
    - les processus de vérification et de production de rapports liées à la conformité en matière de gestion des correctifs comportaient des lacunes;
    - dans le cas d'un organisme, les exemptions liées à l'installation des correctifs étaient insuffisamment étayées par des documents.
- Les deux organismes qui avaient fait l'objet d'une vérification à cet égard ne géraient pas efficacement l'accès des utilisateurs privilégiés au Active Directory (qui est le service d'annuaire ou service de répertoire de Microsoft) conformément aux exigences du Cadre de gestion de la sécurité de l'information. On avait relevé certains cas, où l'accès des utilisateurs privilégiés sur des ordinateurs locaux était potentiellement excessif. On avait aussi constaté les points suivants :
    - l'absence d'un examen systématique et périodique de la liste des utilisateurs privilégiés pouvant accéder au Active Directory;
    - des lacunes dans les politiques et procédures ayant trait à l'accès des utilisateurs et à la sécurité des TI;
    - des cas où des rapports sur des employés ayant cessé leurs fonctions n'avaient pas été reçus ou examinés promptement;
    - des activités d'utilisateurs privilégiés qui n'avaient pas été suffisamment « journalisées » [enregistrées dans un journal de vérification] et surveillées.
- Les deux organismes qui avaient fait l'objet d'une vérification à cet égard prévoyaient améliorer les contrôles pour gérer de manière adéquate la gestion des appareils mobiles pour accéder aux ressources et aux données de l'organisme. Les deux organismes avaient établi des politiques et

procédures pour gérer les appareils mobiles, mais les travaux d'audit avaient mené aux constatations suivantes :

- les contrôles de sécurité applicables aux appareils mobiles n'étaient pas conformes aux lignes directrices sur les pratiques exemplaires;
- il n'y avait pas suffisamment de rapports sur l'usage des appareils mobiles au sein de l'agence
- les politiques et procédures applicables aux appareils mobiles ne faisaient pas l'objet d'un examen ou d'une approbation périodiques.

- Les deux organismes qui avaient fait l'objet d'une vérification à cet égard n'avaient pas mis en œuvre une liste blanche d'applications. Les travaux d'audit ont aussi mené aux constatations suivantes :
  - un organisme n'effectuait pas d'examen périodique des applications et dans le cas d'un autre organisme, on ne consignait pas en dossier des documents indiquant que l'organisme effectuait de tels examens;
  - les politiques sur la sécurité de l'information d'un autre organisme étaient à l'état d'ébauche, en attente d'un examen et d'une approbation.

Sélection de recommandations de l'audit

- Les organismes devraient mettre hors service les anciens serveurs Windows dans les meilleurs délais possible.
- D'ici à la mise hors service des anciens serveurs, les organismes devraient envisager de mettre en œuvre des contrôles supplémentaires pour atténuer les risques plus élevés que présente l'exploitation d'anciens serveurs. Ces mesures devraient comprendre les suivantes :
  - la mise en œuvre de listes blanches d'applications sur les serveurs en question;
  - l'évitement du recours à des comptes d'utilisateur privilégié sur les serveurs à des fins non administratives;
  - la mise en œuvre d'une solution logicielle pour l'application de correctifs informatiques faisant appel à un système de détection et de prévention des intrusions;
  - la désactivation des fonctionnalités non nécessaires ou des fonctionnalités qui sont vulnérables aux méthodes d'intrusion les plus courantes.
- Les organismes devraient :
  - recenser les serveurs dans lesquels on a détecté des correctifs informatiques manquants et s'assurer que tous les correctifs de sécurité y seront installés;
  - veiller à déterminer promptement les correctifs informatiques à installer, en surveillant et en examinant de façon régulière les bulletins de sécurité;
  - formuler et consigner des politiques en matière de gestion des correctifs informatiques et de gestion des changements; veiller à revoir régulièrement et à mettre à jour au besoin les politiques et procédures en la matière;
  - prévoir dans les pratiques de certification ou d'expression d'assurance une évaluation régulière des niveaux de conformité à l'égard de l'installation des correctifs sur les serveurs et les postes de travail;

    - maintenir en dossier une documentation suffisante à propos des exemptions ayant trait à l'installation des correctifs, pour tous les serveurs.
- Restreindre les droits d'accès d'administrateur de système local en fonction des tâches de l'utilisateur.
- Prévoir la création de comptes utilisateurs séparés qui sont réservés expressément et distinctement aux activités d'administrateur et aux activités non administratives.
- Formuler et consigner une politique de gestion de l'accès des utilisateurs. Veiller à revoir régulièrement et à mettre à jour au besoin les politiques et procédures ayant trait aux TI.
- S'assurer que les rapports sur les employés ayant cessé leurs fonctions sont produits et communiqués régulièrement et promptement. Dès que les organismes les ont reçus, ils devraient en prendre connaissance et supprimer les comptes utilisateurs correspondants, dans les meilleurs délais possible.
- Le ministère du Premier ministre et du Cabinet (DPC) devrait communiquer des lignes directrices supplémentaires aux organismes à propos de l'installation de logiciels de gestion des appareils mobiles ou d'autres contrôles techniques.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

SaskPower – La gestion des risques liés aux cyberincidents

Date de publication : 2015

Bureau d'audit : Vérificateur provincial de la Saskatchewan

Hyperlien pour accéder au rapport integral :

https://auditor.sk.ca/pub/publications/public_reports/2015/Volume_1/18_SaskPower-Cyber Incidents.pdf (en anglais)

Organisme audité

- SaskPower

Objectif de l'audit

- Évaluer si la société SaskPower avait mis en place des processus efficaces pour gérer les risques liés aux cyberincidents de manière à protéger les systèmes d'alimentation et distribution électrique.

Critères d'audit

- Les critères et sous-critères de l'audit sont présentés à la figure 1 du rapport d'audit.

Principales constatations de l'audit

- La société SaskPower avait bien dressé et gardé à jour une liste des actifs électroniques qu'elle estimait comme étant critiques, mais elle n'avait toutefois pas désigné de manière précise lesquels de ces actifs pouvaient être la cible éventuelle d'un cyberincident.
- En mars 2015, SaskPower avait présenté aux cadres supérieurs et au conseil d'administration de la société un résumé de haut niveau des menaces potentielles auxquels les actifs de la société qui servaient à l'alimentation et distribution électrique étaient exposés, ainsi que des répercussions de ces menaces et des mesures de protection qu'elle avait mises en place pour atténuer ces menaces (sa stratégie d'atténuation). Cependant, ce résumé de haut niveau n'était pas forcément complet. SaskPower n'avait pas déterminé précisément les faiblesses potentielles de ses systèmes de technologie opérationnelle ni les menaces auxquelles les systèmes étaient exposés (p. ex., les connexions non autorisées de ces systèmes à Internet, l'utilisation de clés USB), qui pourraient permettre à un cyberpirate d'accéder aux actifs électroniques critiques. Qui plus est, SaskPower n'avait pas évalué la probabilité de telles cyberattaques qui risqueraient d'occasionner un cyberincident.

- SaskPower disposait d'un plan de détection et d'intervention dans l'éventualité où surviendrait un indicent, y compris un cyberincident. Ce plan comprenait des procédures détaillées tant pour détecter les cyberincidents que pour y donner suite. Le plan décrivait les activités de détection à mettre en application, comme le recours à des systèmes de détection des intrusions, et à des logiciels antivirus ainsi que l'examen des journaux de sécurité et des alertes de sécurité. SaskPower avaient mis en œuvre les activités de détection décrites dans le plan, y compris l'examen périodique des alertes et des journaux de sécurité des systèmes. Divers employés avaient été désignés pour effectuer l'examen des journaux de sécurité et des alertes.
- La société SaskPower mettait en application des processus pour détecter divers événements liés à la sécurité des TI et en assurer le suivi, mais l'équipe d'audit a constaté que la société n'avait pas défini dans des documents les critères qui établissaient quels événements liés à la sécurité des TI SaskPower considérait comme étant des cyberincidents (comme une série de tentatives infructueuses de connexion sur une courte période).
- SaskPower avait mis en application ses procédures de changement de droits d'accès des utilisateurs et, à juste titre, avait accordé à un nombre restreint d'employés les droits d'accès d'administrateur aux actifs électroniques critiques.
- SaskPower avait communiqué à ses employés les procédures énoncées dans son plan d'intervention et les avaient mis à leur disposition pour qu'ils puissent facilement les consulter en cas d'incident.
- Le plan d'intervention en cas d'incident exigeait que l'équipe d'intervention reçoive une formation chaque année et que l'intervention en cas d'incident fasse l'objet d'un examen pour tirer les enseignements en vue d'interventions futures. Des éléments probants indiquaient que la formation annuelle avait bien lieu. SaskPower mettait périodiquement à l'épreuve son plan d'intervention au moyen d'exercices de mise à l'épreuve.

Recommandations de l'audit

- SaskPower devrait définir dans des documents les types de menaces les plus probables auxquelles pourraient être exposées ses technologies de l'information et qui pourraient provoquer un cyberincident susceptible de compromettre son aptitude à assurer l'alimentation et la distribution électrique.
- SaskPower devrait confirmer que sa stratégie d'atténuation des cyberrisques répond adéquatement aux menaces importantes de cyberincidents susceptibles de compromettre son aptitude à assurer l'alimentation et la distribution électrique.
- SaskPower devrait donner des orientations à ses employés pour les aider à déterminer quand un événement lié à la sécurité des technologies de l'information constitue un cyberincident et demande le recours au plan d'intervention de son système de gestion des incidents.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Manitoba Hydro – La gestion des cyberrisques liés aux systèmes de contrôle industriels

Date de publication : 2014

Bureau d'audit : Bureau du vérificateur général du Manitoba

Hyperlien pour accéder au rapport integral :

http://www.oag.mb.ca/wp-content/uploads/2014/03/Chapter-8-Manitoba-Hydro-ICS-Security-Web.pdf (en anglais)

Organisme audité

- Manitoba Hydro

Objectif de l'audit

- Déterminer si les pratiques de gestion des risques de Manitoba Hydro permettent de mettre au point des contrôles de sécurité, pour les systèmes de contrôle industriels et les technologies de l'information connexes, ayant pour effet d'atténuer de manière raisonnable les cyberrisques qui ont été définis.

Critères d'audit

- Les critères d'audit étaient fondés sur les normes proposées dans le document intitulé *Programme d'audit et d'assurance de la gestion du risque TI* [version française de *IT Risk Management Audit/Assurance Program*], élaboré par l'Association des professionnels de la vérification et du contrôle des systèmes d'information (ISACA).

Principales constatations de l'audit

- Manitoba Hydro n'avait pas établi l'ordre de priorité de ses systèmes de contrôle industriels et des systèmes de TI connexes quant à leur degré de criticité par rapport aux processus de production, de transport et de distribution de l'électricité. Manitoba Hydro n'avait pas défini le risque lié à la cybersécurité des systèmes de contrôle industriels comme faisant partie du profil de risque de la société, et n'avait pas évalué ce risque. Cet état de fait n'avait pas été communiqué au conseil d'administration de la société. Les directions au sein du secteur Power Supply et du secteur IT Services de Manitoba Hydro ne produisaient pas de rapports sur les risques.
- Manitoba Hydro n'avait pas dressé la liste complète des systèmes de contrôle industriels et des systèmes de TI connexes servant à soutenir les processus de production, de transport et de

distribution de l'électricité, et n'en avait pas non plus établi l'ordre de priorité quant à leur degré de criticité. La société n'avait pas non plus dressé un inventaire complet correspondant du matériel et des logiciels associés aux systèmes de contrôle industriels.

- À chacun des six sites visités par l'équipe d'audit, certains contrôles de sécurité pour les systèmes de contrôle industriels étaient manifestement en place (p. ex., un périmètre de sécurité physique, des contrôles par mots de passe et des contrôles environnementaux des salles d'ordinateurs), mais de graves faiblesses ont été constatées dans les domaines suivants :
    - la segmentation du réseau;
    - la gestion des correctifs informatiques;
    - les contrôles d'accès;
    - le renforcement des systèmes;
    - la détection des intrusions;
    - la sécurité physique;
    - la détection des logiciels malveillants et la protection contre ceux-ci;
    - la gestion des changements de contrôle et de configuration;
    - la planification liée aux incidents et les interventions pour donner suite aux incidents.
- L'isolement physique d'un système permet certes d'atténuer le risque qu'un logiciel malveillant se propage d'une centrale électrique au poste de commande du réseau et vice versa, mais cette façon de faire avait créé un faux sentiment de sécurité au sein de Manitoba Hydro. Cette configuration était en application dans toutes les installations visitées au cours des travaux d'audit. Dans le contexte actuel des cybermenaces, il ne faudrait pas considérer l'isolement physique entre deux réseaux comme étant la solution ultime et complète en matière de contrôles de sécurité. Il faut absolument prévoir des couches de contrôle supplémentaires en vue d'atténuer l'ensemble des risques.
- Au sein de Manitoba Hydro, aucune surveillance à l'échelle de l'ensemble de la société n'était exercée quant à la qualité et à l'adéquation des mesures de cybersécurité qui étaient en place. Chaque secteur ou département au sein de la société était chargé de la gestion de ses propres systèmes de contrôle industriels et des risques qui leur étaient associés, ce qui pouvait avoir entraîné une sous-estimation des risques à l'échelle de l'ensemble de la société. La fragmentation du contrôle peut mener à des pratiques ou contrôles incohérents ou incompatibles.
- En raison de possibles préoccupations opérationnelles et sécuritaires, les politiques de la société en matière de TI ne s'appliquaient pas aux systèmes de contrôle industriels. Aucune autre politique n'était en place pour orienter les directions et secteurs de la société dans la gestion de leurs systèmes de contrôle industriels et dans leurs efforts en vue d'assurer la sécurité de ces systèmes.
- Lors des visites aux sites, il a été possible de constater que certains contrôles de sécurité physiques étaient en place à chacun des sites pour restreindre l'accès du public mais les contrôles n'étaient pas appliqués de la même manière d'un site à un autre, ce qui augmentait le risque d'un accès non autorisé aux systèmes de contrôle industriels. Il n'a pas été possible d'obtenir une justification pour expliquer la variation des mesures de sécurité d'un site à un autre.

- La formation sur la sensibilisation à la cybersécurité donnée par Manitoba Hydro ne mettait pas suffisamment l'accent sur les menaces et vulnérabilités liées aux systèmes de contrôle industriels. Par ailleurs, les communications de la société sur la sensibilisation à la sécurité ne traitaient pas des cyberrisques liés aux systèmes de contrôle industriels.

Recommandations de l'audit

Manitoba Hydro devrait :

- déterminer, évaluer et atténuer tous les risques de cybersécurité liés aux systèmes de contrôle industriels, et le faire selon un ordre de priorité des actifs électroniques quant à leur degré de criticité par rapport aux opérations de la société;
- une fois que les risques de cybersécurité auront été évalués, ajouter la cybersécurité au profil de risque de la société décrit dans le rapport annuel sur la gestion des risques présenté au conseil d'administration de la société;
- attribuer à un cadre supérieur la responsabilité de la cybersécurité à l'échelle de l'ensemble de la société;
- élaborer et mettre en œuvre des instruments de politique en matière de cybersécurité des systèmes de contrôle industriels, et veiller à ce qu'ils s'appliquent à tous les systèmes de contrôle industriels;
- attribuer à un cadre supérieur la responsabilité de la sécurité physique à l'échelle de l'ensemble de la société;
- élaborer et mettre en œuvre des instruments de politique en matière de sécurité physique pour contrôler l'accès physique aux systèmes de contrôle industriels;
- élaborer et mettre en œuvre un programme complet de formation et de sensibilisation à la cybersécurité des systèmes de contrôle industriels, à l'intention de tout le personnel chargé de l'exploitation, de la maintenance et de la sécurité des systèmes de contrôle industriels;
- élaborer une stratégie en vue d'amener la gestion des TI et des technologies opérationnelles, y compris la sécurité des TI, à converger.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit
Sécurité des réseaux sans fil

Date de publication : 2014

Bureau d'audit : Vérificateur général de la Ville de Montréal

Hyperlien pour accéder au rapport integral :

http://www.bvgmtl.ca/wp-content/uploads/2014/06/RA2013_section5-4.pdf

Organismes audités

- Service des technologies de l'information (STI)
- Division des ressources informationnelles, arrondissement de Saint-Laurent
- Division de l'informatique, arrondissement de Saint-Léonard

Objectif de l'audit

- Déterminer si les contrôles mis en place permettent que seuls les réseaux sans fil dûment autorisés soient présents à la Ville et que leurs mécanismes de sécurité empêchent les accès illicites au réseau corporatif de la Ville.

Critères d'audit

- Les critères d'audit n'ont pas été rendus publics, mais ils étaient basés sur les sources de bonnes pratiques suivantes :
    - *Recommandations de sécurité relatives aux réseaux WiFi*, Agence nationale de la sécurité des systèmes d'information, Secrétariat général de la défense et de la sécurité nationale, ministère français de la Défense;
    - *Establishing Wireless Robust Security Networks: A Guide to IEEE802.11i*, Special Publication 800-97, National Institute of Standards and Technology (NIST).

Principales constatations de l'audit

- Globalement, les réseaux sans fil sont adéquatement protégés. Cependant, la gestion de la sécurité des réseaux sans fil nécessite certaines améliorations.
- Le STI n'avait pas mis en place un processus de détection des réseaux sans fil non autorisés. Au cours des tests d'audit, les auditeurs ont trouvé un point d'accès sans fil caché au sein d'un édifice de la Ville pour lequel il a été impossible de déterminer le propriétaire.

- L'équipe d'audit a découvert plusieurs points d'accès sans fil ouverts et non sécurisés dans deux des huit édifices échantillonnés.
- L'équipe d'audit a découvert neuf points d'accès sans fil configurés pour utiliser le protocole WPA2, mais ils permettaient aussi l'utilisation de protocoles moins robustes, dont le WPA et le WPS (répartis dans cinq édifices).
- L'équipe d'audit a découvert, au sein d'un édifice, deux imprimantes dont la fonctionnalité sans fil était activée, mais non protégée. Ces imprimantes étaient utilisées par des employés traitant de l'information confidentielle.

Recommandations de l'audit

- Le Service des technologies de l'information devrait :
    - mettre en place un processus récurrent de détection des réseaux sans fil non autorisés et, le cas échéant, prendre les actions correctives nécessaires pour les supprimer.
    - s'assurer que tous les points d'accès sans fil sont configurés avec un protocole de sécurité robuste.
    - s'assurer, avec les arrondissements concernés, que les équipements des réseaux sans fil utilisent uniquement les protocoles de sécurité les plus robustes.
    - désactiver l'accès sans fil de ces imprimantes si celui-ci n'est pas absolument nécessaire. Dans le cas contraire, l'utilisation d'un protocole de sécurité robuste est recommandé.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Les cyberattaques : Sécuriser les systèmes de TIC

Date de publication : 2014

Bureau d'audit : Bureau du vérificateur général de l'Australie

Hyperlien pour accéder au rapport integral :

https://www.anao.gov.au/sites/g/files/net4181/f/AuditReport_2013-2014_50.pdf (en anglais)

Organismes audités

- Bureau australien de la statistique (Australian Bureau of Statistics)
- Service australien des douanes et de la protection des frontières (Australian Customs and Border Protection Service (Customs)
- Administration australienne de la sécurité financière (Australian Financial Security Authority)
- Bureau de l'impôt de l'Australie (Australian Taxation Office)
- Ministère des Affaires étrangères et du Commerce international (Department of Foreign Affairs and Trade)
- Ministère des Services à la personne (Department of Human Services)
- IP Australia [organisme du gouvernement de l'Australie chargé de la propriété intellectuelle]

Objectif de l'audit

- Évaluer la conformité des organismes audités, aux quatre stratégies obligatoires de sécurité des TIC et aux contrôles connexes du Manuel de la sécurité de l'information du gouvernement de l'Australie (Australian Government Information Security Manual (ISM)).

Critères d'audit

- Les contrôles obligatoires prescrits dans le Manuel de la sécurité de l'information, centrés sur les quatre premières stratégies d'atténuation, ont été mis en œuvre.
- Des processus adéquats de gestion de l'accès logique et de gestion des changements en vue d'autoriser l'installation de correctifs de sécurité critiques, pour les applications et les systèmes d'exploitation, sont mis en œuvre.
- Des dispensations approuvées sont déjà établies pour tout écart de conformité aux contrôles obligatoires prescrits dans le Manuel de la sécurité de l'information.

Principales constatations de l'audit

- Les organismes audités avaient établi des cadres internes en matière de sécurité de l'information, mis en œuvre des contrôles destinés à protéger l'environnement des TIC de l'entité contre les cyberattaques externes, et élaboré des processus de gestion des changements en vue d'autoriser l'installation des correctifs de sécurité pour les applications et les systèmes d'exploitation. Bien que ces mesures aient contribué à la protection de l'information des entités visées, les organismes audités ne s'étaient toujours pas conformés intégralement aux quatre premières stratégies d'atténuation prescrites par le gouvernement de l'Australie en 2013. En outre, aucun des organismes audités ne prévoyaient être en mesure de s'y conformer intégralement d'ici le milieu de 2014, la date cible fixée par le gouvernement.
- Les travaux d'audit avaient fait ressortir que, compte tenu de l'étape de mise en œuvre des quatre premières stratégies d'atténuation et de mise en œuvre des contrôles généraux visant les TI que les organismes avaient atteinte, la situation générale des organismes audités à l'égard de la sécurité de l'information représentait une protection raisonnable contre les atteintes à la sécurité de l'information et contre la divulgation de renseignements attribuables à des sources internes, mais qu'elle comportait toujours des vulnérabilités aux cyberattaques en provenance de sources externes contre les systèmes des TIC des entités.
- Trois des sept organismes avaient mis en œuvre des listes blanches d'applications pour l'ensemble de leurs ordinateurs de bureau, tandis qu'un des organismes s'affairait à mettre en œuvre des listes blanches d'applications pour l'ensemble de ses serveurs. Au cours de l'audit, le Bureau national de vérification de l'Australie a par ailleurs exprimé des préoccupations à propos du fait que, dans le cas de deux des organismes, la liste blanche des applications était réglée au mode « vérification seulement » [« audit-only mode »] faisant donc en sorte que les événements que la liste blanche « aurait bloqués » si la liste blanche avait réellement été activée, étaient simplement répertoriés mais non bloqués. Dans le cas de quatre des organismes, la politique par défaut n'était pas réglée de manière à prévoir le refus d'exécuter le logiciel, ce qui présentait la possibilité que des employés ne détenant pas des droits d'administrateur de système puissent néanmoins installer un logiciel sur les systèmes de l'entité.
- Dans tous les cas, les organismes n'étaient pas en conformité avec les exigences obligeant l'installation des correctifs de sécurité critiques dans les deux jours suivant la mise à disposition des correctifs, et seulement deux des organismes avaient adopté des pratiques vérifiables liées à l'installation des correctifs, qui leur permettaient de donner suite à la mise à disposition périodique ou ponctuelle de correctifs par les fournisseurs de produits, comme les correctifs de sécurité diffusés chaque mois par Microsoft.
- Les travaux d'audit ont amené le Bureau national de vérification de l'Australie à conclure que la politique des organismes quant à la saisie et au maintien d'un journal de vérification des comptes d'utilisateurs privilégiés n'était pas mise en application la plupart du temps. Cette faiblesse systémique des contrôles soulevait des questions quant à l'aptitude des organismes à détecter les épisodes d'accès non autorisé à des comptes d'utilisateurs privilégiés ou les activités inappropriées de la part d'utilisateurs privilégiés, d'y donner suite ou d'enquêter sur ces événements.

Recommandations de l'audit

- Pour se conformer intégralement aux stratégies obligatoires prescrites dans le Manuel de la sécurité de l'information, les organismes devraient :
    - mener à leur terme les activités en cours de réalisation, en vue de mettre en œuvre les quatre premiers contrôles prescrits dans le Manuel dans l'ensemble de l'environnement des TIC de l'entité;
    - définir des marches à suivre en vue de renforcer la mise en œuvre de listes blanches d'applications, l'installation des correctifs informatiques pour les applications et les systèmes d'exploitation, et la gestion des comptes d'utilisateurs privilégiés.
- Pour atténuer les risques de cyberattaques visant l'information stockée dans les bases de données des organismes, les organismes devraient renforcer les contrôles d'accès logiques aux bases de données auxquels il faudrait assujettir les comptes d'utilisateurs privilégiés, en éliminant les comptes partagés, en enregistrant les activités dans un journal de vérification et en surveillant les activités associées aux comptes d'utilisateurs.
- Pour renforcer leur situation en matière de sécurité des TIC, les organismes devraient :
    - mener chaque année une évaluation des menaces, portant sur l'ensemble des systèmes des TIC, en tenant compte des 35 premières stratégies d'atténuation (Top 35 Mitigations Strategies) proposées par le Australian Signals Directorate [organisme australien chargé du renseignement et de la sécurité électronique des transmissions de la Défense et de l'État];
    - mener une évaluation et un examen périodiques dirigés par le directeur de la sécurité de l'entité, pour dresser un état de la situation générale de l'organisme en matière de sécurité des TIC.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Cadre de gestion de la sécurité de l'information à l'échelle de l'ensemble du gouvernement de l'État de Victoria

Date de publication : 2013

Bureau d'audit : Bureau du vérificateur général de l'État de Victoria (Australie)

Hyperlien pour accéder au rapport integral :

https://www.audit.vic.gov.au/report/wovg-information-security-management-framework (en anglais)

Organismes audités

- Ministère du Premier ministre et du Cabinet (Department of the Premier and Cabinet)
- Ministère du Développement de l'État, des Entreprises et de l'Innovation (Department of State Development, Business and Innovation (DSDBI))
- Ministère du Trésor et des Finances (Department of Treasury and Finance)
- Ministère des Services à la personne (Department of Human Services)
- Ministère de la Justice (Department of Justice)
- CenITex
- Agence du revenu de l'État (State Revenue Agency)
- Société du trésor [de l'État] de Victoria (Treasury Corporation of Victoria)
- Société de gestion des fonds [de l'État] de Victoria (Victorian Funds Management Corporation)
- Solutions de TI partagés (IT Shared Solutions)

Objectif de l'audit

- Évaluer l'efficacité de la politique de sécurité des technologies de l'information et des communications (TIC), des normes et des mécanismes de protection en la matière, en ce qui a trait aux systèmes de TIC et aux données de l'État de Victoria.

Critères d'audit

- Des orientations de politique et des lignes directrices adéquates sont en place pour assurer une protection continue des systèmes de TIC et des données de l'État.
- Les organismes centraux de l'État surveillent les menaces auxquelles l'information et les systèmes sont exposés à l'échelle de l'ensemble du gouvernement de Victoria, et coordonnent les interventions pour contrer ces menaces.

- Les organismes sélectionnés ont établi une politique, des normes et des processus en matière de sécurité de l'information, et s'y conforment.

Principales constatations de l'audit

- Une politique et un cadre adéquats en matière de sécurité de l'information sont en place, mais ils sont applicables à seulement 20 organismes au sein du gouvernement proprement dit. D'autres entités publiques, dont les organismes externes du gouvernement visés par le présent audit, n'étaient pas tenus de respecter une politique ou des normes en particulier.
- À l'exception de certaines exigences en matière de rapports visant les organismes au sein du gouvernement proprement dit, et sauf un programme de formation et de séances d'information, aucun élément probant n'indiquait que les organismes centraux avaient entrepris la moindre initiative pour aider les organismes mentionnés à mettre en application la politique et le cadre.
- Le ministère du Développement de l'État, des Entreprises et de l'Innovation (DSDBI) n'assurait aucune coordination et ne transmettait aucune communication à l'égard des questions liées à la sécurité de l'information à l'intention des organismes publics externes du gouvernement. Les organismes en question ne reçoivaient pas de soutien de la part des organismes centraux à propos des questions liées à la sécurité de l'information. Aucune attente n'était formulée pour indiquer aux organismes qu'ils devraient élaborer une politique ou des normes internes, et aucune directive ou orientation ne leur était adressée sur la façon de prendre en charge leurs besoins en matière de sécurité de l'information.
- Le point de vue du gouvernement et des organismes centraux était exprimé de la façon suivante :
    - un sentiment que les domaines dans lesquels une aide pourrait être apportée en vue de réduire les risques de cyberattaques n'étaient pas manifestes ou apparents;
    - un sentiment d'inaptitude à évaluer les risques auxquels les systèmes de TIC des organismes externes du gouvernement étaient exposés dans un environnement hostile, de menace de cyberattaques;
    - l'absence de moyens pour réaliser facilement une évaluation fiable de la menace et du profil de risque actuels à l'échelle de l'ensemble du gouvernement;
    - le manque d'assurance que les organismes publics externes du gouvernement prenaient en charge les questions liées à la sécurité de l'information.
- Les politiques de sécurité de l'information des organismes au sein du gouvernement proprement dit avait fait l'objet d'un examen en 2010, mais peu d'indications laissaient penser qu'une surveillance avait été exercée depuis ce temps, quant aux normes, aux contrôles et à la conformité des organismes.
- Comme les rapports des organismes pour signaler les cyberattaques dont ils avaient été victimes n'étaient pas consolidés, il n'existait pas de service central d'archivages ou un référentiel de données qui permettait au gouvernement d'analyser le type ou la fréquence des cybermenaces ou encore d'évaluer l'aptitude des systèmes à résister aux cyberattaques.

- Il n'existait pas non plus de mécanismes d'observation centrale et consolidée des cybermenaces, ni de dispositif qui permettait de renseigner le gouvernement en cas d'une attaque visant plusieurs organismes ou en cas d'une attaque soutenue.
- Le ministère du Développement de l'État, des Entreprises et de l'Innovation (DSDBI) et les organismes pris séparément ne gèraient pas les données IP pour en assurer l'exactitude et veiller à ce qu'elles soient à jour. Cette démarche est essentielle pour permettre de réagir efficacement aux cybermenaces qui sont détectées.
- Aucun des organismes visés par le présent audit ne s'était conformé intégralement à la politique et aux normes du gouvernement en matière de sécurité de l'information. Chacun des organismes s'étaient toutefois doté d'éléments de politique sur la sécurité de l'information.
- La sensibilisation générale à la façon dont les systèmes de TIC du secteur public se comporteraient en cas d'une cyberattaque était insatisfaisante. Un engagement plus sérieux et concret de la part des organismes centraux était nécessaire jusqu'à ce qu'un niveau acceptable de maturité à l'égard de la sécurité de l'information soit atteint dans l'ensemble des organismes du secteur public.

Recommandations de l'audit

- Le ministère du Développement de l'État, des Entreprises et de l'Innovation (DSDBI) devrait :
    - soumettre au gouvernement la politique de gestion de la sécurité de l'information pour examen officiel;
    - modifier la politique et les normes sur la sécurité de l'information pour y intégrer et assujettir les organismes publics externes du gouvernement qui exploitent des systèmes de technologies de l'information et de communications qui gèrent des opérations financières de très haute valeur et sont donc essentiels à l'égard des recettes de l'État, des systèmes essentiels à l'égard de la sécurité publique, ou des systèmes qui détiennent des données personnelles sensibles pouvant présenter une valeur pour des tierces parties;
    - obliger les organismes publics à l'échelle de l'ensemble du gouvernement de Victoria à signaler toute variation entre les normes en matière de sécurité de l'information et le cadre de gestion de la sécurité de l'information appliqué par l'organisme en question, et qui a reçu l'approbation du chef de cet organisme, dans le cadre du processus annuel de reddition de comptes sur l'autoévaluation du cadre de gestion de la sécurité de l'information;
    - élaborer à l'intention des organismes externes du gouvernement, des processus qu'il faudrait intégrer aux séances d'information et aux forums sur la sécurité de l'information.
- Le ministère du Premier ministre et du Cabinet (Department of the Premier and Cabinet) et le ministère du Développement de l'État, des Entreprises et de l'Innovation (DSDBI) devraient :
    - une fois que le Emergency Management Bill 2013 [projet de loi 2013 sur la gestion des urgences] aura été adopté, confirmer leurs rôles et responsabilités respectifs à l'égard de la sécurité de l'information;
    - confirmer que, à titre d'organisme principalement responsable des technologies de l'information et des communications de l'ensemble du gouvernement de Victoria, le ministère du Développement de l'État, des Entreprises et de l'Innovation (DSDBI) présentera

des séances d'information sur les cyberattaques au State Crisis and Resilience Council, et que, à son tour, le State Crisis and Resilience Council recommandera au besoin des séances d'information à l'intention des ministres.

- Le ministère du Développement de l'État, des Entreprises et de l'Innovation (DSDBI) devrait :
  - prendre les dispositions nécessaires pour qu'un service d'alerte de cyberattaques offert par un fournisseur approprié soit accessible et que chaque organisme du gouvernement puisse s'y abonner;
  - élaborer et mettre en œuvre un processus pour maintenir un registre de toutes les adresses IP utilisées par les ministères et les organismes du secteur public.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Les pratiques de gestion de la sécurité des technologies de l'information

Date de publication : 2013

Bureau d'audit : Bureau du vérificateur général du Manitoba

Hyperlien pour accéder au rapport integral :

http://www.oag.mb.ca/wp-content/uploads/2013/01/WEB-Chapter-3-IT-Security-Mgmt-Practices.pdf (en anglais)

Organisme audité

- Technologie et transformation opérationnelle (Business Transformation and Technology (BTT) [une direction générale du ministère des Finances du Manitoba]

Objectif de l'audit

- Déterminer si Technologie et transformation opérationnelle (BTT) a conçu et mis en œuvre des pratiques et contrôles adéquats en matière de gestion de la sécurité des technologies de l'information (TI).

Critères d'audit

- Technologie et transformation opérationnelle (BTT) :
  - a établi des processus pour déterminer, évaluer, atténuer et accepter les risques liés à la sécurité des TI;
  - a établi des stratégies sur la sécurité de l'information qui soutiennent les objectifs organisationnels et les objectifs liés aux TI;
  - a établi des politiques pour gérer les risques importants liés à la sécurité des TI;
  - met à jour et communique les politiques ayant trait à la sécurité des TI;
  - classifie et sauvegarde les actifs informationnels;
  - veille à ce des contrôles de sécurité adéquats soient en application pour les services externalisés;
  - assure la sécurité des opérations des systèmes et des réseaux pour les protéger contre les menaces et les vulnérabilités.

Principales constatations de l'audit

- BTT ne connaissait pas tous les risques importants liés à la sécurité des TI; l'organisme n'avait commencé que tout récemment à évaluer certains risques courants liés à la sécurité des TI. Il restait

beaucoup à faire pour déterminer et évaluer les risques, décider de la façon de les atténuer, désigner les intervenants responsables, et mobiliser les ressources. L'équipe d'audit était particulièrement préoccupée par le fait que des évaluations du risque n'avaient pas été menées et qu'aucun évaluation de cette nature n'était prévue en ce qui avait trait aux opérations du groupe chargé des systèmes d'information de l'édifice de l'assemblée législative. Les pratiques de BTT en matière de gestion des risques liées à la sécurité des TI ne s'étaient pas améliorées de manière sensible malgré les commentaires et recommandations formulés antérieurement.

- BTT n'avait toujours pas élaboré de plan stratégique ayant trait aux TI, lequel devrait comprendre un plan stratégique en matière de sécurité des TI, malgré les commentaires et recommandations formulés antérieurement.
- BTT n'avait pas mis en œuvre une politique sur la sécurité des TI, malgré les commentaires et recommandations formulés antérieurement. Des instruments de politique n'avaient pas été mis en place pour les activités suivantes auxquelles étaient associés certains risques liés à la sécurité des TI : la virtualisation, les appareils mobiles, les réseaux sans fil, et la sécurité physique.
- Plusieurs années s'étaient écoulées depuis que BTT avait fait appel aux services d'une tierce partie indépendante pour auditer ses pratiques de gestion de la sécurité des TI. L'examen le plus récent remontait à l'exercice 2005-2006. Le rapport de cet examen avait été remis en mars 2006. De nombreuses failles et recommandations y avaient été présentées. BTT n'avait pas examiné les recommandations pour en déterminer la pertinence, et n'avait pas non plus élaboré de plan d'action ni effectué de suivi à l'égard de la mise en œuvre des recommandations.
- L'équipe d'audit était préoccupée par le fait que la politique sur les vérifications de sécurité ne prévoyait pas de vérifications de sécurité périodiques pour les employés déjà en poste. Comme il était mentionné plus haut, pour certains postes, les vérifications de sécurité étaient obligatoires uniquement au moment de l'embauche. Aucune exigence n'était formulée pour mener des vérifications de sécurité périodiques visant des employés déjà en poste. Cet aspect est important en particulier pour les postes qui donnent accès à des ressources d'information sensible.
- BTT n'avait pas défini d'exigences minimales relatives aux mots de passe.
- BTT n'avait pas défini d'exigences minimales pour créer, maintenir et désactiver l'accès.
- BTT n'avait pas non plus établi d'exigences pour surveiller les activités des utilisateurs.
- BTT avait externalisé la gestion de ses cinq principaux centres de données mais n'en avait pas défini les exigences de sécurité physique. Par conséquent, il y avait des différences marquées quant aux contrôles mis en application d'un centre de données externalisé à un autre. La justification sur laquelle s'appuyaient les contrôles relatifs à la sécurité physique à chacune des centres de données, y compris les évaluations des risques connexes, n'était pas consignée en dossier.
- L'équipe d'audit avait examiné les correctifs de sécurité installés dans le cas d'un des fournisseurs, et avait constaté un retard important dans l'installation des correctifs informatiques pour parer aux vulnérabilités qui présentaient un risque élevé quant à la sécurité, exposant ainsi pendant une période prolongée les systèmes et les données, sans raison valable.

- Les courriels n'étaient pas cryptés, ce qui augmentait le risque que les données sensibles soient accessibles à des personnes non autorisées. Il s'agissait là d'une préoccupation particulière compte tenu du fait aussi que le réseau n'était pas non plus crypté.
- Pour protéger l'information stockée sur le disque dur des ordinateurs portatifs, BTT employait un mode de cryptage qui, selon le fournisseur du produit, convenait raisonnablement bien à des données de risque faible, mais non à des données hautement sensibles. Le Centre de protection de l'information (Information Protection Centre) avait signalé que 14 ordinateurs portatifs avaient été perdus ou volés au cours de l'année civile 2011, mais le Centre n'avait toutefois pas déterminé la sensibilité des données stockées dans ces ordinateurs.

Sélection de recommandations de l'audit

- BTT devrait, à titre prioritaire, réaliser une évaluation complète des risques liés aux TI, ce qui devrait comporter une évaluation des risques liés à la sécurité des TI.
- BTT devrait réaliser une évaluation complète des risques liés aux opérations du groupe chargé des systèmes d'information de l'édifice de l'assemblée législative.
- BTT devrait élaborer un plan stratégique ayant trait aux TI ainsi qu'un plan adéquatement harmonisé en matière de sécurité des TI.
- BTT et le Centre de protection de l'information (Information Protection Centre) devraient établir des indicateurs de rendement pour la gestion des opérations liées à la sécurité des TI et fixer des cibles précises correspondant à chacun des indicateurs. Une fois que le plan en matière de sécurité des TI sera établi, les indicateurs de rendement et les cibles connexes devraient s'aligner sur les buts et objectifs formulés à l'égard de la sécurité.
- BTT et le Centre de protection de l'information (Information Protection Centre) devraient présenter à la haute direction des rapports trimestriels centrés particulièrement sur :
    - les principaux indicateurs de rendement (convenus avec la haute direction);
    - le rendement par rapport aux cibles fixées;
    - les mesures à prendre pour corriger les écarts de rendement par rapport aux objectifs visés.
- BTT devrait, à intervalles réguliers, faire effectuer par une tierce partie indépendante des audits sur ses pratiques en matière de sécurité des TI, et obtenir des rapports périodiques sur la mise en œuvre des recommandations.
- BTT devrait renforcer son cadre de gestion des politiques (Policy Management Framework) en exigeant que les évaluations des risques liés aux TI et les objectifs stratégiques servent d'assises pour établir le besoin de nouveaux instruments de politique ou de mises à jour en la matière.
- BTT devrait mettre en œuvre une politique de portée générale en matière de sécurité des TI.
- Après avoir réalisé des évaluations des risques liés à la sécurité des TI, BTT devrait mettre en œuvre des instruments de politique supplémentaires ayant trait aux TI en vue d'atténuer les risques liés à la sécurité des TI.
- BTT devrait renforcer son cadre de gestion des politiques en déterminant la fréquence des examens portant sur les instruments de politique en matière de TI.

- BTT devrait élaborer un calendrier ou un plan comportant un ordre de priorité pour l'examen et la mise à jour de tous les instruments de politique en vigueur en matière de TI et devrait surveiller activement les progrès réalisés par rapport à ce qui est énoncé dans le plan.
- Le Centre de protection de l'information (Information Protection Centre) devrait améliorer le programme de sensibilisation à la sécurité des façons suivantes :
    - en intégrant de l'information à propos des tendances concernant les incidents relatifs à la sécurité des TI et à propos des risques répertoriés et attestés;
    - en élaborant des activités de formation et de sensibilisation supplémentaires concernant la sécurité, expressément à l'intention des utilisateurs occupant des postes à risque élevé;
    - en faisant appel à des techniques de sensibilisation supplémentaires.
- BTT devrait obtenir périodiquement l'assurance que les employés des fournisseurs de services ayant un accès aux ressources informationnelles du gouvernement font l'objet de vérifications de sécurité.
- BTT devrait établir des exigences de contrôle d'accès logique.
- BTT devrait établir et mettre en œuvre des exigences minimales de sécurité physique pour les centres de données.
- Le Centre de protection de l'information devrait établir des exigences normalisées en matière de sécurité des TI. Une fois que ces exigences seront en vigueur, le Centre devrait évaluer si les pratiques de sécurité des fournisseurs de services sont conformes à ces exigences, et dans les cas d'écarts en la matière, il devrait veiller à ce que leurs pratiques soient renforcées.
- Le Centre de protection de l'information devrait élaborer et mettre en œuvre une méthode d'évaluation de la vulnérabilité.
- Après avoir réalisé une évaluation des risques liés à la sécurité des TI et après avoir mis en œuvre des normes de classification des données, BTT devrait mettre en œuvre une stratégie de prévention de la perte de données.
- Le Centre de protection de l'information devrait mettre en œuvre des modes de cryptage des courriels et des disques durs des ordinateurs portatifs qui protègent adéquatement les données, quel que soit leur niveau de sensibilité.
- Le Centre de protection de l'information devrait consigner en dossier, surveiller et analyser tous les événements et incidents ayant trait à la sécurité de l'information.
- Le Centre de protection de l'information devrait tester régulièrement les processus de gestion des incidents ayant trait à la sécurité de l'information et apporter des améliorations au besoin.

Retour à la table des matières

Série *Pleins feux* – La sécurité des technologies de l'information

Résumé de l'audit

Titre de l'audit

Assurer la sécurité du système JUSTIN : Audit sur l'accès et la sécurité au ministère de la Justice

Date de publication : 2013

Bureau d'audit : Bureau du vérificateur général de la Colombie-Britannique

Hyperlien pour accéder au rapport integral :

http://www.bcauditor.com/pubs/2013/report9/securing-justin-system-access-and-security-audit-ministry (en anglais)

Organisme audité

- Ministère de la Justice de la Colombie-Britannique (Ministry of Justice)

Objectif de l'audit

- Évaluer si le système JUSTIN est géré de manière à assurer une protection adéquate contre l'accès non autorisé à l'information stockée dans le système.

Critères d'audit

- La sécurité du système est protégée de manière adéquate contre les menaces internes et externes.
- Les atteintes à la sécurité de l'information du système JUSTIN seront très probablement détectées.

Principales constatations de l'audit

- Les pirates informatiques pouvaient accéder aux systèmes du ministère de la Justice, exposant ainsi l'information critique du système JUSTIN. Le ministère de la Justice n'avait pas mis en place des contrôles adéquats pour protéger ses infrastructures et empêcher les cyberpirates d'accéder à des informations sensibles du système JUSTIN et de s'en saisir.
- L'accès aux systèmes était excessif, posant un risque accru de divulgation inappropriée d'information, et représentait ainsi une menace à la confidentialité des renseignements et à la sécurité des personnes. Le Ministère avait accordé à des milliers d'utilisateurs un niveau d'accès au système JUSTIN qui s'étendait bien au-delà du critère défini comme étant le « besoin de savoir » [« need to know »]. Au moment de l'audit, 3 300 utilisateurs du système JUSTIN avaient accès à l'intégralité des rapports au procureur de la Couronne, y compris les détails des enquêtes policières, les sommaires de dépositions des témoins, et les coordonnées de victimes et de témoins.
- Des renseignements de nature très sensible n'étaient pas « verrouillés », de sorte que leur sécurité et confidentialité s'en trouvaient compromises. Certains contrôles avaient été intégrés au

système JUSTIN pour protéger certains renseignements; cependant, ces contrôles n'étaient pas utilisés correctement ou il était possible de les contourner, permettant ainsi d'accéder ouvertement à des renseignements de nature sensible.

- Il y avait un manque de visibilité et des contrôles inefficaces concernant la copie d'information tirée du système JUSTIN et sa diffusion à l'extérieur du Ministère. Les contrôles étaient inadéquats et ne permettaient pas de détecter les utilisateurs qui copiaient de manière non autorisée des renseignements tirés du système JUSTIN ou de les empêcher de le faire; il était donc impossible de déterminer quelle information était mise en circulation à l'extérieur du Ministère et à quel endroit cette information était acheminée.
- L'incapacité de détecter les divulgations non autorisées de renseignements tirés du système JUSTIN empêchait de prendre des mesures proactives pour contrer les atteintes à la sécurité de l'information. Les contrôles du Ministère étaient inadéquats et ne permettaient pas de détecter l'accès non autorisé de la part de sources tant internes qu'externes. L'absence d'une sensibilisation adéquate rendait impossible la prise de mesures visant à atténuer les dommages attribuables à la communication illicite de renseignements.
- Certains utilisateurs du système JUSTIN n'avaient pas fait l'objet d'une vérification du casier judiciaire. En vertu des exigences de la politique, seuls les nouveaux employés devaient faire l'objet d'une telle vérification. Certains employés de soutien technique des TI au sein d'organismes chargés du soutien du système JUSTIN n'avaient pas fait l'objet d'une vérification du casier judiciaire.

Recommandations de l'audit

- Les contrôles intégrés aux composants du système et du réseau associés au système JUSTIN devraient être examinés, reconfigurés, définis dans des documents, et mieux gérés pour faire en sorte que des dispositifs de sécurité multicouches soient en place.
- L'accès des utilisateurs à l'information stockée dans le système JUSTIN devrait être accordé et géré en s'appuyant sur le principe du « besoin de savoir » [« need to know »].
- L'information de nature très sensible stockée dans le système JUSTIN devrait être catégorisée et protégée de manière appropriée et être assujettie à des mécanismes de surveillance exhaustifs.
- Il faudrait mettre en place des pistes d'audit et des outils d'audit plus efficaces pour permettre de détecter les activités suspectes ou non autorisées, et d'enquêter sur celles-ci.
- Il faudrait mettre en place un programme efficace de surveillance pour permettre de détecter de manière proactive l'accès non autorisé à l'information stockée dans le système JUSTIN ainsi que la copie et l'extraction de cette information.

Retour à la table des matières

Annexe 2
Glossaire de certains termes techniques

Retour à la table des matières

Application *[application]*
Programme informatique ou logiciel. Cela comprend les logiciels de traitement de texte, les tableurs (également appelés chiffriers, chiffriers électroniques ou tableurs électroniques), les programmes de bases de données, les logiciels de comptabilité, et autres.

Base de données *[database]*
Collection intégrée de données reliées entre elles et organisée pour offrir un accès pratique par la voie d'un système informatique.

Centre informatique *[data centre]*
Également appelé centre de traitement de l'information, le centre informatique est un lieu central où sont regroupés le matériel informatique et les logiciels d'un réseau informatique, plus particulièrement les dispositifs de stockage de données.

Codage sécurisé *[secure coding]*
Pratique consistant à élaborer des logiciels d'application de manière à réduire le risque de créer accidentellement une vulnérabilité informatique dans le logiciel avant sa distribution générale.

Configuration *[configuration]*
Arrangement et installation du matériel informatique et des logiciels pour créer un système informatique.

Contrôles d'accès des utilisateurs *[user access controls]*
Il s'agit des contrôles en place pour que seules les personnes autorisées puissent utiliser les systèmes informatiques et les données. Cela comprend par exemple les contrôles physiques comme les salles et les cabinets fermés à clé ainsi que les contrôles informatiques comme la nécessité de créer un compte comportant des droits d'accès définis, l'emploi d'un mot de passe et d'autres exigences.

Contrôles d'accès physique *[physical access controls]*
Il s'agit des contrôles en place pour empêcher les personnes non autorisées à accéder physiquement à des ordinateurs ou à l'équipement de réseau informatique. Cela comprend par exemple les salles et les cabinets fermés à clé ainsi que les systèmes de vidéosurveillance.

Correctif ou programme correctif *[patch]*
Également appelé retouche, le correctif ou programme correctif vise à corriger un problème connu ou à éliminer une vulnérabilité connue dans un programme ou système informatique.

Cyberacteur malveillant *[hostile actor]*
Personne ou organisme, y compris un organisme ou une agence d'un État-nation, qui lance des cyberattaques.

Cyberattaque *[cyber attack]*
Acte délibéré, posé par l'intermédiaire d'Internet, en vue de manipuler, de bloquer, d'endommager ou de détruire des ordinateurs ou des réseaux informatiques, ou des données qui y sont stockées ou sauvegardées. Les cyberattaques visent à porter sérieusement atteinte à la sécurité, à la stabilité ou à la prospérité.

Cybermenace *[cyber threat]*
Il s'agit de la menace que présente un accès non autorisé à un dispositif ou à un réseau de contrôle de systèmes. Cet accès peut aussi bien provenir de l'intérieur d'un organisation (par exemple, de la part d'un employé mécontent), que de la part d'un intervenant inconnu dans un lieu éloigné (par exemple un gouvernement hostile, un groupe terroriste ou un intrus malveillant).

Cyberrésilience *[cyber resilience]*
Capacité de continuer d'offrir des services tout en contrant les cyberattaques et en luttant contre celles-ci.

Défense en profondeur *[defence-in-depth]*
Il s'agit de la pratique consistant à employer des mécanismes de sécurité multi-niveaux pour accroître la sécurité d'un système informatique dans son ensemble. Si une cyberattaque entraîne la défaillance d'un mécanisme de sécurité, d'autres mécanismes sont en mesure d'assurer la sécurité nécessaire pour protéger le système.

Environnement d'exploitation standard *[standard operating environment (SOE)]*
Mise en œuvre standard d'un système d'exploitation et des logiciels associés.

Événement de sécurité *[security event]*
Événement à l'occasion duquel un système ou réseau informatique a fait l'objet d'une intrusion ou d'une atteinte à la sécurité, une règle de sécurité a été violée ou un mécanisme de sécurité a été déjoué.

Hameçonnage *[phishing]*
Tentative d'obtenir de l'information sensible, tel que des noms d'usagers, des mots de passe et des numéros de carte de crédits, souvent avec une intention malicieuse, en se faisant passer, dans un message électronique, pour un représentant d'une organisation digne de confiance.

Liste blanche d'applications *[application whitelisting]*
Il s'agit d'un contrôle de sécurité visant à bloquer l'exécution sur un ordinateur de programmes informatiques non autorisés ou malveillants. Fonctionnant à partir d'une liste blanche prédéfinie, ce contrôle fait en sorte que seuls les programmes et logiciels de certaines bibliothèques définies de programmes et de logiciels puissent être exécutés, et que l'exécution de programmes ou de logiciels de toute autre bibliothèque soit bloquée.

Liste de contrôle d'accès *[access control list (ACL)]*
Une liste de contrôle d'accès liée à un système de fichiers informatiques est une liste d'autorisations associées à un objet. La liste de contrôle d'accès définit quels utilisateurs ou quels processus système sont autorisés à accéder à des objets, ainsi que les opérations qui sont autorisées à l'égard d'objets donnés.

Logiciel *[software]*
Ensemble d'instructions lisibles par machine qui permettent à un ordinateur d'effectuer des opérations précises.

Logiciel rançonneur *[ransomware]*
Un type de logiciel malveillant qui menace ses victimes de publier leur données ou d'en bloquer l'accès de manière permanente si une rançon n'est pas payée.

Matériel informatique *[hardware]*
Le matériel ou matériel informatique comprend les appareils, les fils et d'autres composantes physiques d'un ordinateur ou d'un autre système électronique.

Médias électroniques *[electronic media]*
Il s'agit de divers types de supports informatiques pour le stockage des données, y compris les lecteurs de disque dur (ou unités de disque dur), les disques compacts, les DVD, les cartes mémoire flash, et les clés USB.

Menace *[threat]*
Tout élément qui peut permettre d'exploiter une vulnérabilité informatique, de façon intentionnelle ou accidentelle, et d'obtenir l'accès à un actif ou à un bien, ou de l'endommager ou de le détruire.

Navigateur Web *[web browser]*
Logiciel qui permet à un ordinateur de localiser, d'extraire ou récupérer l'information d'un site Web et de l'afficher (p. ex., Internet Explorer de Microsoft, Mozilla Firefox et Google Chrome).

Pare-feu (ou coupe-feu) *[firewall]*
Logiciel ou matériel informatique destiné à restreindre ou à bloquer l'accès à un réseau informatique ou à un ordinateur. Les paramètres du pare-feu (ou coupe-feu) peuvent être réglés de manière à autoriser seulement le passage de certains types de données.

Plan de continuité des activités *[business continuity plan]*
Également appelé plan de continuité des opérations ou plan de poursuite des activités, le plan de continuité des activités sert à prévoir la poursuite des activités si des conditions physiques adverses se présentent dans un établissement, bureau ou centre informatique, par exemple, en raison d'intempéries, d'un incendie ou d'un acte criminel. Un tel plan comporte habituellement une description des démarches et procédures pour permettre à l'organisation visée de reprendre ou poursuivre ses activités ou de les déplacer dans un autre lieu. Par exemple, si un incendie détruisait ou endommageait un immeuble de bureaux ou un centre informatique, le personnel et les activités de l'organisation seraient déplacés dans un autre lieu où les activités pourraient reprendre ou se poursuivre.

Plan de reprise après catastrophe *[disaster recovery plan]*
Également appelé plan de rétablissement après catastrophe, plan antisinistre ou plan de reprise après sinistre, le plan de reprise après catastrophe comporte l'énoncé d'un processus ou d'une série de procédures en vue de rétablir et de protéger l'infrastructure de technologie de l'information d'une organisation en cas d'urgence ou de catastrophe. Le plan de reprise après catastrophe est une composante du plan de continuité des activités d'une organisation, qui lui, englobe l'ensemble de l'organisation en tant que tel.

Poste de travail ou station de travail *[workstation]*
Ordinateur spécial conçu pour les applications techniques ou scientifiques. Destinés principalement à l'usage d'un utilisateur à la fois, ces appareils sont connectés à un réseau local sur lequel fonctionnent des systèmes d'exploitation à utilisateurs multiples. On emploie aussi librement le terme « poste de travail » pour désigner aussi bien un terminal d'ordinateur central qu'un ordinateur personnel connecté à un réseau.

Réseau de périmètre (ou DMZ) *[perimeter network (or DMZ)]*
Également appelé « zone démilitarisée » ou DMZ d'après l'abréviation anglaise, un réseau de périmètre est un sous-réseau physique ou logique du système informatique d'une organisation dont les services sont exposés à un réseau plus vaste et non fiable, le plus souvent Internet. L'objectif d'un réseau de périmètre est d'ajouter une couche de sécurité supplémentaire pour protéger le réseau local d'une organisation; un cyber-attaquant n'a ainsi accès qu'aux équipements qui se trouvent dans la « zone démilitarisée », c'est-à-dire qu'il n'a accès qu'au réseau de périmètre de l'organisation, plutôt qu'aux autres parties du réseau.

Réseau informatique *[network]*
Groupe d'ordinateurs qui communiquent les uns avec les autres.

Réseau local *[local area network]*
Également appelé réseau local d'entreprise (RLE), le réseau local (RL) est un réseau informatique qui relie entre eux des ordinateurs dans un lieu circonscrit, comme une maison, une école, un laboratoire informatique, un immeuble de bureaux, à l'aide de supports de transmission. L'élément caractéristique d'un RL ou RLE, par rapport à un réseau étendu (RE ou WAN) [également appelé réseau longue distance, réseau longue portée ou réseau général], est le fait que sa portée géographique est plus restreinte et que le réseau ne fait pas appel à des lignes de télécommunications louées.

Réseau privé virtuel (RPV) ou réseau virtuel privé (RVP) *[virtual private network (VPN)]*
Il s'agit de l'élargissement d'un réseau informatique privé par l'intermédiaire d'un réseau public comme Internet. Il permet à un ordinateur de transmettre et de recevoir des données par l'intermédiaire de réseaux communs ou publics comme s'il était connecté directement au réseau privé, y compris quant à l'application des règles liées à la fonctionnalité, à la sécurité et à la gestion du réseau privé.

Risques de cybersécurité *[cyber security risk]*
Il s'agit des risques que représentent les événements adverses qui pourraient avoir une incidence sur les activités ou les ressources d'une organisation en raison d'un accès non autorisé à de l'information, à des technologies de l'information ou à des technologies opérationnelles, ou en raison de l'utilisation, du dévoilement, de la modification ou de la destruction de telles données ou technologies.

Sécurité logicielle *[logical security]*
Également appelée sécurité logique, la sécurité logicielle consiste en des mesures de sécurité visant à protéger les systèmes informatiques d'une organisation. Elle comprend notamment l'emploi d'un identificateur d'utilisateur et de mots de passe d'accès, de procédures d'authentification, ainsi que la définition du droit d'accès et de niveaux d'autorisation. Ces mesures sont destinées à faire en sorte que seuls les utilisateurs

autorisés puissent effectuer certaines opérations ou accéder à l'information stockée dans un réseau informatique ou à un poste de travail. Il s'agit d'un sous-ensemble d'éléments liés à la sécurité informatique.

Serveur *[server]*
Ordinateur qui héberge des systèmes et des données utilisés par d'autres ordinateurs au sein d'un réseau. Les serveurs les plus courants sont les serveurs de bases de données, les serveurs de fichiers, les serveurs de courrier électronique, les serveurs d'impression, les serveurs Web, les serveurs de jeux et les serveurs d'applications.

Système d'exploitation *[operating system]*
Le système d'exploitation d'un ordinateur est le programme informatique qui gère tous les autres programmes et logiciels d'application de l'ordinateur.

Système de détection d'intrusion *[intrusion detection system]*
Dispositif ou logiciel d'application qui assure la surveillance des activités du système ou du réseau en vue de détecter les activités malveillantes et les violations de règles, et qui permet de produire et d'acheminer des rapports à un centre de gestion.

Système de gestion de la sécurité de l'information (SGSI) *[information security management system]*
Il s'agit d'un processus de gestion comportant des politiques en matière de gestion de la sécurité de l'information ou à l'égard des risques liés à la sécurité et à la disponibilité des technologies de l'information. Le principe directeur sous-jacent au SGSI est de faire en sorte que l'organisation élabore, mette en œuvre et maintienne un ensemble cohérent de politiques, de procédures et de systèmes destinés à permettre la gestion des risques de sécurité auxquels les données ou renseignements détenus par l'organisation sont exposés, pour que ces risques soient maintenus à des niveaux acceptables.

Test d'intrusion *[penetration test]*
Un test d'intrusion sert à évaluer la sécurité d'un système ou d'un réseau informatique en simulant une cyberattaque. Le test d'intrusion vise à déterminer concrètement la réalisabilité d'une cyberattaque et les répercussions éventuelles d'une telle attaque sur les activités d'une organisation.

Vulnérabilité en matière de sécurité *[security vulnerability]*
Une faille, un bogue ou une mauvaise configuration qui pourrait être exploité et permettre un accès non autorisé à un réseau ou à une information.

Zone de sécurité *[security zone]*
Il s'agit d'une zone au sein d'un réseau où sont regroupés des systèmes et composantes qui comportent des exigences communes en matière de protection de l'information, et certaines caractéristiques associées à ces exigences. Ces exigences et caractéristiques communes comprennent un système commun de classification des données, y compris les éléments communs suivants :

- les exigences à l'égard de la confidentialité et de l'intégrité des données;
- les contrôles d'accès;
- les exigences à l'égard de l'audit, de la procédure de connexion et de la surveillance.