1re édition
Le 31 octobre 2013

# Pratiques exemplaires de sécurité pour les fournisseurs de services de télécommunications canadiens (FST)

Préparé par le Comité consultatif canadien pour la sécurité des télécommunications (CCCST)

# Table des matières

# 1. Introduction

## 1.1. Aperçu

Les Canadiennes et les Canadiens comptent sur Internet pour trouver de l'information, conclure des affaires et garder le contact. Selon des statistiques publiées par Sécurité publique Canada, des ventes en ligne totalisant plus de 62 milliards de dollars ont été réalisées au Canada en 2007. Par ailleurs, en 2010, plus de 80 % des foyers canadiens disposaient de services Internet, et plus de la moitié de ces foyers effectuaient des achats en ligne[1]. En 2012, 87 % des entreprises canadiennes utilisaient Internet[2]. Les fournisseurs de services de télécommunication canadiens (FST) reconnaissent l'importance de leur rôle afin « d'accroître la sûreté, la sécurité et la résilience du Canada ». Les FST réalisent que les services de communication qu'ils offrent les placent dans une position unique, étant donné que la « capacité de communiquer » est un enjeu majeur pour les autres secteurs essentiels.

La Stratégie nationale sur les infrastructures essentielles énonce que « La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public ». Les FST s'engagent à assurer la sécurité de leur infrastructure, à réduire le risque d'interruptions non prévues et à contribuer à régler des problèmes.

Étant donné que les technologies continuent de se développer et de converger, les dangers liés aux cybermenaces n'ont cessé de croître. Les dommages potentiels se sont aggravés et de plus en plus de systèmes informatiques risquent d'être endommagés. Les logiciels malveillants représentent une économie clandestine de plusieurs milliards de dollars. De nos jours, les programmes malveillants sont indétectables et sont souvent plus complexes que bon nombre de logiciels commerciaux. La plupart du temps, leur but est de s'emparer des renseignements concernant les cartes de crédit, les données de compte, les mots de passe ou les secrets commerciaux.

Le présent document définit les pratiques courantes que les FST devraient adopter pour protéger les infrastructures essentielles et pour garantir la sécurité de leurs réseaux. Par ailleurs, les FST jouent un rôle essentiel pour ce qui est d'assurer la disponibilité de l'infrastructure sous-jacente des communications qui fournit le service aux utilisateurs.

## 1.2. Objectif

Les pratiques exemplaires définies dans le présent document se veulent des pratiques volontaires, élaborées dans le but de conseiller les FST sur la meilleure façon de sécuriser leurs réseaux. Par ailleurs, elles permettent de s'assurer que les FST s'entendent sur la définition d'un service de communication sécurisé, résistant et disponible, et sur leur gestion.

[1] Statistique Canada - http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-fra.htm

[2] Statistique Canada - http://www.statcan.gc.ca/daily-quotidien/130612/dq130612a-fra.pdf

## 1.3. Portée

En tant que produit du Comité consultatif canadien pour la sécurité des télécommunications (CCCST), les pratiques exemplaires s'appliquent aux FST qui assurent et soutiennent l'infrastructure essentielle des télécommunications du Canada. Toutefois, pour satisfaire aux exigences, il n'y a rien dans ces pratiques qui empêchent les autres fournisseurs d'employer les contrôles qui y sont énoncés ou de tirer parti des contrôles mis en place par un fournisseur branché.

Les pratiques exemplaires s'appliqueront aux communications filaires traditionnelles de même qu'aux réseaux sans fil des FST de télécommunications, tels que les accès AMRC et HSPA, ou les réseaux téléphoniques de nouvelle génération. Les pratiques exemplaires ne couvrent pas le Wi-Fi ou d'autres réseaux spéciaux, mais ces derniers pourraient être ajoutés aux prochaines versions du présent document.

Les pratiques exemplaires visent à déterminer les contrôles dont devraient se prévaloir les FST pour détecter les menaces à la cybersécurité et leur permettre de protéger les intérêts de leurs clients et leur propre infrastructure.

La portée du présent document comprend les contrôles de base qui devraient être appliqués pour surveiller la redondance et la disponibilité, ainsi que d'autres sujets, comme la gestion des fournisseurs, dans la mesure où ils ont trait à l'objectif du présent document.

Les éléments suivants sont explicitement hors de la portée du présent document :

- la disponibilité et la redondance visant à offrir une protection contre les pannes d'installation importantes ou les facteurs externes tels que des catastrophes naturelles;
- la sécurité du matériel extérieur et des installations fixes;
- les interventions d'urgence autres que celles se rapportant à la cybersécurité.

Les pratiques exemplaires décrivent en détail les fonctionnalités et les pratiques que les FST doivent adopter pour leurs réseaux. Toutefois, la résilience sur le plan de la sécurité en périphérie des réseaux, variera selon les niveaux de service en sécurité demandés par les clients. Ces pratiques exemplaires ne limitent en rien la capacité d'un fournisseur de services de restreindre les fonctionnalités disponibles à un niveau de service ou d'exiger des frais pour ces fonctionnalités. Bon nombre de fonctionnalités, en lien avec les pratiques exemplaires, exigent un investissement important, en plus d'offrir des niveaux de service fondés sur les besoins des clients.

Dans l'ensemble des pratiques exemplaires, des exigences visent à informer les utilisateurs lorsque leur ordinateur est contaminé par un logiciel malveillant ou lorsqu'ils doivent mettre en place des mesures additionnelles. Bien que ces mesures profitent aux clients, elles visent principalement à protéger l'infrastructure du fournisseur de services. Il n'incombe pas aux FST de décontaminer les ordinateurs infectés de leurs clients.

## 1.4. Comité consultatif canadien pour la sécurité des télécommunications (CCCST)

*La Stratégie nationale sur les infrastructures essentielles, le Plan d'action sur les infrastructures essentielles, ainsi que la Stratégie de cybersécurité du Canada* exigeaient la coopération du gouvernement et de l'industrie dans le but de garantir la sécurité de l'Infrastructure essentielle du

Canada. Le secteur des communications a répondu à cette exigence en créant le Comité consultatif canadien pour la sécurité des télécommunications (CCCST).

Le CCCST est constitué d'un groupe constitué d'intervenants de l'industrie et du gouvernement dont le but est d'améliorer la sécurité générale de l'infrastructure essentielle des télécommunications du Canada.

Le Groupe de travail sur la protection cybernétique des télécommunications canadiennes (GT sur la PCTC) relève du CCCST, et forme un groupe de niveau opérationnel chargé de définir les pratiques exemplaires et de mettre en œuvre les recommandations du CCCST liées à son mandat.

## 2. Lignes directrices

Les pratiques exemplaires tirent profit des travaux réalisés par d'autres organismes de normalisation, notamment :

- L'Organisation internationale de normalisation (ISO) 27001, 27002, 27011, 27032 et 27035
- Les *Lignes directrices sur la chaîne d'approvisionnement des technologies pour l'équipement et les services de télécommunication* du Centre de la sécurité des télécommunications Canada (CSTC)
- Le document australien *Internet Service Providers' Voluntary Code of Practice*;
- Les demandes de commentaires de l'Internet Engineering Task Force au besoin (comme les demandes de commentaires de sécurité, considérations de sécurité, filtrage des entrées pour les réseaux multi-hôtes).

Les réseaux des FST sont occupés par un croisement de trafic en plus du trafic généré à l'interne et le trafic généré à l'externe par les clients. Les cyberattaques ont une incidence sur ces deux types de trafic. Les pratiques exemplaires tiennent compte des différentes préoccupations sur le plan de la confidentialité en lien avec ces réseaux disparates. Les pratiques exemplaires tenteront de faire une distinction entre la surveillance et la résolution de problèmes et chercheront à identifier des moyens pour procéder sans porter atteinte à la vie privée des consommateurs.

Pour les FST, l'un des meilleurs moyens d'accroître la sécurité de leurs clients et la stabilité de leur partie du réseau Internet consiste à partager entre eux les renseignements sur les cyberattaques. Ces renseignements se limiteront aux caractéristiques de la menace et à la nature de l'intervention, et ne porteront aucunement sur les clients individuels. Les mécanismes d'échange de renseignements de cette nature seront définis dans le mandat du CCCST.

## 3. Protection de l'infrastructure essentielle des fournisseurs de services

### 3.1. Architecture et conception du réseau

Sur le plan conceptuel, les réseaux des FST se composent de trois différentes couches - différents types de trafic étant rattachés à chacune d'entre elles. La **couche de gestion** sert aux communications en lien avec l'exploitation et la gestion du trafic sur le réseau. La **couche de commande** sert à l'acheminement et à la signalisation du trafic sur le réseau. La **couche d'utilisateurs** ou **de données** sert au trafic des utilisateurs du réseau (communication de données).

Chacune de ces couches relie divers systèmes ou dispositifs et leur permet de communiquer. Étant donné que les communications de chaque couche sont de nature différente, les communications d'une couche sont séparées de celles des autres couches.

### 3.1.1 Segmentation du réseau

**Objectif :**

Pour garantir le fonctionnement sécuritaire des réseaux et éviter que le trafic d'une couche ait une incidence sur les autres couches, il est important que les FST mettent en place quelques caractéristiques architecturales de base dans leurs réseaux.

Les contrôles ci-dessous ont trait au réseau de base de chaque FST. Ces contrôles n'ont pas été conçus dans le but d'être appliqués à chacune des composantes du réseau. D'autant plus qu'une telle opération serait impossible à réaliser pour tous les types et toutes les architectures de réseau.

**Contrôles :**

Les FST devraient :

1. s'assurer que les couches de gestion, de commande et d'utilisateurs sont, à tout le moins, séparées logiquement et physiquement, dans la mesure du possible;

2. fournir des diagrammes pour illustrer la séparation des couches au sein des infrastructures de leur réseau.

### 3.1.2 Couche de gestion

**Objectif :**

La couche de gestion est formée par l'ensemble des segments du réseau servant à la gestion de celui-ci et des composantes de l'infrastructure connexe. Cet ensemble comprend l'accès à distance aux systèmes ainsi que des fonctions de gestion telles que la sauvegarde, la remise du programme de correction et l'extraction du journal. La couche de gestion est également porteuse du trafic d'approvisionnement et constitue l'interface réseau par l'intermédiaire de laquelle les communications avec des systèmes de facturation et de service à la clientèle secondaire sont transmises.

Si la couche de gestion n'est pas protégée adéquatement, les composantes du réseau sont alors compromises et exposées aux attaques. Il est donc essentiel de protéger les composantes de la couche de gestion.

**Contrôles :**

Les FST devraient :

1. mettre en place des contrôles pour isoler les fonctions de gestion;

2. établir des restrictions d'accès pour autoriser expressément les hôtes et les services connus et approuvés;

3. filtrer l'accès gestion aux dispositifs;

4. utiliser, le plus souvent possible, des protocoles de gestion sécuritaires;

5. tenir des registres concernant les événements de nature délicate pour tous les éléments du réseau;

6. déterminer la source des incidents reliés à des logiciels malveillants.

### 3.1.3 Couche de commande

**Objectif :**

La couche de commande se définit comme étant les réseaux par lesquels s'effectuent l'établissement des communications et la signalisation de gestion. Ces réseaux doivent être protégés si l'on veut garantir le bon fonctionnement du réseau du fournisseur de services.

**Contrôles :**

Les FST devraient :

1. valider tous les partenaires de signalisation;

2. valider toutes les entrées extérieures provenant des partenaires de signalisation;

3. placer/filtrer la signalisation à l'extérieur de contiguïtés définies et autorisées;

4. empêcher l'adressage des points de signalisation à partir du réseau général;

5. maintenir une séparation entre le trafic de la couche de données et celui de la couche de commande;

6. mettre en place des mécanismes pour protéger les canaux de commande sans fil et le trafic de signalisation;

7. utiliser des mécanismes de validation pour leurs terminaux pour empêcher tout terminal non autorisé de se brancher;

8. recourir à des contrôles pour le filtrage de sortie.

### 3.1.4 Couche de données

**Objectif :**

La couche de données est la voie par laquelle les communications du réseau se rendent au client final. Il faut s'assurer que cette voie n'est pas utilisée pour transmettre des données malveillantes à l'utilisateur final ou de voie d'attaque contre l'infrastructure essentielle canadienne.

**Contrôles :**

Les FST devraient :

1. valider l'intégrité du trafic externe qui entre dans leur réseau lorsque cela est possible;

2. empêcher le trafic provenant de sources ou de dispositifs usurpés (faux expéditeur) d'entrer dans leur réseau;

3. empêcher le trafic non valide d'entrer dans leur réseau. Ces mesures comprennent des filtres de protocole, d'adresse ou de volume;

4. éviter que des attaques volumétriques (attaques tentant de dépasser la largeur de bande du réseau ou du dispositif) visent leur infrastructure;

5. veiller à ce que les ressources de gestion et les réseaux de l'infrastructure ne puissent être ciblés par le trafic de la couche de données;

6. appliquer des restrictions liées au trafic – fondées sur une approche de « liste noire » qui autorise tout le trafic par défaut tout en permettant au fournisseur de bloquer (ou d'inscrire sur la liste noire) le trafic malveillant ou inapproprié au besoin;

7. être en mesure de retracer l'origine ou le point d'entrée du trafic malveillant qui pénètre dans leur réseau;

8. être en mesure d'associer le trafic provenant de leur réseau à des abonnés individuels;

9. veiller à l'intégrité du trafic qui quitte leur réseau;

10. mettre en œuvre des mécanismes pour bloquer le trafic non validé;

11. se comporter comme des citoyens responsables et prendre des mesures pour éviter tout préjudice aux autres réseaux;

12. donner suite aux plaintes raisonnables en provenance de l'extérieur de leur réseau concernant des cas d'abus qui n'ont pu être écartés.

## 3.2. Contrôles de sécurité pour l'équipement de base

Les réseaux des FST se composent d'un certain nombre d'éléments allant de commutateurs téléphoniques, d'enregistreurs de localisation nominaux, de plateformes de messagerie vocale et de plateformes de service à valeur ajoutée qui fournissent des services à des composantes plus traditionnelles, comme des routeurs, des commutateurs et d'autres composantes de TI basées sur des systèmes, de même que des services de TI de base, comme la résolution des systèmes de noms de domaine, les services de courrier au moyen d'un protocole de transfert de courrier simple et la synchronisation des réseaux au moyen d'un protocole NTP.

Il importe de s'assurer que ces systèmes sont conçus et configurés de façon à réduire au minimum leur exposition aux menaces.

### 3.2.1 Renforcement du système et des composantes

**Objectif :**

Les réseaux des FST et leurs composantes ne fonctionneront correctement que si toutes les composantes sont bien protégées et renforcées. Les contrôles recommandés suivants facilitent la configuration adéquate des composantes de l'infrastructure des FST. Il ne s'agit pas d'une liste exhaustive ni obligatoire, puisque les contrôles nécessaires se fonderont sur les composantes individuelles.

**Contrôles :**

Le processus fondamental de renforcement des dispositifs devrait être appliqué selon les guides des fournisseurs et les pratiques exemplaires de l'industrie. La liste qui suit n'est pas complète, mais touche notamment les sujets suivants.

Les FST devraient :

1. consulter des guides sur le renforcement des systèmes et des dispositifs. Il existe des publications émises par des organismes réputés offrant des recommandations détaillées sur le renforcement de différents types de systèmes et de dispositifs;

2. choisir des normes de renforcement reconnues par l'industrie ou en élaborer à l'interne en les amenant au même niveau d'efficacité que les normes publiques reconnues et les imposer au sein de leur organisme;

3. obliger les FST de tierces parties à se conformer aux exigences de renforcement par le truchement d'obligations contractuelles en lien avec la fourniture et le maintien des services.

### 3.2.2 Renforcement du DNS et sécurité

**Objectif :**

Le système de noms de domaine (DNS) est un protocole de contrôle fondamental dans les réseaux IP et il est essentiel pour se brancher à Internet. Les serveurs DNS des FST devraient être sécuritaires et résilients aux incidents mettant la sécurité en jeu, en plus de fournir des données exactes.

**Contrôles :**

Les FST devraient :

1. s'assurer de déployer, de configurer et de sécuriser l'infrastructure DNS et les services, conformément aux normes reconnues;

2. s'assurer de protéger leur propre nom de domaine en plus de ceux sous leur responsabilité;

3. s'assurer, en tant que source faisant autorité, de fournir les coordonnées valides des personnes-ressources;

4. surveiller l'activité DNS en vue de détecter des abus susceptibles d'influer sur les clients ou sur les autres fournisseurs de services, et d'y donner suite;

5. donner suite aux cas d'abus en temps opportun;

6. s'assurer de la diversité géographique des serveurs DNS faisant autorité et utilisés aux fins de résolution de noms.

## 3.3. Essai de sécurité

### 3.3.1 Évaluation de la vulnérabilité

**Objectif :**

L'environnement des FST se compose de nombreuses composantes interconnectées qui forment les couches de gestion, de commande et de données. Avant de procéder à leur déploiement, l'équipement et les services doivent être testés en laboratoire afin de s'assurer qu'ils satisfont aux spécifications en matière de sécurité du fournisseur et de valider que la configuration de sécurité appliquée par les FST ne compromet pas la sécurité du réseau.

**Contrôles :**

Les FST devraient :

1. inclure des essais de sécurité dans tous les plans de mise à l'essai d'un processus de développement de système;
2. effectuer des essais sur les dispositifs pour vérifier leur conformité aux normes de sécurité en matière de renforcement adoptées;

3. effectuer des essais de sécurité avant d'approuver les systèmes aux fins de mise en production;

4. s'assurer que les couches du réseau sont sécuritaires en effectuant une évaluation régulière des risques de chaque couche et donner suite lorsque des risques inacceptables ont été observés.

### 3.3.2 Surveillance continue de la conformité et audit

**Objectif :**

Après avoir procédé à la mise en œuvre d'un service ou d'une technologie, il faut s'assurer de leur sécurité continue. Pour ce faire, la mise en application d'un programme de surveillance de la conformité et la tenue d'audits permettent de s'assurer que les normes de sécurité ne se sont pas dégradées au fil du temps dans l'environnement de production, et que les systèmes s'adaptent aux nouvelles normes de sécurité au fur et à mesure de leur mise à jour.

**Contrôles :**

Les FST devraient :

1. mettre en place un Programme de gestion de la vulnérabilité, incluant des processus et des outils d'analyse pour vérifier la vulnérabilité de l'équipement du réseau et des systèmes de production;

2. documenter des procédures et des processus pour détecter et traiter les vulnérabilités;

3. percevoir le besoin d'ajouter de l'équipement au réseau.

## 3.4. Procédures de contrôle des changements

**Objectif :**

Un Programme complet de gestion du changement permettra de s'assurer que les innovations apportées aux environnements de production sont gérés pour répondre aux besoins opérationnels. Une bonne gestion du changement permettra de vérifier que les modifications sont évaluées en fonction des risques, approuvées et mises en œuvre dans un milieu contrôlé et constant et que seuls les changements autorisés sont mis de l'avant.

**Contrôles :**

Les FST devraient :

1. mettre en œuvre un programme de gestion du changement qui permet d'introduire les changements à des systèmes et à des environnements de production dans un milieu contrôlé en vue d'atténuer les risques et de s'assurer que tous les changements sont conformes aux exigences en matière de sécurité;

2. s'assurer que le programme de gestion du changement prévoit les fonctions du Comité consultatif sur les changements formé de représentants de tous les secteurs concernés pour s'assurer que les changements sont examinés de façon adéquate;

3. s'assurer que les changements sont approuvés par la direction directement responsable de l'exploitation des composantes qui sont modifiées;

4. s'assurer que les procédures de contrôle des changements décrivent les essais requis pour valider les changements;

5. s'assurer que les essais postérieurs aux changements peuvent permettre de valider l'intégrité de tous les contrôles de sécurité effectués avant les changements.

## 4. Capacité de surveillance du réseau et de détection des risques

En plus de sécuriser l'infrastructure des FST, il est également nécessaire d'effectuer une surveillance de la sécurité et de procéder à la détection des incidents dans l'environnement. Les environnements les plus sécuritaires demeurent vulnérables aux incidents et aux attaques.

### 4.1. Obligation pour les FST de surveiller l'infrastructure du réseau

**Objectif :**

Les FST devraient être en mesure de surveiller le trafic sur le réseau afin de détecter les comportements malveillants ou potentiellement malveillants sur leurs réseaux. Les FST devraient également consulter les journaux d'événements et étudier les systèmes de surveillance en lien avec la cybersécurité afin d'être à l'affût des tendances et demeurer alertes aux comportements anormaux pouvant donner lieu à des enquêtes approfondies.

**Contrôles :**

Les FST devraient :

1. examiner l'infrastructure utilisée pour la prestation des services principaux aux clients;

2. surveiller les éléments essentiels contre les menaces externes et internes;

3. disposer d'un système de gestion des informations et de régie des événements de sécurité pour recueillir et corréler les renseignements provenant de différents systèmes et dispositifs;

4. surveiller une ou plusieurs connexions;

5. permettre une surveillance volumétrique du trafic;

6. surveiller les indicateurs de menace *ad hoc* des secteurs public, privé et de tierces parties, lorsque c'est possible;

7. contrôler le trafic au sein de leurs réseaux pour détecter les anomalies;

8. définir des plans d'intervention pour le trafic perçu comme malveillant et signalé dans le cadre de leurs activités de surveillance.

## 4.2. Types de trafic à surveiller

### 4.2.1 Logiciel malveillant

**Objectif :**

On ne peut pas toujours localiser le trafic malveillant sur le matériel infecté parce les concepteurs de logiciels malveillants prennent des mesures pour éviter la détection. À l'aide de mécanismes comme des piles TCP/IP distinctes ou des crochets de noyau, les applications malveillantes sont dissimulées dans des listes leur permettant d'échapper à la détection. Il peut arriver qu'un fournisseur de services localise des signes de malveillance, mais les clients, par contre, ne sont pas en mesure de tirer les mêmes conclusions. Si, dans le cadre de son travail de surveillance, un fournisseur de services se rend compte qu'un client est touché par des logiciels malveillants, il doit immédiatement l'alerter.

Le rôle des FST n'est pas de remplacer les logiciels antivirus ou les autres outils de sécurité informatique normalement intégrés aux systèmes du client. Par contre, les FST devraient intervenir lorsque le trafic malveillant devient excessif ou s'il est porté à leur attention par une tierce partie digne de confiance.

**Contrôles :**

Les FST devraient :

1. être en mesure de retracer la source du trafic malveillant sur leur réseau;

2. donner suite aux rapports valides sur les activités malveillantes sur leurs réseaux;

3. être en mesure de surveiller un certain nombre de types de trafic malveillant;

4. être en mesure de détecter les logiciels malveillants en fonction des caractéristiques de signature et de volume.

### 4.2.2 Surveillance de l'utilisation abusive du service de réseau

**Objectif :**

Bien que les systèmes clients compromis ne constituent pas nécessairement une menace pour la fiabilité ou le rendement des services essentiels de réseau et des protocoles, comme DNS ou DHCP, si on les laisse en grand nombre sans surveillance, ils peuvent collectivement avoir un effet négatif sur le service, ce qui nuirait aux autres clients et ferait grimper les coûts des immobilisations (p. ex. par le truchement des coûts d'approvisionnement supérieurs associés à la capacité des FST).

**Contrôles :**

Les FST devraient :

1. être en mesure de surveiller le flux de trafic provenant des clients internes et se dirigeant vers les services de réseau liés à l'infrastructure essentielle du fournisseur;

2. régler les anomalies détectées en utilisant les procédures pour réagir aux incidents.

### 4.2.3 Utilisation abusive de la messagerie

**Objectif :**

L'abus des services de messagerie électronique peut souvent entraîner le blocage de ces services à l'externe et nuire à la réputation du fournisseur. Il est donc important que les FST surveillent les services de courriel et veillent à ce qu'ils soient utilisés à bon escient.

**Contrôles :**

Les FST devraient :

1. surveiller leurs services de courriel pour vérifier qu'il n'y a pas d'abus, notamment la surveillance particulière du volume de messages sortants et du nombre élevé de destinataires prévus, s'ils fournissent des services de messagerie électronique;

2. s'assurer que les clients qui dépassent les seuils prévus (volume de message et nombre élevé de destinataires) puissent être identifiés et que des mesures de suivi soient prises;

3. s'assurer que les ententes de services de courriel fournis par des tiers prévoient des contrôles et des processus permettant de surveiller l'utilisation abusive de la messagerie et d'appliquer des mesures de suivi appropriées.

### 4.2.4 Pourriel sortant

**Objectif :**

Les services relatifs au courriel devraient être surveillés pour relever les pourriels sortants provenant des adresses IP individuelles des clients. Les indicateurs utilisés pour la détection devraient provenir de tierces parties fiables telles que SenderBase. Ce genre d'entreprise peut dénombrer les pourriels sortants.

**Contrôles :**

Les FST devraient :

1. prendre des mesures pour surveiller le volume élevé de trafic relatif à des pourriels provenant d'adresses IP individuelles de leurs clients dans le but d'aviser ces derniers d'une infection potentielle ou de prendre d'autres mesures pour mettre un terme à un tel trafic.

## 5. Capacité à réagir aux incidents relatifs à la sécurité

### 5.1. Capacité des FST à réagir aux incidents

**Objectif :**

S'assurer que les FST aient les ressources nécessaires pour régler des incidents liés à la sécurité, tant à l'interne qu'à l'externe. Pour ce faire, les FST devraient établir des processus définis et reproductibles. Ils doivent également disposer d'une équipe capable de régler des incidents de sécurité dès qu'ils surviennent. Il peut s'agir d'une équipe fonctionnelle répartie sur un grand territoire ou d'une équipe centralisée d'intervention (p. ex. : Centre des opérations de sécurité).

**Contrôles :**

Les FST devraient :

1. gérer les incidents liés à la cybersécurité par le truchement d'un programme défini, testé et reproductible;

2. mettre en oeuvre une structure de gouvernance pour leur programme de gestion des incidents liés à la cybersécurité;

3. donner suite aux incidents de sécurité opérationnelle qui se produisent durant, ou en dehors des heures normales;

4. Signaler tout comportement abusif à des points de contact mandatés pour surveiller et contrer ce genre d'incident.

## 5.2. Mode d'intervention dans les cas touchant les clients

### 5.2.1 Incidents liés à la technologie de l'information (TI) ou aux ordinateurs personnels des clients

**Objectif :**

Il peut arriver qu'un fournisseur de services se rende compte d'une intrusion ou d'une infection par un logiciel malveillant dans l'ordinateur d'un client, que ce dernier soit victime ou auteur d'une attaque (délibérée ou non). Lorsqu'il se rend compte d'une telle intrusion dans le système ou les données d'un client, le fournisseur de services doit en informer immédiatement tous les clients ou partenaires visés afin de limiter les dégâts.

En outre, les FST devraient tenter de réduire l'incidence de cette attaque par tous les moyens à leur disposition, notamment, en atténuant le trafic malveillant (voir l'article 5.3 ci-dessous), ou en suspendant l'activité du client jusqu'à ce que la menace soit neutralisée.

**Contrôles :**

Les FST devraient :

1. élaborer des procédures de notification aux clients;

2. être en mesure d'effectuer le suivi des avis envoyés aux clients, y compris les méthodes de transmission utilisées et la fréquence des avis publiés;

3. valider l'information liée à un incident en provenance d'une tierce partie avant d'y donner suite;

4. protéger la source de leurs renseignements dans l'avis lorsqu'il s'agit de renseignements confidentiels fournis par des tiers;

5. mettre en place des mécanismes pour détecter et donner suite à des intrusions connues ou à des situations de pertes potentielles ayant une incidence sur les clients.

### 5.2.2 Fuite de renseignements personnels concernant les clients

**Objectif :**

Lorsqu'un FST découvre une intrusion dans son propre réseau et que cette intrusion est susceptible d'entraîner la divulgation de renseignements permettant d'identifier une personne ou de révéler des renseignements au sujet de la configuration d'un réseau, il est tenu d'avertir immédiatement tous les clients ou partenaires visés afin de les protéger contre des fraudes potentielles.

**Contrôles :**

Les FST devraient :

1. définir des procédures de notification applicables à court terme (deux jours au maximum) pour protéger les clients et les partenaires;

2. dresser une liste et la publier à l'interne, des personnes responsables de communiquer avec les clients, les partenaires et le grand public;

3. disposer d'une méthode éprouvée pour aviser les clients d'incidents ou de fuite de renseignements;

4. établir des mécanismes de sécurité afin que les clients et les partenaires puissent reconnaître les communications émanant des FST.

### 5.3 Remédier ou atténuer le trafic malveillant ou inapproprié

**Objectif :**

Il arrive parfois que certains types de trafic causent un préjudice aux clients ou aux FST. Par exemple, une attaque contre un client sous forme de déni de service distribué est susceptible d'avoir des répercussions sur le fournisseur de services ou sur d'autres clients. Certains types de logiciels malveillants peuvent causer un trafic excessif sur le réseau et produire le même effet qu'une attaque par déni de service distribué. Dans le but de protéger leurs infrastructures, leurs clients et les infrastructures de télécommunication essentielles canadiennes, les FST devraient être en mesure de remédier ou atténuer le trafic leur causant d'importants dommages.

**Nota :** *La partie suivante a trait au trafic jugé malveillant ou préjudiciable aux réseaux des FST. On y trouve des solutions que les FST, capables de fournir de tels services, peuvent appliquer afin de remédier au trafic malveillant ou de l'atténuer. Dans la présente, il n'y a aucune obligation pour les FST de bloquer un contenu qu'une tierce partie juge inadmissible ou qui porte préjudice à une tierce partie. On y mentionne seulement les mécanismes de contrôles qui doivent être mis en place advenant que les FST décident de prendre des mesures.*

**Contrôles :**

Les FST devraient :

1. déterminer les catégories de trafic à atténuer, filtrer ou bloquer, et s'assurer d'avoir la capacité de le faire;

2. définir les conditions en vertu desquelles ils pourront atténuer, filtrer ou bloquer le trafic malveillant et prévoir sur quels réseaux appliquer ces conditions;

3. dans le but de protéger les réseaux essentiels, envisager en dernier lieu le filtrage ou le blocage pour éviter toute possibilité de nuire au trafic légitime;

4. cibler les sources de renseignements fiables et en lien avec le trafic malveillant;

5. adopter une politique publique sur la résolution et l'atténuation du trafic malveillant;

6. établir leurs politiques sur la résolution et l'atténuation du trafic malveillant dans les accords sur les niveaux de services conclus avec leurs clients.

## 6. Partage de l'information et rapports

Le partage de l'information et la production de rapports représentent des éléments cruciaux dans la protection de l'infrastructure essentielle. L'étendue, l'ampleur et la complexité des menaces actuelles sont telles que la collaboration entre les FST est nécessaire pour protéger l'infrastructure essentielle du Canada.

En plus du partage direct de renseignements avec le Gouvernement et d'autres FST canadiens, les FST devraient participer à des groupes de travail pertinents pour les besoins de leur entreprise et pour leurs responsabilités en matière de sécurité. Cela procure des occasions de collaborer et de partager l'information, ce qui améliore grandement la capacité d'une organisation à se préparer à intervenir en cas de problèmes touchant la cybersécurité.

Exemples de groupes de travail et de groupes de confiance actuellement établis :

1. Groupe de travail contre les abus de messagerie électronique (MAAWG)
2. Forum des équipes de sécurité et d'intervention en cas d'incident (FIRST)
3. Microsoft Security Response Alliance (MSRA),
4. Protection cybernétique des télécommunications canadiennes (PCTC)
5. North American Network Operators' Group (NANOG).

En outre, les FST devraient encourager leurs employés à participer aux activités d'un certain nombre de groupes de confiance individuels.

Les critères d'adhésion varient. Des frais d'adhésion sont exigés pour certains groupes (p. ex. MAAWG et FIRST), alors qu'une contribution volontaire convient pour d'autres (p. ex. MSRA et PCTC). Une participation régulière en personne est obligatoire pour tous ces groupes.

Les communautés de partage d'information, qu'elles soient officielles ou non, ouvertes ou privées, peuvent appliquer leurs propres restrictions, notamment des ententes de non-divulgation, des validations et des exigences en matière de Web de confiance (p. ex. le retrait des certificats de sécurité).

Le partage de l'information entre les FST, les ministères et les organismes du gouvernement canadien, et les autres entités pertinentes doit respecter le niveau de classification des renseignements défini par les propriétaires des renseignements, se conformer aux lois (p. ex. *Loi sur l'accès à l'information*) et aux directives sur le partage de l'information du Conseil du Trésor du Canada.

### 6.1. Partage de l'information pour la protection de l'infrastructure essentielle des télécommunications

**Objectif :**

Faire en sorte que les FST du Canada participent activement au partage d'information relative à la cybersécurité tant pour la protection de l'infrastructure essentielle du Canada que pour celle de leurs clients.

**Contrôles :**

Les FST devraient :

1. être en mesure de recevoir de l'information de la part des autres opérateurs de réseaux et des organismes d'intervention en cas de menace et avoir la capacité d'y réagir;

2. définir et mettre en œuvre des pratiques de partage d'information sur les menaces dans le but d'échanger des renseignements avec des tierces parties;

3. participer au Groupe de travail sur la protection cybernétique des télécommunications canadiennes s'ils sont responsables de l'infrastructure essentielle des télécommunications, telle que définie par Industrie Canada.

### 6.2. Établissement des mécanismes de partage de l'information

**Objectif :**

Tous les FST devraient disposer d'un ensemble de ressources communes leur permettant de partager l'information en toute sécurité. Ces ressources constituent les exigences minimales pour pouvoir échanger en toute sécurité des renseignements sur le traitement des menaces et des incidents. Bien qu'il existe certainement des mécanismes plus perfectionnés, ce ne sont pas tous les organismes qui pourront s'en prévaloir. C'est pourquoi il faut établir un ensemble de ressources de base. En plus de protéger les données, les mécanismes utilisés devraient aussi permettre d'authentifier l'expéditeur afin d'éviter les attaques d'hameçonnage ou l'usurpation d'identité.

**Contrôles :**

Les FST devraient :

1. soutenir les mécanismes de sécurité appropriés pour le partage fiable de l'information tel qu'exigé par les forums où l'information circule;

2. établir et imposer des politiques internes de classification, de confidentialité (y compris la cueillette, l'utilisation et la divulgation).

3. établir et imposer une politique sur l'utilisation acceptable ou des politiques sur les modalités de services aux clients, plus précisément aux fins de gestion des abus;

4. restreindre le partage de données à celles requises pour la résolution de problèmes, et éviter de partager des renseignements personnels.

## 7. Gestion des distributeurs

### 7.1. Chaîne d'approvisionnement en équipement

Les FST sont perçus comme des distributeurs pour leurs clients. Toutefois, ils sont également des clients, car ils doivent se procurer des systèmes et une technologie auprès de distributeurs afin de concevoir l'infrastructure qui fournira des services à la population canadienne.

**Objectif :**

Dans le but de réduire les menaces contre leur infrastructure et leurs clients, les FST devraient fournir des efforts raisonnables pour garantir la sécurité de leur équipement réseau.

**Contrôles :**

Les FST devraient :

1. définir des normes de sécurité pour l'approvisionnement en systèmes, dispositifs ou logiciels;

2. s'assurer que les normes de sécurité pertinentes figurent dans les ententes d'achat, les demandes de propositions et les contrats;

3. exiger que les tierces parties mettent à l'essai et vérifient l'ensemble de l'équipement, des systèmes et des logiciels en fonction des pratiques exemplaires bien connues (p. ex. : critères communs);

4. refuser de conclure des affaires avec des distributeurs qui ne satisfont pas aux normes de sécurité, sauf si le distributeur est prêt à régler le problème ou qu'il est possible de mettre en place des contrôles d'atténuation;

5. définir des procédures permettant de s'assurer que les distributeurs suivent les normes définies par le fournisseur;

6. établir un Programme de vérification de la conformité pour s'assurer que les distributeurs respectent les normes définies par le fournisseur;

7. s'assurer que les exigences en matière de renforcement sont transmises aux fournisseurs.

### 7.2. Gestion de la sécurité du distributeur

**Objectif :**

Les distributeurs de services de télécommunication offrent souvent des niveaux de soutien élevés aux FST. Par conséquent, les FST doivent mettre en place des contrôles de sécurité pour vérifier l'accès à leur équipement par des distributeurs.

**Contrôles :**

Les FST devraient :

1. limiter l'accès du distributeur uniquement aux systèmes dont le soutien est assuré par ce même distributeur;

2. démontrer que les pratiques de leurs distributeurs en télécommunication n'ont aucune incidence sur le niveau de sécurité des infrastructures des FST ni ne dégradent ce niveau;

3. surveiller l'activité du distributeur pour s'assurer de l'intégrité et de la sécurité de leurs réseaux;

4. s'assurer d'inclure les exigences en matière de renforcement dans les dispositions d'un accord sur les niveaux de service conclu avec les tiers fournisseurs.

## 8. Protection de la vie privée

**Objectif :**

Le droit au respect de la vie privée des Canadiens est protégé par un certain nombre de lois fédérales et provinciales, de même que par certains règlements sur le respect de la vie privée imposés par le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). Ces exigences légales ont préséance sur les lignes directrices énumérées dans les pratiques exemplaires. On s'attend à ce que les FST qui suivent les pratiques exemplaires maintiennent également le même niveau d'engagement concernant le respect de la vie privée de leurs clients.

Plus précisément, le partage de renseignements personnels est rarement nécessaire pour la résolution d'abus ou de problèmes. Le fournisseur de services qui dessert un client doit être en mesure d'identifier l'utilisateur dont l'ordinateur est contaminé ou l'utilisateur qui abuse d'un service. Toutefois, ces renseignements ne doivent pas être partagés avec d'autres entités, sauf si la divulgation de ces renseignements est conforme aux règles de confidentialité et aux conditions d'utilisation du fournisseur.

Bien que les lois applicables soulignent le droit à la vie privée des citoyens, de même que l'obligation des FST à protéger la vie privée des citoyens, d'autres pratiques exemplaires doivent également être appliquées.

**Contrôles :**

Les FST devraient :

1. s’assurer que leurs solutions et leurs services soient conformes aux lois applicables en matière de protection de la vie privée;

2. résoudre rapidement et avec transparence, les problèmes en lien avec la vie privée;

3. tenir compte de la vie privée de leurs clients dans leurs prises de décision afin de ne pas la compromettre.

## Annexe A — Acronymes

| | |
|---|---|
| AMRC | Accès multiple par répartition en code |
| BGP | Protocole de passerelle frontière |
| CLI | Interface de ligne de commande. |
| CSTC | Centre de la sécurité des télécommunications Canada |
| CCCST | Comité consultatif canadien sur la sécurité des télécommunications |
| DDoS | Attaque cybernétique par déni de service distribué |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Système de noms de domaine |
| DP | Demande de propositions |
| DoS | Attaque par déni de service |
| E/S | Entrée/sortie |
| FST | Fournisseurs de services de télécommunications |
| GPRS | Service général de paquets radio |
| GSM | Système mondial de communication avec les mobiles |
| GTP | Protocole de tunnellisation GPRS |
| GTPCTC | Groupe de travail sur la protection cybernétique des télécommunications canadiennes |
| HSPA | Accès par paquets haut débit |
| HTTP | Protocole de transfert hypertexte |
| HTTPS | Protocole de transfert hypertexte sécurisé |
| IP | Protocole Internet |
| ISO | Organisation internationale de normalisation, |
| ISP | Fournisseur de services Internet |
| LAN | Réseau Local |
| LTE | Technologie d'évolution à long terme |
| MAC | Contrôle d'accès au support. |
| MD5 | Condensé de message 5 |
| PIE | Protection de l'infrastructure essentielle |
| SIM | Module d'identité d'abonné |
| SSH | Protocole SSH |
| SFTP. | Protocole sécurisé de transfert de fichiers |
| SNMP | Protocole de gestion de réseau simple |
| SVA | Service à valeur ajoutée |
| QOS | Qualité du service |
| UMTS | Système universel de télécommunication mobile |
| URPF | Acheminement individuel par le chemin inverse |
| USB | Bus série universel |
| USIM | Universal Subscriber Identity Module |
| VLAN | Réseau local virtuel |
| Wi-Fi | Technologie Wi-Fi |

# Annexe B — Ressources

**Centre canadien de réponses aux incidents cybernétiques**

Le Centre canadien de réponses aux incidents cybernétiques (CCRIC) est chargé de surveiller les cybermenaces et de donner des conseils sur les méthodes d'atténuation.

**National Institute of Standards and Technology** (Site anglais seulement)

Le National Institute of Standards and Technology (NIST) publie des guides de normes s'appliquant aux systèmes de traitement de l'information du gouvernement américain et d'autres renseignements utiles portant sur la sécurité.

**Center for Internet Security** (Site anglais seulement)

Le Center for Internet Security (CIS) publie des normes visant le renforcement de divers types de réseaux et de matériel informatique. Il publie également des outils de notation servant à évaluer les composantes du réseau en fonction des normes établies.

**Cyberaide!ca**

Cyberaide est le service pancanadien de signalement d'enfants exploités sexuellement sur Internet.

**Commissariat à la protection de la vie privée**

Le Commissariat à la protection de la vie privée du Canada (CPVP) assure le respect de la *Loi sur la protection des renseignements personnels* (LPRP) et de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

Le CPVP fournit un document contenant les principales étapes à suivre par les organisations en cas d'atteinte à la vie privée en vertu de la LPRPDE, et un formulaire de rapport d'incident en cas d'atteinte à la vie privée.

**Secrétariat du Conseil du Trésor du Canada**

Le Conseil du Trésor du Canada a publié des lignes directrices sur le partage de l'information entre les organismes du gouvernement du Canada. Ces lignes directrices devraient être respectées lorsque des ministères gouvernementaux sont concernés.