Transport Canada Transports Canada

BULLETIN OPÉRATIONNEL DE SÛRETÉ MARITIME

Nº : 2021 - 001

EXIGENCES EN MATIÈRE DE SIGNALEMENT DES MENACES, INFRACTIONS ET INCIDENTS DE CYBERSÉCURITÉ ET DE SIGNALEMENT VOLONTAIRE DE LA CYBERACTIVITÉ SUSPECTE / SGDDI No. 15495583

OBJET

L'objectif de ce bulletin est de donner des directives sur les méthodes qui permettent de satisfaire aux exigences en matière de signalement lié aux menaces, infractions et incidents de cybersécurité et de signalement volontaire de la cyberactivité suspecte.

Ce bulletin appuie le BOSM 2014-001, *Clarification des exigences en matière de signalement obligatoire de menaces, d'infractions et d'incidents relatifs à la sûreté maritime de Transports Canada (TC)* et le BOSM 2016-002, *Le signalement d'activité suspecte*, et doit être lu en conjonction avec ces derniers. Le présent bulletin s'applique aux intervenants visés par le *Règlement sur la sûreté du transport maritime* (RSTM), le *Règlement sur la sûreté des traversiers intérieurs* (RSTI), la *Mesure de sûreté sur les navires de croisière et les terminaux pour navires de croisière*, la *Mesure de sûreté visant les rassemblements désignés de grands voiliers*, ainsi que la *Mesure de sûreté visant les grands voiliers et les installations maritimes ayant des interfaces avec des grands voiliers*, ci-après appelés les « intervenants réglementés ».

De plus, ce bulletin présentede l'information et de la sensibilisation au sujet des autres ressources que les intervenants réglementés peuvent utiliser en cas d'incident de cybersécurité, comme le Centre canadien pour la cybersécurité (Centre de cybersécurité) et de l'information sur d'autres exigences fédérales en matière de signalement applicables aux intervenants de l'industrie, particulièrement en ce qui concerne les infractions de cybersécurité qui concernent la protection des renseignements personnels, comme l'a établi le Commissariat à la protection de la vie privée du Canada (CPVP).

CONTEXTE

L'industrie maritime est devenue de plus en plus tributaire de la cybertechnologie, pour presque tous les aspects du transport maritime. La prolifération des cybersystèmes à l'échelle du réseau de transport maritime continue de transformer le paysage des risques, car les cyberrisques représentant une portion croissante de tous les risques de sûreté auxquels font face les intervenants maritimes. Par conséquent, le signalement rapide et uniforme des menaces, des infractions et des incidents de cybersécurité est essentiel à la compréhension, à l'amélioration et au maintien de la sûreté du réseau de transport maritime du Canada.

La nature ambiguë et le nombre de menaces, d'infractions et d'incidents de cybersécurité font en sorte qu'il est difficile, pour les intervenants, de déterminer les cas à signaler. Par exemple, en raison de l'interconnectivité des cybersystèmes, il n'est pas toujours évident d'évaluer l'impact

ou la gravité d'une menace, d'une infraction ou d'un incident. En outre, la possibilité d'une cyberattaque de masquer sa véritable intention et le volume considérable d'événements potentiels et concrétisés peuvent exacerber la détermination des cas à signaler. Transports Canada reconnaît ces difficultés de signalement et s'attend à ce que les intervenants réglementés fassent preuve de jugement, misent sur leur expérience et utilisent les documents d'orientation mis à disposition dans le présent bulletin, lors de la siganlisation d' événements.

Transports Canada traite tous les signalements de menaces, d'infractions et d'incidents de sûreté, de même que les signalements d'activités suspectes, comme des renseignements délicats pour la sûreté, qu'il s'agisse d'un événement physique ou informatique. Une fois que l'information est signalée, Transports Canada la communique, au besoin, aux organismes d'application de la loi et aux partenaires de la sécurité publique compétents, en fonction des risques cernés pour le Canada. L'information provenant des signalements de menaces, d'infractions et d'incidents de sûreté, de même que celle provenant des signalements d'activités suspectes, permet également à Transports Canada d'identifier des tendances, de prendre des décisions pendant l'examen des menaces potentielles qui peuvent être mises en évidence et d'aider les personnes responsables de la conception des évaluations de sûreté des intervenants réglementés.

DÉFINITIONS

Le BOSM 2014-001, *Clarification des exigences en matière de signalement obligatoire de menaces, d'infractions et d'incidents relatifs à la sûreté maritime de Transports Canada (TC)*, donne des conseils pour l'interprétation des définitions de ***menace contre la sûreté***, **d'*infraction à la sûreté*** et **d'*incident de sûreté,*** comme l'indique le paragraphe 1(1) du RSTM et du RSTI. Le BOSM 2016-002, *le signalement d'activité suspecte* comprend une définition du terme ***activité suspecte.***

Menace contre la cybersécurité : Type de *menace contre la sûreté* (voir le paragraphe 1(1) du RSTM, le paragraphe 2(1) du RSTI et le BOSM 2014-001) – tout acte ou circonstance suspect concernant la collecte, la perturbation, le refus, la détérioration ou la destruction d'une ressource du système d'information ou de l'information elle-même qui pourrait compromettre la sûreté d'un bâtiment, d'une installation maritime, d'un port, d'un traversier intérieur, d'une installation de traversier intérieur ou du réseau de l'interface et l'information transmise par le réseau

Infraction à la cybersécurité : Type d'*infraction à la sûreté* (voir le paragraphe 1(1) du RSTM, le paragraphe 2(1) du RSTI et le BOSM 2014-001) – violation d'une mesure, d'une règle ou d'une procédure de sûreté donnant lieu à un accès non autorisé à des données, des applications, des services, des réseaux et/ou des appareils, mais qui ne cause pas d'incident de sécurité.

Incident de cybersécurité:Type d'*incident de sûreté* (voir le paragraphe 1(1) du RSTM, le paragraphe 2(1) du RSTI et le BOSM 2014-001) – événement au cours duquel la sûreté d'un bâtiment, d'une installation maritime, d'un port, d'un traversier intérieur, d'une installation de traversier intérieur ou d'une interface est compromise à la suite d'une attaque qui modifie, détruit, supprime ou rend inaccessible tout réseau informatique ou ressource du système.

Cyberactivité suspecte : Type d'*activité suspecte* (voir le BOSM 2016-002) – activité menée dans les systèmes informatiques d'un bâtiment, d'une installation maritime, d'un port, d'un traversier intérieur, d'une installation de traversier intérieur ou d'une interface qui ne correspond pas à un modèle de comportement normal (c.-à-d. si la précision, le volume, la persistance ou la sophistication de l'activité ou de l'attaque sort de l'ordinaire). Par exemple, même si les cyberactivités malveillantes comme les attaques d'hameçonnage et le balayage de réseau font souvent partie du paysage normal des technologies de l'information, les attaques plus ciblées (p. ex. campagnes d'hameçonnage ciblé) ou plus intenses (p. ex. augmentation marquée des balayages de réseau) sont plus justement classées comme étant des activités suspectes. La détermination des cyberactivités suspectes dépend toujours du contexte.

Événement de cybersécurité : Un changement à la cybersécurité qui peut avoir une incidence sur l'exploitation d'un bâtiment, d'une installation maritime, d'un port, d'un traversier intérieur, d'une installation de traversier intérieur ou d'une interface opérationnelles, y compris la mission, les capacités ou la réputation. Les événements de cybersécurité comprennent les menaces, infractions et incidents relatifs à la cybersécurité, de même que les cyberactivités suspectes.

DIRECTIVES

Les intervenants réglementés doivent utiliser le présent bulletin pour évaluer et signaler les menaces, infractions et incidents relatifs à la cybersécurité. Les intervenants réglementés peuvent également utiliser ce bulletin pour évaluer et signaler la cyberactivité suspecte.

1. Pour les administrations portuaires, les installations maritimes, les installations maritimes à usage occasionnel et les installations de traversier intérieur

Les intervenants réglementés doivent signaler toutes les menaces, et les infractions et les incidents relatifs à la cybersécurité survenant lors d'interfaces entre une installation maritime et /ou installation maritime a usage occasionel, et/ou une installation pour traversiers, et/ou un port, et/ou un batiment, incluant les traversiers, et/ou un grand voilier; auprès des organismes d'application de la loi compétents, à Transports Canada et, s'il y a lieu, à l'administration portuaire le plus tôt possible après les faits, afin qu'une enquête soit menée. Les intervenants réglementés doivent également examiner et vérifier que tous les plans et toutes les procédures et mesures de protection techniques en matière de sûreté sont à jour et ne sont pas liés à la cause du cyberévénement.

Les intervenants réglementés sont encouragés à signaler la cyberactivité suspecte à Transports Canada dès que possible.

2. Pour les bâtiments, traversiers intérieurs et grands voiliers battant pavillon canadien

Les menaces et incidents relatifs à la cybersécurité doivent être signalés au capitaine, à l'agent de sûreté de l'entreprise, aux organismes d'application de la loi compétents, à Transports Canada et, s'il y a lieu, à l'administration portuaire, le plus tôt possible. En ce qui a trait aux bâtiments

battant pavillon canadien assujettis au RSTM qui sont exploités en eaux étrangères, ces exigences de signalement doivent être respectées, quel que soit l'emplacement du bâtiment. Les infractions à la cybersécurité doivent également être signalées à Transports Canada le plus tôt possible après les faits, peu importe l'emplacement du bâtiment, du traversier ou du grand voilier. Les intervenants réglementés doivent également examiner et vérifier que tous les plans et toutes les procédures et mesures de protection techniques en matière de sûreté sont à jour et ne sont pas liés à la cause du cyberévénement.

Les intervenants réglementés sont encouragés à signaler la cyberactivité suspecte à Transports Canada dès que possible. Dans le cas des navires qui suivent les lignes directrices de l'Organisation maritime internationale (OMI) sur la gestion des cyber-risques maritimes (MSC-FAL.1/Circ.3), les exigences énoncées dans le MTSR (c'est-à-dire les articles 212, 218 et 229(k)), remplacent ces lignes directrices. Cette approche est conforme à la recommandation du Comité de la sécurité maritime de l'OMI selon laquelle le Code international pour la sûreté des navires et des installations portuaires ne devrait pas exiger qu'un navire établisse un système de gestion de la cybersécurité distinct qui fonctionne en parallèle avec un système de gestion de la sécurité des navires (CSM 101/WP.1/Add.1) ; et, réaffirme la résolution MSC.428(98) et les exigences organisationnelles pour les administrations afin de garantir que les cyber-risques sont traités de manière appropriée.

CONSEILS SUR LE SIGNALEMENT

1) Administrer l'évaluation de l'impact interne de l'événement de cybersécurité

Bien qu'il puisse être difficile de déterminer la portée et l'incidence d'un événement de cybersécurité (et de savoir s'il correspond à la définition ou au seuil selon lesquels il est considéré comme une menace, un incident ou une infraction), nous encourageons les intervenants réglementés à envisager des cybersystèmes qui exécutent une fonction essentielle ou qui sont reliés aux mesures de protection, aux processus ou aux procédures de sûreté décrits dans le plan de sûreté de l'installation ou du bâtiment.

Pour déterminer si l'événement de cybersécurité doit être signalé, l'intervenant réglementé doit déterminer si cet événement :

- a contourné des politiques, des mesures de protection, des mesures ou procédures de sûreté établies, quelle que soit la nature de l'événement (intentionnel ou accidentel) et ce, peu importe si la sûreté d'un bâtiment, d'une installation ou d'un port a été compromise;
- avait la possibilite de menacer ou de compromettrel'intégrité de la sûreté de l'installation réglementée ou du bâtiment ou l'intégrité des biens et de l'infrastructure;
- pourrait avoir une incidence sur des bâtiments, des installations ou des ports, ou sur leur exploitation;

- pourrait avoir une incidence sur la sûreté nationale ou la sûreté générale et sur le fonctionnement constant du réseau de transport maritime et de son infrastructure;
- nécessite une liaison et une coordination avec les communautés de réglementation, de sûreté ou du renseignement;
- nécessite la présence d'un inspecteur de la Sûreté maritime de TC ou une discussion avec lui (pour donner une orientation réglementaire);
- a créé la nécessité de mettre en place d'autres mesures de protection de la sûreté;
- a affaibli la capacité d'un intervenant réglementé de mettre entièrement en œuvre son plan de sûreté maritime.

Transports Canada reconnaît qu'aucune description ne peut tenir compte de tous les événements possibles et s'attend donc à ce que les intervenants réglementés fassent preuve de jugement, misent sur leur expérience et utilisent les documents d'orientation fournis pour déterminer à quel moment il faut signaler les événements. S'ils sont incertains de devoir signaler un événement de cybersécurité, les intervenants réglementés sont encouragés à faire preuve de prudence et à signaler l'événement.

L'**ANNEXE A** présente un inventaire non exhaustif des événements de cybersécurité – menaces, infractions et incident relatifs à la cybersécurité y compris des directives de signalement pour chaque événement.

2) **Signaler toutes les menaces, s infractions et tous les incidents relatifs à la cybersécurité à l'organisme d'application de la loi compétent et à l'administration portuaire ou à l'agent de sécurité de l'entreprise (s'il y a lieu) , conformément aux exigences réglementaires (RSTM, RSTI).**

L'**ANNEXE A** présente un inventaire non exhaustif des événements de cybersécurité – menaces, infractions et incidents relatifs à la cybersécurité – devant être signalés (et auprès de quelles personnes).

3) **Signaler une menace, une infraction ou un incident relatif à la cybersécurité ou une cyberactivité suspecte à Transports Canada, conformément aux exigences réglementaires (RSTM, RSTI).**

Nous vous informons que les menaces, infractions, incidents relatifs à la cybersécurité et les cyberactivités suspectes doivent être signalés au Centre d'intervention national de Transports Canada (CITC), en utilisant les coordonnées ci-dessous :

Centre d'intervention national de Transports Canada

1-888-857-4003 (sans frais au Canada et aux États-Unis) ou 1-613-995-9737 (toutes les autres régions).

Le CITC est exploité en tout temps.

Les rapports de suivi ou la documentation peuvent être transmis par courriel à Sitcen@tc.gc.ca, accompagnés d'une copie conforme à votre bureau régional de la sûreté maritime de TC.

Les intervenants doivent fournir les renseignements suivants lors d'un signalement :

- Nom de l'organisme ou de la source de l'information (nom, numéro de téléphone, adresse de courriel)
- Date et heure de l'incident
- Date et heure du signalement (le cas échéant, lorsque l'information est reçue d'une source secondaire)
- Lieu de l'incident (province, ville, nom de l'installation maritime, emplacement dans l'installation ou le bâtiment où l'incident s'est produit et lenom de l'administration portuaire, s'il y a lieu)
- Description de l'activité (décrire le cyberévénement, les réseaux touchés, l'incidence sur la sûreté, etc.)
- Mesures prises par l'intervenant ayant fait le signalement
- Autres personnes ayant été informées
- Autres renseignements pertinents

Lors d'un signalement initial, il n'est pas nécessaire de discuter des détails des vulnérabilités de sûreté révélées par l'incident. Transports Canada collaborera avec la source du signalement et d'autres autorités compétentes pour faire enquête et donner suite au signalement.

4) Envisager de signaler les incidents de cybersécurité à l'organisme locale d'application de la loi compétent au Centre canadien pour la cybersécurité.

Les intervenants réglementés et les autres intervenants sont encouragés à signaler les incidents de cybersécurité à l'organisme d'application de la loi ainsi qu'au Centre pour la cybersécurité. Transport Canada recommande aux intervenants d'envisager de signaler les évènements de cybersécurité aux organismes d'application de la loi dans leur juridiction, car ils ont intérêts à entendre les personnes directement touchées par les évènements de cybersécurité. Cela permet d'ouvrir une enquête, qui ne peut être lancée par les parties concernées. De plus, l'ouverture d'une enquête liée à un incident de cybersécurité est une étape importante et critique pour déterminer éventuellement la source et la cause de l'attaque, et peut contribuer à prévenir d'autres attaques de même nature.

Au sein du Centre de la sécurité des télécommunications, le Centre canadien pour la

cybersécurité (Centre pour la cybersécurité) est l'autorité canadienne en matière de cybersécurité. Le Centre pour la cybersécurité est la seule source unifiée de conseils d'expert, d'orientation, de services et de soutien en matière de cybersécurité. Le Centre pour la cybersécurité est exploité 24 heures par jour, 7 jours par semaine par un personnel présent au centre 15 heures par jour et sert les organismes d'infrastructures essentielles au Canada.

Le rôle du Centre pour la cybersécurité est d'aider les organismes d'infrastructures essentielles du Canada à protéger leurs cybersystèmes contre la compromission. Il offre gratuitement de l'aide aux intervenants afin de les aider à prévenir, à atténuer et à détecter les cyberactivités malveillantes.

Les agents de sûreté des ports, des installations maritimes, des bâtiments et des grands voiliers, les exploitants de bâtiments et le personnel des installations, des ports et de l'industrie qui remarquent des activités inhabituelles dans leurs systèmes, qui découvrent un virus mis en place par un logiciel malveillant ou sont la cible d'autres types de cyberévénements sont encouragés à signaler ces activités au Centre pour la cybersécurité. L'information échangée avec le Centre pour la cybersécurité est rendue anonyme avant d'être partagée avec d'autres partenaires, et n'est partagée qu'avec la permission des organismes concernés. Le Centre pour la cybersécurité encourage également le signalement de tout événement où l'échange de renseignements avec la grande communauté électronique serait utile pour atténuer les cyberrisques pour le Canada et les Canadiens.

Centre canadien pour la cybersécurité (Centre pour la cybersécurité)

Sans frais : 1-833-292-3788

contact@cyber.gc.ca

5) Faire un signalement au Commissariat à la protection de la vie privée du Canada, s'il y a lieu.

Les intervenants réglementés doivent se familiariser avec les nouvelles exigences en matière de signalement établies par le Commissariat à la protection de la vie privée du Canada (CPVP). Depuis le 1er novembre 2018, les entreprises (petites et grandes) assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) doivent :

- signaler au Commissaire à la protection de la vie privée du Canada toute infraction à la protection de la sûreté qui sous-tend l'utilisation de renseignements personnels qui pourrait causer un préjudice aux personnes visées;
- informer les personnes concernées de ces infractions;
- conserver un registre de toutes les infractions.

Une violation des mesures de sécurité est définie dans la LPRPDE comme la perte, l'accès non autorisé ou la divulgation non autorisée de renseignements personnels découlant d'une violation des mesures de sécurité d'une organisation mentionnées à la clause 4.7 de l'Annexe 1 de la LPRPDE, ou du défaut d'établir ces mesures de protection.

Un Rapport d'atteinte à la LPRPDE est accessible dans le site Web du Commissariat à la protection de la vie privée du Canada (CPVP). Le site Web contient également des directives précises et d'autres documents de formation, notamment des conseils pour contenir et réduire les risques d'atteinte à la vie privée et sécuriser les renseignements personnels.

RENSEIGNEMENTS ADDITIONNELS

Le Centre pour la cybersécurité peut aider les organismes d'infrastructures essentielles canadiennes du secteur du transport maritime à protéger leurs cybersystèmes contre la compromission.

Un partenariat avec le Centre pour la cybersécurité permettra aux intervenants de l'industrie d'avoir accès à ce qui suit :

- Des experts de la cybersécurité, pour obtenir des conseils et du soutien en matière d'atténuation
- La capacité d'analyse des logiciels malveillants du Centre pour la cybersécurité
- Une perspective intersectorielle, pancanadienne et mondiale sur divers types d'activités malveillantes
- Des produits de sensibilisation sur les tendances en matière de cybersécurité
- La compréhension unique du cyberespace au Canada que possède le Centre pour la cybersécurité
- Une aide dans la prévention des cyberévénements, grâce à l'échange autorisé d'information anonymisée avec d'autres partenaires

Pour devenir un partenaire et vous inscrire à la liste de diffusion, communiquez à l'adresse suivante : contact@cyber.gc.ca.

Certains produits du Centre pour la cybersécurité sont disponibles dans le site Web publique du Centre pour la cybersécurité. De plus, le Centre pour la cybersécurité dispose d'un portail de communauté sécurisé pour ses partenaires des secteurs public et privé. Vous trouverez également des renseignements et des conseils supplémentaires, ainsi que des alertes et des avis émis par le Centre pour la cybersécurité au sujet des cybermenaces, vulnérabilités ou incidents potentiels, imminents ou réels qui ont une incidence sur les infrastructures essentielles du Canada.

Dans le portail de communauté, on y trouve tous les produits du Centre pour la cybersécurité, y compris ceux qui ne sont pas affichés dans le site Web public, ainsi que d'autres outils conçus pour améliorer l'atténuation des incidents pour les partenaires. Le portail propose également une

série de sites séparés (aussi appelés sous-sites) organisés par secteur ou par communauté d'intérêts.

QUESTIONS

Si vous avez des questions, des préoccupations ou des commentaires au sujet du présent BOSM, adressez-les par courriel au directeur, Opérations de sûreté maritime, à dirops.marsec-sumar@tc.gc.ca.

Malick Sidibé
Directeur, Opérations de sûreté maritime
4 mars 2021

ANNEXE A – ÉVÉNEMENTS DE CYBERSÉCURITÉ

Lorsqu'il s'agit de déterminer si un cyberévénement doit être signalé ou non, il importe de tenir compte de l'incidence réelle ou potentielle de cet événement sur les cybersystèmes essentiels. Voici une liste de scénarios possibles.

Parmi les cyberévénements ayant une incidence considérable, mentionnons les suivants :

- Une attaque par déni de service (DS) soutenue et de grande envergure contre un cybersystème essentiel, qui rend celui-ci inaccessible aux exploitants et cause la perte d'une fonction essentielle.
- Une attaque sophistiquée et ciblée à l'aide d'un courriel d'hameçonnage ou d'un site Web de point d'eau visant à infecter les utilisateurs, qui se traduit par l'installation d'un logiciel malveillant sur leur ordinateur. Les auteurs malveillants utiliseraient ensuite cet ordinateur pour parcourir le réseau afin de le compromettre davantage et peut-être d'exfiltrer des données.
- Un utilisateur clique sur un lien ou une pièce jointe dans un courriel, ce qui provoque une attaque de rançongiciel, qui permet de chiffrer les fichiers et systèmes essentiels sur le réseau, causant ainsi la perte d'une fonction essentielle.
- Un système essentiel qui exécute une version vulnérable d'un logiciel, à l'égard duquel on a récemment annoncé qu'il présentait une vulnérabilité de sécurité mal gérée qui n'a pas été résolue (aussi appelée vulnérabilité du jour zéro), et qui est activement exploité par des auteurs malveillants.

Parmi les cyberévénements ayant une faible incidence, mentionnons les suivants :

- Une attaque sophistiquée et ciblée à l'aide d'un courriel d'hameçonnage ou d'un site Web de point d'eau infectant les utilisateurs, ce qui donne lieu à une infection par un logiciel malveillant. Même si le système a été compromis, si aucune autre exploitation n'a eu lieu, l'incidence potentielle de l'attaque est considérée comme faible.
- Courriels d'hameçonnage visant à installer un logiciel malveillant ciblant les justificatifs bancaires.

Voici une liste de scénarios de cyberrisques à signaler, ainsi que les méthodes par lesquelles un ordinateur peut répandre un virus (aussi appelé vecteur d'infection). Soulignons que cette liste n'est pas exhaustive et qu'elle ne doit être utilisée qu'à titre de référence.

Cyberscénarios à signaler		
Vecteurs	**Exemples**	**Définitions**
Support externe ou amovible	Logiciel malveillant diffusé à l'aide de supports amovibles infectés (p. ex. clé USB, DC ou disques durs amovibles, etc.)	

Attrition	Déni de service	Attaque qui empêche ou compromet la fonctionnalité autorisée normale des réseaux, systèmes ou applications en épuisant ses ressources. Cette activité comprend le fait d'être la victime d'un DS ou d'y participer involontairement.
	Rançongiciel	Un système ou un appareil informatique est infecté par un logiciel malveillant qui limite l'accès à celui-ci et exige que l'utilisateur paie une rançon pour éliminer la restriction.
	Force brute	Le pirate tente d'obtenir un accès non autorisé en vérifiant systématiquement toutes les clés ou les mots de passe possibles, jusqu'à ce qu'il trouve les bons.
Web	Attaques de point d'eau	Un site Web qu'un groupe ou un employé utilise souvent héberge un logiciel malveillant.
	Attaques d'applications Web et attaques par injection (injection de code : SQL, XSS)	Des applications Web personnalisées intégrées aux sites de médias sociaux sont utilisées pour installer un code malveillant sur les ordinateurs, dans le but d'obtenir un accès non autorisé.
	Téléchargement furtif	Un téléchargement furtif renvoie au téléchargement involontaire d'un virus ou d'un logiciel malveillant (maliciel) sur votre ordinateur ou votre appareil mobile.
Courriel	Attaques par hameçonnage ciblé	Les employés reçoivent un courriel ciblé qui a été conçu de façon à établir un lien de confiance factice et ainsi amener la victime à révéler certains secrets commerciaux ou personnels que l'adversaire peut exploiter.
	Attaques par hameçonnage	Les employés reçoivent des courriels frauduleux, apparemment légitimes, au moyen desquels l'auteur tente de recueillir des renseignements personnels et financiers auprès des destinataires. Habituellement, les messages semblent provenir de sites Web bien connus et fiables.
	Pourriels ou courriels infectés	Recevoir des messages de courriel

	non sollicités	non sollicités, non souhaités ou illégaux qui peuvent contenir une pièce jointe ou un lien infecté.
Utilisation inadéquate	Tout incident résultant de la violation d'une politique d'utilisation acceptable.	Par exemple, téléchargement de logiciels piratés dans le réseau de l'entreprise, installation de logiciels de partage de fichiers, etc.
Perte ou vol d'équipement	Perte ou vol d'un appareil informatique ou d'un support utilisé par l'organisme.	Par exemple, la perte ou le vol de l'ordinateur portable, du téléphone intelligent ou du jeton d'authentification d'un employé.
Autres	Programmes malveillants furtifs	Activation ou installation de logiciels malveillants de type furtif (p. ex. logiciels conçus pour cacher le fait qu'un système d'exploitation a été infecté, parfois par le remplacement des logiciels exécutables essentiels).
	Outil d'accès à distance (OAD)	Un logiciel doté de capacités d'administration à distance est infecté, ce qui permet à un pirate de contrôler l'ordinateur de la « victime ».
	Trousses d'exploitation	Trousse logicielle conçue pour fonctionner sur les serveurs Web dans le but de déterminer les vulnérabilités logicielles des appareils des clients qui communiquent avec elle, et de découvrir et d'exploiter les vulnérabilités pour télécharger et exécuter un code malveillant sur les appareils des clients.
	Virus et cheval de Troie	Programme conçu pour violer la sécurité d'un système informatique tout en exécutant apparemment une fonction inoffensive.
	Élévation des privilèges	Les bogues, défauts de conception ou erreurs de configuration dans un système d'exploitation ou une application logicielle sont exploités pour obtenir un accès plus grand aux ressources.
	Logiciel malveillant mobile	Logiciel malveillant qui cible les téléphones mobiles, les tablettes sans fil/cellulaires et les ordinateurs mobiles, en causant l'effondrement du système ou la perte ou la fuite d'information.
	Logiciel espion ou logiciel	Logiciel visant à recueillir des

	publicitaire trompeur	renseignements sur une personne ou sur un organisme à son insu.
	Reconnaissance et sondage	Cette catégorie d'incidents comprend toute activité visant à accéder à un ordinateur, à des ports ouverts, à des protocoles, à un service ou à une combinaison de ces derniers, en prévision d'une exploitation ultérieure. Cette activité n'entraîne pas nécessairement un compromis ou un déni de service.

Terme	Définition
Menace persistante avancée (MPA)	Adversaire possédant une très grande expertise et des ressources importantes qui poursuit des objectifs à long terme, s'adapte aux efforts des défenseurs pour lui résister et est déterminé à maintenir une présence sur le réseau ciblé.
Réseau de zombies	Un réseau de zombies est un ensemble d'ordinateurs infectés (« robots ») assujetti au contrôle d'un auteur malveillant.
Vulnérabilité du jour zéro	Une vulnérabilité du jour zéro (aussi appelée à heure zéro ou jour 0) est une vulnérabilité logicielle non divulguée que des auteurs malveillants pourraient exploiter pour nuire à des programmes informatiques, à des données, à d'autres ordinateurs ou à un réseau.
Logiciel criminel	Logiciel malveillant installé secrètement sur des ordinateurs et capable de « voler » des renseignements confidentiels et de les faire parvenir aux cybercriminels.
Cyberattaque	Accès involontaire ou non autorisé à des renseignements électroniques ou à des appareils électroniques, des systèmes ou des réseaux informatiques utilisés pour traiter, communiquer ou stocker des renseignements, et utilisation, manipulation, interruption ou destruction de ces renseignements, appareils, systèmes ou réseaux par voie électronique.
Cybersécurité	Ensemble des technologies, processus, pratiques et mesures d'intervention et d'atténuation visant à protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés et à assurer la confidentialité, l'intégrité et la disponibilité.
Déni de service (DS)	Attaque qui empêche ou compromet la fonctionnalité autorisée normale des réseaux, systèmes ou applications en épuisant ses ressources. Cette activité comprend le fait d'être la cible d'une attaque de DS ou d'y participer contre son gré.
Événement	Changement observable dans le comportement normal d'un ordinateur, d'un système de TI, d'un environnement, d'un processus ou d'un flux de travail qui peut avoir une incidence sur le système, l'intégrité des données, la sécurité et la sûreté, ou représenter une menace. Un événement peut devenir un incident s'il devient évident que le changement observé a un impact négatif probable.
Hacktivisme	Combinaison d'activités de piratage et d'activisme.
Utilisation inadéquate	Toute activité qui contrevient aux politiques acceptables d'utilisation informatique.
Incident	Événement unique ou série d'événements imprévus ou indésirables liés à la sûreté de l'information ayant une forte probabilité de compromettre les opérations commerciales, la sûreté nationale ou la sécurité publique.
Code malveillant	Installation *réussie* d'un logiciel malveillant (p. ex. virus, ver, cheval de Troie ou autre entité malveillante utilisant un code) qui infecte un système d'exploitation ou une application.
Hameçonnage	Forme numérique d'ingénierie sociale qui utilise des courriels qui semblent

et courriels ciblés	authentiques, mais qui sont malveillants, pour demander de l'information aux utilisateurs ou les diriger vers un faux site Web qui demande de l'information.
Recherche (type d'incident)	Incidents *non confirmés* qui peuvent représenter une activité malveillante ou anormale que l'entité effectuant le signalement juge nécessaire d'examiner plus à fond.
Balayages, essais et tentatives d'accès	Cela comprend toute activité visant à avoir accès à un ordinateur, à des ports ouverts, à des protocoles, à un service ou à une combinaison de ceux-ci, en prévision d'une exploitation ultérieure, ou à identifier les éléments qui précèdent. Cette activité ne cause pas directement une compromission ou un déni de service.
Hameçonnage ciblé	Catégorie d'hameçonnage qui consiste à cibler des personnes précises.
Accès non autorisé	Toute activité par laquelle une personne obtient un accès logique ou physique, sans permission, à un réseau, à un système, à une application, à des données ou à d'autres ressources.