Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Décision de télécom CRTC 2018-79

Version PDF

Ottawa, le 23 février 2018

Dossier public : 8621-C12-01/08

Groupe de travail Services d'urgence du Comité directeur du CRTC sur l'interconnexion – Rapport de consensus ESRE0077 concernant les pratiques exemplaires en matière de cybersécurité des centres d'appels de la sécurité publique dans un écosystème canadien du 9-1-1

En vue de la transition vers les réseaux et les services 9-1-1 de prochaine génération (9-1-1 PG) au Canada, le Groupe de travail Services d'urgence (GTSU) du Comité directeur du CRTC sur l'interconnexion (CDCI) a examiné les pratiques exemplaires en matière de cybersécurité des centres d'appels de la sécurité publique (CASP) qui établissent des interconnexions avec les réseaux 9-1-1 actuels et les futurs réseaux 9-1-1 PG. Le GTSU a déposé auprès du Conseil un rapport de consensus établissant des pratiques exemplaires proposées en matière de cybersécurité, y compris la mise en œuvre d'une stratégie claire sur la cybersécurité des réseaux 9-1-1 PG, de politiques améliorées en matière de cybersécurité et d'un plan d'action sur la cybersécurité.

Le Conseil estime qu'il est important que les CASP adoptent des pratiques exemplaires qui profiteront aux Canadiens. Après avoir examiné le rapport de consensus du GTSU, le Conseil encourage les CASP de partout au Canada à mettre en œuvre les pratiques exemplaires énoncées dans le rapport de consensus du GTSU.

Contexte

1. Au Canada, lorsqu'un appel au 9-1-1 est fait, l'appel est transmis du réseau sur lequel il a été fait (réseau d'origine)[1] vers le réseau 9-1-1 spécialisé local. Le réseau 9-1-1 détermine quel centre d'appels 9-1-1, également appelé centre d'appels de la sécurité publique (CASP), dessert la région d'où provient l'appel et dirige celui-ci vers le CASP concerné. Les intervenants d'urgence appropriés, comme le service d'incendie, la police ou le service ambulancier, sont alors ciblés et déployés, au besoin.

2. Les gouvernements municipaux, provinciaux et territoriaux sont responsables des intervenants d'urgence ainsi que de l'établissement et de la gestion des CASP qui en assurent le déploiement. Les politiques, les procédures et les normes internes des CASP et des intervenants d'urgence ne sont pas déterminées par le Conseil, bien qu'il existe une collaboration nationale au sein du Groupe de travail Services d'urgence

[1]Les réseaux d'origine comprennent les réseaux filaires traditionnels, les réseaux sans fil et les réseaux de communication vocale sur protocole Internet (VoIP), comme il a été déterminé dans la politique réglementaire de télécom 2016-165.

(GTSU)[2] du Comité directeur du CRTC sur l'interconnexion (CDCI) lorsque les politiques, les procédures et les normes sont directement liées aux services fournis par les fournisseurs de services téléphoniques (FST).

3. La compétence du Conseil se limite aux réseaux d'origine et aux réseaux 9-1-1. Dans le contexte du service 9-1-1, le rôle du Conseil consiste à assurer une surveillance réglementaire sur l'accès fourni par les FST afin de permettre aux Canadiens de communiquer avec les CASP partout où ils ont été établis par le gouvernement local. Il s'agit notamment de déterminer les politiques nationales, les normes, les conditions de service, les ententes, l'admissibilité, et l'approbation des tarifs pour les services de télécommunication.

4. Dans la politique réglementaire de télécom 2017-182, le Conseil a établi ses conclusions relativement à la mise en œuvre et à la fourniture des réseaux et des services 9-1-1 de prochaine génération (9-1-1 PG)[3] au Canada. Le Conseil a, entre autre, imposé des obligations aux fournisseurs des réseaux 9-1-1 PG, notamment de i) garantir la fiabilité, la résilience et la sécurité des réseaux 9-1-1 PG; ii) déposer un rapport sur les pannes du réseau 9-1-1 PG; et iii) protéger la vie privée dans l'environnement 9-1-1 PG.

5. Dans cette décision, le Conseil a également demandé au CDCI de formuler des recommandations et des lignes directrices concernant la mise en œuvre des pratiques exemplaires et des normes spécifiques de l'industrie. Celles-ci comprenaient notamment des normes de rendement et des niveaux de service en ce qui a trait à la fiabilité, à la résilience et à la sécurité des réseaux 9-1-1 PG. Comme il est indiqué dans cette décision, le CDCI est le mieux placé pour formuler ces recommandations et ces lignes directrices étant donné qu'il surveille actuellement l'élaboration des normes connexes de la National Emergency Number Association[4] et les leçons apprises par d'autres administrations qui mettent en place le 9-1-1 PG.

6. Le Conseil n'a pas abordé précisément le sujet de la cybersécurité des CASP dans l'écosystème canadien du 9-1-1 dans la politique réglementaire de télécom 2017-182, étant donné que les CASP ne relèvent pas de sa compétence.

---

[2]Le GTSU est un groupe de travail qui traite les problèmes techniques et opérationnels liés aux services 9-1-1 au Canada.

[3]Les services 9-1-1 PG comprennent les réseaux 9-1-1 modernisés qui sont fondés sur le protocole Internet (IP), ainsi que d'éventuels services 9-1-1 nouveaux, améliorés et novateurs offerts au moyen de ces réseaux. Par exemple, les Canadiens pourront transmettre, à partir du lieu de l'incident, des vidéos à diffusion en continu, des photos des dommages ou d'un suspect en fuite, ou même des renseignements médicaux personnels, y compris les besoins en matière d'accessibilité, susceptibles d'aider grandement les intervenants en cas d'urgence.

[4]La National Emergency Number Association travaille avec des chefs de file des politiques publiques, des partenaires des services d'urgence et de l'industrie des télécommunications, des associations de sécurité publique et d'autres groupes d'intervenants afin d'élaborer et de réaliser des programmes et des initiatives essentiels visant à faciliter la création d'un système 9-1-1 PG utilisant la technologie IP et à établir des normes, une formation et des certifications de pointe au sein de l'industrie.

Rapport du GTSU

7. En vue de la transition vers les réseaux 9-1-1 PG, le GTSU a décidé, en septembre 2015, d'examiner les pratiques exemplaires en matière de cybersécurité des CASP qui établissent des interconnexions avec les réseaux 9-1-1 actuels et les futurs réseaux 9-1-1 PG. En entreprenant cette tâche, le GTSU estimait que les problèmes de cybersécurité pourraient avoir des répercussions sur la fiabilité, la résilience et la sécurité des services d'urgence compte tenu de la migration des réseaux sur le protocole Internet (IP) et de l'introduction des bases de données 9-1-1 PG en temps réel.

8. Le 16 octobre 2017, le Conseil a reçu le rapport de consensus suivant (rapport) du GTSU :

    - *Cybersecurity Best Practices for PSAPs in a Canadian 9-1-1 Ecosystem*, 14 septembre 2017 (ESRE0077, pratiques exemplaires en matière de cybersécurité des centres d'appels de la sécurité publique dans un écosystème canadien du 9-1-1)

9. Le rapport s'appuie sur les opinions des intervenants du 9-1-1, y compris les fournisseurs de réseaux 9-1-1, les CASP et les FST. Il peut être consulté sous la rubrique « Rapports » de la page du GTSU, dans la section du CDCI sur le site Web du Conseil à l'adresse www.crtc.gc.ca.

10. Le GTSU a présenté le rapport au Conseil aux fins d'examen et a demandé au Conseil d'encourager les CASP canadiens à examiner et à mettre en œuvre un certain nombre de pratiques exemplaires en matière de cybersécurité[5] à l'intention des CASP. Les pratiques exemplaires ciblées dans le rapport consistent en un processus en trois étapes, comme il est expliqué ci-dessous.

11. La première étape consiste à élaborer et à mettre en œuvre une stratégie de cybersécurité claire pour les réseaux 9-1-1 et 9-1-1 PG indiquant les biens et leurs propriétaires, y compris les vulnérabilités, les menaces et les risques liés à ces biens, ainsi que les méthodes pour les atténuer. Cette stratégie peut être appuyée par un certain nombre de rapports et recommandations approuvés par l'industrie, de livres blancs, d'outils et de méthodes, ainsi que par l'utilisation d'une terminologie commune du domaine de la cybersécurité. Tous les CASP devraient adopter les normes de la stratégie de cybersécurité, et celles-ci devraient inclure notamment ce qui suit :

---

[5]Le GTSU a adopté la définition de cybersécurité établie par le National Institute of Standards and Technology. Ce dernier définit officiellement la cybersécurité comme « la prévention de tout dommage aux ordinateurs, aux systèmes de communication électronique, aux services de communication électronique, aux communications par fil, aux communications électroniques, y compris les renseignements qui y sont inclus, ainsi que la protection et la restauration de ces éléments afin d'assurer leur disponibilité, leur intégrité, leur authentification, leur confidentialité et leur non-répudiation ».

- la réalisation d'une auto-évaluation des capacités actuelles et futures intégrant les facteurs relatifs à la cybersécurité dans toutes les nouvelles architectures;
- la sélection d'un cadre de cybersécurité adaptable (par exemple, le dernier cadre sur la cybersécurité du National Institute of Standards and Technology [NIST]) et l'application des approches et des caractéristiques recommandées pour atteindre les buts;
- l'utilisation de pratiques exemplaires de base en matière de cybersécurité, d'une approche non exclusive afin de faciliter l'interopérabilité avec les réseaux IP des services d'urgence[6] 9-1-1 PG et les conceptions de services;
- la création, la promotion et la facilitation d'un environnement de travail et de formation dans les CASP au sein duquel les programmes de sensibilisation à la cybersécurité et les programmes pertinents sont omniprésents et complétés par un examen régulier des mesures de sécurité, des vérifications, des programmes de mise à jour individuels, ainsi que des suivis;
- la création d'évaluations régulières des risques et des vulnérabilités liés à la cybersécurité dans les services d'accès au réseau IP des services d'urgence, y compris les évaluations des risques liés aux points d'interconnexion conjoints avec les CASP voisins;
- la transmission d'avis et de renseignements en temps opportun avec d'autres CASP qui sont branchés au même réseau 9-1-1 PG;
- l'inclusion de spécifications et d'exigences en matière de cybersécurité, y compris le libellé des modalités de rendement, les délais de réponse, et les rapports sur les pannes, dans les contrats des fournisseurs des services ou de l'équipement liés aux réseaux 9-1-1 ou 9-1-1 PG.

12. La deuxième étape consiste à adopter les recommandations supplémentaires en matière de cybersécurité présentées dans un rapport de la Task Force on Optimal PSAP Architecture (TFOPA)[7] de la Federal Communications Commission (FCC) des États-Unis. Dans ce rapport, la TFOPA a déterminé qu'une couche de sécurité supplémentaire, appelée Emergency Communications Cybersecurity Center (EC3)[8],

---

[6]Les réseaux IP des services d'urgence sont des réseaux IP gérés, utilisés pour les communications d'urgence qui peuvent être partagés par tous les organismes de service public.

[7]La TFOPA de la FCC a reçu l'ordre d'étudier la structure et l'architecture et de rendre compte de ses constatations et de ses recommandations à cet égard. La TFOPA est un comité consultatif fédéral des États-Unis créé afin de formuler des recommandations à la FCC à propos des étapes que les CASP peuvent suivre pour optimiser la sécurité, les opérations et le financement à mesure qu'ils migrent vers les réseaux 9-1-1 PG.

[8]Le modèle EC3 sert à aider les intervenants du réseau 9-1-1 PG et les fournisseurs de services du réseau IP des services d'urgence avec la conception, la mise en œuvre et la gestion des justificatifs et des certificats, et à leur donner des conseils à cet égard. Cela comprend l'utilisation de pratiques exemplaires; l'élaboration d'exercices de formation; le traitement des violations, des vulnérabilités et des attaques; ainsi que la collecte de renseignements sur les risques et l'échange de tels renseignements avec tous les intervenants autorisés, y compris les CASP.

devrait être introduite dans la future architecture. Comme elle l'a indiqué dans son rapport, la TFOPA a élaboré une liste de vérification et une feuille de route détaillée[9] pouvant servir de base de référence pour créer un document de travail pour la mise en œuvre progressive de services de cybersécurité conjointement avec l'établissement de tout système ou service 9-1-1 PG proposé.

13. La troisième étape consiste à établir un plan d'action adapté au CASP à l'aide de la stratégie de cybersécurité et de la feuille de route élaborées au cours des première et deuxième étapes. Le GTSU a recommandé que les CASP assurent la surveillance, la vérification, la sécurité et la protection, et rendent compte des événements liés à la cybersécurité qui ont des répercussions sur les éléments fonctionnels du logiciel et du matériel des réseaux 9-1-1 PG et IP des services d'urgence.

Résultats de l'analyse du Conseil

14. Comme l'a fait remarquer le GTSU, l'objectif principal du rapport est de promouvoir la sensibilisation à la cybersécurité auprès des divers intervenants des services 9-1-1, et de sécuriser les environnements 9-1-1 et 9-1-1 PG globaux. Le Conseil fait remarquer que les CASP ne relèvent pas de sa compétence; par conséquent, on ne demande pas au Conseil d'approuver les recommandations contenues dans le rapport. Cependant, le Conseil estime qu'il est pertinent d'examiner les recommandations importantes qui figurent dans le rapport, comme l'a demandé le GTSU, et d'encourager les CASP à adopter des pratiques exemplaires en matière de cybersécurité dans l'intérêt des Canadiens.

15. Le Conseil estime que la représentation des intervenants lors de l'élaboration du rapport du GTSU sur les pratiques exemplaires en matière de cybersécurité des CASP dans un écosystème canadien du 9-1-1 était appropriée, et que les membres du GTSU se sont entendus sur l'établissement des recommandations contenues dans le rapport.

16. Le Conseil préconise donc les recommandations formulées par le GTSU à cet égard et fait remarquer que ce dernier avait tenu compte du fait que le cadre sur la cybersécurité du NIST et le rapport de la TFOPA sont appuyés par la totalité des organisations responsables de l'élaboration des normes des services d'urgence.

17. Le modèle EC3, mentionné dans le rapport de la TFOPA, aidera à déterminer les ressources requises en matière de cybersécurité pour ce qui est du personnel responsable des systèmes et du soutien, afin de contribuer à la stratégie de cybersécurité actuelle et future à l'aide des pratiques exemplaires, de l'élaboration de programmes de formation, de la planification des processus en cas de cyberattaque, ainsi que de la gestion et l'échange de renseignements sur les risques avec d'autres CASP.

---

[9]La TFOPA s'est fondée sur le travail effectué précédemment par diverses organisations pour élaborer la liste de vérification et la feuille de route détaillée.

18. Après avoir examiné le rapport du GTSU, le Conseil encourage les CASP canadiens à mettre en œuvre les processus de cybersécurité améliorés indiqués dans le rapport du GTSU à titre de pratiques exemplaires pour les systèmes 9-1-1 actuels et 9-1-1 PG.

19. De plus, après avoir réalisé les étapes d'élaboration de politiques présentées dans le rapport du GTSU, les CASP sont invités à mettre en œuvre les plans d'action sur la cybersécurité appropriés pour atteindre les résultats précis escomptés en matière de cybersécurité. Le plan d'action pourrait inclure des étapes visant à surveiller, à vérifier, à améliorer et à protéger la sécurité du système, ainsi qu'à établir des rapports sur celle-ci, et inclure des étapes sur les mesures d'atténuation axées sur une intervention efficace, le rétablissement du système et la résolution en cas de cyberattaque.

20. En résumé, le Conseil encourage les CASP de partout au Canada à :

    - mettre en œuvre une stratégie de cybersécurité claire pour les réseaux 9-1-1 PG indiquant les biens et leurs propriétaires, y compris les vulnérabilités, les menaces et les risques liés à ces biens, ainsi que les méthodes pour les atténuer;

    - utiliser les méthodes et les directives de la feuille de route incluses dans le modèle EC3 de la TFOPA afin d'élaborer des politiques de cybersécurité améliorées;

    - établir un plan d'action sur la cybersécurité pour assurer la surveillance, la vérification, la sécurité et la protection, et rendre compte des événements liés à la cybersécurité.

Secrétaire général

Documents connexes

- *9-1-1 de prochaine génération – Modernisation des réseaux 9-1-1 afin de satisfaire aux besoins des Canadiens en matière de sécurité publique*, Politique réglementaire de télécom CRTC 2017-182, 1er juin 2017

- *Questions ayant trait à la fiabilité et à la résilience des réseaux 9-1-1*, Politique réglementaire de télécom CRTC 2016-165, 2 mai 2016