Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1207

(04/2008)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Cybersécurité

Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable

Recommandation UIT-T X.1207

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	**X.1200–X.1229**
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1207

Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable

Résumé

La Recommandation UIT-T X.1207 contient des lignes directrices à l'intention des fournisseurs de services de télécommunication (TSP, *telecommunication service provider*) pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable. Elle vise à promouvoir, dans le cadre des services d'hébergement de pages web des fournisseurs TSP, les meilleures pratiques fondées sur les principes suivants: obligation d'informer clairement les utilisateurs, nécessité d'obtenir leur consentement et possibilité pour eux d'exercer un contrôle. Elle vise également à élaborer et à promouvoir les meilleures pratiques à l'intention des utilisateurs sur la sécurité des ordinateurs personnels (PC), notamment sur l'installation d'anti-espiogiciels, d'antivirus, de pare-feu personnels et de mises à jour de sécurité sur les systèmes des clients.

Source

La Recommandation UIT-T X.1207 a été approuvée le 18 avril 2008 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Logiciel espion (espiogiciel), logiciel potentiellement indésirable, logiciel trompeur, sécurité sur l'Internet.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1207

Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable

1 Domaine d'application

La présente Recommandation fait partie de l'ensemble des orientations mises au point par l'UIT-T pour améliorer la situation actuelle en matière de cybersécurité. Elle porte sur les pratiques de base que doivent appliquer les fournisseurs de services de télécommunication (TSP, *telecommunication service providers*) et les utilisateurs finals en matière de sûreté et de sécurité, en mettant l'accent sur le problème des logiciels espions (espiogiciels) ou autres logiciels potentiellement indésirables, qui peuvent être malveillants et/ou trompeurs. Dans le contexte de la présente Recommandation, le terme "fournisseurs de services de télécommunication (TSP)" désigne les fournisseurs TSP qui fournissent des services Internet, notamment des services d'hébergement de pages web à des organisations commerciales, ou l'accès Internet aux utilisateurs finals.

2 Références

Aucune.

3 Définitions

Le terme "logiciel espion (espiogiciel)" est utilisé improprement pour désigner de nombreuses formes de logiciels qui présentent certains comportements portant atteinte à l'intimité de la vie privée, non sollicités par les utilisateurs finals. Pour assurer l'utilisation cohérente et une compréhension commune de ce terme, une définition de travail du terme "logiciel espion (espiogiciel)" et du terme connexe "logiciel trompeur" est présentée ici.

3.1 logiciel trompeur: logiciel qui effectue des opérations sur l'ordinateur d'un utilisateur sans: 1) informer préalablement cet utilisateur de la nature exacte des opérations que le logiciel va effectuer sur son ordinateur ou 2) demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations. Comme exemple de logiciels trompeurs, citons les programmes de piratage de configurations d'utilisateur ou les programmes qui déclenchent l'affichage ininterrompu de fenêtres publicitaires intempestives dont l'utilisateur a du mal à se débarrasser.

3.2 logiciel potentiellement indésirable: le terme "logiciel potentiellement indésirable" désigne diverses formes de logiciel trompeur, dont les logiciels malveillants (maliciels) tels que virus, vers informatiques et chevaux de Troie, ainsi que les logiciels non malveillants qui présentent les caractéristiques d'un logiciel trompeur ou d'un espiogiciel.

3.3 logiciel espion (espiogiciel): dans la présente Recommandation, on entend par "logiciel espion (espiogiciel)" un type particulier de logiciel trompeur qui collecte des informations personnelles auprès d'un internaute. Ces informations personnelles peuvent porter sur les sites web les plus souvent visités, par exemple, ou sur des informations plus sensibles telles que les mots de passe.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CERT équipe d'intervention en cas d'urgence informatique (*computer emergency response team*)

CIRT équipe d'intervention en cas d'incident informatique (*computer incident response team*)

ISMS système de gestion de la sécurité de l'information (*information security management system*)

ISMS-T système de gestion de la sécurité de l'information – prescriptions pour les télécommunications (*information security management system – requirements for telecommunications*)

ISV fournisseur de logiciels indépendant (*independent software vendor*)

SQL langage de requêtes structuré (*structured query language*)

TIC technologies de l'information et de la communication

TSP fournisseur de services de télécommunication (*telecommunication service provider*)

URI identificateur universel de ressource (*uniform resource identifier*)

5 Conventions

Aucune.

6 Aperçu général

L'essor de l'Internet a favorisé la création de nouvelles entreprises et apporté de nombreux avantages aux consommateurs chez eux et sur leur lieu de travail. De par l'accessibilité universelle qui le caractérise, ainsi que l'interconnectivité et la vitesse d'accès qu'il offre, l'Internet s'est en outre mué en une plate-forme de communication d'une grande efficacité pour les entreprises et les consommateurs, ainsi qu'à des fins de promotion commerciale de produits destinés au grand public. Depuis quelques années, l'accessibilité universelle de l'Internet et la facilité d'utilisation de ses modes de communication et de connectivité sont de plus en plus mises à profit par des cybercriminels et des entreprises sans scrupules, par le biais de diverses formes de logiciels malveillants, pour soutirer de l'argent et à d'autres fins criminelles.

L'un des problèmes qui se pose avec de plus en plus d'acuité en matière de sûreté et de sécurité, est celui des logiciels espions et des logiciels trompeurs, qui sont capables de porter atteinte à la confidentialité des informations personnelles, engendrant ainsi d'importantes baisses de productivité et jetant le discrédit, en sapant la confiance des utilisateurs finals, dans des entreprises aux activités parfaitement licites sur l'Internet.

Les fournisseurs de services de télécommunication (TSP) sont souvent perçus par les diverses parties prenantes, notamment les régulateurs et les clients des entreprises, comme faisant autorité en matière de fourniture de services Internet sûrs et sécurisés aux utilisateurs finals (y compris aux consommateurs et aux utilisateurs d'entreprise). Lorsqu'il apparaît que des sites web hébergés dans le réseau d'un fournisseur TSP hébergent des contenus malveillants, notamment des logiciels espions ou des logiciels trompeurs, qui affectent la sûreté et la sécurité des systèmes informatiques des utilisateurs finals, on demande à ce fournisseur TSP de prêter son assistance pour remédier aux problèmes et toute manifestation prolongée ou récurrente de tels incidents entamera la confiance des clients dans la capacité du fournisseur TSP à fournir des services sûrs et sécurisés, ce qui incitera les clients, à terme, à s'adresser à d'autres fournisseurs TSP.

D'un point de vue réglementaire, les régulateurs de nombreux pays réclament de plus en plus aux fournisseurs TSP de leur fournir des garanties quant aux mesures de sécurité et de sûreté qu'ils ont prises, et leur demandent d'accroître l'assistance qu'ils fournissent aux consommateurs et aux utilisateurs finals en vue d'assurer la sûreté et la sécurité des systèmes informatiques sur l'Internet.

Compte tenu de cette évolution du paysage Internet en matière de sûreté et de sécurité, il importe que les fournisseurs TSP adoptent une série de règles en matière de meilleures pratiques qui pourraient être reconnues par l'ensemble de la profession comme règles de base minimales[1] qui permettraient non seulement d'assurer de manière sûre et sécurisée la fourniture de services Internet hébergés par les fournisseurs TSP, mais aussi de promouvoir les meilleures pratiques auprès des utilisateurs finals qui s'abonnent aux réseaux de ces fournisseurs TSP. La mise en œuvre de ces règles de base permettra en outre aux fournisseurs TSP de démontrer aux régulateurs et aux utilisateurs finals qu'elles sont conformes aux meilleures pratiques de la profession, et de renforcer, ou du moins de conserver, la confiance des régulateurs et des utilisateurs finals dans la sûreté et la sécurité des réseaux et des services des fournisseurs TSP.

7 Objectifs

La présente Recommandation poursuit les objectifs suivants:

1) Promouvoir, dans le cadre des services d'hébergement de pages web, les meilleures pratiques fondées sur les principes suivants: obligation d'informer clairement les utilisateurs, nécessité d'obtenir leur consentement et possibilité pour eux d'exercer un contrôle.

2) Promouvoir les meilleures pratiques (par le biais des fournisseurs de services de télécommunication) à l'intention des particuliers sur l'utilisation sûre et sécurisée des ordinateurs personnels et de l'Internet, notamment sur l'installation d'antivirus, d'anti-espiogiciels, de pare-feu personnels et de mises à jour de sécurité automatiques.

8 Logiciel trompeur et logiciel espion

La caractéristique commune que partagent tous les programmes de logiciel trompeur (y compris les logiciels espions), qui les distingue des applications licites, réside dans le fait que l'utilisateur n'est pas informé de leur installation et qu'aucun choix ne lui est laissé. Fait important, il est communément fait valoir que, à condition que l'utilisateur en soit dûment informé, qu'il y consente et qu'il puisse exercer un contrôle, la plupart des tâches effectuées par un logiciel trompeur/espion apportent des avantages aux utilisateurs. Ainsi, de tels programmes peuvent faciliter la personnalisation, favoriser des modifications de configuration approuvées par l'utilisateur et acheminer de la publicité autorisée qui, à son tour, peut financer le coût d'un service très prisé comme le courrier électronique. En somme, ce qui pose véritablement problème dans les logiciels trompeurs n'est pas tant la technologie qu'ils utilisent; c'est surtout le comportement trompeur ou frauduleux auquel ils ont recours.

Tant au niveau mondial que local, les logiciels trompeurs et espions sont devenus une des préoccupations majeures des pouvoirs publics, des entreprises et des consommateurs en ce sens qu'ils vont au-delà des considérations liées à une question de politique dans le domaine des TIC. S'ils utilisent manifestement l'Internet et l'ordinateur comme supports, les logiciels trompeurs posent fondamentalement un problème de protection des consommateurs qui découle de leur comportement trompeur.

---

[1] De telles règles de base n'existent pas actuellement, mais la présente Recommandation constitue un premier pas vers l'adoption d'une règle de base minimale.

9 En quoi les logiciels trompeurs et les logiciels espions sont-ils un problème?

Au niveau des consommateurs, de tels logiciels dégradent la qualité des services informatiques et/ou en ligne constatée par l'utilisateur (parfois au point de rendre l'ordinateur inutilisable), engendrant chez lui un sentiment de frustration lui donnant l'impression qu'il ne contrôle plus rien. Il n'est pas exagéré d'affirmer qu'au niveau des clients résidentiels, notamment, il existe une proportion importante d'utilisateurs pour lesquels les logiciels trompeurs menacent de réduire à néant les avantages extraordinaires qu'offrent *intrinsèquement* l'Internet et l'informatique.

Bien qu'ils aient manifestement une incidence sensible sur les consommateurs, les logiciels trompeurs constituent également un problème de taille pour beaucoup d'entreprises dans le domaine des TIC. D'un côté, maints consommateurs attribuent à tort les dysfonctionnements de leur ordinateur aux fabricants et concepteurs de logiciels, ce qui porte atteinte à la réputation de ceux-ci et altère la manière dont les consommateurs perçoivent leurs produits. A l'évidence, les problèmes imputables aux logiciels trompeurs conduisent également à dépenser des millions de dollars dans des appels d'assistance inutiles, tant au niveau des logiciels que du matériel.

Comme nous l'avons vu plus haut au § 6, les fournisseurs TSP ne sont pas à l'abri de devoir faire face aux problèmes causés par les logiciels espions et les logiciels trompeurs, étant donné qu'ils hébergent des sites web que des entreprises sans scrupules ou des cybercriminels peuvent détourner directement à leur profit, avec les conséquences dommageables directes que cela aura pour les abonnés, qui appelleront leur fournisseur TSP pour solliciter son aide et son assistance. Qui plus est, les régulateurs et les utilisateurs finals attendent généralement des fournisseurs TSP qu'ils prennent des mesures de sûreté et de sécurité appropriées pour contrer ce genre de problèmes. Naturellement, tout fournisseur TSP qui se soustrairait à l'obligation qui lui incombe de remédier à ce genre de problèmes compromettrait sa réputation et perdrait la confiance des utilisateurs finals.

10 Recommandations

Le moyen le plus efficace de faire face aux problèmes des logiciels espions passe probablement par la conjonction de plusieurs stratégies, mobilisant les diverses parties prenantes:

- Les meilleures pratiques d'entreprise, conjuguées à la collaboration des différents acteurs de premier plan afin d'identifier les logiciels espions et autres logiciels indésirables et de remédier aux problèmes qu'ils causent.
- Sensibilisation du grand public aux moyens d'éliminer et d'éviter les logiciels espions et autres logiciels indésirables, en vue de constituer un environnement sécurisé.
- Solutions technologiques innovantes contribuant à protéger les utilisateurs contre les logiciels espions et autres logiciels potentiellement indésirables, et les aidant à se tenir au courant des moyens disponibles pour déjouer les programmes permettant d'exploiter les failles de sécurité informatique.
- Adoption par les pouvoirs publics, avec l'aide d'entreprises, de mesures législatives dissuasives en matière de conception de logiciels trompeurs et de logiciels espions, ayant force exécutoire.

La présente ligne directrice porte sur la diffusion des meilleures pratiques d'entreprise et sur les efforts de sensibilisation du grand public pour aider les fournisseurs TSP à contribuer activement à contrer les problèmes causés par les logiciels trompeurs et les logiciels espions.

11 Conseils à l'intention des fournisseurs de services de télécommunication (TSP)

Pour aider à faire face aux problèmes que causent les logiciels trompeurs et les logiciels espions, la présente ligne directrice porte sur trois recommandations principales, à savoir: la gestion de la sécurité interne de l'organisation TSP proprement dite; les prescriptions de sécurité que les fournisseurs TSP devraient inviter les clients de services d'hébergement de sites web à respecter; et

les conseils de sécurité utiles pour les utilisateurs finals (ou les abonnés) des services d'accès à l'Internet. Ces recommandations sont présentées respectivement dans les trois sous-sections suivantes:

a) Gestion des risques liés à la sécurité de l'information au sein de l'entreprise.

b) Prescriptions de sûreté et de sécurité pour les services d'hébergement de sites web.

c) Conseils à l'intention des utilisateurs finals en matière de sûreté et de sécurité.

11.1 Gestion des risques liés à la sécurité de l'information au sein de l'entreprise

11.1.1 Système de gestion de la sécurité de l'information

Au niveau de l'entreprise, l'implémentation d'un système de gestion de la sécurité de l'information structuré s'impose pour identifier et gérer les risques liés à la sécurité de l'information dans le cadre des activités des fournisseurs TSP. Le document [b-UIT-T X.1051] indique les principes et les meilleures pratiques à suivre pour implémenter un tel système.

Un principe fondamental pour un fournisseur TSP qui se propose d'implémenter un système ISMS-T consiste à faire en sorte, en tant qu'organisation entrepreneuriale, de se doter d'un système lui permettant d'identifier, d'évaluer, de traiter et de gérer continûment les risques liés à la sécurité de l'information dans le cadre des services qu'il fournit sur Internet, directement aux abonnés/utilisateurs finals, et indirectement par l'intermédiaire de services d'hébergement de sites web offerts à des clients.

Grâce aux processus ISMS-T de gestion continue des risques, le fournisseur TSP sera non seulement mieux à même d'évaluer son profil d'exposition aux risques mais aussi en mesure de démontrer la sécurité de son réseau et ses services aux régulateurs et aux autres parties intéressées.

Le fournisseur TSP peut également songer à certifier formellement qu'il respecte bien les recommandations ISMS-T, dans le cadre du système de certification ISO/CEI 27001.

Dans le cadre de l'implémentation du système ISMS-T ou d'un système de gestion de la sécurité de l'information approprié, les fournisseurs TSP devraient aussi mettre en place des moyens de surveillance et d'intervention en cas d'incident affectant la sécurité, et coordonner leurs interventions dans ce domaine avec les équipes d'intervention en cas d'incident informatique (CIRT) ou les équipes d'intervention en cas d'urgence informatique (CERT) du pays considéré. Les mesures d'intervention prises en cas d'incident ou d'urgence devraient notamment consister à surveiller et évaluer le niveau de sécurité des utilisateurs finals et des sites web hébergés sur les réseaux des fournisseurs TSP, et à donner des conseils aux parties concernées pour les aider à faire face efficacement aux incidents affectant la sécurité.

11.1.2 Fourniture de produits sûrs et sécurisés

Certains fournisseurs TSP peuvent développer[2] et mettre sur le marché leurs propres barres d'outils de navigateur web, composeurs de numéros ou codes de tout type pour offrir aux utilisateurs finals des services à valeur ajoutée, ou leur faciliter l'accès aux services Internet. En pareil cas, les utilisateurs finals devront être clairement informés des politiques de ces fournisseurs TSP en matière de codage et de protection des données personnelles et déclarer qu'ils acceptent ces politiques; par ailleurs, ils devraient pouvoir changer d'avis ultérieurement ou soumettre à une instance supérieure tout litige qu'ils pourraient avoir concernant la politique ou les pratiques de ces fournisseurs TSP. Lorsqu'une telle déclaration d'acceptation est utilisée, les fournisseurs TSP devraient s'assurer que les utilisateurs finals la signent et procèdent toujours au suivi de ses différentes versions.

---

[2] Soit en interne ou par l'intermédiaire d'un fournisseur tiers.

Les fournisseurs TSP devraient en outre recueillir des informations sur le comportement de code et procéder à une évaluation afin de déterminer si ce comportement peut éventuellement être imputé à des logiciels espions ou des logiciels trompeurs. Si tel est le cas, les fournisseurs TSP devraient charger un expert compétent de déterminer si le code peut relever des critères objectifs des fournisseurs d'anti-espiogiciels, puis adhérer aux meilleures pratiques de manière que les outils logiciels fournis par lesdits fournisseurs TSP aux utilisateurs finals ne soit pas qualifié d'espiogiciels ou de publiciels par les fournisseurs d'anti-espiogiciels. Nombre de ces fournisseurs publient les critères selon lesquels ils évaluent les logiciels[3].

Les fournisseurs TSP devraient implémenter la signature de code numérique pour leurs fichiers binaires, de manière que les fournisseurs d'anti-espiogiciels puissent identifier aisément le propriétaire d'un fichier, et que les fournisseurs de logiciels indépendants (ISV) qui produisent invariablement des logiciels conformes aux meilleures pratiques soient classés comme offrant toutes garanties de sécurité, avant même d'être soumis à analyse.

Au cas où ils découvriraient des techniques logicielles pouvant utilement contribuer à atténuer les problèmes causés par les espiogiciels, les fournisseurs TSP devraient songer à s'associer et à collaborer avec le fournisseur de logiciels pour rendre ces techniques accessibles au plus grand nombre.

11.1.3 Surveillance du réseau et interventions nécessaires

La surveillance du réseau est pratique courante chez les fournisseurs TSP pour assurer la fiabilité et la qualité des services de réseau. En même temps, cette pratique peut être mise à profit pour rechercher des conditions de trafic de réseau exceptionnelles et détecter l'apparition d'activités malveillantes sur le réseau. En règle générale, les fournisseurs TSP devraient procéder comme suit:

- Bien percevoir la nature du trafic sur le réseau – ce qui est normal et ce qui ne l'est pas.
- Utiliser des outils de gestion de réseau pour identifier les pointes de trafic, le trafic ou les ports inhabituels et faire en sorte que des outils soient disponibles pour déceler la cause de ces problèmes et y remédier.
- Tester les moyens d'intervention avant d'en avoir effectivement besoin. Perfectionner les techniques, processus et outils d'intervention d'après les résultats d'exercices réguliers.
- Discerner le profil des utilisateurs au cas par cas: si un utilisateur habituellement peu actif commence subitement à utiliser 100% de la largeur de bande qui est mise à sa disposition, l'implémentation d'une isolation de réseau s'impose peut-être jusqu'à ce que la cause de cette utilisation puisse être déterminée. L'isolation de réseau peut éviter la propagation d'un logiciel malveillant (maliciel), mais certaines implémentations nécessitent parfois le consentement de l'utilisateur ou des mises à jour des conditions d'utilisation des services.

11.1.4 Assistance et prolifération accrue des maliciels

Les fournisseurs TSP disposent normalement d'un service d'assistance pour répondre aux réclamations de ses clients et fournir aux utilisateurs finals l'assistance et la prise en charge techniques dont ils ont besoin pour surmonter leurs problèmes. Avec la prolifération accrue des maliciels sur l'Internet, les fournisseurs TSP recevront des rapports leur signalant des infections par maliciel et espiogiciel et les problèmes qui en découlent. De telles informations sont importantes et utiles pour les fournisseurs concernés, leur permettant d'évaluer les risques liés à ces infections et d'apporter des mises à jour aux outils nécessaires pour faire en sorte que tout nouveau maliciel ou espiogiciel détecté puisse être éliminé ou neutralisé efficacement. A cet égard, les fournisseurs TSP devraient prendre contact avec des fournisseurs de sécurité et leur soumettre les rapports en question avec des échantillons de maliciel pour suite à donner – notamment s'il semble y avoir un

[3] L'AntiSpyware Coalition, qui représente de multiples professionnels, propose elle aussi un ensemble de définitions et de critères publiés sur son site web. Pour de plus amples informations, voir l'Appendice I.

pic de prévalence. La plupart des fournisseurs tiennent à jour une liste de contacts auxquels de tels rapports/échantillons peuvent être envoyés par courrier électronique pour analyse et suite à donner. Voir, par exemple, le Tableau I.1.

11.1.5 Se tenir au courant des derniers progrès

Dans le cadre de l'implémentation du système ISMS-T, pour gérer les risques liés à la sécurité de l'information dans leur entreprise, ainsi que pour veiller à se tenir au courant des meilleures pratiques d'entreprise et des dernières failles de sécurité informatique et exploits/attaques, les fournisseurs TSP devraient participer à des associations professionnelles ou des forums d'entreprise compétents en la matière, pour mettre en commun leurs meilleures pratiques et tirer les enseignements de leur expérience mutuelle.

NOTE – Pour de plus amples informations, voir l'Appendice I.

11.2 Prescriptions de sûreté et sécurité pour les services d'hébergement de sites web

La plupart des fournisseurs TSP assurent des services d'hébergement de sites web sur leurs réseaux et dans leurs centres de données, dans le cadre de leurs services commerciaux. Ces services seront accessibles aux utilisateurs finals/abonnés et/ou à de petites entreprises une fois restructurés par les abonnés des services d'hébergement de sites web et revendus aux utilisateurs finals. Au cas où les abonnés des services d'hébergement de sites web mettraient en place un serveur non sûr, ou hébergeraient des contenus malveillants dans leurs sites web, la sûreté et la sécurité des utilisateurs finals en pâtiraient. En conséquence, il importe que les fournisseurs TSP définissent, dans le cadre de leurs meilleures pratiques, une norme minimale de sûreté et de sécurité que devront respecter les abonnés des services d'hébergement de sites web en vertu des termes de l'accord.

Les termes de l'accord devraient inclure les éléments suivants:

a) Des notes d'information claires, indiquant les pratiques du site web en matière de sécurité et de protection des données personnelles, les pratiques en matière de collecte de données, et le comportement de tout code (BHO, *browser helper object*, par exemple) que le site web peut distribuer et activer dans l'ordinateur de bureau des utilisateurs finals ou dans l'environnement du navigateur web.

b) Le consentement de l'utilisateur, qui favorise l'acceptation ou la non-acceptation par celui-ci des conditions d'utilisation des services énoncées dans les notes d'information susmentionnées. Les utilisateurs auraient ainsi toute latitude de se déterminer librement et, en conséquence, de décider s'ils peuvent accepter les conditions d'utilisation des services.

c) Des contrôles utilisateurs, permettant aux utilisateurs de modifier leurs paramètres ou, à défaut, de dénoncer leur acceptation à tout moment à compter de la date de la conclusion de l'accord initial.

Les termes des accords sont importants pour s'assurer que les utilisateurs finals sont bien informés du comportement et des pratiques du site web, en ce qui concerne la sûreté, la protection des données personnelles et la sécurité des utilisateurs finals. Les termes des accords devraient être mis au point avec l'aide d'un juriste pour veiller à ce qu'ils prévoient également le remboursement des éventuels frais judiciaires engagés par le fournisseur TSP pour défendre des utilisateurs finals ayant subi des pertes ou des dommages déterminés imputables à des contenus malveillants ou à des politiques et des pratiques peu claires sur le site web.

Outre les dispositions relatives à la protection des données, au respect de la vie privée et à la sécurité sur les sites web, les fournisseurs TSP devraient imposer aux sites web qu'ils hébergent sur leur réseau l'obligation d'appliquer un ensemble de mesures de sécurité conformes aux meilleures pratiques au niveau de l'application, avant d'autoriser ces sites web à entrer en service. Ces mesures de sécurité devraient notamment porter sur les éléments suivants:

a) Principes de développement de sites web sécurisés et pratiques de codage de pages web, à savoir:

   i) affichage de brèves notes d'information sur le respect de la vie privée, indiquant clairement, sous la forme d'un résumé succinct d'une page (en langage profane) les pratiques essentielles de l'entreprise en matière de protection des données personnelles en ligne. Les utilisateurs seront ainsi à même de faire des choix en meilleure connaissance de cause en ce qui concerne le partage de leurs informations en ligne. Ces brèves notes d'information devraient être conformes à toutes les dispositions réglementaires et comporter des liens vers des déclarations juridiques exhaustives (mentions légales) et d'autres informations utiles, de manière que les clients qui souhaitent de plus amples précisions puissent passer d'un lien à l'autre pour consulter la version intégrale. Une note d'information unique donnera aux utilisateurs une vue d'ensemble plus cohérente des droits de propriété de l'entreprise, répondant aux mêmes normes et aux mêmes attentes en matière de protection des données personnelles que beaucoup de sites;

   ii) traitement sécurisé des cookies;

   iii) validation et traitement sécurisés des données d'entrée pour éviter les attaques courantes telles que les attaques par injection SQL. Etant donné que les sites web qui sont de plus en plus fréquentés sont utilisés pour distribuer des codes malveillants, il faut valider les données d'entrée et les données de sortie aussi bien sur le contenu actif que sur le contenu dynamique;

   iv) scriptage sécurisé de pages web pour éviter les attaques courantes telles que les attaques par scriptage CSS (*cross-site scripting*);

   v) contrôle et test de sécurité des codes.

Dans le cadre de l'infrastructure d'hébergement de sites web du fournisseur TSP, les mesures de sécurité suivantes devraient également être prises pour protéger les serveurs web contre tout accès non autorisé et dans le cas où ces serveurs sont mis en péril par des contenus malveillants qu'ils hébergent, tels que des logiciels trompeurs ou des logiciels espions:

b) Configurer le serveur web, y compris les systèmes d'exploitation sous-jacents, conformément à un guide de configuration de sécurité de base. Cette opération devrait consister à bien définir les utilisateurs du serveur web par rapport aux administrateurs, à appliquer des contrôles d'accès au programme et aux répertoires et fichiers de systèmes, et à produire des traces d'audit, notamment, pour la sécurité et d'autres pannes du système. Il est en outre recommandé d'installer sur le serveur un système minimal afin de réduire le vecteur d'attaque.

c) Implémenter un système d'essai et de déploiement de mises à jour de sécurité, et veiller à ce que les systèmes d'exploitation et les applications du serveur web soient tenus à jour sans retard chaque fois que de nouvelles mises à jour de sécurité sont disponibles.

d) Surveiller la qualité de fonctionnement du serveur web, en termes de sécurité, par un examen régulier des traces d'audit.

e) Installer un antivirus et un anti-espiogiciel sur le serveur.

f) Analyser régulièrement tous les contenus hébergés et téléchargés selon les définitions à jour. Etre conscient qu'un fichier peut toujours être un espiogiciel ou un maliciel même si les définitions en vigueur non pas permis de le détecter, en raison des limitations inhérentes au caractère imparfait des informations.

g) Procéder régulièrement à des essais de pénétration des sites web pour s'assurer que leur sécurité est dûment préservée et qu'ils n'ont pas été mis en péril par des criminels.

Pour permettre d'appliquer ces mesures de sécurité, notamment celles qui ont trait à la sécurité des sites web, les fournisseurs TSP devraient songer à incorporer ces dispositions dans l'accord relatif aux conditions d'utilisation des services.

11.3 Conseils à l'intention des utilisateurs finals en matière de sûreté et de sécurité

11.3.1 Conseils et informations à l'intention des utilisateurs

Fourniture de conseils sur la manière de surfer en ligne en toute sécurité. Les fournisseurs TSP peuvent soit conseiller directement les utilisateurs, soit les inviter à consulter des sites de conseils pouvant les renseigner. Il est indispensable de sensibiliser les utilisateurs finals à la manière dont ils peuvent contribuer à la sécurité sur Internet. Comme exemples d'informations ou d'activités utiles, on peut citer:

a) Bulletin d'information périodique (mensuel, par exemple) consacré aux questions de sécurité, donnant des conseils sur certaines techniques de sécurité (comment choisir un bon mot de passe, par exemple); mises à jour des tendances en matière de sécurité; notes d'information sur la sécurité des diffusions sur le web, et autres vidéos à la demande, diffusions audio, et informations de sécurité accessibles via le portail web du fournisseur TSP ou d'autres fournisseurs de contenus de sécurité.

b) Diffusion directe de vidéos à la demande visant à sensibiliser les utilisateurs à la sécurité et/ou diffusions sur le web consacrées à diverses questions de sécurité visant à sensibiliser les utilisateurs finals à ces questions et à améliorer leurs pratiques dans le domaine de la sécurité.

c) Incorporation d'une rubrique consacrée à la sécurité dans la version papier du Bulletin d'information du fournisseur TSP qui est envoyé à l'adresse privée ou professionnelle des utilisateurs finals, faisant la synthèse des principaux événements ou contenus liés à la sécurité.

d) Séminaires ou expositions itinérantes consacrés à la sécurité des utilisateurs finals, organisés annuellement ou selon une périodicité différente, le cas échéant en partenariat avec d'autres professionnels, fournisseurs et représentants des pouvoirs publics.

11.3.2 Mesures techniques de sécurité à prendre par les utilisateurs finals

Dans le cadre de la campagne d'information et de sensibilisation des utilisateurs aux mesures de sécurité à prendre pour se protéger contre les logiciels trompeurs et les espiogiciels, les fournisseurs TSP devraient donner des conseils aux utilisateurs finals sur les mesures techniques de sécurité à prendre pour protéger leurs systèmes contre les attaques et les exploits (programme permettant d'exploiter une faille de sécurité informatique) connus. Il convient de recourir aux mesures de protection minimales suivantes:

a) Utiliser des systèmes d'exploitation dernier cri, munis des modèles des plus récents de patchs de sécurité.

b) Utiliser des outils antivirus et anti-espiogiciel. Si possible, les fournisseurs TSP devraient s'associer à des fournisseurs de sécurité[4] pour offrir ces outils dans le cadre de leur offre groupée d'abonnement afin que les mesures de sécurité soient offertes au moment de la signature, ou du renouvellement, de l'abonnement.

c) Activer un blocage des fenêtres intruses. Les barres d'outils courantes de navigateur web et de navigateur incorporent désormais cette capacité, qui empêchera les sites web malveillants d'afficher des fenêtres contenant des espiogiciels ou des logiciels trompeurs

[4] Les fournisseurs de sécurité peuvent être les partenaires commerciaux des fournisseurs TSP et/ou des fournisseurs dont les produits et les services ont été jugés conformes aux politiques et prescriptions de sécurité des fournisseurs TSP.

qui pourraient exploiter les failles de sécurité informatique du système ou du navigateur ou de recourir à l'ingénierie sociale pour inciter les utilisateurs, en abusant de leur confiance, à télécharger ces espiogiciels ou logiciels trompeurs dans leurs systèmes. Il convient de dresser une liste des outils recommandés pour bloquer les fenêtres intruses, et d'en favoriser l'utilisation en précisant leurs modalités d'activation et la manière de procéder pour permettre l'affichage des fenêtres intruses à partir de sites web, avec l'autorisation des utilisateurs.

d) Activer des pare-feu personnels. Les pare-feu personnels sont un autre outil des plus utiles pour contrôler l'accès des services de réseau aux systèmes utilisateurs, et vice versa. Un certain nombre des systèmes d'exploitation les plus récents sont munis d'origine de pare-feu personnels. Bien qu'ils soient activés par défaut, ces pare-feu peuvent être désactivés par les utilisateurs ou par d'autres applications, ce qui risque de compromettre inopinément la sécurité du réseau. Les fournisseurs TSP devraient préconiser l'utilisation de pare-feu personnels, et/ou proposer d'autres produits analogues tiers dont ils ont testé la fiabilité, et former les utilisateurs pour les aider à mettre en œuvre une sécurité de réseau de base au niveau des systèmes des utilisateurs finals.

e) Activer des mises à jour automatiques. Bien qu'elles soient en mesure de faire face aux pires logiciels malveillants, aux différents niveaux où elles interviennent, les mesures techniques de sécurité susmentionnées ne sont pas très efficaces contre l'exploitation des failles de sécurité informatique qui existent dans les systèmes d'exploitation et les logiciels d'application. Pour éviter l'exploitation de telles failles, les fonctions de mise à jour offertes dans le système d'exploitation, ainsi que par des applications dont la fiabilité a été testée par l'utilisateur (un tiers de confiance, par exemple, dans le cas de produits anti-espiogiciels et antivirus), devraient être activées pour permettre l'exécution de mises à jour automatiques. Cela permettrait ensuite d'assurer la mise à jour des systèmes à l'aide des derniers modèles de patchs de sécurité, lorsqu'on peut en trouver, supprimant ainsi l'intervalle de temps mis à profit pour exploiter la faille de sécurité informatique.

On trouvera dans l'Appendice I une liste de références et de ressources en ligne utiles aux fins de l'application des recommandations susmentionnées.

Appendice I

Ressources supplémentaires

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

I.1 Références relatives à la sécurité en ligne et aux anti-espiogiciels

Il existe un certain nombre de sites web que l'on pourra consulter utilement pour obtenir de plus amples informations au sujet de la sûreté et de la sécurité sur Internet, à savoir:

- **AntiSpyware Coalition** (http://www.antispywarecoalition.org/) – Groupe qui s'emploie à dégager un consensus sur les définitions et les meilleures pratiques dans le débat autour des espiogiciels et autres technologies potentiellement indésirables. Composé de représentants des fabricants d'anti-espiogiciels, du monde universitaire et de groupes de consommateurs, l'ASC vise à faire la synthèse de toute une série de points de vue sur le problème du contrôle des espiogiciels et des autres technologies potentiellement indésirables.
- **Be Web Aware (WebAverti)** (http://www.bewebaware.ca) – Programme national bilingue de sensibilisation du public à la sécurité sur Internet, conçu pour faire en sorte que les jeunes Canadiens tirent parti de l'Internet, tout en naviguant en toute sécurité et en étant responsable de leurs activités en ligne.
- **Center for Safe and Responsible Internet Use** (http://csriu.org) – Organisation offrant des services de vulgarisation sur les questions relatives à l'utilisation de l'Internet en toute sécurité et de manière responsable.
- **Childnet International** (http://www.childnet-int.org) – Organisation à but non lucratif qui travaille en partenariat avec d'autres organisations dans le monde entier afin d'aider à faire de l'Internet un lieu fantastique et sûr pour les enfants.
- **ECPAT** (http://www.ecpat.net) – Réseau international d'organisations travaillant ensemble afin d'éradiquer la prostitution enfantine, la pornographie enfantine et le trafic d'enfants à des fins sexuelles.
- **GetNetWise** (http://www.getnetwise.org) – Service public offert par une coalition d'entreprises spécialisées dans l'Internet et d'organisations d'intérêt public soucieuses de faire en sorte que les utilisateurs ne soient qu'à un clic de distance des ressources dont ils ont besoin pour décider en connaissance de cause de l'usage qu'eux et leurs familles souhaitent faire de l'Internet.
- **Global Infrastructure Alliance for Internet Safety** (GIAIS) (http://www.microsoft.com/security/msra/default.mspx) – Alliance de fournisseurs de services, qui se sont organisés pour améliorer la sécurité et la sûreté sur le web, gérer de manière cohérente les menaces de toutes sortes, et identifier les failles existantes en vue de les réduire.
- **INHOPE** (http://inhope.org) – Association internationale qui a pour mission de faciliter la tâche des hotlines Internet dans les efforts qu'elles déploient pour donner suite aux rapports signalant des contenus illégaux afin de rendre l'Internet plus sûr.
- **Internet Safety Group (**www.netsafe.org.nz) – Le site web NetSafe est la page d'accueil en ligne de l'Internet Safety Group (ISG) de Nouvelle-Zélande et de Hector Protector.
- **International Centre for Missing & Exploited Children** (http://www.icmec.org) – Organisation mondiale qui œuvre pour la sécurité et le bien-être des enfants par l'action militante, l'élaboration de politiques et la coordination multinationale au service de la défense de leurs droits.
- **Interpol** (http://www.interpol.int) – Organisation internationale de police criminelle qui facilite la coopération transfrontalière entre les services de police, et apporte un appui et

une assistance à tous les services, organisations et autorités ayant pour mission de prévenir et de combattre la criminalité internationale.

- **iSafe** (http://www.isafe.org) – Leader mondial en matière de sensibilisation du public à la sécurité sur Internet; intègre dans le programme des études une action d'information dynamique de proximité auprès des élèves, des enseignants, des parents, des responsables de la lutte contre la cybercriminalité et des adultes afin de leur donner des moyens d'agir pour rendre l'Internet plus sûr.
- **Microsoft Security At Home** (http://www.microsoft.com/protect) – Informations et ressources visant à aider les utilisateurs à protéger leurs ordinateurs, à se protéger eux-mêmes et à protéger leurs familles.
- **National Council for Motherhood and Childhood** (http://www.nccm.org.eg) – Organisation égyptienne ayant pour mission d'assurer la protection de l'enfance et de la maternité du point de vue du droit.
- **Net Family News** (http://netfamilynews.org) – Service public à but non lucratif qui propose un forum de discussion et la rubrique kid-tech news destinée aux parents et aux éducateurs de plus de 50 pays.
- **NetAlert Limited** (http://www.netalert.gov.au) – Organisation locale à but non lucratif créée par les pouvoirs publics australiens pour former les utilisateurs aux méthodes de gestion de l'accès aux contenus en ligne et leur donner des conseils indépendants.
- **NetSmartzKids** (http://www.netsmartzkids.org) – NetSmartz est un didacticiel interactif sur la sécurité édité par le National Center for Missing & Exploited Children (NCMEC) et Boys & Girls Clubs of America (BGCA) à l'usage des enfants et des jeunes de 5 à 17 ans, des parents, des tuteurs, des éducateurs et des responsables de la lutte contre la cybercriminalité, proposant des activités en 3D adaptées à chaque tranche d'âge pour apprendre aux enfants à naviguer en toute sécurité sur Internet.
- **Safe Kids Worldwide** (http://www.safekids.org) – Réseau mondial d'organisations ayant pour mission de prévenir les blessures accidentelles chez les enfants, une des premières causes de mortalité chez les jeunes de 0 à 14 ans.
- **SafeKids.com** (http://www.safekids.com) – Ressources visant à aider les familles à faire de l'Internet une technologie distrayante, sûre et utile.
- **StaySafe.org** (http://www.staysafe.org) – Site éducatif visant à sensibiliser les utilisateurs tant aux aspects positifs de l'Internet qu'aux méthodes de gestion des divers problèmes de sûreté et de sécurité auxquels ils seront confrontés en ligne.
- **UNICEF** (http://www.unicef.org) – Première organisation mondiale de défense des droits de l'enfant, ayant pour mission de fournir une assistance humanitaire, et en matière de développement, à long terme aux enfants et à leurs parents dans les pays en développement.
- **WebSafe Crackerz** (http://www.websafecrackerz.com) – Jeux et puzzles interactifs conçus pour aider les adolescents en leur proposant des stratégies pour faire face à différentes situations en ligne, dont le spam, le hameçonnage (phishing) et les scams.

I.2 Liste type de contacts auxquels la multiplication des incidents informatiques peut être signalée

Le Tableau I.1 contient une liste type de contacts auxquels la multiplication des incidents informatiques affectant la sûreté et la sécurité sur Internet peut être signalée:

Tableau I.1 – Liste type de coordonnées d'organisations à contacter pour signaler la multiplication des incidents informatiques affectant la sécurité

Organisations	Contact
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/about/organization/teams/
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html

Bibliographie

[b-UIT-T X.1051] Recommandation UIT-T X.1051 (2004), *Système de gestion de la sécurité de l'information – Prescriptions pour les télécommunications (ISMS-T).*

[b-ISO/CEI 27001] Norme ISO/CEI 27001:2005, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences*. http://www.iso.org/iso/catalogue-detail?csnumber=42103

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2009