Tendances technologiques

Prévention des fuites de données

Architecture d'entreprise, Direction générale du dirigeant principal de la technologie

Version 0.1
Date : 2019-07-31

Services partagés Canada
Shared Services Canada

Canada

Table des matières

Sommaire opérationnel

La prévention des fuites de données, également connue sous le nom de « prévention de la perte de données », est une solution de cybersécurité qui comprend une variété de stratégies, de processus et d'outils dont le but est d'empêcher que des utilisateurs non autorisés accèdent aux données précieuses d'une organisation et que ces données soient diffusées dans un environnement non fiable ou qu'elles soient détruites.

Le terme « fuite de données » ou « atteinte à la protection des données » s'entend de la divulgation de renseignements confidentiels par une personne interne ou une menace externe à des fins malveillantes. Parmi les exemples de renseignements précieux d'une organisation, citons notamment les données financières, comme les numéros de carte de crédit, les renseignements personnels identifiables, tels que l'identité d'un utilisateur, son nom d'utilisateur, son mot de passe et ses activités, la propriété intellectuelle, comme les brevets, les secrets commerciaux ou le code source, ou les documents classés.

Si elle ne met pas en œuvre des mesures de prévention, une organisation met en péril la *confidentialité, l'intégrité et la disponibilité* de ses données, ce que l'on appelle la triade CID ou la triade DIC, en s'exposant aux cyberattaques. Par le passé, des exemples de tels incidents ont coûté des millions de dollars à des organisations en dommages-intérêts et ont porté atteinte à leur réputation.

La prévention des fuites de données fournit des outils permettant d'atténuer les risques de fuite de données au sein d'une organisation. Un logiciel de prévention des fuites de données comprend généralement les fonctionnalités suivantes :

- **Protection :** Les outils de prévention des fuites de données mettent en œuvre des mesures de protection, comme des chiffrements, des contrôles d'accès et des restrictions, afin d'atténuer les vulnérabilités possibles. Une organisation peut réglementer l'accès aux fichiers en classant les données en fonction de leur niveau de sécurité et en définissant un ensemble de règles auxquelles chaque utilisateur doit se conformer.

- **Détection :** Le logiciel de prévention des fuites de données peut alerter les administrateurs en générant un rapport détaillé en temps réel sur les violations des politiques, par exemple lorsqu'un attaquant tente d'accéder à des données sensibles. En créant un profil comportemental de base des habitudes courantes, le logiciel peut détecter les activités anormales ou suspectes des utilisateurs. Pour ce faire, certaines solutions utilisent l'apprentissage machine.

- **Surveillance :** Le logiciel de prévention des fuites de données surveille le comportement des utilisateurs en ce qui concerne la façon dont les données sont consultées, utilisées et transférées au sein de l'infrastructure de technologie de l'information (TI) afin de détecter les activités irrégulières ou dangereuses des utilisateurs. Si un événement est déclenché par une violation des règles, le système

en informera le personnel de sécurité. Le système augmente la visibilité afin de s'assurer de manière proactive que les données ne quittent pas l'organisation en cas de violation des politiques.

Sommaire technique

La prévention des fuites de données est la pratique qui consiste à détecter et à protéger les renseignements confidentiels contre la perte de données, les fuites de données et les atteintes à la protection des données. Les cyberattaques sont causées par des pirates, des espions ou même des personnes internes dont l'objectif consiste, entre autres, à endommager l'infrastructure de TI dans le but d'obtenir un gain financier ou politique, d'atteindre un statut ou de se venger.

Dans ce contexte en constante évolution, plusieurs facteurs contribuent à l'augmentation des menaces :

- **Valeur des données :** La monétisation des données a créé un environnement qui encourage la persistance de la cybercriminalité.
- **Nombreux points d'accès :** Plusieurs entreprises adoptent les nouvelles technologies, comme les médias sociaux et les appareils mobiles, mais elles augmentent ainsi leur exposition aux menaces internes en offrant des voies de sortie aux données.
- **Unités de stockage de TI bon marché :** Les unités de stockage modernes sont légères et moins coûteuses, ce qui permet à un employé de sortir facilement avec des gigaoctets de données.
- **Systèmes de TI décentralisés :** Ce type d'architecture offre de nombreux avantages, comme l'ouverture et l'échange de renseignements, mais fait qu'il est difficile pour les organisations d'effectuer le suivi et le contrôle de leurs renseignements en raison d'un manque de gouvernance.

La technologie de prévention des fuites de données est généralement divisée en trois composantes différentes liées à chaque état du cycle de vie des données : les données au repos, les données en mouvement et les données utilisées. La plupart des produits de prévention des fuites de données comportent également un serveur central de gestion qui sert de centre de contrôle pour le déploiement de la prévention des fuites de données. C'est généralement à cet endroit que les politiques de prévention des fuites de données sont gérées, que les données sont recueillies à partir des capteurs et des agents de points de terminaison, et que la sauvegarde et la restauration sont gérées. Les composantes d'un outil de prévention des fuites de données sont, en général, les suivantes :

Prévention des fuites de données concernant le stockage : Les « données au repos » désignent les données stockées sur un « dispositif », par exemple sur un serveur, une base de données, des postes de travail, des ordinateurs portables, des appareils mobiles, un support de stockage portable ou un support amovible. Le terme désigne les données inactives qui ne sont pas actuellement transmises sur un réseau ou qui ne sont pas traitées activement. La prévention des fuites de données concernant le stockage protège ce type de données à l'aide de plusieurs outils de sécurité :

- Le masquage de données cache les renseignements de nature délicate comme les données personnelles identifiables.

- Les contrôles d'accès empêchent tout accès non autorisé.

- Le chiffrement des fichiers constitue une mesure de protection supplémentaire.

- La classification des données utilise un agent de prévention des fuites de données pour étiqueter les données en fonction de leur niveau de sécurité. En adoptant également un ensemble de règles, une organisation peut réglementer l'accès des utilisateurs à l'utilisation, à la modification et à la suppression des renseignements.

- Un outil de surveillance de l'activité des bases de données inspecte les bases de données, les entrepôts de données ainsi que les ordinateurs centraux et envoie des alertes sur les violations des politiques. Pour classer les données, certains mécanismes utilisent des définitions conceptuelles, des mots-clés ou la correspondance d'expressions régulières.

Prévention des fuites de données concernant le réseau : Les « données en mouvement » sont les données qui circulent activement sur un réseau, comme les courriels ou les fichiers transférés au moyen du protocole de transfert de fichier ou du protocole SSH. La prévention des fuites de données concernant le réseau se concentre sur l'analyse du trafic réseau pour détecter les transferts de données sensibles qui enfreignent les politiques de sécurité et fournir des outils pour assurer la sécurité du transfert des données. En voici des exemples :

- Un outil de surveillance des courriels peut déterminer si un courriel contient des renseignements sensibles et bloquer l'action ou chiffrer le contenu.

- Le système de détection d'intrusion surveille toute activité malveillante se produisant sur le réseau et fait généralement rapport à un administrateur ou au serveur central de gestion au moyen d'un système de gestion des événements et des informations de sécurité.

- Les pare-feu et les logiciels antivirus sont des produits couramment disponibles qui font partie d'une stratégie de prévention des fuites de données.

Prévention des fuites de données concernant les points de terminaison : Les « données utilisées » désignent les données qui sont actuellement traitées par une application. Les données de cette nature sont en train d'être générées, mises à jour, consultées ou effacées sur un appareil local. La protection de ce type de données est une tâche difficile en raison du grand nombre de systèmes et de dispositifs, mais elle s'effectue généralement au moyen d'un agent de prévention des fuites de données concernant les points de terminaison qui est installé sur l'appareil local. Voici certaines caractéristiques :

- L'outil fournit une authentification forte des utilisateurs, une gestion de l'identité et des autorisations de profil pour sécuriser un système.

- Il peut surveiller et signaler les activités non autorisées que les utilisateurs peuvent effectuer intentionnellement ou non, comme l'impression et la télécopie, le copier/coller et la capture d'écran.

- Certains agents de prévention des fuites de données peuvent offrir le contrôle des applications afin de déterminer les applications qui peuvent accéder aux données protégées.

- Il existe des solutions avancées qui utilisent l'apprentissage machine et des algorithmes de raisonnement temporel pour détecter les comportements anormaux sur un appareil local.

Utilisation par l'industrie

La mise en œuvre de mesures de prévention contre les atteintes à la protection des données et les fuites de données constitue une préoccupation majeure pour l'industrie. Au fil des ans, un large éventail d'entreprises très en vue ont été victimes de tels incidents. La plus importante brèche de sécurité de tous les temps s'est produite à Yahoo lors d'une série de brèches en 2013 et 2014, ce qui a entraîné le piratage des trois milliards de comptes utilisateurs et la fuite de renseignements personnels. La société n'a divulgué ces événements pour la première fois qu'en 2016. À l'époque, la société était en voie d'être vendue à Verizon, mais ces événements avaient réduit le prix de vente de 350 millions de dollars. De plus, elle a fait l'objet de 43 recours collectifs en conséquence.

En raison du risque constant de brèches possibles, comme dans l'exemple ci-dessus, la technologie de prévention de la perte de données est largement adoptée au sein de l'industrie technologique pour protéger les données. Lorsqu'il s'agit de solutions d'entreprise, Gartner indique quatre principaux fournisseurs de logiciels de prévention des fuites de données : Digital Guardian, Forcepoint, McAfee et Symantec. Le marché entourant la prévention des fuites de données est en croissance : en 2015, sa valeur estimée était d'environ 0,96 million de dollars et devrait atteindre environ 2,64 milliards de dollars d'ici l'année prochaine, à un taux de croissance annuel composé de 22,3 %. Même si les atteintes à la protection des données et les cyberattaques ont toujours été le moteur de la demande, la croissance du stockage infonuagique fera augmenter la demande à l'avenir. De plus, à mesure que l'utilisation des services numériques, des médias sociaux, d'Internet des objets et du commerce électronique prend de l'ampleur, la production de données, même de mégadonnées, augmentera avec elle, de même que les besoins de stockage, que ce soit dans le nuage ou par d'autres moyens. Par conséquent, le désir et les obligations réglementaires de protéger les données, par exemple par la prévention des fuites de données, augmenteront également.

Le marché de la prévention des fuites de données avait auparavant la même approche en ce qui concerne la surveillance et la protection des données d'une organisation, mais les solutions modernes diffèrent considérablement et sont devenues plus personnalisées. L'approche traditionnelle, parfois appelée approche projet ou suite, comporte une passerelle réseau qui agit en tant qu'intermédiaire pour surveiller le trafic. Elle exige que la source, la destination et le type de renseignements sensibles soient connus et bien définis. La nouvelle méthode, parfois appelée visibilité des données ou approche individuelle, utilise un agent installé localement sur chaque système pour surveiller toutes les activités des utilisateurs et du système. Cette approche fonctionne bien si une organisation est encore dans une ère de découverte en ce qui concerne la transmission et l'échange de ses données et que la plupart des utilisateurs des réseaux peuvent avoir accès à des formes de données sensibles. La majorité des

organisations utilisent les deux approches de prévention des fuites de données à divers degrés.

Utilisation par le gouvernement du Canada

Le gouvernement du Canada a la responsabilité de protéger non seulement ses données et ses biens de TI, mais également ceux de ses citoyens, ainsi que les données recueillies à leur sujet. Malgré cela, le gouvernement du Canada lui-même n'est pas à l'abri de fuites de données. Par exemple, l'Agence du revenu du Canada a signalé 3 763 atteintes à la protection des données en 2013, y compris des incidents où les renseignements des contribuables ont été perdus, compromis ou communiqués accidentellement. Afin de prévenir de tels incidents, ainsi que ceux à petite et à grande échelle, divers protocoles de prévention des fuites de données sont en place dans l'ensemble du gouvernement du Canada. Actuellement, les opérations de prévention des fuites de données sont exécutées de façon indépendante dans chaque ministère. Toutefois, cette façon de faire est conforme aux politiques et aux procédures fédérales de soutien, dont certaines s'appliquent également à l'industrie.

Depuis le 1er novembre 2018, les entreprises et les industries privées canadiennes, ainsi que le secteur de la santé, qui sont assujettis à la *Loi sur la protection des renseignements personnels et les documents électroniques*, sont tenus de signaler toute atteinte à la protection des données touchant des renseignements personnels qui pourrait nuire à une personne, de tenir un registre de toutes les atteintes à la protection des données et d'informer les personnes concernées. Le but de cette loi est de s'assurer que les renseignements personnels des citoyens sont protégés par des mesures de protection appropriées, conformément à leur droit d'accès à leurs renseignements personnels. De même, la *Loi sur la protection des renseignements personnels* du gouvernement fédéral stipule la façon dont les ministères du gouvernement du Canada peuvent échanger des renseignements personnels sur des citoyens canadiens et donner accès à ces renseignements, et exige également le signalement des atteintes à la sécurité concernant ces données.

Étant donné que le gouvernement du Canada s'appuie largement sur les TI pour fournir ses services, la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information ainsi que la Norme de sécurité opérationnelle – Programme de planification de la continuité des activités définissent une base de référence des exigences de sécurité que les ministères et les organismes fédéraux doivent respecter pour assurer la sécurité des renseignements sous leur contrôle. Ces mesures de prévention comprennent l'intégration de l'identification et de l'authentification dans tous les réseaux et les systèmes, l'autorisation et le contrôle de l'accès pour restreindre l'accessibilité selon le principe du « besoin de savoir », des protocoles cryptographiques et de chiffrement appropriés ainsi que des méthodes concernant la sécurité des signaux de valeur comme TEMPEST. En cas d'atteinte à la protection des données, la Politique sur la sécurité du gouvernement établit un mécanisme pour coordonner l'intervention et le rétablissement. Étant donné que les atteintes à la protection des données sont principalement causées par des personnes,

le Centre canadien pour la cybersécurité offre des publications à jour dans le cadre d'une campagne de sensibilisation.

La Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada ainsi que le Plan stratégique du gouvernement du Canada pour la gestion de l'information et la technologie de l'information de 2017 à 2021 décrivent une tendance vers une utilisation accrue des services d'informatique en nuage pour le stockage et le traitement des données. L'externalisation vers des nuages privés présente un certain niveau de risque si les fournisseurs ne sont pas vigilants face aux cyberattaques ou s'ils sont eux-mêmes malveillants. Le gouvernement du Canada a élaboré diverses stratégies, lignes directrices et pratiques exemplaires afin d'atténuer les risques liés au nuage et aux fournisseurs de services d'informatique en nuage. Par exemple, l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité décrit des mesures, telles que les assurances indépendantes de tiers, les algorithmes cryptographiques et de chiffrement et les alertes de vulnérabilité, entre autres, dans le cadre de sa tentative pour minimiser les risques et accroître la prévention de la perte de données.

Comme pour d'autres pays, la création d'un gouvernement ouvert, accessible et fondé sur la collaboration est d'une importance primordiale pour le gouvernement du Canada. Tel qu'il est décrit dans le Plan stratégique des opérations numériques, on estime que l'échange des données et des renseignements avec les Canadiens et les entreprises favorisera la croissance de l'économie et permettra une participation plus active à la vie publique. Les portails et les renseignements ouverts peuvent cependant présenter une plus grande possibilité d'atteintes et d'attaques. Par conséquent, la transition vers un gouvernement ouvert doit comprendre des contrôles de prévention des fuites de données. Le fait d'accroître l'ouverture des données et des renseignements comporte des risques inhérents; cela expose les réseaux, les systèmes, les dispositifs et les données, y compris les renseignements personnels, à des atteintes accidentelles ou malveillantes. Par conséquent, il est d'une importance capitale d'avoir des protocoles de sécurité des TI fiables au sein du gouvernement du Canada. Une approche de sécurité à plusieurs niveaux, comme l'utilisation d'un accès sécurisé, de biens protégés et de protocoles sécurisés par défaut, ainsi qu'une surveillance continue sont déjà en vigueur et continueront d'être mises en œuvre au gouvernement du Canada.

Répercussions pour Services partagés Canada (SPC)

Proposition de valeur

La proposition de valeur de la prévention des fuites de données est directement liée au mandat de SPC visant à concevoir et à exploiter une infrastructure de TI sécurisée qui protège les données et les biens technologiques du gouvernement du Canada. La principale valeur opérationnelle de la mise en œuvre d'une stratégie de prévention des fuites de données est la réduction des risques et des répercussions associés aux fuites de données. Ces incidents ont souvent des répercussions sur les aspects suivants d'une organisation :

- **Opérationnel :** Une atteinte à la protection des données entraîne souvent une interruption des services jusqu'à la fin du processus d'enquête. Ce processus peut prendre des semaines ou des mois, ce qui peut coûter des activités ou d'autres ressources à l'organisation entre-temps. La prévention des fuites de données permet de s'assurer que des redondances sont mises en place pour contrer les pertes de données importantes, évitant ainsi des coûts pour les ressources opérationnelles afin de remédier à la perte de données. En 2015, SPC a mis en œuvre la Directive sur l'utilisation de périphériques USB et d'autres dispositifs de stockage externes pour aider à gérer ces types de risques. Tous les biens électroniques de SPC sont dotés d'un outil logiciel de prévention des fuites de données qui surveille l'utilisation de dispositifs non autorisés sur le réseau. Cela empêche la suppression de données du système de SPC ou l'infection du système par des logiciels malveillants, des virus ou d'autres entités malveillantes. Une deuxième phase du programme de prévention des fuites de données de SPC est en cours de planification et permettra de surveiller les données d'entreprise en mouvement et au repos; ce qui se fait toutefois déjà pour les données secrètes.

- **Financier :** Les atteintes à la protection des données entraînent d'importantes pertes financières, notamment des amendes, des honoraires de vérification et des frais juridiques. Le Ponemon Institute a estimé, dans une étude de 2018, que le coût global moyen d'une atteinte à la protection des données s'élève à 3,9 millions de dollars, et à 5 millions de dollars au Canada en particulier. En comparaison, le coût annuel moyen d'une solution de prévention des fuites de données par abonnement est d'environ 175 000 $, selon Forrester.

- **Réputation :** Les pertes de données nuisent à la réputation et à la marque. Souvent, les organisations observent une baisse de leur évaluation, ce qui entraîne la perte potentielle de revenus futurs, de leur avantage concurrentiel et de leurs parts de marché. Par conséquent, la confiance des consommateurs à l'égard de l'organisation diminue également, ce qui peut avoir des répercussions importantes sur les revenus à court et à long terme. Le fait d'avoir une solution de prévention des fuites de données aide à remédier aux inquiétudes de l'utilisateur en matière de sécurité et renforce la confiance des clients.

Défis

L'intégration d'une solution de prévention des fuites de données dans l'infrastructure est une entreprise complexe qui comprend plusieurs composantes, comme un analyseur de bases de données, un système de courriel, un serveur mandataire Web, etc. Pour ajouter à la complexité, les initiatives en matière de sécurité des données et de prévention des fuites de données sont confrontées à plusieurs difficultés en raison du paysage technologique moderne. SPC fait face à plusieurs difficultés et problèmes en ce qui concerne l'intégration d'une solution de prévention des fuites de données :

- **Intégration complexe de la prévention des fuites de données :** En général, l'application des technologies de prévention des fuites de données est complexe, varie en fonction de l'architecture de réseau de l'organisation et nécessite de travailler avec de nombreuses composantes, telles que la sécurité, la réseautique, l'infrastructure, les courriels, le Web, les points de terminaison, le stockage et les bases de données. Le déploiement, la configuration et la gestion de ces systèmes de prévention des fuites de données sont également compliqués. Afin de protéger pleinement une infrastructure de TI, il est important d'adopter une approche globale; cependant, les organisations n'ont souvent pas une stratégie claire à l'égard de la prévention des fuites de données et doivent trouver un équilibre entre les nouvelles méthodes de travail.

- **Sensibilisation et mobilisation des utilisateurs :** Les organisations font face à plusieurs difficultés concernant le contrôle des actions de leurs employés. Il y a souvent un manque de sensibilisation et de responsabilisation des employés à l'égard de leurs actions. Certaines formations et campagnes de sensibilisation ne mettent pas suffisamment l'accent sur la protection des données sensibles et l'utilisation d'outils de sécurité comme le chiffrement des fichiers. De plus, l'impression générale est qu'il n'y a aucun risque à enfreindre les règles.

Les tendances suivantes continueront de poser des difficultés pour les fournisseurs de services de TI en ce qui concerne la protection des données :

- **Consumérisme émergent :** La disponibilité des appareils informatiques et de la connectivité à Internet n'importe où et n'importe quand comporte des avantages. Malheureusement, elle facilite la divulgation de renseignements personnels ou exclusifs en offrant plusieurs points de sortie vers le Web. Les politiques de type « apportez votre équipement personnel de communication » sont vulnérables à la perte de biens matériels, comme les ordinateurs portables, et les utilisateurs finaux peuvent diffuser involontairement des renseignements confidentiels dans les médias sociaux.

- **Continuité des activités et reprise après sinistre :** Le climat technologique oblige les organisations à offrir une disponibilité du système en tout temps. Les pannes qui interrompent la continuité des services de TI peuvent entraîner des pertes financières et de réputation.

- **Persistance de la cybercriminalité :** Comme les données ont une valeur réelle, les cyberattaques sont de plus en plus fréquentes et sophistiquées. Même si la majorité des attaques proviennent de sources externes, l'étude de Verizon estime que 15 % des attaques concernent la perte ou le vol de dispositifs par des personnes internes, le transfert de données vers un support de stockage personnel, etc.

Considérations

Comme pour tout programme ou outil, il est nécessaire d'harmoniser les politiques avec les contrôles. Le gouvernement du Canada a déjà mis en place diverses politiques concernant l'infrastructure de GI-TI, y compris la sécurité de ces ressources et de ces renseignements. Toutefois, si une organisation adopte des politiques qui interdisent ou surveillent certaines activités, mais qu'il n'y a aucun contrôle ou que le contrôle n'est pas encore en place, alors la fuite de données représente toujours un risque important pour l'organisation. Il existe des politiques de sécurité, mais la conformité ministérielle et la mise en œuvre des contrôles demeurent un problème.

Même si des protocoles et des contrôles de prévention des fuites de données ont déjà été mis en œuvre dans une grande partie de l'infrastructure de TI de SPC, des améliorations devraient être envisagées dans certains domaines. En raison des stratégies pangouvernementales axées sur le « gouvernement ouvert » et l'« informatique en nuage », SPC devra composer avec la nécessité croissante d'adapter les outils de prévention des fuites de données à ces plateformes au fur et à mesure de leur évolution et de leur expansion.

Après avoir harmonisé ses contrôles avec les politiques, lesquelles peuvent changer et évoluer au fil du temps et des progrès technologiques, SPC doit se préparer pour que ses contrôles de prévention des fuites de données changent avec elles. Les principaux experts dans le domaine de la prévention des fuites de données définissent celle-ci comme étant un processus dynamique et non un état final. Un solide programme de prévention des fuites de données est une occasion de travailler avec les intervenants et d'établir les attentes selon lesquelles les protocoles devraient changer et être adaptés au fil du temps. La prévention des fuites de données doit également être prise en compte lorsque l'architecture de réseau et les outils changent; SPC doit évaluer comment les vérifications de sécurité sont intégrées dans les nouveaux projets.

De plus, même si SPC jouera un rôle de premier plan dans l'acquisition des outils de prévention des fuites de données pour les ministères et la prestation de ces services, la protection des données exige un effort d'équipe. Une collaboration en matière de suivi, de surveillance et d'octroi de l'accès aux ressources et aux réseaux locaux ou ministériels sera nécessaire. De plus, la participation des intervenants aidera à cibler les vulnérabilités qui pourraient autrement être oubliées. Une mentalité de responsabilité collective constitue une pratique exemplaire pour garantir l'efficacité optimale de la prévention des fuites de données.

Une façon de contribuer à l'adoption de la prévention des fuites de données en tant que processus continu et de créer une culture de responsabilité collective pourrait être pour SPC, de concert avec ses ministères partenaires au sein du gouvernement du Canada, de désigner des « champions de la sécurité ». Le gouvernement du Canada a désigné un champion national, M. David Jean, le champion de la sécurité du gouvernement du Canada, pour faire le lien entre la sécurité ministérielle et les intérêts

de sécurité nationale en ce qui concerne toutes les formes de menaces ou de problèmes de sécurité, et pas seulement celles qui sont liées à la cybersécurité. Cependant, des champions de la cybersécurité pourraient également être désignés à l'échelle locale et faire progresser la prévention des fuites de données « sur le terrain », comme il est proposé dans le document Consultations été-automne 2016 : Plan de transformation de la technologie de l'information – Rapport final *Ce que nous avons entendu*. Ces employés peuvent aider à promouvoir l'importance des protocoles et des comportements de sécurité, et peuvent constituer un élément important du cadre de prévention des fuites de données.

Cependant, les outils et les processus de prévention des fuites de données ne peuvent fonctionner isolément des systèmes et des utilisateurs. Sans une opérationnalisation adéquate, la prévention des fuites de données risque d'offrir un faux sentiment de sécurité et de devenir simplement un générateur de risques. Le Plan ministériel de SPC pour le programme de cybersécurité et de sécurité de la TI indique les cinq risques suivants en matière de cybersécurité, dont la prévention des fuites de données fait partie :

- **Capacité en matière de ressources :** Il se peut que SPC ne dispose pas des ressources financières et humaines adéquates pour améliorer les services et introduire les plus récentes technologies afin de contrer les cybermenaces.
- **Systèmes de TI vieillissants :** L'infrastructure de TI actuelle présente des risques de défaillance, car elle est en fin de vie utile.
- **Cybersécurité et sécurité de la TI :** SPC risque de ne pas être en mesure de réagir efficacement aux menaces à la sécurité de la TI et à la cybersécurité, ce qui pourrait compromettre les renseignements exclusifs et entraver les activités de reprise après sinistre.
- **Gestion et prestation des services :** Il est possible que les outils et les processus d'entreprise de SPC ne soient pas en mesure d'améliorer la prestation des services aux organisations partenaires.
- **Disponibilité et qualité des renseignements :** Le manque de disponibilité et d'intégrité des renseignements nuira à la planification et à la prise de décisions efficaces.

Références

Arellano, N. E. (2014, March 31). *Data breaches in federal departments soar in 10 months*. Retrieved from IT World Canada: https://www.itworldcanada.com/post/revenue-agency-bumps-up-government-data-breach-numbers

Brooks, R. (2018, November 29). *What to Know about a Data Breach: Definition, Types, Risk Factors and Prevention Measures*. Retrieved from Netwrix: https://blog.netwrix.com/2018/11/29/what-to-know-about-a-data-breach-definition-types-risk-factors-and-prevention-measures/

Canadian Centre for Cyber Security. (2019, May 15). *Five practical ways to make yourself cybersafe*. Retrieved from cyber.gc: https://cyber.gc.ca/en/guidance/five-practical-ways-make-yourself-cybersafe

Digital Guardian Guest Contributor. (2018, February 5). *Getting Successful with DLP: Two Approaches for Quick DLP Wins.* Retrieved from Digital Guardian: https://digitalguardian.com/blog/getting-successful-dlp-two-approaches-quick-dlp-wins

DLPexperts. (2019, may 17). *DATA LOSS PREVENTION BUYER'S GUIDE & VENDOR COMPARISON*. Retrieved from DLPexperts: https://dlpexperts.com/data-loss-prevention-buyers-guide-and-vendor-comparison/

Ernst & Young. (2011, October). *Data loss prevention*. Retrieved from EY: https://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf

Governement of Canada. (2004, May 31). *Operational Security Standard: Management of Information Technology Security (MITS)*. Retrieved from Governement of Canada: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328

Government of Canada. (2018, December 13). *The Privacy Act.* Retrieved from Government of Canada: https://laws-lois.justice.gc.ca/eng/acts/P-21/

Hughes, C. (2014, September 3). *The Three States of Digital Data*. Retrieved from ASPG: http://aspg.com/three-states-digital-data/#.XN7E0aBKi71

Imperva. (2019, May 17). *Insider Threats*. Retrieved from Imperva: https://www.imperva.com/learn/application-security/insider-threats/

Imperva. (2019, May 17). *Security information and event management (SIEM)*. Retrieved from Imperva: https://www.imperva.com/learn/application-security/siem/

Imperva. (2019, May 17). *What is a Data Breach | Tips for Data Leak Prevention | Imperva*. Retrieved from impperva: https://www.imperva.com/learn/data-security/data-breach/

Imperva. (2019, May 17). *What is Data Loss Prevention (DLP) | Data Leakage Mitigation | Imperva*. Retrieved from imperva: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/

Janacek, B. (2015, December 1). *Best Practices: Securing Data at Rest, in Use, and in Motion*. Retrieved from DataMotion: https://www.datamotion.com/2015/12/best-practices-securing-data-at-rest-in-use-and-in-motion/

Larson, S. (2017, October 4). *Every Single Yahoo Account was Hacked - 3 billion in all.* Retrieved from CNN Business: https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

Markets and Markets. (2015, September). *Data Loss Prevention Market by Solution Type (Network DLP, Storage DLP, Endpoint DLP), by Deployment Type (On-Premise, Cloud), by Applications, by Service, by Organization Size, by Vertical, and by Regions - Global Forecast to 2020.* Retrieved from Markets and Markets: https://www.marketsandmarkets.com/Market-Reports/data-loss-prevention-advanced-technologies-market-531.html

Meizlik, D. (2008, February 5). *The ROI of Data Loss Prevention*. Retrieved from Websense, Inc. : http://img2.insight.com/graphics/uk/media/pdf/whitepaper_roiofdlp_en.pdf

Office of the Privacy Commissioner of Canada. (2018, January). *PIPEDA in brief*. Retrieved from priv.gc: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Osakwe, M. (2018, July 19). *Data Breaches vs. Data Leaks: What's the Difference?* Retrieved from NextAdvisor: https://www.nextadvisor.com/blog/data-breaches-vs-data-leaks-whats-the-difference/

McCarthy, Niall. (2018, July 13). *The Average Cost of a Data Breach is Highest in the U.S.* Retrieved from Forbes: https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#58c9dcd32f37

Shared Services Canada. (2018, April 24). *2017–18 Cyber and Information Technology Security Branch Business Plan*. Retrieved from Shared Services Canada:

http://myssc-monspc.ssc-spc.gc.ca/en/worktools-processes/integrated-business-planning/CITS

Shared Services Canada. (2018, February 2). *Data Loss Prevention and the Use of Portable Storage Devices.* Retrieved from Shared Service Canada: http://myssc-monspc.ssc-spc.gc.ca/en/employee-centre/security/it-security/data-loss

Shared Services Canada. (2019, April 11). *SSC business planning*. Retrieved from Shared Services Canada: http://myssc-monspc.ssc-spc.gc.ca/en/worktools-processes/integrated-business-planning

Treasury Board of Canada Secretariat. (2018). *Digital Operations Strategic Plan: 2018-2022.* Retrieved from Treasury Board of Canada Secretariat: https://www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html#ToC8

Treasury Board of Canada Secretariat. (2017, November 1). *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)*. Retrieved from Treasury Board of Canada Secretariat: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html

SiteUptime. (2017, June 8). *Data Leakage Vs Data Loss: What's The Difference?* Retrieved from SiteUptime: https://www.siteuptime.com/blog/2017/06/08/data-leakage-vs-data-loss-whats-the-difference/

Verizon Enterprise Solutions. (2019, May 17). *2019 Data Breach Investigations Report*. Retrieved from Verizon Enterprise Solutions: https://enterprise.verizon.com/resources/reports/dbir/

Wikipedia. (2019, May 10). *Data Breach*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Data_breach

Wikipedia. (2019, May 5). *Information Security*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Information_security

Zhang, Ellen. 2019, January 3). *What is Data Loss Prevention (DLP): a Definition of Data Loss Prevention.* Retrieved from Digital Gaurdian: https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention