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

Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022

12 décembre 2023

RAPPORT PRÉSENTÉ PAR : Xona Partners Inc.

Xona Partners Inc.
2969, Sable Ridge Drive, Ottawa, Ontario K1T 3S3 Canada
www.xonapartners.com

ISBN : 978-0-660-69964-6
Numéro de catalogue : BC92-130/1-2024F-PDF

XONA PARTNERS

Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022

Un rapport au Conseil de la radiodiffusion et des télécommunications canadiennes

2023-12-12

Ce rapport a été préparé par Xona Partners Inc. (Xona) en réponse à la demande de propositions du CRTC no 23-0049 : « Évaluation de la résilience du réseau de Rogers liée à la panne du 8 juillet 2022 ».

Le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a retenu les services de Xona pour effectuer les tâches spécifiées dans l'énoncé des travaux résultant de la demande de propositions susmentionnée.

Xona a préparé le rapport en fonction des renseignements fournis par Rogers Communications Inc. (Rogers), sous réserve de l'article 39 de la *Loi sur les télécommunications*. Lors de l'élaboration de ce rapport, Xona a examiné les réponses de Rogers à la demande de renseignements du CRTC datée du 12 juillet 2022 et s'est engagé avec Rogers dans une série de questions et de réunions supplémentaires afin de remplir son mandat et ses obligations envers le CRTC.

Table des matières

1. Glossaire

Fournisseur de réseau 9-1-1	Le fournisseur de réseau 9-1-1 est l'exploitant local historique qui fournit le service d'intervention d'urgence 9-1-1 à l'autorité locale conformément à un tarif ou à un accord. Le tarif ou l'accord du fournisseur du réseau 9-1-1 met l'accès aux appels d'urgence 9-1-1 à la disposition des utilisateurs finaux situés dans la zone de desserte.
Filtre de gestion de la liste de contrôle d'accès	Un filtre de gestion de la liste de contrôle d'accès dans un routeur est une table qui fournit les règles sur la façon dont le routeur doit gérer le trafic de paquets. La liste de contrôle d'accès est décrite comme un filtre de gestion parce qu'elle définit le trafic qui passera par le routeur et comment il sera dirigé en fonction de l'ensemble des règles (filtres).
Border Gateway Protocol (BGP)	Le BGP est un protocole de routage de passerelle extérieure qui permet l'échange d'informations sur les itinéraires entre les routeurs de différents systèmes autonomes, dans le but de sélectionner le meilleur chemin pour les paquets de données.
Routeur central	Un routeur central est un routeur situé dans le réseau central, ou couche, d'un réseau IP.
Processus de gestion du changement	Le processus de gestion du changement est une approche systématique de la gestion des modifications de l'infrastructure et des services du réseau. Il s'agit d'un processus conçu pour réduire le risque d'interruption des services et pour garantir que les changements sont contrôlés et mis en œuvre de manière efficace.
Routeur de distribution	Un routeur de distribution est un routeur de la couche de distribution du réseau IP d'un fournisseur de services de télécommunication. Il se situe entre la couche d'accès qui connecte les utilisateurs finaux au réseau et la couche centrale qui regroupe tout le trafic du réseau.
Serveur de noms de domaine	Un serveur de noms de domaine est comme un carnet d'adresses pour l'Internet. Un serveur de noms de domaine

	traduit les adresses Web conviviales (comme www.rogers.com) en adresses numériques de protocole Internet.
Processus de gestion des incidents	Le processus de gestion des incidents est une approche systématique du recensement, de la réponse et de la résolution des incidents qui touchent les services du réseau. Il est conçu pour réduire l'effet des incidents sur les utilisateurs en rétablissant le service normal aussi rapidement que possible.
Entreprise de services locaux titulaire (ESLT)	L'entreprise de services locaux titulaire est le fournisseur du réseau 9-1-1 dans le cadre de ce rapport.
Intermediate System to Intermediate System	Intermediate System to Intermediate System est un protocole de routage par passerelle intérieure qui permet l'échange d'informations sur les itinéraires entre les routeurs au sein du réseau d'un exploitant afin de sélectionner le meilleur chemin pour les paquets de données. Il s'agit d'un type de protocole similaire à Open Shortest Path First (OSPF).
Système d'agrégation et de dissémination national d'alertes (système ADNA)	Le Système d'agrégation et de dissémination national d'alertes reçoit les alertes d'urgence des agences gouvernementales autorisées. Ces alertes sont ensuite mises à la disposition des radiodiffuseurs et autres distributeurs de médias qui les diffusent volontairement au public canadien. Pelmorex Communications Inc. est désigné comme regroupeur et distributeur national de messages d'alerte en cas d'urgence.
Système national d'alertes au public (SNAP)	Le Système national d'alertes du public est un système fédéral, provincial et territorial qui permet aux organisations de gestion des urgences de partout au Canada d'avertir le public des dangers imminents ou en cours.
Open Shortest Path First (OSPF)	Open Shortest Path First est un protocole de routage par passerelle intérieure qui permet l'échange d'informations sur les itinéraires entre les routeurs du réseau d'un exploitant afin de sélectionner le meilleur chemin pour l'acheminement des paquets de données.

Fournisseurs de réseau d'origine	Le réseau à l'origine d'un appel 9-1-1. Il comprend le réseau d'accès et le réseau d'appels. Il est généralement exploité par des entreprises ou d'autres fournisseurs de services.
Messagerie par contournement	La messagerie par contournement est un service de messagerie offert par une application qui n'est généralement pas liée au fournisseur de services de télécommunication et qui fonctionne indépendamment de lui. Par exemple, des services comme WhatsApp, Signal, Telegram, WeChat et d'autres sont des services de messagerie par contournement, contrairement au service de messages courts et au service de messagerie multimédia, qui sont des technologies intégrées à la technologie cellulaire (p. ex., GSM, 3G ou LTE).
Réseau de production	Le réseau de production est un terme couramment utilisé par les fournisseurs de services pour distinguer les éléments de réseau actifs de ceux utilisés dans un environnement de laboratoire. Dans ce contexte, la production consiste à traiter le trafic des clients dans un environnement réel.
Centre d'appels de la sécurité publique (CASP)	Lieu de réponse aux appels 9-1-1 provenant d'une zone donnée. Un CASP peut être conçu comme primaire ou secondaire, ce qui fait référence à l'ordre dans lequel les appels sont dirigés pour y répondre. Les CASP primaires interviennent en premier. Il s'agit d'une installation de communication ouverte 24 heures sur 24, 365 jours par année, chargée de rediriger ou de transférer les appels d'urgence vers des CASP secondaires qui reçoivent les appels sur la base d'un transfert uniquement et qui servent généralement de position de réponse centralisée pour un type particulier d'appel d'urgence. Les employés des CASP secondaires proviennent d'organismes ou de services comme la police, les pompiers ou les agences médicales d'urgence, ou d'un bureau commun desservant un groupe d'entités de ce type.
Routeurs	Les routeurs sont des dispositifs de mise en réseau qui reçoivent et transmettent des paquets de données dans les réseaux IP. Les routeurs dirigent le trafic au sein des réseaux ou entre eux.

Protocole de routage	Un protocole de routage spécifie comment les routeurs transmettent les paquets d'une source à une destination. Les protocoles de routage sont regroupés en deux grandes catégories : les protocoles de passerelle intérieure et les protocoles de passerelle extérieure. Les protocoles de passerelle intérieure sont conçus pour fonctionner au sein d'un système autonome, c.-à-d. un réseau contrôlé par voie administrative par une seule organisation. Les protocoles de passerelle externe sont conçus pour gérer le transfert de renseignements entre les systèmes autonomes.

2. Acronymes

API	Interface de programmation d'applications
BGP	Border Gateway Protocol
BRI	Indice de risque de base
SSE	Systèmes de soutien aux entreprises
CRMS	Capacité, fiabilité, sécurité obligatoire et service (réseau d'accès)
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
CCCST	Comité consultatif canadien pour la sécurité des télécommunications
PD	Passerelle de distribution
DNS	Système de nom de domaine
DOCSIS	Data Over Cable Service Interface Specification
HAE	Heure avancée de l'Est
FCC	Commission fédérale des communications des États-Unis
IETF	Internet Engineering Task Force
PPI	Protocole de passerelle intérieure
ESLT	Entreprise de services locaux titulaire
IP	Protocole Internet
IPv 4	IP version 4
IPv 6	IP version 6
ISDE	Innovation, Sciences et Développement économique Canada (Ministère d')
FSI	Fournisseurs de services Internet
IRC	Indicateur de rendement clé
LTE	Technologie d'évolution à long terme
MPLS	Commutation multiprotocole par étiquette
RPVM	Réseau privé virtuel multidiffusion
ADNA	Système d'agrégation et de dissémination national d'alertes
DCR	Demande de changement au réseau
NIST	National Institute of Standards and Technology
CER	Centre d'exploitation du réseau
SNAP	Système national d'alertes au public
LNP	Lancement d'un produit nouveau
LNT	Lancement d'une nouvelle technologie
OSPF	Open Shortest Path First
SSO	Systèmes de soutien opérationnel
ICP	Infrastructure à clés publiques

CASP	Centre d’appels de la sécurité publique
RCMIN	Réseau IP de gestion de Rogers Communications
RFC	Demande de commentaires
DDR	Demande de renseignements
SD-WAN	Réseau étendu défini par logiciel
SIM	Module d’identité d’abonné
ANS	Accord sur les niveaux de service
FST	Fournisseur de services de télécommunication
RPV	Réseau privé virtuel

3. Sommaire

3.1. Aperçu

Au petit matin du 8 juillet 2022, Rogers Communications Inc. (Rogers) a connu une panne de service majeure dans son réseau central de protocole Internet (IP) qui a touché ses services sans fil et filaires partout au Canada (panne de juillet 2022). La panne de juillet 2022 a duré du 8 juillet 2022 à 4 h 58 HAE au 9 juillet 2022 à 7 h HAE, lorsque les services ont été progressivement rétablis. Plus de 12 millions de clients ont perdu des services sans fil et filaires, notamment des abonnés mobiles, des utilisateurs d'Internet à domicile, des entreprises et des clients institutionnels qui fournissent des services essentiels (p. ex., Interac e-Transfer et des services de paiement électronique).

Ce rapport détaille les résultats d'une évaluation indépendante de la fiabilité et de la résilience de l'architecture du réseau de Rogers[1], ainsi que les processus en place chez Rogers pour gérer les changements de réseau (processus de gestion du changement[2]) et répondre aux incidents de réseau tels que les pannes (processus de gestion des incidents[3]), car ces processus ont joué un rôle central dans la panne de juillet 2022.

Dans ce rapport, nous présentons en détail les résultats obtenus avant et pendant la panne et nous décrivons les mesures que Rogers a mises en œuvre depuis lors pour remédier aux lacunes dans la conception de son réseau et dans ses processus. Ce rapport est principalement basé sur un examen indépendant approfondi des réponses de Rogers à plusieurs séries de questions et de réunions avec le personnel technique et de gestion de Rogers au cours de cette évaluation, ainsi que sur les renseignements fournis par Rogers en réponse à la demande de renseignements (DDR) du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) après la panne.

3.2. Description de la panne

Contexte. Pour situer le contexte, Rogers exploite des réseaux sans fil et filaires qui partagent un réseau central IP commun, comme le montre le tableau Figure 1

[1]La fiabilité est une mesure de la capacité du réseau à fournir des services conformément aux spécifications prévues. La résilience est une mesure de la manière dont le réseau réagit pour réduire l'incidence des défaillances et de la vitesse à laquelle il se remet des perturbations.

[2]Le processus de gestion du changement est une approche systématique de la gestion des modifications de l'infrastructure et des services du réseau. Il s'agit d'un processus conçu pour réduire le risque d'interruption des services et pour garantir que les changements sont contrôlés et mis en œuvre de manière efficace.

[3]Le processus de gestion des incidents est une approche systématique du recensement, de la réponse et de la résolution des incidents qui touchent les services du réseau. Il est conçu pour réduire l'incidence des incidents sur les utilisateurs en rétablissant le service normal aussi rapidement que possible.

ci-dessous, sous une forme simplifiée. Le réseau central est une partie du réseau de télécommunications qui est responsable de l'agrégation et de l'acheminement du trafic de données à la fois en interne au sein du réseau de Rogers et en externe avec Internet et d'autres fournisseurs de services. Ainsi, pour Rogers, le trafic de données sans fil et filaire est traité par le même réseau central IP. Dans les semaines qui ont précédé le jour de la panne, le 8 juillet 2022, Rogers a mis en œuvre un processus en sept phases pour moderniser son réseau central IP. La panne s'est produite au cours de la sixième phase de ce processus de mise à niveau.

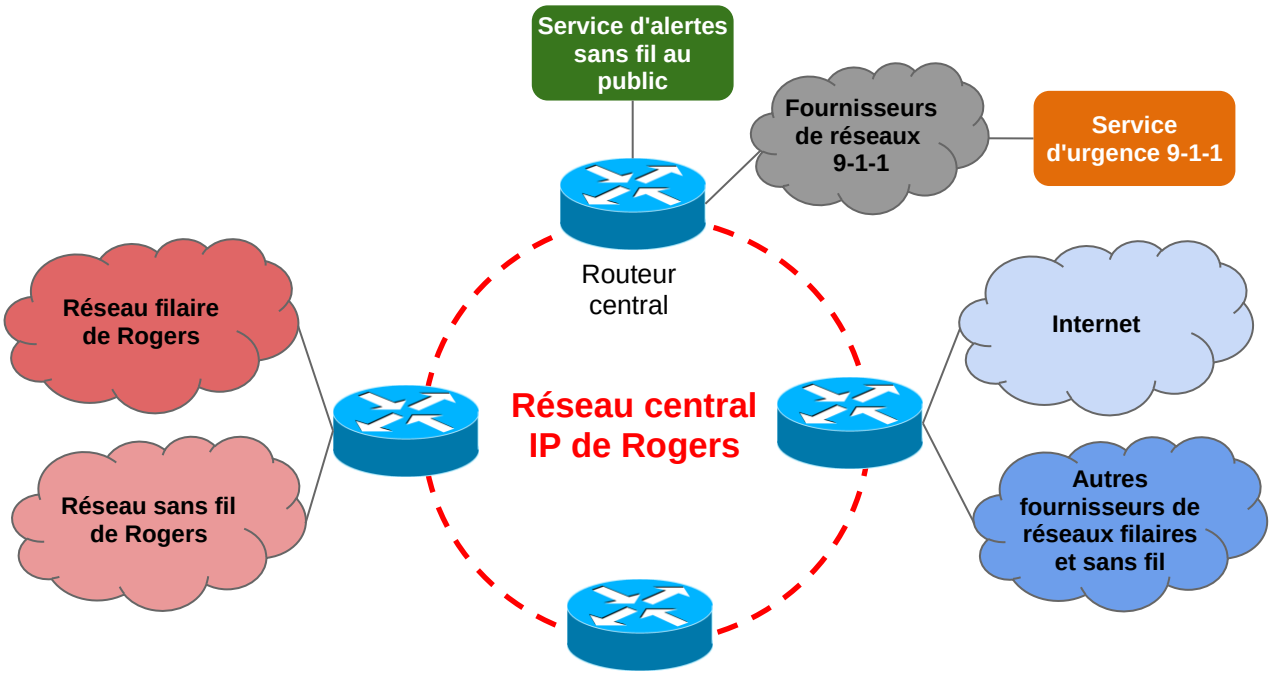

Figure 1 Topologie simplifiée de l'architecture de réseau de Rogers.

Cause profonde de la défaillance du réseau. La panne de juillet 2022 est attribuée à une erreur de configuration des routeurs de distribution[4] au sein du réseau IP de Rogers. Le personnel de Rogers a supprimé le filtre de gestion de la liste de contrôle d'accès[5] de la configuration des routeurs de distribution. Il en a résulté un afflux d'information de routage IP dans les routeurs du réseau central, ce qui a déclenché la panne. Les routeurs du réseau central permettent aux clients des services filaires et sans fil de Rogers d'accéder à des services comme la voix et les

[4]Un routeur de distribution est un routeur qui dirige le trafic entre la couche d'accès, qui connecte les utilisateurs au réseau, et le réseau central, qui regroupe tout le trafic du réseau.

[5]Une liste de contrôle d'accès dans un routeur est une table qui fournit les règles sur la façon dont le routeur doit gérer le trafic de paquets. La liste de contrôle d'accès est décrite comme un filtre de gestion parce qu'elle définit quel trafic passera par le routeur et comment il sera dirigé en fonction de l'ensemble des règles (filtres).

données. L'afflux de données de routage IP des routeurs de distribution vers les routeurs centraux a dépassé leur capacité de traitement de l'information[6]. Les routeurs principaux sont tombés en panne dans les minutes qui ont suivi la suppression du filtre de gestion de la configuration des routeurs de distribution. Lorsque les routeurs du réseau central sont tombés en panne, le trafic des utilisateurs ne pouvait plus être acheminé vers la destination appropriée. En conséquence, des services comme la téléphonie mobile, la téléphonie résidentielle, Internet, la connectivité filaire des entreprises et les appels 9-1-1 ont cessé de fonctionner.

Absence de protection contre les surcharges du routeur. La panne de juillet 2022 a mis en évidence l'absence de protection contre les surcharges sur les routeurs du réseau central. La panne du réseau aurait pu être évitée si les routeurs du réseau central avaient été configurés avec une limite de surcharge qui spécifie le nombre maximum acceptable de données de routage IP que le routeur peut prendre en charge. Cependant, les routeurs du réseau central de Rogers n'ont pas été configurés avec de tels mécanismes de protection contre les surcharges. Par conséquent, lorsque le filtre de gestion a été supprimé du routeur de distribution, une quantité excessive de données de routage a inondé les routeurs principaux, ce qui les a fait tomber en panne.

Lacunes dans le processus de gestion du changement. L'erreur de configuration, qui a conduit à la suppression du filtre de gestion de la configuration des routeurs de distribution, est le résultat d'un oubli de gestion du changement par le personnel de Rogers. Le personnel de Rogers a supprimé le filtre de gestion qui empêchait l'inondation des routes IP afin de nettoyer les fichiers de configuration des routeurs de distribution. Le processus de gestion du changement, qui comprend des vérifications des paramètres de changement, n'a pas permis de détecter la modification erronée de la configuration.

Comme indiqué ci-dessus, ce changement de configuration constituait la sixième phase d'un processus de mise à niveau du réseau en sept phases qui avait débuté quelques semaines auparavant. Avant cette sixième phase de mise à jour de la configuration, les précédentes mises à jour de la configuration ont été effectuées avec succès, sans aucun problème. Rogers avait initialement évalué le risque de ce processus en sept phases comme étant « élevé ». Toutefois, comme les modifications des phases précédentes ont été menées à bien, l'algorithme d'évaluation des risques a ramené le niveau de risque de la sixième phase du changement de configuration à un risque « faible », soit la modification à l'origine de la panne de juillet 2022. L'évaluation des risques étant faible, le personnel de Rogers n'a pas été tenu de procéder à un examen plus approfondi, de passer par des niveaux d'approbation plus élevés et d'effectuer des essais en laboratoire pour

[6]Rogers a déclaré qu'environ 10 000 routes sont annoncées dans le routeur principal lorsque le filtre de gestion de la de liste de contrôle d'accès est présent sur le routeur de distribution. Lorsque ce filtre a été supprimé, un seul routeur de distribution a transmis plus de 900 000 données d'itinéraires aux routeurs principaux.

ce changement de configuration. L'abaissement de l'évaluation du risque à « faible » pour la modification du filtre de la liste de contrôle d'accès dans une politique de routage est contraire aux normes de l'industrie, qui exigent un examen minutieux pour de tels changements de configuration, notamment des essais en laboratoire avant le déploiement dans le réseau de production.

3.3. Fiabilité de l'architecture de réseau de Rogers

Le réseau de Rogers est un réseau national de niveau 1 dont l'architecture est conçue pour être fiable. Il est typique de ce que l'on attendrait d'un tel réseau de fournisseurs de services de niveau 1. La panne de juillet 2022 n'était pas due à un défaut de conception dans l'architecture du réseau central de Rogers. Cependant, comme les réseaux sans fil et filaires partagent un réseau central IP commun, l'ampleur de la panne a été extrême, puisqu'elle a entraîné une perte catastrophique de tous les services. Une telle architecture de réseau est commune à de nombreux fournisseurs de services et constitue un exemple de la tendance à la convergence des réseaux de télécommunications filaires et sans fil. Il s'agit d'un choix de conception des fournisseurs de services, notamment Rogers, qui cherche à trouver un équilibre entre le coût et le rendement.

3.4. Facteurs relatifs au rétablissement du réseau

Infrastructure de gestion de réseau. Un réseau de gestion permet d'accéder aux sites d'infrastructures essentielles ou aux équipements d'un réseau afin d'en permettre le dépannage et la réparation. Au moment de la panne de juillet 2022, Rogers disposait d'un réseau de gestion qui s'appuyait sur le réseau central IP de Rogers. Lorsque le réseau central IP est tombé en panne pendant l'interruption, les employés de Rogers qui travaillent à distance n'ont pas pu accéder au réseau de gestion. En outre, Rogers n'a pas fourni à son centre d'exploitation du réseau et à d'autres sites d'infrastructures essentielles éloignés une connectivité redondante provenant de fournisseurs de services de rechange pour la gestion du réseau. Cela a limité l'accès aux équipements essentiels du réseau pendant la panne de juillet 2022 pour effectuer le dépannage et l'analyse des causes profondes. Rogers a dû envoyer du personnel sur des sites éloignés pour accéder physiquement aux routeurs concernés, ce qui a retardé les efforts de rétablissement du réseau. Selon notre évaluation, la résilience du réseau exige que les exploitants de réseaux de télécommunications disposent d'un accès de rechange sécurisé à des éléments de réseau essentiels et éloignés qui ne dépendent pas du réseau de données. L'incapacité du personnel à distance de Rogers à accéder au réseau de gestion et l'absence de connectivité de secours provenant de fournisseurs de services de rechange vers le centre d'exploitation du réseau et d'autres sites critiques et éloignés ont contribué à prolonger la panne de juillet 2022.

Communication limitée au sein du personnel de Rogers. Le personnel de Rogers s'appuyait sur les services mobiles et Internet de l'entreprise pour communiquer entre eux. Lorsque les réseaux sans fil et filaires sont tombés en panne, le personnel de Rogers, en particulier le personnel chargé de la gestion des

incidents critiques, n'a pas été en mesure de communiquer efficacement pendant les premières heures de la panne. Rogers a dû envoyer des cartes SIM (module d'identité d'abonné) d'autres exploitants de réseaux mobiles à ses sites éloignés pour permettre à son personnel disposant d'une connexion sans fil de communiquer entre eux. L'absence d'autres moyens de communication suffisants a ralenti la réponse de Rogers à la panne de juillet 2022.

Accès rapide à l'information essentielle pour le rétablissement du réseau. Le manque de renseignements a entravé le processus de gestion des incidents de Rogers. Le personnel de Rogers n'avait pas accès aux journaux d'erreurs des routeurs défaillants et ne pouvait pas déterminer la cause profonde de la panne pendant environ 14 heures après le début de la panne. De plus, Rogers avait effectué de multiples changements de configuration pendant la fenêtre de maintenance le jour de la panne. Cela a eu une incidence négative sur les efforts de rétablissement de la panne, et il a été difficile de décider quelle demande de changement au réseau devait être annulée. Ces deux facteurs ont contribué à un mauvais diagnostic de la cause profonde de la défaillance du réseau dans les premières heures de la panne de juillet 2022. Cependant, une fois la cause profonde déterminée, les activités de rétablissment du réseau ont commencé méthodiquement et les services ont été progressivement rétablis.

3.5. Mesures prises par Rogers pour améliorer la fiabilité et la résilience de son réseau

Traiter la cause profonde de la panne et les lacunes de l'architecture du réseau de gestion. Dans les mois qui ont suivi la panne de juillet 2022, Rogers a pris une série de mesures et d'initiatives pour remédier aux graves lacunes révélées par la panne. Plus important encore, Rogers a mis en place des mesures de protection dans la configuration des routeurs de son réseau central afin d'empêcher l'inondation des données de routage IP, ce qui permet d'éviter qu'une panne similaire ne se reproduise. Rogers a également mis en place un réseau de gestion physique et logique distinct pour accéder aux éléments du réseau à des fins de dépannage et d'analyse des causes profondes. En outre, Rogers a déployé une connectivité de secours auprès de fournisseurs de services tiers pour son centre d'exploitation du réseau et d'autres sites d'infrastructures essentielles éloignés, et a investi dans des outils qui aideraient à valider les changements de configuration des routeurs.

Noyau IP séparé pour les réseaux sans fil et filaires. À la suite de cette panne, Rogers a annoncé qu'il avait décidé de séparer le réseau central IP pour ses réseaux sans fil et filaires. Cette décision implique le déploiement d'un nouveau noyau IP pour le réseau sans fil, tandis que le noyau IP existant resterait en place pour desservir le réseau filaire. Par conséquent, si un réseau central IP était touché par une panne, l'autre réseau central IP resterait intact et opérationnel.

Rogers n'a pas encore terminé de mettre en œuvre la séparation du réseau central IP, qui demeure en cours. Lorsqu'ils seront mis en œuvre, les réseaux IP centraux

distincts pour les réseaux sans fil et filaires permettront de limiter une panne à leur réseau d'accès respectif et, par conséquent, d'éviter le type de panne de réseau catastrophique que l'on a connu lors de la panne de juillet 2022, où les services sans fil et filaires n'étaient pas disponibles en raison d'une panne du réseau central IP commun. La séparation du réseau central IP améliorerait la résilience globale des réseaux sans fil et filaires de Rogers.

Améliorer le processus de gestion du changement. Après la panne de juillet 2022, Rogers a apporté plusieurs améliorations à son processus de gestion du changement. Ces améliorations comprennent un nouvel algorithme d'évaluation des risques, des changements organisationnels visant à améliorer la collaboration entre les équipes d'exploitation et d'ingénierie du réseau, un processus amélioré pour l'introduction de nouveaux équipements et de nouvelles technologies, des améliorations dans la mise en œuvre des modifications du réseau, comme l'introduction de l'automatisation pour rationaliser le processus de gestion du changement, et des essais de laboratoire supplémentaires pour les changements prévues à la configuration du réseau.

Améliorer le processus de gestion des incidents. Après la panne de juillet 2022, Rogers a apporté des améliorations à son processus de gestion des incidents, notamment en renforçant ses lignes directrices en matière de gestion des incidents afin d'englober divers scénarios de panne; en rationalisant sa réponse aux incidents grâce à des rôles de leadership bien définis; en mettant en œuvre une solution pour hiérarchiser les alarmes pendant la panne; en améliorant les retours automatisés aux configurations précédentes lorsque les nouveaux changements ne réussissent pas et en mettant en œuvre des mesures supplémentaires afin d'améliorer ses protocoles de communication. Rogers a également équipé tous les membres de l'équipe de réponse aux incidents et de gestion de crise de moyens de communication de secours provenant de fournisseurs de services tiers afin de maintenir les capacités de communication pendant les pannes.

3.6. Évaluation et recommandations à Rogers

Notre évaluation globale est que la combinaison des mesures prises par Rogers après la panne de juillet 2022 est satisfaisante pour améliorer la résilience et la fiabilité du réseau de Rogers ainsi que pour traiter la cause profonde de la panne de juillet 2022.

La diligence dans la mise en œuvre des processus améliorés de gestion du changement serait le moyen le plus efficace d'éviter qu'une panne similaire ne se reproduise. L'amélioration des processus de réponse aux incidents permettrait à Rogers de réagir plus rapidement en cas de défaillance du réseau. Nous avons formulé plusieurs recommandations concernant des mesures supplémentaires que Rogers pourrait prendre pour améliorer la résilience de son réseau. Ces recommandations sont les suivantes :

1. Mettre à l'essai l'itinérance d'urgence avec d'autres exploitants de réseaux mobiles et l'étendre à un ensemble plus complet de scénarios d'essai. Rogers a signé le protocole d'entente sur la fiabilité des télécommunications, qui prévoit l'itinérance d'urgence avec d'autres exploitants de réseaux mobiles afin de permettre aux clients de Rogers d'accéder aux services d'urgence (p. ex., les appels 9-1-1) lors de pannes majeures. Ces essais supplémentaires permettraient de s'assurer que l'itinérance d'urgence est possible dans différents scénarios de défaillance du réseau, en particulier le scénario observé lors de la panne de juillet 2022 (où le réseau radio était en service et le réseau central en panne).
2. Élaborer une analyse détaillée des causes profondes des futures pannes majeures. Cela faciliterait le processus d'évaluation de la panne et de son incidence, ainsi que la détermination des mesures d'atténuation appropriées.
3. Assurer une large couverture et une grande rigueur dans les mises à l'essai des changements de configuration. Cela permettrait d'éviter les erreurs susceptibles d'entraîner des pannes. Rogers devra exploiter de nouveaux outils d'essai pour modéliser des scénarios d'essai qui reproduisent le réseau de production et pour tenir compte de l'évolution des technologies de réseau.
4. Élargir la portée des exercices de gestion des incidents. Cela permettrait d'améliorer la préparation du personnel et du réseau aux situations d'urgence et de découvrir les faiblesses de manière proactive.
5. Institutionnaliser l'apprentissage à partir de ses propres défaillances de réseau et de celles d'autres fournisseurs de services afin de mettre en œuvre des mesures préventives, de réduire l'incidence des pannes de réseau et d'améliorer la qualité du service.
6. Informer les clients sur la manière de joindre les services 9-1-1 pendant une panne.
7. Faire connaître les causes profondes des pannes et les stratégies d'atténuation à l'ensemble de la communauté Internet (représentée par des organismes comme le North American Network Operator's Group [NANOG]), afin d'aider les autres exploitants de réseaux de télécommunications à prévenir des pannes similaires.

3.7. Recommandations aux exploitants de réseaux de télécommunications

Leçons tirées de la panne de juillet 2022. Voici un résumé des principales leçons tirées de la panne de juillet 2022 :

1. Mettre en œuvre une protection contre la surcharge des routeurs dans les réseaux IP centraux et de distribution.

2. Séparer physiquement et logiquement la couche de gestion du réseau de données.
3. Fournir au centre d'exploitation du réseau et à d'autres sites critiques et éloignés une connectivité de secours sécurisée provenant d'exploitants de réseaux de télécommunications tiers.
4. Veiller à ce que le processus de vérification des changements de configuration du réseau soit efficace et implique différentes équipes au sein de l'organisation, comme l'ingénierie, les opérations et la gestion de projet. Il est également conseillé d'impliquer les fournisseurs d'équipement lorsque les changements de configuration concernent des infrastructures essentielles, comme le réseau central IP.
5. Effectuer des essais en laboratoire des changements de configuration prévus et s'assurer que l'équipement de laboratoire et les scénarios d'essais reflètent fidèlement le réseau de production.
6. Gérer avec soin le nombre de changements de configuration effectués au cours d'une seule fenêtre de maintenance et tirer parti des outils et des processus pour le retour automatisé des paramètres de configuration.
7. Mettre en œuvre une solution automatisée de hiérarchisation des alarmes afin de supprimer les alarmes inutiles pour chaque type de changement et de permettre au personnel de se concentrer sur les alarmes importantes.
8. Fournir au personnel critique des moyens de communication secondaires, tels que des cartes SIM d'exploitants de réseaux tiers.
9. Simuler et pratiquer des scénarios de défaillance et de panne du réseau afin de mettre en évidence les lacunes de l'architecture du réseau et du processus de gestion des incidents.

Évolution des tendances des réseaux de télécommunications. Les tendances évolutives des réseaux de télécommunications ont une incidence sur la fiabilité et la résilience des réseaux. Il s'agit notamment de l'évolution vers des plateformes publiques de télécommunications en nuage, de la logiciellisation et de la virtualisation des réseaux, de l'utilisation accrue de l'intelligence artificielle (IA) dans l'automatisation des réseaux, de la préparation à la cybersécurité post-quantique et de la convergence des réseaux terrestres et non terrestres. Les fournisseurs canadiens de services de télécommunication en sont à intégrer certaines de ces tendances dans l'évolution de leur réseau. Nous soulignons quelques recommandations technologiques et de processus qui permettraient de renforcer la résilience des réseaux face à ces tendances évolutives. Ces recommandations comprennent ce qui suit :

1. Recommandations technologiques :

A. Tirer parti des nouvelles constellations de satellites en orbite non géostationnaire (p. ex., les constellations de satellites en orbite basse) pour fournir une connectivité de secours aux sites éloignés et envisager les nouvelles constellations à liaison directe pour les appels d'urgence 9-1-1.

B. Suivre et préparer la mise en œuvre des normes d'itinérance en cas de catastrophe qui sont en cours de planification au sein de l'organisme de normalisation du 3rd Generation Partnership Project (3GPP).

C. Envisager l'utilisation d'applications de messagerie en ligne comme méthode de communication de rechange, notamment pour les services d'urgence. Cela serait utile en cas de défaillance de certains systèmes essentiels, tels que le système multimédia IP.

D. Exploiter les technologies SIM dynamiques axées sur les logiciels, qui offrent différents niveaux de programmabilité et permettent de nouveaux modèles d'itinérance vers d'autres fournisseurs en cas de pannes majeures.

E. Étudier l'applicabilité des techniques de partage du spectre et de la capacité d'urgence pour atténuer l'incidence des défaillances du réseau et œuvrer en ce sens. Ces techniques augmentent temporairement et dynamiquement la capacité du réseau pour répondre aux besoins des utilisateurs itinérants.

F. Envisager de collaborer avec les réseaux de diffusion de contenu et les fournisseurs d'applications en ligne pour définir des modèles d'interaction précis en cas d'urgence. Par exemple, la gestion dynamique du trafic permet aux fournisseurs de contenu d'adapter leur comportement en fonction des renseignements fournis par les exploitants de télécommunications.

G. Envisager d'offrir aux fournisseurs de services d'infrastructures essentielles des options secondaires pour des services de connectivité redondants.

2. Recommandations relatives au processus :

A. Mettre en œuvre des formations et des exercices de réponse aux incidents afin de découvrir les faiblesses de l'architecture, des opérations et des processus opérationnels qui ont une incidence négative sur les efforts de rétablissement des pannes.

B. Mettre en place des indicateurs de rendement clés pour la réponse à la gestion des incidents afin d'évaluer l'effort de réponse aux incidents et d'en améliorer l'efficacité.

C. Définir clairement les rôles et les responsabilités du personnel afin de mieux répondre aux pannes de réseau.

D. Envisager de calculer l'incidence financière d'une panne de réseau afin d'atténuer les conséquences des incidents en prenant des décisions sur l'affectation des ressources et en communiquant avec les intervenants pour préserver l'image de marque et la stabilité financière.

E. Pendant une panne, il est conseillé aux fournisseurs de services de rappeler au public comment accéder aux services d'appels d'urgence et d'alertes au public.

4. Introduction

Tôt le vendredi 8 juillet 2022, Rogers a connu une panne majeure de son réseau sans fil et filaire qui a duré près de 24 heures du début de la panne jusqu'à ce que la plupart des clients retrouvent leurs services de connectivité. La panne, localisée dans le réseau central IP, a touché tous les services de connectivité sans fil et filaire, tant pour les particuliers que pour les entreprises. Elle a également touché les appels vitaux au 9-1-1 et les alertes d'urgence ou au public du Système national d'alertes au public (SNAP).

La panne s'est produite au cours du processus de mise à niveau de certains éléments du réseau central IP de Rogers. Une mauvaise configuration du routage IP a entraîné une panne généralisée que l'on pourrait qualifier de catastrophique. Tous les réseaux sans fil et filaires de Rogers dans l'ensemble du Canada étaient hors service. La connectivité vitale avec le centre d'exploitation du réseau (CER) de Rogers et d'autres sites éloignés, ainsi qu'avec le personnel de Rogers, a été compromise, ce qui a d'autant plus retardé les efforts de rétablissement.

Immédiatement après la panne, le CRTC a lancé une enquête pour comprendre les événements qui ont mené à la panne et le processus de gestion des incidents de Rogers. À la suite de cette enquête, le CRTC a déterminé qu'il était nécessaire de procéder à un examen technique détaillé des réseaux de télécommunications sans fil et filaires de Rogers afin de vérifier la résilience et la fiabilité de tous les aspects qui ont mené à la panne du 8 juillet 2022, y compris l'architecture de réseau, les processus et les contrôles de gestion des affaires, les processus de gestion du changement et les processus de gestion des incidents. Le présent rapport fait état des résultats de l'examen technique et de l'évaluation visant à déterminer si les changements proposés et apportés par Rogers en réponse à la panne sont suffisants pour améliorer la résilience du réseau.

Les sections suivantes composent le présent rapport :

- La section 5 décrit la panne du 8 juillet 2022, principalement à partir des renseignements fournis par Rogers.
- La section 6 approfondit notre analyse de la panne. Elle présente des conclusions qui s'appuient sur la synthèse des données disponibles sur la panne. Pour compléter l'analyse, nous avons défini plusieurs points à examiner, notamment la cause profonde, l'architecture de réseau et les processus de gestion du changement et des incidents. Plus important encore, nous nous concentrons sur l'efficacité de l'exécution par rapport aux processus en place avant la panne et aux pratiques exemplaires de l'industrie.
- La section 7 présente les mesures correctives que Rogers a prises à la suite de la panne pour améliorer la fiabilité et la résilience du réseau, ainsi que notre évaluation de ces mesures.

- La section 8 présente les leçons tirées et les recommandations qui, selon nous, pourraient s’appliquer à d’autres exploitants de réseaux de télécommunications en vue d’améliorer la résilience des réseaux de télécommunications.

5. Description de l'incident

5.1. Architecture de réseau de Rogers

Rogers exploite un réseau sans fil national utilisant les technologies GSM (2G), UMTS (3G), LTE (4G) et 5G, ainsi que des services Wi-Fi. Rogers exploite également un réseau filaire qui comprend des services de téléphonie et Internet à large bande axés sur la fibre optique et le câble selon la norme DOCSIS (Data-Over-Cable-Service-Interface-Specifications).

[caviardé]

Le réseau central IP utilise des routeurs provenant de deux grands fournisseurs d'équipement différents : [caviardé] pour les routeurs de distribution et [caviardé] pour les routeurs centraux. La panne a mis hors service les routeurs du réseau central de Rogers, ce qui a interrompu les services de connectivité pour tous les clients de Rogers. La connectivité a également été interrompue avec les fournisseurs de réseaux 9-1-1 par l'intermédiaire des réseaux sans fil et filaires de Rogers. Les alertes d'urgence diffusées par Pelmorex, l'administrateur du Système d'agrégation et de dissémination national d'alertes (système ADNA) au Canada[7], n'ont pas pu atteindre les clients sans fil de Rogers.

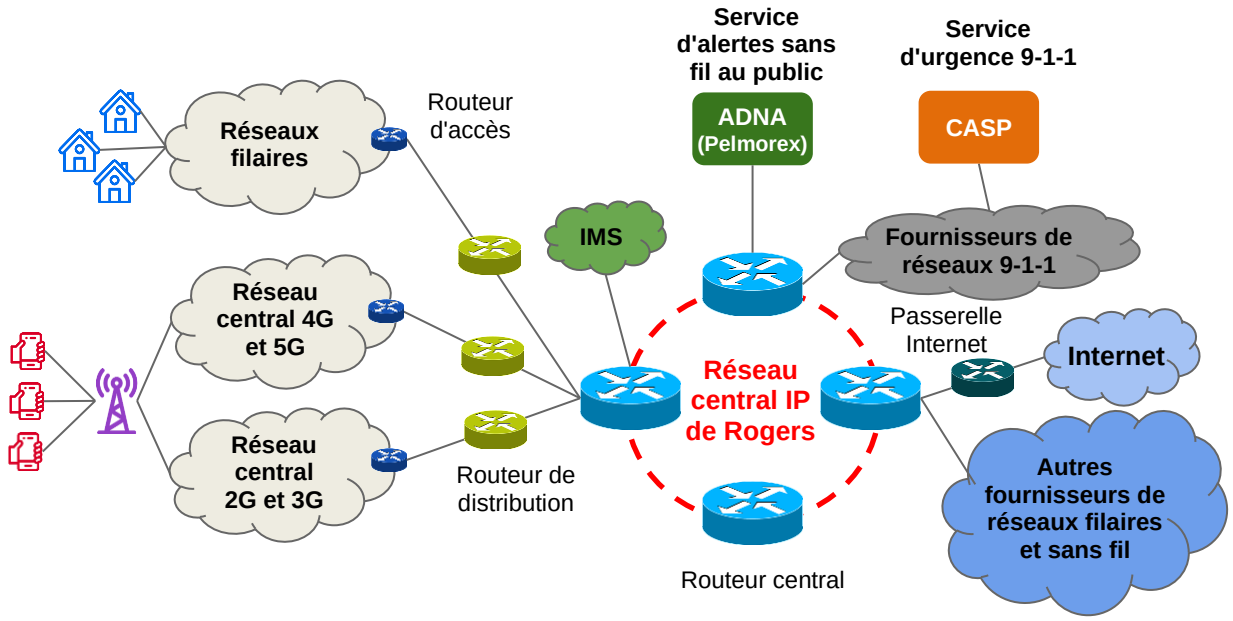

Figure 2 Illustration simplifiée du réseau de Rogers.

La panne a également coupé l'accès à d'importants systèmes qui gèrent les réseaux sans fil et filaires de Rogers. Cela comprend l'accès au CER et aux systèmes

[7] L'administrateur du Système ADNA recueille et valide les alertes d'urgence des agences gouvernementales autorisées dans l'ensemble du Canada et les rend accessibles au public par l'intermédiaire des fournisseurs de services de télécommunications.

essentiels tels que le registre des abonnés locaux, le serveur d'abonnés résidentiels et la base de données centralisée des utilisateurs.

5.2. Élément déclencheur de l'incident

La panne s'est produite lors de l'exécution d'un vaste processus en vue de modifier [caviardé]. Pour mener à bien le processus, Rogers a déterminé qu'elle devait supprimer un filtre de gestion dans les routeurs de distribution. [caviardé]

La modification de la configuration du routeur de distribution permet la distribution directe des adresses du système de noms de domaine (DNS) sans fil de l'infrastructure infonuagique au protocole OSPF (Open Shortest Path First). La modification de la configuration a entraîné la redistribution de l'ensemble des tables de routage du BGP (Border Gateway Protocol) vers le protocole OSPF. Ce flot de mises à jour a surchargé les routeurs centraux et a épuisé l'unité centrale de traitement et les ressources de mémoire, ce qui a finalement provoqué l'interruption des routeurs centraux et déclenché la panne.

5.3. Chronologie de l'incident et efforts de rétablissement

Le filtre de gestion a été supprimé de [caviardé] à 4 h 43 HAE le 8 juillet 2022 (événement déclencheur). La figure 3 montre les étapes clés de la chronologie de l'incident; des détails supplémentaires sont disponibles à l'annexe 1. En l'espace de deux minutes, toutes les passerelles centrales de Rogers ont commencé à tomber en panne; [caviardé]. Tous les services sans fil et filaires de Rogers ont cessé de fonctionner au Canada.

[caviardé] En outre, la défaillance du réseau sans fil a entravé la communication entre les membres du personnel de Rogers, qui avaient un accès limité aux services sans fil d'autres exploitants de réseaux mobiles (c'est-à-dire que Rogers disposait d'un nombre limité de cartes SIM de tiers).

[caviardé]

En raison de la panne, les ingénieurs de Rogers ont perdu l'accès à la gestion du réseau [caviardé]. Ils ont alors constaté que les routeurs de distribution, qui inondaient les routeurs centraux d'annonces de routes, étaient à l'origine de la panne.

Une fois la cause profonde déterminée, Rogers a procédé au rétablissement du réseau, en commençant par les régions du Centre et de l'Est. Rogers a dû prendre certaines précautions pour assurer un rétablissement ordonné des services. Il s'agissait notamment de ralentir artificiellement le trafic de l'entité de gestion de la mobilité afin d'éviter les tempêtes de signalisation provoquées par le grand nombre de téléphones mobiles tentant de se connecter au réseau.

Le trafic a été progressivement rétabli dans la soirée du 8 juillet 2022 et dans la matinée du 9 juillet 2022. [caviardé].

[caviardé]

Comme toutes les régions semblent en bon état, Rogers a annulé le ralentissement artificiel du trafic qui avait été institué pour l'entité de gestion de la mobilité du réseau sans fil dans toutes les régions. [caviardé]

5.4. Clients touchés

Tous les clients des services filaires et sans fil de Rogers, y compris les clients des marques Fido et Chatr, ont été touchés par la panne, de même que les clients de gros et les entreprises qui utilisent les services de Rogers. [caviardé]

[caviardé]

Rogers fournit des services de gros et d'itinérance à d'autres fournisseurs de services de télécommunication (FST) ainsi que des services de connectivité à des entreprises, y compris des institutions financières telles qu'Interac, ainsi qu'à des organisations gouvernementales. En outre, certaines stations de radiodiffusion de Rogers Media utilisent les services du réseau de Rogers. Dans l'ensemble, la panne a touché les clients suivants :

- **FST**
  - FST qui utilisent le réseau sans fil de Rogers pour communiquer et exploiter leur réseau
  - Partenaires d'itinérance sans fil
  - Fournisseurs de services Internet (FSI) tiers qui utilisent principalement le réseau filaire de Rogers

- **Gouvernement** : Rogers fournit des services filaires, sans fil, de voix sur IP, interurbains, sans frais et de machine à machine à différents organes de gouvernement. [caviardé] Différents ordres de gouvernement ont été touchés :
  - Gouvernement fédéral
  - Gouvernements provinciaux
  - Gouvernements municipaux

- **Fournisseurs d'infrastructures essentielles** : Organisations qui s'appuient principalement sur des services filaires comme le réseau de commutation multiprotocole par étiquette (MPLS), le réseau étendu défini par logiciel (SD-WAN), Ethernet et les protocoles de communication fondés sur l'optique. Voici des exemples :
  - Institutions financières [caviardé]
  - Énergie et services publics
  - Services de transport
  - Hôpitaux

- **Sociétés** : Sociétés desservies par différents services sans fil et filaires de Rogers, y compris les services de MPLS et du SD-WAN.

- **Clients de la radiodiffusion**
  - Les services de radiodiffusion de Rogers Media utilisent principalement une connectivité Internet filaire, et quelques-uns utilisent des modems sans fil.
  - Entreprises clientes de distribution par relais terrestre

- **Autres sociétés de Rogers**
  - La banque Rogers utilisait le VPN et les services de téléphonie de Rogers.

5.5. Répercussions sur les services d'urgence et d'alertes

5.5.1. Service d'urgence 9-1-1

La panne du réseau central IP a interrompu la connectivité avec les fournisseurs de réseaux 9-1-1 et, par conséquent, avec les centres d'appels de la sécurité publique (CASP). Par conséquent, une grande partie des clients sans fil et filaires de Rogers n'ont pas pu joindre les services d'urgence 9-1-1 pendant la panne. [caviardé]

Pendant la panne, le réseau radio est demeuré opérationnel alors que le réseau central était en panne, ce qui a fait que les téléphones des clients ne passaient pas automatiquement à d'autres réseaux pour les appels d'urgence 9-1-1. Certains clients des services sans fil de Rogers ont pu accéder aux services 9-1-1 dans deux cas. Dans le premier cas, certains appels 9-1-1 ont été effectués avec succès en utilisant le réseau 2G et 3G, où le trafic et la signalisation pouvaient atteindre l'infrastructure à commutation de circuits de Rogers lorsque le réseau central IP fonctionnait par intermittence. Cela n'était pas possible à l'aide du LTE, car le réseau mobile 4G central dépend entièrement du réseau central IP. Comme la connectivité centrale LTE était en panne, certains téléphones ont tenté d'utiliser le réseau 2G et 3G. Rogers a confirmé avoir enregistré un volume d'appels plus important sur son réseau 2G et 3G.

Dans le second cas, Rogers a déclaré que certains téléphones mobiles récents sont automatiquement programmés pour rechercher et utiliser le réseau d'un autre fournisseur de services afin de passer un appel 9-1-1 lorsque le réseau d'origine n'est pas disponible.

[caviardé]

Pour le 8 juillet 2022, Rogers a déclaré avoir été en mesure de traiter [caviardé] de la moyenne quotidienne habituelle d'appels 9-1-1 réussis sur son réseau sans fil. Si l'on ajoute les clients de Rogers qui ont réussi à passer des appels 9-1-1 sur les

réseaux de Bell et de TELUS, Rogers a déclaré que le pourcentage était d'environ [caviardé].

Compte tenu du volume d'appels 9-1-1 sans fil enregistré le 8 juillet 2022, Rogers a pu traiter [caviardé] de ces appels. Rogers a déclaré qu'il n'est pas rare que, pendant une panne, les clients passent des appels 9-1-1 supplémentaires pour tester leur téléphone ou pour s'informer sur la panne. Rogers a ajouté qu'un volume plus élevé d'appels 9-1-1 pourrait être dû au fait que les clients des services sans fil recomposent le 9-1-1 après des appels infructueux.

Pour le réseau filaire, [caviardé] appels 9-1-1 ont réussi le 8 juillet 2022. Cela représente environ [caviardé] de la moyenne quotidienne habituelle. Rogers a déclaré ne pas disposer de statistiques sur le nombre total d'appels 9-1-1 filaires et sur le nombre d'appels au 9-1-1 infructueux.

Pour le 9 juillet 2022, le taux de réussite des appels 9-1-1 s'est amélioré, en atteignant [caviardé] et [caviardé] de la moyenne quotidienne habituelle pour les réseaux sans fil et filaire, respectivement.

5.5.2. Service d'alertes au public

Les clients des services sans fil de Rogers n'ont pas été en mesure de recevoir les messages du service d'alertes sans fil au public de Pelmorex, l'administrateur du service d'alertes au public, qui regroupe les alertes émises par les autorités d'alerte fédérales, provinciales, territoriales ou locales. La plateforme Centre de diffusion de messages de Rogers a pu recevoir des alertes de Pelmorex, mais Rogers n'a pas pu transmettre les alertes à ses clients. [caviardé]

Le service de télévision par câble de Rogers, qui utilise le réseau central IP de Rogers, était en panne et ne permettait pas d'envoyer des alertes.

La plupart des stations de télévision et de radio de Rogers utilisent la connectivité du réseau IP de Rogers et elles n'ont pas pu recevoir les alertes de Pelmorex. [caviardé]

5.6. Communication et avis

Communications avec les clients. Après la panne, la première communication avec les clients de Rogers a été reçue sur Twitter à 8 h 54 HAE, soit 4 h 11 min après l'événement déclencheur. Ce message a été suivi de messages similaires sur Facebook. Les comptes de médias sociaux de Rogers, Fido et Chatr ont publié des mises à jour périodiques au cours de la journée.

Les centres d'appels de Rogers et de Fido ont diffusé un avis sous forme de réponse vocale interactive à partir de 9 h 30 HAE. Les sites Web de Rogers et de Fido ont affiché un message sous forme de bannière quelques minutes plus tard, ainsi que des mises à jour de la bannière de l'assistant virtuel. Certains messages ont également été publiés sur des forums communautaires.

Les stations de radio de Rogers Sports & Media et leurs sites Web ont diffusé un message d'intérêt public à partir de midi le 8 juillet 2022, qui a été répété tout au long de l'après-midi.

Les messages informaient les clients de la panne qui touchait les réseaux sans fil et filaires et indiquaient que le personnel de Rogers s'efforçait de résoudre les problèmes de réseau dès que possible. Ils n'indiquaient pas le délai prévu pour le rétablissement du service. À 17 h 4 HAE, le personnel de Rogers a indiqué pour la première fois que Rogers créditerait les clients pour la perte de service.

Le vice-président principal des réseaux d'accès et de l'exploitation de Rogers a accordé trois entrevues télévisées au cours de l'après-midi et de la soirée du 8 juillet 2022. À 22 h 48 HAE, le directeur général de Rogers a publié un message sur son blogue afin d'indiquer que Rogers travaillait à déterminer la cause du problème et a confirmé que Rogers créditerait les clients.

Communications avec Pelmorex. Pelmorex a communiqué avec Rogers à 9 h 25 HAE (4 h 42 min après le début de la panne) après avoir entendu les médias parler de la panne. Environ 15 minutes plus tard, Pelmorex a diffusé une alerte émise à Langham, en Saskatchewan. Pelmorex a communiqué avec Rogers une seconde fois à 9 h 54 HAE pour demander si l'émission d'une alerte avait aidé Rogers à déterminer si les alertes parvenaient à ses clients. Rogers a confirmé que l'alerte avait été reçue par son Centre de diffusion de messages, mais qu'elle vérifiait la distribution aux appareils sans fil du réseau de Rogers.

À 11 h 19 HAE, Rogers a envoyé un courriel à Pelmorex pour l'informer de la panne nationale et l'aviser que toute agence qui tenterait de diffuser des alertes d'urgence aux clients de Rogers sur les réseaux de Rogers n'y parviendrait pas.

Pendant la panne, Rogers a envoyé deux mises à jour à Pelmorex. La première mise à jour a eu lieu dans l'après-midi du 8 juillet 2022 pour confirmer que les alertes d'urgence émises par le système ADNA ne seraient pas transmises aux utilisateurs de services sans fil qui sont connectés au réseau de Rogers. La deuxième mise à jour a eu lieu dans l'après-midi du 9 juillet 2022 pour informer Pelmorex que le réseau avait été rétabli.

Communications avec les fournisseurs de réseaux 9-1-1. Rogers a prévenu les fournisseurs de réseaux 9-1-1 à 8 h 39 HAE le 8 juillet 2022 (3 h 56 min après le début de la panne). Le message indiquait que le réseau de Rogers était incapable d'émettre et de recevoir des appels à l'échelle nationale, y compris au 9-1-1. Le message demandait aux fournisseurs de réseaux 9-1-1 d'avertir les CASP.

À 17 h 1 HAE, Rogers a envoyé une mise à jour aux fournisseurs de réseaux 9-1-1 pour les informer que la panne était toujours en cours.

À 10 h 51 HAE le 9 juillet 2022, Rogers a informé les fournisseurs de réseaux 9-1-1 que ses réseaux avaient été rétablis.

Communications avec les autorités gouvernementales. Rogers a informé le CRTC de la panne à 11 h 19 HAE le 8 juillet 2022. Rogers a également informé Innovation, Sciences et Développement économique Canada (ISDE) de la panne.

Communications avec les entreprises clientes. Rogers Affaires n'était pas en mesure de communiquer directement avec ses clients. Cependant, certains employés qui disposaient d'autres services de télécommunication ont pu envoyer une réponse automatique à l'aide de l'application logicielle de gestion des relations avec la clientèle en nuage qui est utilisée par les clients de Rogers Affaires. Les clients qui ont pu accéder à l'application auraient pu être avertis en conséquence.

Communications avec d'autres fournisseurs de services. À 6 h HAE le 8 juillet 2022, le dirigeant principal de la technologie de Rogers a communiqué avec ses homologues de Bell et de TELUS pour les informer de la panne et les mettre en garde contre d'éventuelles cyberattaques.

6. Analyse des causes de la panne et de sa résolution

La présente analyse évalue la cause profonde de la panne, l'état du réseau et les procédures opérationnelles mises en place avant et pendant la panne. Elle porte également sur l'architecture globale du réseau de Rogers, ainsi que sur les processus de gestion du changement et des incidents (y compris la communication avec les tiers). Les différents éléments de l'analyse s'appliquent à un ensemble plus large de pannes.

6.1. Analyse de la cause profonde de la panne

Le réseau central IP de Rogers utilise le BGP comme protocole de passerelle extérieure pour annoncer les routes IP aux autres systèmes autonomes, et le protocole OSPF ou le protocole Intermediate System to Intermediate System (IS-IS) comme protocole de passerelle intérieure (PPI) pour annoncer les routes IP à l'intérieur de son propre système autonome. Lorsque le filtre de gestion de la liste de contrôle d'accès a été supprimé de la configuration du routeur de distribution [caviardé].

Rogers a déclaré que la suppression du filtre de gestion de la liste de contrôle d'accès qui distribue les anciennes adresses DNS du BGP au protocole OSPF [caviardé].

Au fil des ans, les FST ont commis des erreurs dans la configuration des mises à jour de la politique du BGP. En conséquence, l'industrie a élaboré des pratiques exemplaires pour se prémunir contre les inondations d'annonces de routes à la suite de mises à jour incorrectes de la politique du BGP[8] :

A. Protection contre les surcharges sur les routeurs centraux [caviardé].

B. Limite du nombre de routes BGP annoncées dans le protocole OSPF par les routeurs de distribution [caviardé].

C. Vérifications manuelles et automatisées des commandes de politique en relation avec la redistribution des routes BGP.

D. Retour automatisé à une configuration antérieure, ce qui permet de limiter la gravité de la panne.

[caviardé]

[8] À titre d'exemple de pratiques exemplaires de l'industrie en la matière, nous suggérons de consulter le document « Meilleures pratiques de déploiement de Cisco IOS XR pour le routage OSPF/IS-IS et BGP » disponible à l'adresse suivante : https://www.cisco.com/c/fr_ca/support/docs/ios-nx-os-software/ios-xr-software/IOS-XR-Best-Practices/IOSXR-Deployment-BestPractices.html#_Toc152750752

[caviardé] La configuration standard de Rogers pour les routeurs de distribution [caviardé] permettait la distribution des routes BGP Internet dans le protocole OSPF. Ainsi, lorsque le filtre de gestion a été supprimé de la déclaration de politique, la configuration standard a mené à la distribution d'un nombre excessif de routes BGP dans le protocole OSPF. Les annonces d'état de liens du protocole OSPF provenant du routeur de distribution surchargent les routeurs centraux de données, ce qui les fait tomber en panne.

Le fait de ne pas avoir mis en œuvre les mesures de protection susmentionnées était un oubli de la part de Rogers et n'a pas [caviardé].

[caviardé]

[caviardé]

6.2. Architecture et résilience du réseau

Vous trouverez ci-dessous notre évaluation des différents éléments de l'architecture et de la conception du réseau par rapport à la panne de Rogers de juillet 2022 et la cause profonde sous-jacente, qui s'applique à un ensemble plus large d'aspects liés à la résilience du réseau.

Redondance du réseau central IP. Rogers dispose d'un réseau de transport redondant qui relie les différents sites du réseau central IP sur lequel reposent les réseaux filaires et sans fil. [caviardé]

Selon notre évaluation, l'architecture de réseau de Rogers est conçue pour être fiable et suit les pratiques exemplaires de l'industrie. [caviardé] Des modèles visant une séparation logique du routage pour mieux isoler les nœuds défectueux font partie des choix de conception.

Redondance du réseau central par paquets sans fil. Le réseau central national sans fil qui comprend le réseau central mobile par paquets (données mobiles) et le réseau central de services (voix, messagerie texte, messagerie multimédia, [caviardé] Chaque région dispose d'une redondance physique et logique, avec [caviardé] sites par région pour la redondance interrégionale. Le réseau central sans fil dépend du réseau central IP, ce qui l'a rendu inopérant pendant la panne du réseau central IP.

Conception d'un réseau central IP filaire et sans fil convergent. Le réseau central IP prend en charge les réseaux filaires et sans fil. La panne de juillet 2022 était limitée au réseau central IP commun, ce qui a eu une incidence considérable, car elle a touché à la fois les services sans fil et les services filaires. Selon notre évaluation, il ne s'agit pas d'un défaut de conception, mais plutôt d'un choix de conception de réseau que Rogers a fait et dont la topologie est similaire à celle adoptée par de nombreux autres fournisseurs de services de niveau 1 dans le monde. Toutefois, des réseaux centraux IP sans fil et filaires distincts pourraient aider à limiter une défaillance à un seul de ces réseaux.

Conception d'un réseau central IP multifournisseur. L'explication de Rogers sur la différence entre la façon dont les routeurs [caviardé] gèrent les annonces d'état de liens ne doit pas être interprétée comme un problème d'interopérabilité entre les deux routeurs [7 : Q5 et Q6; 13 : Q40]. [caviardé]

Les fournisseurs de services du monde entier déploient des systèmes provenant de plusieurs fournisseurs pour diverses raisons, notamment pour éviter la dépendance à l'égard d'un fournisseur ou pour des caractéristiques et des résultats spécifiques qui les distinguent. Les routeurs [caviardé] sont parmi les plus courants dans les réseaux de télécommunications. Leurs systèmes d'exploitation [caviardé] sont parmi les plus connus de l'industrie. Les deux solutions offrent une mise en œuvre robuste du protocole OSPF : l'interopérabilité du routage n'est pas un problème. Toutefois, il existe des différences entre les solutions des deux fournisseurs en ce qui concerne les structures de configuration[9], l'automatisation, la syntaxe de l'interface de ligne de commande et certains comportements par défaut. Les ingénieurs qui travaillent sur les routeurs d'un fournisseur dans un réseau multifournisseur doivent connaître les routeurs des autres fournisseurs pour les configurer et les dépanner efficacement.

Plus précisément, le déploiement de [caviardé] à la périphérie et de [caviardé] au cœur est un modèle de déploiement commun à différents exploitants de télécommunications, avec des pratiques exemplaires bien documentées.

Architecture du service d'urgence. Les services 9-1-1 partagent des voies physiques et logiques communes avec les réseaux publics filaires et sans fil fixes. Dans la configuration du réseau de Rogers, nous supposons qu'aucun mécanisme de résilience supplémentaire n'a été mis en œuvre pour acheminer spécifiquement le trafic de données 9-1-1 vers d'autres voies à la périphérie et au cœur du réseau. Nous notons que certains exploitants de réseaux de télécommunications prévoient une infrastructure de secours consacrée au trafic d'urgence, en plus de mécanismes de priorisation précis.

Infrastructure de gestion de réseau. Un réseau de gestion permet d'accéder aux sites d'infrastructures essentielles ou aux équipements d'un réseau afin d'en permettre le dépannage et la réparation. Pendant la panne de juillet 2022, Rogers a perdu l'accès aux éléments du réseau pendant plusieurs heures et a dû envoyer physiquement des techniciens sur les sites pour les rétablir. [caviardé]

Surveillance et dépannage du réseau. [caviardé]

Essai et validation en laboratoire. Lorsque des changements de configuration sont planifiés sur des éléments du réseau central, il est d'usage d'essayer la nouvelle configuration et de la valider en laboratoire, en particulier pour les changements de liste de contrôle d'accès et de filtre. Il s'agit d'une précaution,

[9] Par exemple, [caviardé].

compte tenu des conséquences désastreuses d'éventuelles défaillances dans le réseau central.

Rogers a classé le processus global – dont la configuration du filtre de gestion n'est qu'un des nombreux éléments – comme à « haut risque ». Toutefois, comme certaines parties antérieures du processus ont été menées à bien, le niveau de risque a été ramené à « faible ». Il s'agit d'un oubli dans la gestion des risques, car le risque élevé associé aux changements de la politique du BGP qui ont été mis en œuvre à la périphérie et qui ont affecté le cœur du réseau n'a pas été pris en compte.

[caviardé]

Conception d'un scénario de gestion de la résistance du réseau. Les tests de résistance du réseau portent sur plusieurs composantes du réseau, y compris les scénarios de contrainte de routage et les scénarios de tempête de signalisation. Les actions de Rogers pendant la résolution de la panne montrent une bonne planification pour faire face aux tempêtes de signalisation (principalement celles qui touchent le système multimédia IP et le réseau central mobile par paquets). [caviardé]

6.3. Processus de gestion des affaires

Les processus de gestion des affaires comprennent les processus de gestion du changement et de gestion des incidents. Nous présentons ci-dessous notre évaluation des activités relatives à ces deux processus dans le cadre de la panne de juillet 2022. L'évaluation porte sur les processus d'exploitation et de gestion du réseau et sur les processus de gestion des interactions avec les clients et les partenaires.

6.3.1. Processus de gestion du changement

La gestion du changement est une approche systématique de la gestion des modifications de l'infrastructure et des services du réseau. Il s'agit d'un processus conçu pour réduire le risque d'interruption des services et pour garantir que les changements sont contrôlés et mis en œuvre de manière efficace. Nous présentons ci-dessous notre évaluation des processus de gestion du changement de Rogers en ce qui concerne les activités liées à la panne de juillet 2022. [caviardé]

Évaluation des risques dans la gestion du changement. Rogers a déclaré que la modification de la configuration des routeurs centraux et de distribution spécifiée par [caviardé], qui a ensuite causé la panne, était la sixième de sept phases d'un processus de mise à niveau du réseau qui avait commencé quelques semaines plus tôt. Cette mise à jour de la configuration faisait partie d'une série de changements requis dans le cadre des exigences opérationnelles et de la conception de l'architecture de réseau.

Avant que cette mise à jour de la configuration ne soit mise en œuvre, il y avait une autre mise à jour de la configuration pour [caviardé], qui était « Terminée – sans problème » avant l'exécution de [caviardé]. Les deux demandes de changement au réseau (DCR) ont été désignées par l'équipe de gestion des incidents de Rogers comme des causes potentielles de la panne. Les premiers efforts de rétablissement se sont concentrés sur le retour à [caviardé].

Rogers avait évalué le risque du premier changement de ce processus en sept phases comme étant « élevé ». Les modifications ultérieures de la série ont été classées comme un risque « moyen ». [caviardé] présentait un risque « faible » selon l'algorithme de Rogers qui prend en compte les succès antérieurs dans l'évaluation des risques. La valeur du risque lié à [caviardé] a donc été ramenée à « faible » en raison de la réussite des modifications précédentes.

L'évaluation du risque comme étant « faible » n'est pas conforme aux pratiques exemplaires de l'industrie pour les changements de configuration des protocoles de routage, en particulier lors de la distribution des routes BGP dans le protocole OSPF au sein du réseau central IP. Une telle modification de la configuration devrait être considérée comme présentant un risque élevé et être mise à l'essai en laboratoire avant d'être déployée dans le réseau de production.

Vérification des changements de configuration. Les pratiques exemplaires prévoient des vérifications manuelles et automatisées propres aux changements de configuration. [caviardé].

Hiérarchisation des alarmes liées à la mise à niveau. [caviardé]

Retour automatisé à la configuration. Le retour automatisé à la configuration n'a pas été configuré sur les routeurs centraux et de distribution[10]. Ce mécanisme ramènerait le routeur à une configuration antérieure si l'ingénieur qui effectue les mises à niveau perdait l'accès au routeur avant de confirmer les mises à niveau et après un certain laps de temps à compter de la saisie des commandes. En ce qui concerne la panne de juillet 2022, il est difficile de savoir si le retour automatisé à la configuration aurait été utile dans le cas des routeurs de distribution.

Accès limité à l'assistance des fournisseurs. La présence et la participation directe d'ingénieurs experts en routage de [caviardé] auraient été essentielles pour vérifier les changements de configuration et le dépannage. Les fournisseurs n'ont pas été activement impliqués dans les premières phases de la panne. [caviardé]

[caviardé]

Effet de la mise en œuvre de changements multiples. Plusieurs changements de configuration ont été planifiés au cours de la même fenêtre de maintenance[11]. Cette situation a nui aux efforts de rétablissement de la panne, car il était difficile

[10] Comme l'a indiqué Rogers lors d'un appel téléphonique le 1er septembre 2023.
[11] Ces changements n'ont pas été détaillés par Rogers, mais nous avons pu les déduire de la chronologie et des réponses de Rogers.

de décider quelle DCR devait être annulée. Les nombreux changements de configuration ont contribué à un mauvais diagnostic de la cause profonde dans les premières heures de la panne. Ainsi, les techniciens se sont d'abord concentrés sur les routeurs centraux au lieu d'adopter une vision holistique qui tient compte des routeurs de distribution dans le contexte des changements.

6.3.2. Processus de gestion des incidents

La gestion des incidents est une approche systématique du recensement des incidents qui touchent les services du réseau, de la réponse à ceux-ci et de leur résolution. Elle vise à réduire l'incidence des incidents sur les utilisateurs en rétablissant le service normal le plus rapidement possible. Vous trouverez ci-dessous notre évaluation des processus de gestion des incidents de Rogers et de la manière dont Rogers a réagi à l'incident une fois que la panne s'est produite. Plus précisément, le temps nécessaire pour déterminer la cause profonde de la panne et rétablir les services témoigne de l'efficacité et de l'efficience des processus de gestion des incidents.

Processus de continuité des activités – exécution. Rogers dispose d'un programme de reprise après sinistre et de continuité des activités qui englobe une série de politiques, de protocoles et de procédures soutenus par « une équipe diversifiée ». Le programme de continuité des activités s'appuie sur une équipe centrale dédiée à la continuité des activités, un organe directeur et des ressources départementales localisées. Selon Rogers, l'équipe de la continuité des activités suit une formation annuelle, se perfectionne en permanence, fait l'objet d'évaluations régulières et adopte des pratiques formelles en matière de réponse aux incidents [10 : Q54]. Cependant, la panne de juillet 2022 a mis en évidence des lacunes dans l'exécution des processus de continuité des activités (p. ex. le nombre limité de cartes SIM pour la communication et le manque de connectivité de secours). [caviardé]

Processus de continuité des activités – gestion des incidents. Rogers a déclaré qu'elle dispose d'un processus complet de réponse aux incidents pour le CER. Rogers classe les incidents selon trois niveaux en fonction de critères précis, comme la perturbation de l'infrastructure, les répercussions financières, le risque pour la sécurité des employés, les répercussions sur les clients et la durée estimée de ces répercussions [12 : Q68].

Chaque niveau d'incident correspond à une intervention et à une équipe prédéfinies. Rogers a déclaré suivre une approche structurée qui oriente les réponses tactiques et opérationnelles en faisant appel à l'équipe de gestion de crise appropriée, à l'équipe interfonctionnelle de gestion des incidents et aux équipes départementales de gestion des incidents en fonction de la classification de l'incident.

Les incidents de niveaux 2 et 3 sont considérés comme particulièrement perturbateurs et ils sont classés comme « critiques ». Dans ce tels cas, l'équipe de

gestion des incidents de l'exploitation réseau est convoquée par le directeur de la gestion du réseau national du centre d'exploitation du réseau, qui activera le centre des opérations d'urgence (également connu sous le nom de « cellule de crise ») et lancera le plan de gestion des incidents critiques.

Rogers a correctement classé la panne de juillet 2022 au niveau 3. Une telle classification nécessite que le centre des opérations d'urgence soit entièrement doté en personnel et que des intervenants externes soient impliqués (p. ex. l'assistance des fournisseurs, les partenaires de l'écosystème 9-1-1, etc.). Cependant, le processus de convocation et de rassemblement du personnel à des points prédéfinis a été entravé, car la plupart des employés de Rogers dépendaient des réseaux sans fil et filaire de Rogers qui étaient en panne.

Préparation aux situations d'urgence. [caviardé]

Prise de décision et flux de travail interservices. Au cours des premières heures de la panne, il y a eu certaines lacunes dans la façon dont les différents départements de Rogers ont interagi. Bien que cela puisse être dû à une communication limitée entre les employés, cela pourrait indiquer d'autres lacunes dans la façon dont les différents services interagissent les uns avec les autres.

L'équipe de gestion des incidents a désigné deux demandes de changement au réseau comme étant la cause profonde possible de la panne :

[caviardé]

Connectivité de secours pour les sites éloignés. Il n'y avait pas de liaison de connectivité de secours vers le CER et vers d'autres sites éloignés. Cela a retardé l'accès aux éléments essentiels du réseau auxquels il fallait accéder physiquement en envoyant du personnel sur certains sites. L'absence d'accès de secours au réseau vers le CER et les sites éloignés indique que le plan de reprise après sinistre n'a pas fait l'objet d'exercices et d'essais approfondis.

Communication limitée entre les membres du personnel de Rogers. La panne a entravé la communication entre les membres du personnel technique de Rogers qui ne disposaient pas d'un nombre suffisant de lignes d'accès au réseau mobile d'un autre fournisseur de services à utiliser en cas de défaillance du réseau. Rogers a obtenu des cartes SIM d'autres exploitants de réseaux mobiles et les a acheminées physiquement aux sites pour permettre aux employés de Rogers de communiquer avec la cellule de crise quelques heures après le début de la panne. Tard dans la journée du 8 juillet 2022, des membres du personnel ont été envoyés sur place pour apporter les ressources nécessaires.

[caviardé]

Retard ou manque d'implication des fournisseurs. [caviardé]

Rapport d'analyse de la cause profonde. [caviardé]

Accès physique aux centres de données et aux nœuds d'infrastructure. Le personnel de Rogers est arrivé au CER 2 h 7 min après le début de la panne. Il est difficile de savoir quand le personnel est arrivé aux autres sites éloignés et aux centres de données. Cependant, Rogers a déclaré qu'elle avait envoyé des cartes SIM d'autres exploitants aux sites éloignés près de cinq heures après le début de la panne. Il s'agit d'un délai relativement long, compte tenu de la criticité de la panne. Les pratiques exemplaires exigent une présence physique à proximité des sites éloignés s'ils sont jugés essentiels pour l'ensemble de l'infrastructure.

Hiérarchisation du rétablissement des services. Rogers a accordé la plus haute priorité au rétablissement des services sans fil selon l'ordre de priorité suivant :

1. Services sans fil
2. Services filaires
   [caviardé]

Avec plus de 10 millions d'abonnés sans fil, Rogers a eu raison de se concentrer d'abord sur le rétablissement des services sans fil pour permettre au plus grand nombre de clients d'accéder aux services 9-1-1.

Les services filaires figurent en deuxième position sur la liste des priorités, suivis par [caviardé]

Rogers a fait remarquer que de nombreux services de soins intensifs et clients d'infrastructures majeures disposent d'une connectivité de secours. La mise en place d'une connectivité de secours fait toujours partie des bonnes pratiques opérationnelles pour cette catégorie d'organisations.

6.3.3. Communication avec les parties externes

La réussite d'une réponse à un incident passe par une communication externe efficace : opportune, précise, claire et concise, cohérente et empathique. Les clients et les partenaires doivent être tenus informés de la situation afin qu'ils puissent prendre les mesures qui s'imposent. La section ci-dessous évalue la communication de Rogers avec ses clients et ses partenaires pendant la panne de juillet 2022.

Avis relatifs aux services d'urgence et aux alertes. Rogers a avisé les fournisseurs de réseaux 9-1-1 quatre heures après le début de la panne. Rogers a envoyé une mise à jour aux fournisseurs de réseaux 9-1-1 avant que le service ne soit rétabli le 9 juillet 2022. Rogers a fait valoir que le CER ne disposait d'aucune connectivité, ce qui empêchait l'envoi plus rapide d'un avis. Ainsi, les fournisseurs de réseaux 9-1-1 ont été informés « dès que le CER de Rogers a été en mesure d'établir des communications et de déterminer les répercussions précises ». [7 : Q11]

La politique réglementaire 2016-165 ne traite pas directement des pannes du service 9-1-1 causées par une défaillance du réseau d'origine. La décision de

télécom 2017-389 [3] exclut les recommandations du Groupe de travail Services d'urgence concernant les avis de panne du réseau d'origine [4]. Bien que Rogers ne soit pas tenu d'informer les fournisseurs de réseaux 9-1-1, différents forums de l'industrie demandent aux fournisseurs de réseaux d'origine, comme Rogers, d'informer les fournisseurs de réseaux 9-1-1 en temps opportun. Par exemple, le Groupe de travail Services d'urgence recommande ce qui suit [4] :

1. Les fournisseurs de réseaux d'origine doivent informer le fournisseur de réseaux 9-1-1 dès que possible.
2. Les fournisseurs de réseaux d'origine qui procèdent à un avis doivent fournir toute mise à jour importante au fournisseur de réseaux 9-1-1 dès que possible.
3. Les fournisseurs de réseaux d'origine qui procèdent à un avis doivent communiquer au fournisseur de réseau 9-1-1 la résolution de tout problème du réseau 9-1-1 d'origine qui a été signalé.

En outre, nous attirons l'attention sur le deuxième rapport et l'ordonnance de la Commission fédérale des communications (FCC) sur l'amélioration de la fiabilité du 9-1-1 du 18 novembre 2022 [5]. La FCC exige que les fournisseurs de réseaux d'origine « informent les installations spéciales des services 9-1-1[12] des pannes dès que possible, mais au plus tard dans les 30 minutes qui suivent la découverte de la panne susceptible de toucher les services 9-1-1 » [notre traduction]. La FCC fixe des exigences supplémentaires concernant les moyens de communication : une double exigence de communiquer par téléphone et par courriel, ainsi que des exigences relatives au contenu et à la fréquence des mises à jour (deux heures).

Rogers a mis encore plus de temps à informer Pelmorex de la panne. En fait, c'est Pelmorex qui a d'abord communiqué avec Rogers à la suite du signalement de la panne par les médias. De plus, dans ce cas, le CRTC n'impose pas à Rogers ou à d'autres fournisseurs de réseaux d'origine d'aviser l'administrateur de l'ADNA.

Le long délai observé avant l'avis aux fournisseurs de réseaux 9-1-1 et à l'administrateur de l'ADNA, ainsi que la manière dont les avis ont été effectués, révèlent que le plan de gestion des incidents de Rogers ne comportait pas de plan de communication bien conçu avec ces parties externes, ou qu'il n'a pas été respecté. L'avis aux fournisseurs de réseaux 9-1-1 et à l'administrateur de l'ADNA ne doit pas provenir du CER, mais d'une personne désignée par Rogers à cette fin. Malgré la gravité de la panne, qui a obligé Rogers à consacrer beaucoup d'attention au rétablissement de ses services, il aurait fallu avoir accès à d'autres moyens de communication et s'entraîner à différents scénarios de panne pour pouvoir aviser en

[12] Toute entité qui fournit des services 9-1-1, E9-1-1 ou 9-1-1, PG tels que l'acheminement des appels, l'affichage automatique d'adresses, l'affichage automatique du numéro, ou l'équivalent fonctionnel de ces services, directement à un CASP.

temps utile les fournisseurs de réseaux 9-1-1 et, par conséquent, les CASP et l'administrateur de l'ADNA.

Communication avec les clients. Rogers a d'abord avisé ses clients de la panne au moyen d'un message sur Twitter à 8 h 54 HAE, [caviardé].

D'autres messages ont été envoyés aux clients de Rogers, de Fido et de Chatr au cours de la journée par l'intermédiaire de différents canaux :

- Médias sociaux : Twitter, Facebook et Instagram
- Soutien à la clientèle par une réponse vocale interactive destinée aux clients de Rogers et de Fido
- Page d'accueil de Rogers, de Fido et de Chatr, soutien et bannières du centre de panne
- Forums communautaires
- Soutien technique par clavardage en direct
- Messages d'intérêt public par l'intermédiaire des stations de radio de Rogers Sports et Media et de leurs sites Web

Les messages étaient de nature générale et ne fournissaient aucun détail sur la nature et la gravité de la panne. Plus important encore, Rogers n'a pas indiqué la manière dont les clients pouvaient accéder aux services d'urgence pendant la panne (p. ex. en ne déconnectant pas l'appel prématurément, ou en retirant les cartes SIM des téléphones portables des clients pour accéder à un réseau tiers).

Communication avec les clients d'affaires. Rogers Affaires n'était pas en mesure de communiquer directement avec les clients d'affaires. Certains employés dotés d'une autre connexion à domicile ont pu configurer une réponse automatique [caviardé]

Coordination tardive avec les exploitants tiers. [caviardé]

Communication avec l'ensemble de la communauté des télécommunications et Internet. Rogers a communiqué certaines informations sur les causes de la panne à d'autres exploitants de télécommunications du Comité consultatif canadien pour la sécurité des télécommunications (CCCST). Nous notons également que de nombreux exploitants de télécommunications qui ont connu des pannes majeures ont fourni des explications détaillées à l'ensemble de la communauté Internet par l'intermédiaire de forums spécifiques, tels que le NANOG ou l'Internet Engineering Task Force (IETF), en vue de communiquer des informations et d'aider d'autres opérateurs de réseaux à éviter des pannes similaires.

7. Analyse des décisions d'amélioration à la suite de la panne

Après la panne, Rogers a pris plusieurs mesures pour améliorer ses processus commerciaux et opérationnels et pour modifier l'architecture de son réseau. Certaines de ces améliorations de la résilience du réseau sont directement liées à la résolution des causes de la panne de juillet 2022 et à la prévention de facteurs similaires susceptibles d'entraîner une panne de service à l'avenir. D'autres sont motivées par la stratégie commerciale et technologique de l'entreprise, comme l'évolution du réseau sans fil vers la technologie 5G. La présente section présente et évalue les avantages potentiels des améliorations apportées par Rogers pour renforcer la résilience du réseau.

7.1. Amélioration de l'architecture et de la résilience du réseau

Les réseaux publics sans fil et filaires sont conçus pour répondre à des objectifs précis en matière de résilience. L'atteinte de ces objectifs nécessite une évaluation continue de toutes les dimensions architecturales qui ont une incidence sur la résilience, y compris les choix technologiques, la sélection des fournisseurs de solutions et le déploiement et le soutien opérationnels. Ces éléments ont une incidence directe sur les coûts d'investissement et d'exploitation. Le choix des solutions à mettre en œuvre entraîne des compromis particuliers qui doivent être analysés. Rogers a décidé de mettre en œuvre plusieurs changements architecturaux afin de s'attaquer aux causes profondes de la panne et de prévenir des pannes plus importantes. Ces changements sont décrits ci-dessous, et ils sont accompagnés de notre évaluation de leur efficacité.

Protection contre les surcharges de routage. La surcharge des routeurs du réseau de Rogers en raison d'une mauvaise configuration est à l'origine de la panne de juillet 2022. La surcharge de routage est une inondation soudaine de données de routage envoyées au routeur qui dépasse les capacités de traitement du routeur. En général, le routeur tombe en panne et ne peut plus acheminer de trafic. [caviardé]

Nous estimons que les mécanismes de protection contre les surcharges de routage mis en place par Rogers sont essentiels pour éviter qu'une panne similaire ne se produise à l'avenir. Rogers et ses fournisseurs doivent procéder à une vérification continue de ces mécanismes, car la technologie et les architectures de réseau connexes évoluent.

Gestion de la surcharge des tempêtes de signalisation. Une tempête de signalisation dans un réseau mobile fait référence à une augmentation soudaine et imprévue du trafic de signalisation. Les tempêtes de signalisation se produisent pour diverses raisons, par exemple lorsque de nombreux appareils tentent simultanément de se connecter au réseau à la suite d'une panne de réseau. Au cours du processus de rétablissement de la panne de juillet 2022, Rogers a mis en

œuvre l'une des leçons les plus importantes de sa panne d'avril 2021, à savoir le ralentissement artificiel du trafic de manière préventive ou l'ajout progressif d'abonnés pour éviter les tempêtes de signalisation lorsque le réseau mobile se rétablit d'une panne. Cela a permis de rétablir progressivement et sans heurts les services du réseau lors de la panne de juillet 2022. La gestion des tempêtes de signalisation est un aspect essentiel de la reprise après une panne, qui devrait faire partie de toute gestion du trafic sur le réseau.

Nous estimons que Rogers a mis en place des mécanismes appropriés de protection contre les tempêtes de signalisation et les a déployés avec succès pendant la panne. Ces mécanismes doivent être mis à l'essai et évalués en permanence, car il s'agit de l'une des causes profondes les plus courantes des pannes pour les exploitants de réseaux mobiles.

Séparation des réseaux centraux IP filaires et sans fil. Les réseaux sans fil et filaires de Rogers partagent un réseau central IP commun qui sert à acheminer le trafic des utilisateurs vers Internet et les services du réseau. La mise en œuvre de réseaux centraux IP distincts pour les réseaux sans fil et filaires permet de limiter une panne à leur réseau d'accès respectif et, par conséquent, d'éviter le type de panne de réseau catastrophique que l'on a connu le 8 juillet 2022, où les services sans fil et filaires n'étaient pas disponibles en raison d'une panne du réseau central IP commun. L'hypothèse sous-jacente pour éviter une panne commune dans les réseaux sans fil et filaires avec des réseaux centraux IP distincts est que les mises à niveau propres au réseau filaire et au réseau sans fil ne se produisent pas simultanément et n'aient pas les mêmes effets. Par conséquent, si un réseau central IP était touché par une panne, l'autre réseau central IP resterait intact et opérationnel.

La séparation du réseau central IP est une décision stratégique qui doit être envisagée dans le contexte des objectifs opérationnels globaux de Rogers et pas uniquement du point de vue de la panne de juillet 2022. Il s'agit avant tout d'une décision de compromis entre les coûts, la résilience et la complexité opérationnelle. Nous constatons que plusieurs grands exploitants de télécommunications ont fait converger leurs réseaux centraux filaires et sans fil.

Rogers affirme qu'un réseau central IP sans fil indépendant améliorerait le rendement et la résilience de son réseau sans fil. Selon Rogers, les avantages du nouveau réseau IP sans fil sont les suivants [12 : Q70] :

A. Offrir de nouvelles expériences sans fil avec une meilleure qualité de service.

B. Prendre en charge les fonctions de mobilité telles que le transfert ininterrompu et la continuité de la session entre les régions afin d'améliorer l'expérience du client et de réduire la latence.

C. Exploiter les outils modernes d'automatisation des flux de travail pour mettre en place le réseau IP dédié et le centre de données.

D. Rationaliser les activités des fenêtres de maintenance à l'aide de tableaux de bord de gouvernance opérationnelle.

E. Fournir des fonctions d'automatisation et d'orchestration complètes.

Nous estimons que la séparation des réseaux centraux filaires et sans fil présente des avantages en termes d'isolation des pannes et de résilience, mais qu'elle s'accompagne d'une augmentation des fonctions de gestion et des coûts du réseau. Cette séparation permettrait à Rogers d'éviter une panne simultanée des noyaux IP pour les réseaux sans fil et filaires, comme cela s'est produit en juillet 2022.

Redondance réciproque entre les réseaux centraux sans fil et filaires. Rogers a décidé de séparer physiquement et logiquement les réseaux centraux IP sans fil et filaire. Rogers est en train d'évaluer la possibilité que le noyau IP d'un réseau d'accès serve de solution de rechange pour l'autre réseau d'accès en cas de défaillance de son réseau central IP. Par exemple, le noyau IP du réseau sans fil servirait de solution de rechange au réseau filaire en cas de défaillance de son noyau IP, et vice versa. Rogers a indiqué qu'il était en train d'évaluer les conceptions de réseau et qu'il n'y avait pas de calendrier pour la mise en œuvre de ce modèle de redondance.

Nous estimons qu'une redondance réciproque entre les réseaux centraux IP sans fil et filaires augmenterait la résilience et permettrait de mieux faire face à certains scénarios de défaillance. Cependant, la redondance réciproque nécessite une conception minutieuse et s'accompagne d'une complexité de mise en œuvre accrue en termes de redondance, d'ingénierie, de capacité du réseau et de gestion du trafic.

Augmentation de la résilience du réseau de gestion. [caviardé] Par conséquent, le personnel de Rogers n'a pas pu accéder à distance aux éléments du réseau pendant la panne. Cela a entravé leurs efforts pour déterminer la cause profonde de la panne et pour prendre rapidement des mesures de rétablissement et de restauration des services. Après la panne, Rogers a apporté les améliorations suivantes pour remédier à cette lacune :

1. Mise en œuvre d'un réseau IP de gestion physique et logique distinct, appelé [caviardé], qui est utilisé pour se connecter à tous les éléments du réseau pour la gestion intrabande et hors bande. [caviardé] possède son propre noyau, sa propre distribution et ses propres couches d'accès. [caviardé] qui dispose d'une connectivité diversifiée et redondante [caviardé] les éléments du réseau sont accessibles à la fois intrabande et hors bande, comme les éléments du réseau de production [9 : Q8].

2. Mise à niveau de [caviardé] pour améliorer la redondance, la résilience, le basculement régional et la latence [13 : Q67, 12 : Q77].

3. Pour les sites [caviardé], Rogers a mis en place un réseau de gestion hors bande dont la connectivité provient de fournisseurs de services tiers. Plus

précisément, cette connectivité s'étend à l'infrastructure de la console qui est en interface avec les éléments du réseau.

Un réseau de gestion doté d'une infrastructure de transmission de données dédiée offre plusieurs avantages, notamment :

A. **Isolation du trafic** : Un réseau de gestion distinct isole le trafic de la gestion à faible bande passante du trafic des utilisateurs à large bande passante et garantit que ces types de trafic ne sont pas en concurrence pour la bande passante.

B. **Sécurité et contrôle d'accès** : Il est plus facile de sécuriser un réseau de gestion distinct que le réseau de transport (plan de données), car le réseau de gestion n'est généralement pas accessible aux utilisateurs ou aux applications du réseau de transport. Cela pourrait contribuer à réduire le risque d'une faille de sécurité au sein des dispositifs et des services critiques du réseau.

C. **Dépannage simplifié** : Un réseau de gestion distinct, à la fois intrabande et hors bande, permet aux administrateurs de réseau de continuer à surveiller, à diagnostiquer et à dépanner le réseau en cas de panne sans dépendre du réseau de production.

Nous estimons que l'utilisation des modèles de redondance est obligatoire pour la gestion du réseau telle qu'elle est décrite ci-dessus. Ces modèles de redondance doivent garantir un accès rapide et efficace au CER et aux éléments du réseau en cas de panne. Nous recommandons d'améliorer davantage la redondance grâce à des technologies supplémentaires d'accès au réseau, comme l'utilisation de réseaux non terrestres.

Partitionnement du réseau. Le partitionnement du réseau est une approche qui sépare ou partitionne le réseau en plusieurs régions afin d'améliorer la résilience du réseau. Chaque partition fonctionne comme une unité indépendante, ce qui permet d'isoler les pannes et les défaillances dans une région spécifique, pour ainsi éviter qu'elles touchent l'ensemble du réseau. Les réseaux de Rogers sont divisés en plusieurs régions, comme on peut s'y attendre pour améliorer la résilience du réseau (isoler les pannes) et l'expérience des utilisateurs (optimiser le flux de trafic, réduire la congestion).

[caviardé]

Un autre élément de différenciation par rapport à l'architecture antérieure à la panne réside dans la conception du noyau de la prestation de services (p. ex. système multimédia IP, messagerie texte, passerelle Internet). Rogers a renforcé la résilience du noyau de la prestation de services en mettant en œuvre ce qui suit :

1. Noyau mobile par région avec redondance physique et géographique au sein de chaque région et entre elles [9 : Q7].

2. Éléments IP clés par région, comme les réflecteurs de route, les interconnexions réseau à réseau à l'interface des réseaux des services filaires et sans fil, et les passerelles Internet dédiées aux réseaux filaires et sans fil.

Nous estimons que cette architecture améliorerait la résilience en isolant mieux les défaillances potentielles au sein d'une région et réduirait le risque que d'autres régions soient touchées [7 : Q2c]. Nous notons que Rogers disposait déjà de plusieurs mécanismes de partitionnement logique lors de la panne de juillet 2022, mais que la nature de la panne a limité leur efficacité. Nous suggérons qu'au fil du temps, Rogers analyse et évalue soigneusement la mise en œuvre d'autres moyens de partitionnement logique du réseau, tels que l'introduction de hiérarchies de routage.

Autre amélioration de la résilience du réseau. Après l'évaluation interne de la panne de juillet 2022 et un dialogue avec ses fournisseurs, Rogers a pris des mesures supplémentaires et a prévu d'introduire des fonctions supplémentaires dans le réseau IP afin d'améliorer la résilience du réseau [9 : Q16, 13: Q66] :

1. Fonctions et mesures qui ont été mises en œuvre ou sont en cours de déploiement :

    [caviardé]

Nous estimons que les améliorations de la résilience proposées ci-dessus ont une incidence directe sur l'amélioration non seulement de la résilience, mais aussi de la cybersécurité et de la mise à l'échelle du réseau. Plus important encore, le processus de décision de ces améliorations, notamment la collaboration étroite avec les fournisseurs de réseaux, devrait faire l'objet d'un processus d'amélioration continue au sein de Rogers, d'autant plus que les technologies de réseau évoluent rapidement, ce qui nécessite des adaptations rapides des mécanismes de résilience du réseau.

Surveillance du réseau. [caviardé] Les événements de panne et les alarmes aident les ingénieurs à résoudre les problèmes et à cerner la cause profonde des défaillances. Rogers a mis à jour sa suite actuelle d'outils de gestion de réseau pour : 1. étendre la portée de la surveillance des événements du réseau et de consignation des événements du système; et 2. mettre les outils de gestion du réseau à la disposition d'un plus grand nombre d'utilisateurs. Rogers a également acquis une nouvelle capacité de corrélation et de surveillance en temps réel de la télémétrie de routage, du trafic et de l'analyse du rendement [12 : Q63].

Voici un résumé des mesures d'adaptation de la surveillance du réseau :

[caviardé]

Nous estimons que l'outil nouvellement acquis et l'amélioration des outils de surveillance existants permettraient à Rogers de mieux prévenir les pannes et de mieux déterminer les causes des erreurs qui surviennent dans l'exploitation du réseau. Cependant, nous suggérons à Rogers de faire évoluer progressivement les

outils qu'elle utilise pour répondre aux tendances actuelles en matière de réseaux, notamment la logiciellisation et la virtualisation, qui sont des priorités absolues pour les exploitants de télécommunications.

Accès à un autre exploitant pour la gestion et l'exploitation du réseau. Rogers s'est appuyée sur son réseau central pour connecter ses sites éloignés, y compris son CER, ses bureaux d'entreprise et ses centres de diffusion. La panne de juillet 2022 du réseau central IP de Rogers a paralysé la communication interne et externe de Rogers et a entravé les efforts de Rogers visant à répondre efficacement et rapidement à la panne dès les premières heures. En réponse, Rogers a déployé sur ses sites une connectivité Internet provenant de FSI tiers afin de pallier la perte de communication au cas où ses réseaux subiraient une panne. Il s'agit des installations suivantes :

[caviardé]

Rogers est également en train d'évaluer l'utilisation d'une connectivité de secours par satellite pour certains emplacements stratégiques [10 : Q73].

Nous estimons que le fait de doter le CER et d'autres sites éloignés d'une connectivité provenant d'exploitants de réseaux de télécommunications tiers offre un niveau adéquat de redondance de la gestion du réseau et augmentera la résilience du réseau. Nous suggérons à Rogers d'y ajouter une connectivité par satellite pour les emplacements du réseau jugés les plus stratégiques.

Protocole d'entente sur la fiabilité des télécommunications. Rogers a indiqué qu'il était signataire du protocole d'entente sur la fiabilité des télécommunications de septembre 2022. Le protocole d'entente a été conclu au CCCST à la demande d'ISDE à la suite de la panne de juillet 2022. Il s'agit d'une entente-cadre entre 12 grands FST[13] relative à l'itinérance d'urgence, l'assistance mutuelle et aux protocoles de communication d'urgence en cas de panne de réseau, en vue d'informer le public et le gouvernement lors de pannes majeures et de situations d'urgence.

1. **Itinérance d'urgence** : Rogers a conclu des accords bilatéraux d'itinérance d'urgence avec Bell, TELUS, SaskTel, Eastlink et Vidéotron ou Freedom concernant les services d'itinérance pour les services d'urgence 9-1-1 et les services vocaux [10 : Q65]. Ces accords précisent les mécanismes, le type et la quantité d'itinérance d'urgence (c'est-à-dire le nombre d'abonnés, le nombre de sessions ou le volume de trafic). L'itinérance d'urgence est soumise à l'approbation des fournisseurs de services homologues et à la capacité disponible sur leurs réseaux pour les clients des services d'itinérance. Étant donné que plus de 10 millions d'abonnés aux services sans fil de Rogers étaient privés de service à l'échelle nationale pendant la

[13] Onze fournisseurs de services à la suite de la fusion de Rogers et de Shaw, et de l'acquisition de Freedom Mobile par Vidéotron.

panne de juillet 2022, il est impossible de savoir si les autres fournisseurs de services auraient été en mesure de répondre à la demande d'itinérance d'urgence de Rogers en raison de l'afflux important d'utilisateurs, même si les services de données n'étaient pas activés et que le service ne se limitait qu'au 9-1-1 et à la voix. Bien que le concept d'itinérance d'urgence soit assez simple, sa mise en œuvre pourrait s'avérer difficile en cas d'urgence ou de panne. L'écosystème sans fil, y compris les exploitants, les fournisseurs et les régulateurs, pourrait collaborer en vue d'une mise en œuvre efficace de l'itinérance d'urgence. Nous notons que quelques organismes de réglementation dans le monde ont demandé l'itinérance en cas de catastrophe[14], et que l'organisme de normalisation 3GPP a commencé à y travailler dans la version 17[15] [17].

2. **Assistance mutuelle** : Le protocole d'assistance mutuelle permet à un fournisseur de services d'étendre son assistance à un autre fournisseur de services qui subit une panne ou une situation d'urgence. Cela inclut, par exemple, le partage de biens matériels, d'équipements ou de ressources humaines. Les avantages de l'assistance mutuelle dans le contexte de la panne de juillet 2022 sont largement hors du champ d'application, bien qu'il ait pu y avoir de légers avantages qui n'ont pas pu être évalués en raison d'une myriade de considérations techniques, procédurales et commerciales pour lesquelles il n'y a pas de visibilité.

3. **Protocole de communication d'urgence en cas de panne de réseau** : Ce protocole définit des lignes directrices pour la communication d'informations sur les pannes de réseau au public et aux autorités gouvernementales (p. ex. le CRTC, ISDE et les ministères responsables des mesures d'urgence et de la sécurité publique). Les lignes directrices comprennent :
    A. Informer le public de la panne de réseau en mentionnant son incidence sur les services 9-1-1. Cet aspect était absent des communications de Rogers sur la panne de juillet 2022.

    B. Fixer un objectif de deux heures pour informer le public à partir du moment où un fournisseur de services fait état d'une panne critique. À

[14] En 2020, les exploitants sud-coréens ont mis en place l'itinérance en cas de catastrophe, à partir d'une mise en œuvre prénorme. L'accord prévoit la disponibilité des services d'itinérance en cas de catastrophe dans l'heure qui suit une panne. Les utilisateurs des réseaux 4G et 5G seraient automatiquement en itinérance sur le réseau d'un autre fournisseur de services.

[15] Le 3GPP appelle cette fonction le « Disaster Roaming » (l'itinérance en cas de catastrophe) qui, selon la définition de la version 17, s'applique aux nœuds du réseau d'accès radio qui sont hors service alors que d'autres parties du réseau sont fonctionnelles. La norme couvre l'itinérance pour les services d'urgence et les services vocaux et de données pour les abonnés. Les prochaines versions devraient élargir le champ des scénarios de panne pour prendre en compte d'autres types de défaillances.

notre avis, il s'agit d'un délai relativement long puisqu'il faut ajouter le temps écoulé entre le début de la panne et la déclaration d'une panne critique. Lors de la panne de juillet 2022, il n'y a pas eu d'heure officielle pour la déclaration d'une panne critique. Nous notons toutefois que le gestionnaire des incidents de Rogers a organisé une conférence téléphonique 47 minutes après l'élément déclencheur de la panne, et que le dirigeant principal de la technologie de Rogers a communiqué avec son homologue 1 h 17 min après le début de la panne. Ainsi, l'envoi du premier avis public aurait pris environ 3 heures après le début de la panne. En outre, nous constatons que le protocole d'entente ne donne aucune précision sur la fréquence des mises à jour sur l'état des pannes.

C. Informer les autorités gouvernementales dans les deux heures suivant la « prise de connaissance » de la panne.

Le protocole d'entente ne contient pas de lignes directrices sur la communication avec d'autres intervenants, comme le CASP et l'administrateur de l'ADNA. Il décrit une série d'engagements généraux qui dépendent du plan d'intervention en cas de panne de chaque fournisseur de services.

Nous estimons que le protocole d'entente constitue une bonne première étape pour garantir une itinérance adéquate en cas de catastrophes ou de situations d'urgence, et que Rogers a réussi à mettre en place des accords avec certains exploitants d'itinérance tiers. Toutefois, la nature des pannes de réseau varie, notamment le type d'éléments qui tombent en panne et l'étendue de la panne (par exemple, pannes dans le réseau d'accès ou dans certains éléments du réseau central). Pour permettre l'itinérance d'urgence, il faut donc que l'infrastructure du réseau et les appareils des utilisateurs répondent à des exigences techniques différentes. Plus précisément, il est nécessaire de valider les scénarios qui exigent que les appareils des utilisateurs respectent les spécifications d'itinérance de bout en bout dans le cadre de scénarios de défaillance précis. Par exemple, si le réseau d'accès radio est opérationnel alors que le réseau central est en panne, les appareils des utilisateurs finaux doivent prendre en charge des messages de signalisation spécifiques qui obligent les appareils à rechercher d'autres réseaux pour l'itinérance et passer des appels d'urgence. Il est également important de procéder à une vérification de la mise en œuvre de l'itinérance d'urgence pour s'assurer qu'elle est efficace.

7.2. Améliorations apportées à la gestion du changement

Rogers a amélioré sa gestion du changement afin de remédier aux lacunes en matière de gestion des risques, de planification, de processus et d'organisation. Ci-après, nous évaluons les améliorations apportées par Rogers en matière de gestion du changement.

Nouvel algorithme d'évaluation des risques. Rogers a conçu un nouvel algorithme pour évaluer et catégoriser le risque associé à un changement

d'éléments de réseau, à des mises à jour logicielles ou à une configuration [11 : Q53]. La nouvelle méthode d'évaluation des risques comprend deux étapes :

[caviardé]

Le nouvel algorithme d'évaluation des risques aurait permis de classer la DCR à l'origine de la panne de juillet 2022 dans la catégorie « risque élevé », car le changement aurait été de type « restreint », ce qui nécessite une vérification et des approbations plus strictes de la part de la hiérarchie technique de Rogers. Le nouvel algorithme d'évaluation des risques est donc plus complet dans la mesure où il prend en compte des paramètres supplémentaires qui affectent le risque du changement au réseau. Cependant, il s'agit d'un algorithme complexe qui ne peut être évalué que lorsqu'il est mis à l'épreuve.

Nous estimons que le nouvel algorithme d'évaluation des risques contribuerait à accroître le niveau de diligence lors de l'application de changements spécifiques au réseau. Nous suggérons de surveiller et d'adapter en permanence l'algorithme pour tenir compte des changements dans les technologies de réseau et des nouveaux modèles de déploiement.

Améliorations organisationnelles. Rogers a apporté les améliorations suivantes :

[caviardé]

Une meilleure collaboration entre les équipes d'exploitation et d'ingénierie permettrait de repérer les défaillances potentielles avant de modifier la configuration et d'améliorer la résolution des problèmes. Le recours aux ingénieurs en poste chez les fournisseurs permettrait de réduire le temps nécessaire pour faire appel à ces derniers pour apporter un soutien au personnel de Rogers en cas de défaillance du réseau [12 : Q68] [caviardé].

Nous estimons qu'une interaction étroite avec les fournisseurs est fondamentale pour améliorer la résilience du réseau aux stades de la conception et du déploiement. Les autres changements organisationnels sont également positifs, mais leur incidence dépendra de la qualité de leur mise en œuvre. Par exemple, il est important de veiller à ce que la communication entre les différentes équipes soit efficace afin de ne pas ralentir l'exécution des tâches.

Processus d'introduction de nouveaux produits. Rogers suit un processus normalisé pour l'introduction de nouveaux produits et l'introduction de nouvelles technologies (INP/INT) dans ses réseaux sans fil et filaires. Le processus, qui repose sur un cadre de gestion des étapes, est typique et commun aux grands exploitants de télécommunications.

Rogers inclut les mises à jour des logiciels de réseau et les changements de configuration dans le cadre de gestion des étapes. Pour la gestion de la configuration, qui est en partie à l'origine de la panne de juillet 2022, Rogers suit

un cadre [caviardé] qui couvre le concept et la définition en passant par la recherche de solutions, les essais et le déploiement [11 : Q46, 13: Q72].

Le cadre INP/INT présenté par Rogers comme régissant la gestion de la configuration est un processus général qui néglige de nombreux détails du processus réel de gestion de la configuration propre à la panne de juillet 2022. Par exemple, le processus d'encadrement présenté par Rogers comprend des essais. Toutefois, il se peut que le processus de configuration réel ne juge pas que les essais sont nécessaires si la modification présente un risque faible, ce qui, soit dit en passant, a été le cas pour la panne de juillet 2022, où la modification de la configuration à l'origine de la panne a été évaluée comme étant un risque faible. Par ailleurs, les modifications de la configuration nécessitent des vérifications et des approbations d'une variété de niveaux et de fonctions au sein de l'organisation de Rogers. Cela varie en fonction de la nature de la modification, ce que le cadre ne prévoit pas. En bref, le cadre INP/INT est valable, mais ce sont les processus au sein du cadre et l'exécution de ces processus qui sont essentiels.

Nous estimons que l'évolution progressive des processus d'introduction de nouveaux produits en fonction des leçons tirées de cette panne et de celles qui l'ont précédée contribue à accroître la résilience du réseau. Toutefois, cela dépendra de la manière dont ces processus seront mis en œuvre, étant donné que leur description demeure très générale.

Amélioration de la mise en œuvre des changements au réseau. Rogers a apporté deux améliorations à la façon dont elle exécute les changements au réseau pendant les fenêtres de maintenance afin de minimiser les risques [12 : Q68] :

1. Introduction d'une nouvelle classification pour le type de changements :

[caviardé]

Nous constatons que lors de la panne de juillet 2022, il y a eu de nombreux changements (le nombre est inconnu, car Rogers n'a pas confirmé les détails de tous les changements). [caviardé]

Nous estimons que les améliorations susmentionnées contribuent à garantir que les changements au réseau les plus risqués fassent l'objet d'un examen plus approfondi. Le choix des changements qui feront l'objet d'un examen plus approfondi dépend des procédures d'évaluation des risques. Il est donc suggéré de procéder continuellement à une vérification et à une mise à jour des procédures d'évaluation des risques.

Automatisation. Rogers a introduit l'automatisation pour rationaliser le processus de gestion du changement afin d'éliminer les erreurs potentielles liées aux procédures manuelles et d'accélérer le processus :

[caviardé]

[caviardé]

Nous estimons que l'automatisation jouera un rôle de plus en plus important dans l'amélioration de la résilience des réseaux. Les mesures prises par Rogers pour exploiter certains outils d'automatisation sont positives et contribueraient à prévenir d'éventuelles pannes à l'avenir. Nous suggérons à Rogers de vérifier continuellement ces outils d'automatisation pour s'assurer qu'ils ne deviennent pas la cause profonde d'éventuelles pannes en raison d'erreurs d'automatisation ou d'une automatisation qui repose sur des données non optimales.

Essais en laboratoire de la gestion des changements de configuration. L'indice de risque de la gestion des changements que Rogers a mis en place après la panne de juillet 2022 comprend des essais en laboratoire comme mesure de réduction du niveau de risque associé aux changements [11 : Q53].

Rogers a mentionné les types d'essais suivants :

[caviardé]

Après la panne d'avril 2021, Rogers a veillé à ce que le laboratoire reproduise l'environnement de production du réseau sans fil et a adopté des processus de déploiement continu pour les solutions logicielles [12 : Q61]. [caviardé]

Les essais en laboratoire contribueraient à réduire le risque associé à l'introduction de nouveaux éléments, de nouveaux logiciels et de nouvelles configurations dans le réseau. L'efficacité des essais en laboratoire dépend de leur portée, c'est-à-dire de l'étendue (ou de la couverture) et de la profondeur (ou de la rigueur) des essais, ainsi que de la capacité à reproduire l'environnement de production en laboratoire. Rogers serait en mesure d'éviter les pannes futures dues à des changements de configuration similaires si le régime d'essais dans ses laboratoires est complet, ce qu'il n'est pas possible d'évaluer dans le cadre du présent rapport.

Nous estimons que l'évolution des méthodologies, des outils et de l'équipement des essais est une bonne mesure pour prévenir les pannes de réseau à l'avenir. Cependant, la complexité d'un essai optimal réside dans la reproduction du réseau de production dans un environnement de laboratoire et dans la simulation d'un grand nombre de scénarios de défaillance possibles. Nous suggérons à Rogers de se concentrer sur des solutions qui répondent à ces deux défis.

7.3. Améliorations apportées à la gestion des incidents

Préparation. Rogers a déclaré avoir renforcé ses lignes directrices en matière de gestion des incidents afin d'englober divers scénarios de panne, comme les pannes des services vocaux ou les échecs d'acheminement des appels, les défaillances des appels 9-1-1 sans fil, les pannes du système de terminaison par modem câble filaire, les coupures de fibre, les phénomènes météorologiques violents, les pannes de diffusion ou de canal, les pannes du service de diffusion continue Ignite TV, les pannes de services de tiers, les pannes d'approvisionnement du contrôle de sélection et les pannes de connectivité aux centres d'appels ou leur mise hors ligne [12 : Q68].

En outre, Rogers a déclaré avoir effectué plusieurs exercices de simulation impliquant des situations spéculatives. Au cours de ces exercices, les membres de l'équipe ont répété les mesures d'intervention en cas d'incident, ont simulé des procédures de communication en cas d'incident et ont vérifié les stratégies et les manuels d'intervention améliorés [12 : Q68].

Les activités susmentionnées, si elles sont menées avec diligence, devraient permettre à Rogers de repérer de manière proactive les lacunes dans les procédures et les outils avant que les pannes ne se produisent, et de mettre en œuvre les mesures correctives nécessaires. Par exemple, les lignes directrices de Rogers en matière de gestion des incidents avant la panne prévoyaient des exercices, mais ces derniers n'ont pas permis de repérer certaines lacunes graves, comme le manque de méthodes de communication entre les membres du personnel et de connectivité de secours du CER. Il est donc impératif que l'entraînement aux situations d'urgence ait une portée globale et que les exercices de simulation fassent partie intégrante de la préparation aux situations d'urgence afin de mettre pleinement à l'essai l'efficacité de la réponse aux incidents. Il est également impératif de procéder à une catégorisation exhaustive des causes profondes d'une panne potentielle, en définissant clairement les répercussions, afin d'orienter la structure des exercices.

Nous estimons que l'amélioration de la préparation aux pannes est positive et qu'elle garantirait une meilleure gestion des incidents en cas de pannes. Il est important de veiller à ce que les scénarios des exercices de simulation soient suffisamment larges pour couvrir un grand nombre de causes de panne potentielles, compte tenu notamment de l'évolution rapide des technologies de réseau et des modèles de déploiement.

Protocoles et organisation. À la suite de la panne de juillet 2022, Rogers a apporté plusieurs améliorations pour rationaliser les efforts de réponse aux incidents, principalement :

1. Utiliser moins de ponts de conférence;
2. Attribuer des rôles de leadership bien définis;
3. Élaborer de nouvelles lignes directrices pour la nomination et l'élection des gestionnaires d'incidents et des responsables techniques en cas d'incidents.

Nous estimons que ces nouveaux protocoles sont positifs et qu'ils constituent un mode efficace de responsabilisation dans les situations d'urgence. Toutefois, leur efficacité dépendra de la manière dont elles seront mises en œuvre dans des contextes réels.

Hiérarchisation des alarmes lors des pannes. [caviardé]

Nous estimons que la hiérarchisation des alarmes est une étape importante pour accélérer le diagnostic des défaillances du réseau et contribuer à améliorer la résilience globale du réseau. Nous suggérons à Rogers de vérifier en permanence le

type d'alarmes, leur ordre de priorité, l'agrégation des données connexes sur les alarmes et les techniques d'analyse pour une efficacité optimale.

Résilience des centres de données. [caviardé]

Nous estimons que la conception de la redondance du centre de données est adéquate et qu'elle a une incidence positive sur la résilience du réseau. Nous suggérons à Rogers de compléter ces conceptions par des vérifications de la résilience des centres de données en utilisant les normes appropriées afin d'éviter les points de défaillance uniques qui pourraient nuire au fonctionnement du réseau.

Amélioration de la gestion des incidents pour les appels 9-1-1. Rogers a amélioré sa gestion des incidents pour les appels 9-1-1 sur deux volets. Le premier volet comprend [caviardé]. Le deuxième volet comprend les accords d'itinérance d'urgence avec les exploitants de réseaux mobiles signataires du protocole d'entente sur la fiabilité des télécommunications d'ISDE [16]. Ces accords permettent à Rogers de transférer conditionnellement des clients à un autre exploitant lors de situations d'urgence qui sont qualifiées de critiques (c'est-à-dire que la nature de la panne a une incidence sur la mise en œuvre de ces accords). L'itinérance d'urgence est le service le mieux adapté, sous réserve de l'acceptation de l'exploitant de remplacement en fonction, entre autres, de la capacité de réseau disponible. L'itinérance d'urgence nécessite une mise en œuvre technique qui peut ou non avoir été réalisée par Rogers et ses partenaires [19]. Un exemple concret serait la validation du comportement des combinés et des appareils des utilisateurs finaux dans des situations où le réseau radio est opérationnel, mais pas le réseau central mobile. Dans ce cas, les appareils des utilisateurs devraient prendre en charge les messages de signalisation qui les informent de l'indisponibilité des appels d'urgence afin de les inciter à rechercher d'autres réseaux pour effectuer les appels d'urgence en itinérance.

Rogers a fourni ses recommandations pour des mesures en vue d'améliorer la résilience du réseau et de réduire les répercussions des pannes en relation avec les appels 9-1-1 et les alertes au public en réponse au formulaire d'identification de la tâche NTFF044 du Groupe de travail Réseau du CRTC [20]. Dans sa réponse, Rogers a fait état d'améliorations en vue de renforcer la fiabilité et la résilience de ses services d'urgence, dont les plus pertinentes comprennent la mise en œuvre d'un routage par défaut vers des centres d'appels tiers et l'établissement de nouveaux centres de diffusion et de nouvelles connexions des systèmes d'alerte à l'ADNA afin d'améliorer les alertes au public. Rogers a également suggéré des mesures supplémentaires, notamment l'obligation pour tous les FST de prendre en charge les appels 9-1-1 en l'absence de service, de mettre en œuvre les appels 9-1-1 par satellite comme solution de secours, d'activer par défaut l'appel vocal par Wi-Fi, d'informer les clients par divers canaux de communication en cas de panne, et d'obliger les fournisseurs de services sans fil à maintenir des pages Web dédiées à l'accès au 9-1-1 et aux alertes au public.

Nous estimons que ces améliorations relatives aux appels 9-1-1 sont favorables à l'amélioration de la résilience des services d'urgence. Toutefois, les diverses améliorations en sont encore à l'étape de l'analyse (par exemple, veiller à ce que les combinés en cours d'utilisation puissent passer en itinérance dans le cas où le réseau radio est en service et le réseau central est en panne). Des décisions doivent être prises quant à ce qu'il convient de mettre en œuvre et de déployer et, plus important encore, quant à la manière de vérifier ces mises en œuvre.

Retours automatisés. Rogers a mis en place un système de retour automatisé aux configurations précédentes lorsque les nouveaux changements échouent sur les routeurs centraux. Le retour automatisé est un outil important pour le processus de gestion des incidents qui manquait lors de la panne de juillet 2022. Rogers a déployé de nouveaux outils pour évaluer si des retours sont nécessaires [15 : Q14]. [caviardé]

Nous estimons que la mise en œuvre de configurations appropriées améliore la résilience du réseau. [caviardé]

Protocoles de communication. Rogers a déclaré avoir renforcé et mis en œuvre de nouvelles mesures pour améliorer ses protocoles de communication. En premier lieu, Rogers a déclaré avoir mis en place un « guide spécialisé en matière de communication d'entreprise » qui aborde [10 : Q73] :

- la prise en charge et les responsabilités;
- l'utilisation de différents canaux de communication;
- la cadence (fréquence) des communications sur les différents canaux;
- le contenu des communications en fonction du moment et de la gravité de la panne.

Le guide de communication s'applique à différents segments [10 : Q54, 15 : Q2], notamment :

- **Les communications internes**
- **Les clients de détail** : Rogers a créé de nouveaux modèles pour une communication cohérente; a accru ses effectifs et amélioré les lignes directrices; a intégré une liste des clients de Rogers, de Fido et de Chatr dans sa gestion des relations avec les clients (GRC) et dans des plateformes de messagerie de tiers; a investi dans le tableau de bord [caviardé] afin d'assurer le suivi des services filaires à domicile; a mis en place des cartes de pannes en ligne en temps réel; et a amélioré les options de libre-service.

  Dans sa réponse à une demande de renseignements du 22 août 2022, Rogers a proposé d'apporter des modifications à sa page Web sur les services

d'urgence[16] (Q14.A) [7]. Les modifications proposées fournissent des informations aux clients sur la manière d'accéder aux services 9-1-1 pendant une panne. Rogers a mis en œuvre ces changements sur son site Web entre le 21 juin 2023 et le 30 août 2023.

- **Les clients d'affaires** : Rogers a étendu le portail « Customer Communities » de Salesforce à tous ses clients d'affaires. La procédure en cas d'incidents majeurs de Rogers Affaires, conçue pour les incidents qui ont des conséquences sur plus de [caviardé] clients, comprend désormais la communication par courriel et [caviardé] systèmes de tickets en ligne.
- **Les intervenants gouvernementaux** : Rogers a mis en place un processus d'avis provisoire par courriel et par CléGC avec le CRTC dans les deux heures suivant la connaissance d'une « panne de service majeure ». Cette mesure est requise à titre provisoire conformément à l'avis de consultation de télécom 2023-39 [21].
- **Pelmorex** : Rogers a mis en place un processus d'avis volontaire afin de prévenir rapidement Pelmorex par courriel en cas d'incident de la plus haute gravité (c'est-à-dire un incident susceptible d'avoir une incidence à long terme sur les clients, la marque ou la réputation de Rogers).
- **Les fournisseurs de réseaux 9-1-1** : Selon les critères de Rogers, les incidents de haute gravité qui ont une incidence sur les services 9-1-1 donneraient lieu à un avis aux fournisseurs de réseaux 9-1-1. L'avis se fait par courriel et est accompagné de directives précises (p. ex., haute importance avec accusé de réception). Rogers demanderait aux ESLT de relayer le message aux CASP. Rogers informerait les ESLT régulièrement, toutes les heures ou à des moments convenus d'un commun accord.
- **Les FST et les organisations de gestion des urgences** : Rogers avise les FST d'une panne au besoin, à sa discrétion. Rogers avise les organisations de gestion des urgences d'un incident de la plus haute gravité à l'aide d'un modèle prédéfini comme celui des fournisseurs de réseau 9-1-1.

Pour maintenir les capacités de communication pendant les pannes, Rogers a pris ou prend les mesures suivantes [10 : Q 55] :

1. Élargissement de la distribution de cartes SIM de tiers à tous les membres de l'équipe de réponse aux incidents et de gestion de crise pour les communications de secours.
2. Mise en place d'un accès Internet redondant par l'intermédiaire de fournisseurs d'accès Internet tiers pour ses différents sites [caviardé].

[16]La page Web des services d'urgence de Rogers est disponible à l'adresse suivante : https://www.rogers.com/support/mobility/911-emergency-service#tips-?-reminders-for-calling-9-1-1-in-the-event-of-a-network-outage

3. Évaluation en cours de la viabilité de la connectivité par satellite pour les emplacements stratégiques critiques dans l'ensemble du Canada, en tant qu'option de secours supplémentaire pour garantir la disponibilité des communications.

Les mesures susmentionnées devraient permettre à Rogers d'être plus réactif pour informer les différents intervenants.

Nous estimons que les diverses améliorations apportées aux lignes directrices en matière de communication sont suffisantes. Nous suggérons à Rogers de procéder à des essais et des vérifications en continu de ces modèles de communication en vue d'une amélioration constante. Cela est d'autant plus important lorsque le type, l'ampleur et les conséquences des pannes de réseau varient.

7.4. Dépenses en capital

Après la panne, Rogers a déclaré que la séparation du réseau central IP sans fil et filaire coûterait 261 millions de dollars et qu'elle dépenserait 11 milliards de dollars supplémentaires sur trois ans pour développer et renforcer son réseau[17].

Il est important de noter que les dépenses en capital de Rogers sont actuellement fortement influencées par deux facteurs :

[caviardé]

7.4.1. Séparation des réseaux sans fil et filaire

Rogers a prévu de dépenser 261 millions de dollars pour séparer physiquement le réseau central IP sans fil. Un nouveau noyau IP serait conçu et élaboré pour le réseau sans fil, tandis que le noyau IP actuel resterait en place pour le réseau filaire. Le projet comprend l'achat et le déploiement de nouvelles passerelles dans différents centres de données de Rogers. Rogers fournira un transport redondant par fibre optique entre ces sites. Les dépenses supplémentaires concerneraient les nouveaux outils et l'automatisation, ainsi que les services de conception, la gestion de projet et d'autres services professionnels.

La séparation des deux réseaux centraux IP permettrait de limiter une panne comme celle du 8 juillet 2022 à la partie du réseau qui est à l'origine de l'erreur. Cela permettrait d'éviter une perte totale des services et de réduire l'incidence sur les clients.

[17]Le chiffre original est de 10 milliards de dollars, comme l'a déclaré Tony Staffieri, directeur général de Rogers, lors de la comparution de Rogers devant le Comité permanent de l'industrie et de la technologie le 25 juillet 2022. Dans sa réponse du 22 août 2022 à la demande de renseignements du CRTC [7], Rogers a déclaré que le montant était de 10,905 milliards de dollars. Dans le présent rapport, ce montant est arrondi à 11 milliards de dollars.

Le réseau central IP de Rogers, dans son architecture préalable à la panne, est une architecture conventionnelle typique de nombreux fournisseurs de services, y compris les opérateurs de réseaux mobiles, les fournisseurs d'accès fixe ou les fournisseurs d'accès fixe-mobile convergent.

[caviardé]

La séparation du réseau sans fil est une décision stratégique de Rogers qui doit être considérée dans une perspective plus large que la panne de juillet 2022. Plus précisément, Rogers est en train de déployer un réseau central 5G et de mettre à niveau son infrastructure en nuage afin de fournir de nouveaux services à des niveaux de rendement plus élevés, par exemple avec une latence plus faible. Un réseau central IP sans fil distinct permet à Rogers d'offrir une résilience supplémentaire, bien que cela entraîne des coûts supplémentaires et une plus grande complexité en raison de l'exploitation de deux réseaux centraux IP, dont la périphérie, le noyau, les passerelles Internet et les diverses interfaces de service et de réseau entre eux.

7.4.2. Développement des infrastructures

À la suite de la panne de juillet 2022, Rogers a annoncé son intention d'investir plus de 11 milliards de dollars en dépenses en capital au cours des trois prochaines années pour développer et renforcer le réseau. Le tableau 3 montre les dépenses en capital allouées aux réseaux sans fil et filaire, ce qui est une représentation légèrement différente des informations présentées par Rogers, où les dépenses étaient allouées aux réseaux d'accès et centraux.

[caviardé]

Les dépenses en capital annoncées par Rogers seraient engagées dans le cadre général des opérations commerciales, des mises à niveau du réseau et de l'amélioration de la résilience. Certains de ces coûts pourraient être directement attribués à la panne de juillet 2022 et à l'amélioration de la résilience du réseau. Ce montant comprend une somme de 261 millions de dollars pour le coût de la séparation des réseaux filaires et sans fil et les outils destinés à améliorer la surveillance du réseau et l'efficacité opérationnelle.

Dépenses liées au réseau d'accès. Rogers prévoit d'étendre la zone de couverture et de moderniser la technologie d'accès pour son réseau filaire et sans fil, pour un coût total de [caviardé] sur trois ans. Ces dépenses ne permettraient pas d'atténuer le type de panne qui est survenue le 8 juillet 2022. L'équipement du réseau d'accès doit généralement répondre aux exigences minimales fixées par les fournisseurs de services en termes de disponibilité (p. ex., disponibilité de classe transporteur, durée moyenne de fonctionnement avant défaillance). Elles ne vont donc pas au-delà de ce qui est considéré comme faisant partie des procédures opérationnelles normales pour les fournisseurs de services, y compris Rogers.

Coûts du réseau central. Rogers a alloué [caviardé] à l'évolution du réseau central filaire et sans fil. [caviardé]

Certaines parties des mises à niveau du réseau central contribuent à améliorer la résilience du réseau. Cependant, il serait difficile de limiter ces améliorations au seul contexte de la panne de juillet 2022.

Dépenses liées au spectre. [caviardé] Il n'en reste pas moins qu'il est essentiel de faire preuve de diligence dans la mise en œuvre des pratiques exemplaires de l'industrie pour la gestion du changement afin de minimiser la probabilité d'une panne critique similaire. Par ailleurs, il faut aussi maîtriser le processus de réponse aux incidents afin de minimiser la durée et l'étendue de la panne.

Outils. Rogers a acquis de nouveaux outils et des licences supplémentaires pour les outils existants afin d'améliorer la surveillance du réseau et la gestion des opérations [12 : Q63]. Après la panne de juillet 2022, Rogers a acquis [caviardé]. Elle a également étendu la disponibilité de plusieurs autres outils qu'elle utilise déjà à un plus grand nombre d'employés pour faciliter la surveillance et le dépannage du réseau. En outre, Rogers met en place un laboratoire et une validation pour le noyau IP sans fil [caviardé]. Ces outils et laboratoires ont un coût, autant pour les logiciels que pour le matériel. Ces coûts, qui seraient directement attribués à la panne de juillet 2022, n'ont pas été explicitement divulgués par Rogers.

7.5. Résumé de l'évaluation et des recommandations à Rogers

La panne de juillet 2022 n'est pas due à un défaut de conception dans l'architecture du réseau central de Rogers. Sur le plan architectural, les réseaux sans fil et filaires de Rogers sont conçus pour assurer la fiabilité et la résilience d'un fournisseur de services de niveau 1. [caviardé]

La panne de juillet 2022 a mis en évidence des lacunes dans les processus de gestion du changement et des incidents de Rogers. L'erreur dans la configuration du routeur de distribution, qui a provoqué un déluge d'annonces de route qui a fait planter les routeurs centraux, est une défaillance dans le processus de gestion du changement. [caviardé] Ces choix de conception du réseau comprennent l'architecture de la gestion du réseau, qui reposait sur le réseau de données de Rogers, l'absence de solutions de connectivité de secours pour accéder aux sites éloignés et la configuration spécifique du routeur utilisée pour éviter la surcharge du trafic de routage.

Le tableau 4 résume les déficiences constatées qui ont mené à la panne de juillet 2022 ou qui y ont contribué. Les déficiences sont classées dans les catégories suivantes :

- **Architecture** : Éléments liés à l'architecture de réseau de Rogers.
- **Gestion du changement** : Éléments liés au processus de gestion du changement.

- **Gestion des incidents** : Éléments relatifs au processus de gestion des incidents.
- **Exploitation** : Éléments liés à l'exploitation des réseaux.
- **Autres** : Éléments qui n'entrant dans aucune des catégories ci-dessus.

Tableau 4 Résumé des lacunes constatées et des mesures correctives prises par Rogers.

No	Catégorie	Description de la lacune constatée	Mesures correctives prises par Rogers
1	**Architecture**	Résilience du réseau de gestion; [caviardé]	• Mise en place de [caviardé] – un réseau IP de gestion physique et logique distinct. • Mise à niveau de l'interconnexion réseau à réseau pour [caviardé].
2	**Architecture**	Absence de connectivité de secours pour les sites d'infrastructures essentielles, y compris le CER	• Déploiement de la connectivité Internet à partir de plusieurs FSI tiers au [caviardé]. • Fourniture de la connectivité par des fournisseurs tiers à d'autres sites clés du réseau, à des centres de radiodiffusion et à des bureaux d'entreprise.
3	**Gestion du changement**	Absence de protection adéquate contre les surcharges de routage sur les routeurs centraux	• Mise en place d'une limite pour la redistribution du BGP dans le protocole OSPF (paramètre de configuration du routeur central). • Mise en place d'une limite pour le nombre d'entrées dans la base de données OSPF.
4	**Gestion du changement**	Vérification et validation inefficaces des nouveaux paramètres de configuration	• Participation de l'équipe des opérations avec celle d'ingénierie plus tôt dans le cycle de conception. • Création d'une équipe centrale d'ingénierie chargée de l'examen par les pairs des configurations ou des modifications logicielles. • Nouvelle catégorisation des types de changements de réseau (« automatisé », « restreint ») qui entraîneraient un examen plus approfondi. • Nouvel algorithme d'évaluation des risques qui pourrait contribuer à un examen plus approfondi.
5	**Gestion du**	Essais systémiques limités	Révision de l'algorithme d'évaluation

No	Catégorie	Description de la lacune constatée	Mesures correctives prises par Rogers
	changement	en laboratoire des paramètres de configuration avant d'introduire les changements dans le réseau de production	des risques pour les changements au réseau. Le nouvel algorithme d'évaluation des risques comprend des essais en laboratoire et introduit un nouveau type de changement [caviardé] pour des examens plus stricts afin de réduire le niveau de risque.
6	**Gestion du changement**	[caviardé]	[caviardé]
7	**Gestion du changement**	Classification inappropriée du risque lié à la modification de la configuration ou à la demande de changement au réseau	Mise au point d'un nouvel algorithme d'évaluation des risques pour évaluer et catégoriser les risques des changements au réseau. Le nouvel algorithme est relativement complet, mais sa viabilité ne pourra être évaluée qu'après avoir été mise à l'essai.
8	**Gestion du changement**	Plusieurs changements simultanés dans la même fenêtre de maintenance sans plan de retour accommodant	• Mise en place d'une limite au volume des activités de changement pendant la fenêtre de maintenance. • Introduction d'une nouvelle catégorisation pour le type de changements.
9	**Gestion du changement et des incidents**	[caviardé]	[caviardé]
10	**Gestion des incidents**	[caviardé]	Mise en œuvre d'une solution automatisée de hiérarchisation des alarmes afin de supprimer les alarmes inutiles pour chaque type de changement et de permettre au personnel de se concentrer sur les alarmes importantes.
11	**Gestion des incidents**	Nombre limité de cartes SIM de tiers pour les membres clés du personnel	Élargissement de la distribution de cartes SIM de tiers à tous les membres de l'équipe de réponse aux incidents et de gestion de crise.
12	**Gestion des incidents**	Formations et simulations limitées ou inefficaces pour le processus de gestion des incidents (surtout pour la préparation aux situations d'urgence)	Réalisation d'exercices de simulation impliquant des situations spéculatives.

No	Catégorie	Description de la lacune constatée	Mesures correctives prises par Rogers
13	**Gestion des incidents**	Retour automatisé (notamment en cas de perte d'accès aux éléments du réseau)	Retour automatisé à la configuration du routeur en cours d'examen.
14	**Gestion des incidents**	Protocoles de communication	Mise à jour des lignes directrices en matière de communication, en définissant la propriété et les responsabilités, les canaux de communication, le contenu et la cadence pour les clients de détail et d'affaires, les intervenants gouvernementaux, l'administrateur de l'ADNA et les fournisseurs de réseaux 9-1-1.
15	**Gestion des incidents**	Mise en œuvre complète de l'itinérance d'urgence pour remédier aux causes profondes des pannes.	Conclusion d'accords d'itinérance d'urgence avec d'autres opérateurs de réseaux mobiles. Toutefois, il est nécessaire de valider des scénarios qui exigent la conformité des appareils des utilisateurs avec les spécifications d'itinérance de bout en bout dans certains scénarios de défaillance. Il est également important de vérifier les mises en œuvre de l'itinérance d'urgence pour s'assurer qu'elles sont efficaces.
16	**Exploitation**	[caviardé]	• Acquisition et déploiement de l'outil [caviardé] qui permettra de remédier à cette lacune. • Achat de licences supplémentaires pour d'autres outils qu'elle utilise déjà pour la surveillance du réseau.

Dans les mois qui ont suivi la panne, Rogers a pris plusieurs mesures pour remédier à ces lacunes. L'une des lacunes les plus critiques est l'absence de protection contre les surcharges du routeur, qui est à l'origine de la panne. Rogers a remédié à cette lacune en mettant en place une protection contre les surcharges sur ses routeurs de distribution et de réseau central, ce qui devrait empêcher qu'une panne similaire ne se reproduise, à condition que ces mesures de protection demeurent en place.

Sur le plan de l'architecture, Rogers a mis en place un réseau de gestion distinct qui améliore la résilience de l'ensemble de son réseau. Grâce à la connectivité de secours vers les sites éloignés fournie par des fournisseurs tiers, Rogers devrait

être en mesure d'accéder aux sites éloignés pour répondre à un type de panne similaire plus rapidement qu'en juillet 2022.

Peu après la panne de juillet 2022, Rogers a annoncé qu'elle séparerait le réseau central IP pour les réseaux sans fil et filaires. Cette mesure permettrait d'isoler une défaillance similaire à celle survenue en juillet 2022 sur leur réseau d'accès respectif. La résilience du réseau serait ainsi améliorée, car la panne n'aurait pas de conséquences simultanées sur les réseaux sans fil et filaires. Toutefois, cette mesure est un choix de conception de Rogers qui entraîne des coûts supplémentaires en termes d'équipement et de gestion.

Rogers a amélioré son processus de gestion de la configuration en mettant en œuvre plusieurs mesures, notamment par un algorithme amélioré d'évaluation des risques des changements, des couches supplémentaires de vérification et d'approbation des changements de configuration, l'amélioration de ses laboratoires par l'acquisition de nouveaux outils et l'extension des licences des outils existants, ainsi que de nouveaux accords sur les niveaux de service (ANS) avec les fournisseurs afin de bénéficier du soutien des ingénieurs résidents des fournisseurs. Ces mesures et d'autres mesures de gestion du changement sont résumées dans les tableaux 5 et 6 ci-dessous.

Rogers a également apporté des améliorations à son processus de gestion des incidents afin d'améliorer son temps de réponse aux défaillances de réseau. Les améliorations comprennent la mise en œuvre d'une solution de hiérarchisation des alarmes pour aider le personnel à se concentrer sur les alarmes de réseau importantes, la mise en œuvre partielle des retours automatisés à la configuration des routeurs de réseaux, l'élargissement de l'utilisation des outils de surveillance du routage de réseau, des outils d'analyse des données relatives au réseau et la fourniture de cartes SIM de tiers à un plus nombre de membres du personnel.

Le tableau 5 résume les mesures supplémentaires prises ou annoncées par Rogers à la suite de la panne de juillet 2022. Les mesures sont classées dans les mêmes catégories que celles décrites ci-dessus pour les lacunes.

Tableau 5 Mesures supplémentaires à la suite de la panne.

N°	**Catégorie**	**Mesures supplémentaires prises après la panne**	**Évaluation**
1	**Architecture**	Séparation et partitionnement du réseau central filaire et sans fil	Un choix de conception qui améliore la résilience du réseau en limitant les pannes à leur réseau d'accès respectif, ce qui empêche la perte catastrophique des réseaux sans fil et filaires comme cela s'est produit en juillet 2022.
2	**Architecture**	Mise en œuvre et plan de	Ces améliorations contribuent à

Nº	Catégorie	Mesures supplémentaires prises après la panne	Évaluation
		mise en œuvre des dispositifs visant à améliorer la résilience : [caviardé]	renforcer la résilience du réseau et la cybersécurité.
3	**Architecture**	Redondance réciproque entre les réseaux centraux IP filaires et sans fil, où le noyau IP filaire sert de réseau de rechange au noyau sans fil et vice versa.	Augmente le niveau de redondance des réseaux filaires et sans fil et répond à des scénarios de défaillance spécifiques (p. ex. le noyau sans fil est hors service alors que le noyau filaire est opérationnel). [caviardé]
4	**Gestion du changement**	Automatisation de certaines parties du processus de gestion du changement pour convertir l'activité de la méthode des procédures en une DCR	L'automatisation peut contribuer à réduire les erreurs à condition que les bonnes vérifications soient mises en œuvre et suivies.
5	**Gestion des incidents**	Amélioration de la réponse de la gestion des incidents : ● Utilisation de moins de ponts de conférence ● Attribution de rôles de leadership bien définis ● Création de nouvelles lignes directrices pour l'attribution des rôles clés de leadership en cas d'incidents	Ces mesures permettraient d'améliorer la coordination des ressources et la réponse à apporter en cas de panne.
6	**Gestion des incidents**	Signature du protocole d'entente sur la fiabilité des télécommunications	Les accords d'itinérance d'urgence, l'assistance mutuelle et le protocole de communication en cas de panne contribuent à simplifier la collaboration entre les fournisseurs de services pendant les pannes. Toutefois, étant donné que le protocole d'entente n'est pas contraignant et que plusieurs de ses mesures font l'objet d'accords bilatéraux entre les fournisseurs de services, son efficacité devra être validée dans le cadre d'une panne réelle ou d'un scénario de crise. En outre, plusieurs mises en œuvre techniques et validations connexes doivent être effectuées.
7	**Gestion des**	Accès aux services 9-1-1	Rogers a mis à jour sa page Web sur

Nº	Catégorie	Mesures supplémentaires prises après la panne	Évaluation
	incidents	pendant la panne	les services d'urgence afin d'y inclure des conseils sur la façon d'accéder aux services 9-1-1 pendant une panne.
8	**Autres**	Dépenses en capital de 11 166 milliards de dollars au cours des trois prochaines années	Principalement sans rapport avec la panne de juillet 2022. Une fraction de ce montant pourrait être attribuée directement à l'amélioration de la fiabilité et de la résilience. Ce montant comprend 261 millions de dollars pour la séparation du réseau central, ainsi que des coûts supplémentaires pour les outils et les laboratoires supplémentaires.

L'ensemble des mesures prises par Rogers après la panne de juillet 2022 ont permis d'améliorer la résilience globale du réseau et de s'attaquer à la cause profonde de cette panne. Cependant, la gravité de la panne du réseau de 2022 est principalement due à une combinaison de défauts de configuration et de défaillances dans les processus. Par conséquent, la diligence dans la mise en œuvre des processus existants ou améliorés serait le meilleur moyen d'éviter qu'une panne similaire ne se reproduise et d'améliorer la réponse pour rétablir les services lorsqu'une panne se produit. Dans cette optique, le tableau 6 résume plusieurs recommandations qui permettraient à Rogers d'améliorer davantage ses processus.

Tableau 6 Recommandations à Rogers.

Nº	Recommandation	Justification
1	Élaborer un document détaillé d'analyse des causes profondes à la suite de pannes et de défaillances du réseau.	Le document d'analyse des causes profondes permettrait d'élaborer les plans d'urgence appropriés, en plus de l'objectif initial du document, qui est de déterminer la raison de la défaillance. Il est à noter que Rogers a fourni un rapport complet d'analyse des causes profondes pour la panne d'avril 2021, mais pas pour la panne de 2022.
2	Assurer une large couverture et une grande rigueur dans les mises à l'essai des changements de configuration liés aux réseaux centraux IP sans fil et filaires.	Les essais en laboratoire permettent de réduire le risque associé à l'introduction de nouveaux éléments, de nouveaux logiciels et de nouvelles configurations dans le réseau. L'efficacité des essais en laboratoire dépend de leur portée, c'est-à-dire de l'étendue (ou de la couverture) et de la profondeur (ou de la rigueur) des essais, ainsi que de la capacité à reproduire

Nº	Recommandation	Justification
		l'environnement de production en laboratoire. Rogers serait en mesure d'éviter les pannes futures dues à des changements de configuration similaires si le régime d'essais dans ses laboratoires est complet, ce qu'il n'est pas possible d'évaluer dans le cadre du présent rapport.
3	Informer les clients sur la manière de joindre les services 9-1-1 et d'alerte au public pendant la panne.	Les répercussions des pannes seraient réduites si les clients recevaient des informations spécifiques sur la manière d'accéder aux services 9-1-1 et d'alertes au public pendant les pannes.
4	Institutionnaliser l'apprentissage à partir de ses propres défaillances de réseau et de celles d'autres fournisseurs de services afin de mettre en œuvre des mesures préventives, de limiter les pannes de réseau et d'améliorer la qualité du service.	Cela aide Rogers à relever les vulnérabilités et les points faibles de ses réseaux afin d'atténuer les risques futurs et de prévenir des incidents similaires de manière proactive. Après la panne d'avril 2021, Rogers a considérablement amélioré ses processus de gestion du changement et des incidents et a renforcé le réseau mobile, mais ces améliorations n'ont pas été étendues à l'ensemble du réseau central IP. La cause profonde de nombreuses pannes prolongées tristement célèbres dans les réseaux de communication du monde entier était l'absence d'accès immédiat aux éléments défaillants du réseau et les lacunes dans le renforcement des systèmes pour les protéger de la surcharge et de la congestion.
5	Élargir la portée des exercices de gestion des incidents, dans la mesure du possible, pour qu'ils soient plus complets que les « exercices de simulation ».	L'inclusion d'exercices spécifiques pour faire face à des pannes générales qui touchent les principaux services de réseau, comme dans le cas de défaillances de routage ou de DNS, aiderait à faire face à ces scénarios et à assurer l'état de préparation si de telles pannes se produisaient.
6	Mettre à l'essai l'itinérance d'urgence avec d'autres exploitants pour s'assurer que le processus est efficace – il ne s'agit pas seulement d'essais techniques, mais aussi de procédures.	La définition de plans d'essais spécifiques pour l'itinérance d'urgence permettra de s'assurer que les scénarios de défaillance spécifiés sont traités correctement pendant les pannes et fournira une plateforme pour améliorer les réponses à mesure que la technologie et les services évoluent.
7	Faire connaître les causes profondes des pannes et les stratégies d'atténuation à l'ensemble de la communauté	Outre le partage des leçons tirées avec les forums de l'industrie canadienne des télécommunications, comme le CCCST, cette recommandation souligne la nécessité de

Nº	Recommandation	Justification
	Internet représentée par des organismes tels que le NANOG.	contribuer à une communauté plus large de forums sur Internet, dans le but d’aider d’autres exploitants à éviter des défaillances de réseau similaires.

8. Recommandations sur la résilience des réseaux pour tous les exploitants

Dans cette section, nous présentons une liste des principales leçons tirées de la panne de juillet 2022 pour les FST. Nous présentons ensuite un aperçu des principales tendances de l'évolution des réseaux de télécommunications qui ont une incidence sur la résilience des réseaux. Nous concluons en formulant quelques recommandations visant à améliorer la fiabilité et la résilience des réseaux de télécommunications au Canada dans le contexte de l'évolution des tendances technologiques. Ces recommandations ne s'adressent pas spécifiquement à Rogers, mais visent à informer tous les fournisseurs de services quant aux moyens d'améliorer la résilience des réseaux et de limiter la probabilité de pannes futures et leurs incidences sur les Canadiens. Certaines de ces recommandations sont applicables immédiatement, tandis que d'autres devront être élaborées à court terme.

8.1. Leçons tirées de la panne de juillet 2022 de Rogers.

Les leçons importantes tirées de la panne de juillet 2022 sont les suivantes :

1. Mettre en œuvre une protection contre la surcharge des routeurs dans les réseaux IP centraux et de distribution.
2. Séparer physiquement et logiquement la couche de gestion du réseau de données.
3. Fournir au centre d'exploitation du réseau et à d'autres sites critiques éloignés une connectivité de secours sécurisée provenant d'exploitants de réseaux de télécommunication tiers.
4. Veiller à ce que le processus de vérification des changements de configuration du réseau soit efficace et implique différentes équipes au sein de l'organisation, comme l'ingénierie, les opérations et la gestion de projet. Il est également conseillé d'impliquer les fournisseurs d'équipement lorsque les changements de configuration concernent des infrastructures essentielles, comme le réseau central IP.
5. Effectuer des essais en laboratoire des changements de configuration prévus et s'assurer que l'équipement de laboratoire et les scénarios d'essais reflètent fidèlement le réseau de production.
6. Gérer avec soin le nombre de changements de configuration effectués au cours d'une seule fenêtre de maintenance et tirer parti des outils et des processus pour le retour automatisé des paramètres de configuration.
7. Mettre en œuvre une solution automatisée de hiérarchisation des alarmes afin de supprimer les alarmes inutiles pour chaque type de changement et de permettre au personnel de se concentrer sur les alarmes importantes.

8. Fournir au personnel critique des moyens de communication secondaires, tels que des cartes SIM d'exploitants de réseaux tiers.

9. Simuler et pratiquer des scénarios de défaillance et de panne du réseau afin de mettre en évidence les lacunes de l'architecture du réseau et du processus de gestion des incidents.

8.2. Tendances de l'évolution de la technologie des réseaux

Les réseaux de télécommunications deviennent de plus en plus complexes au fil du temps, car les nouvelles technologies doivent coexister avec les anciennes. Le nombre de fonctions, ou d'éléments de réseau, ainsi que de leurs interfaces, augmentent. En outre, la mise en œuvre des fonctions de réseau évolue, ce qui a des conséquences sur l'ensemble du cycle de vie du réseau, de la planification et de la conception à l'approvisionnement, en passant par les essais, l'exploitation et la maintenance. Nous présentons quelques-uns des développements les plus significatifs qui ont une incidence directe sur la résilience des réseaux et des services. Ces développements doivent être soigneusement pris en compte dans le cadre de l'évolution des réseaux de télécommunications au cours des prochaines années.

Logiciellisation, virtualisation et répartition de la charge de travail. Au cours de la dernière décennie, nous avons été témoins d'une évolution rapide dans la conception et la mise en œuvre des fonctions des réseaux de télécommunications. Les modèles axés sur le matériel ont progressivement évolué vers des solutions logicielles pour des éléments spécifiques du réseau de télécommunications, qui, dans certains cas, fonctionnent dans des environnements virtualisés, principalement dans des nuages privés hébergés par les exploitants de réseaux de télécommunications eux-mêmes. Cela a permis de distribuer certaines charges de travail du réseau, contrairement au modèle de déploiement centralisé traditionnel (p. ex. les fonctions de réseau virtuelles distribuées pour les réseaux centraux de paquets 4G et 5G). Les fournisseurs de services ont dû trouver un équilibre entre le rendement, les coûts, les fonctionnalités et la disponibilité des fournisseurs pour décider des fonctions de réseau à virtualiser et à distribuer. Nous assistons actuellement à un déploiement rapide de ces fonctions de réseau virtualisées à grande échelle[18]. Par conséquent, les fournisseurs de services doivent principalement gérer et exploiter des systèmes axés sur les logiciels. Cela implique l'adoption de techniques et de processus comme l'intégration continue – une approche de développement logiciel visant à optimiser le processus de distribution et de déploiement des logiciels, en le rendant plus rapide et plus fiable, grâce à des essais, une intégration et un déploiement plus fréquents et automatisés - et des modèles de développement, de sécurité et d'exploitation, qui intègrent la sécurité à

[18] La virtualisation des fonctions de réseau aide les exploitants de réseaux de télécommunications à déployer et à faire évoluer les services avec plus de souplesse, et offre une plus grande flexibilité pour les modèles de déploiement du réseau.

chaque étape du processus de développement et de déploiement des logiciels, dans le but d'accroître la sécurité des applications et l'agilité du déploiement. La virtualisation de réseau influe également sur l'architecture de réseau et la distribution des charges de travail du réseau, ce qui nécessite des approches particulières pour surveiller et traiter les défaillances potentielles afin de garantir la résilience des environnements logiciels distribués.

Migration vers des plateformes de télécommunication en nuage. Après la première vague de virtualisation et de nuagisation des fonctions de réseau de télécommunications, nous constatons aujourd'hui une migration de certaines fonctions de réseau vers des plateformes en nuage qui peuvent rester dans les locaux du fournisseur de services de télécommunication en tant que nuages privés, fonctionner sur l'infrastructure de nuage public du fournisseur ou fonctionner sur des nuages hybrides privés et publics. Cela a commencé par les systèmes de soutien opérationnel et les systèmes de soutien aux entreprises et s'est poursuivi avec les réseaux centraux mobiles pour certains exploitants mobiles de niveau 1, en plus de l'expérimentation avec des composants de réseau radiophonique qui fonctionnent sur des plateformes en nuage. Étant donné que les exploitants de télécommunications dépendent de plus en plus des plateformes en nuage, cette tendance, et surtout l'utilisation de l'infrastructure des fournisseurs de nuages publics, aura des conséquences directes sur la redondance, la disponibilité et la résilience.

Intégration de modèles de données d'IA. Les exploitants de réseaux de télécommunications ont traditionnellement déployé des lacs de données sur plusieurs plateformes et utilisé diverses solutions pour obtenir des informations sur différents cas d'utilisation tels que la gestion des clients, les diagnostics de réseau et l'application de la sécurité. La gestion des données dans les réseaux de télécommunications, y compris la saisie, l'acquisition et le stockage des données, continue d'évoluer. Ces dernières années, différentes techniques d'IA ont été introduites dans diverses applications afin d'améliorer l'efficacité, la fiabilité et la prévisibilité des réseaux; d'optimiser la gestion du trafic (p. ex., en repérant et en atténuant la congestion du réseau et en prédisant les modèles de trafic futurs); de détecter et de prévenir les attaques de cybersécurité; d'interagir avec les utilisateurs finaux (p. ex., vastes modèles de langage pour la gestion de l'expérience client); et d'automatiser les tâches de maintenance du réseau (p. ex., la configuration, l'approvisionnement et le dépannage). L'utilisation de l'IA dans les réseaux de télécommunications soulève des questions sur la manière dont les systèmes d'IA sont utilisés pour l'automatisation et la prise de décision, notamment sur la manière dont les modèles d'interférence et d'apprentissage de l'IA sont construits, sur l'intégrité des données utilisées pour l'apprentissage et sur la base de connaissances utilisée pour le raisonnement.

Convergence des réseaux terrestres et satellitaires. L'intégration des réseaux non terrestres, en particulier des constellations de satellites en orbite basse, dans les réseaux 5G et les futurs réseaux 6G est l'un des développements les plus

importants dans l'évolution des réseaux de télécommunications. Plusieurs exploitants de réseaux mobiles sont en train d'évaluer la connectivité entre les satellites et les appareils. Différents modèles émergent, notamment ceux qui permettent une intégration étroite à l'échelle du réseau et des services. Il est donc possible de renforcer la résilience des réseaux de télécommunications, notamment pour les urgences.

Modèles d'interface de programmation d'applications dans les réseaux de télécommunications. De nouveaux modèles d'interface de programmation d'applications (API) ont émergé pour permettre aux utilisateurs finaux et aux fournisseurs d'applications d'interagir directement avec le réseau et l'infrastructure de services. Un bon exemple est l'API ouverte de la GSMA lancée à l'occasion du Mobile World Congress (Congrès mondial de la téléphonie mobile) en 2023. Les modèles d'API ne sont pas nouveaux, mais le type d'API, les services, l'échelle d'interaction ainsi que le degré d'interopérabilité posent des défis quant à la manière dont les modèles d'API seront gérés, sécurisés et déployés à grande échelle. Les exploitants de réseaux de télécommunications ont la responsabilité supplémentaire de veiller à ce que ces modèles soient déployés en respectant les exigences de résilience et de sécurité du niveau de service requis.

Automatisation et orchestration des réseaux. L'automatisation des réseaux vise à améliorer la souplesse, la fiabilité et l'efficacité des réseaux tout en réduisant les coûts opérationnels et le risque d'erreurs humaines. L'automatisation s'applique à différentes tâches, comme la gestion de la configuration, la gestion du changement, la gestion des pannes, la surveillance du rendement et la sécurité. La technologie de l'automatisation évolue rapidement et s'applique à différentes parties du réseau, notamment l'automatisation de la livraison des applications axée sur l'API, l'orchestration des services du réseau et l'automatisation de l'approvisionnement du réseau. Assurer la résilience des systèmes et processus d'automatisation devrait être une priorité pour les exploitants de réseaux de télécommunications. Cela nécessite des vérifications propres aux systèmes d'automatisation et aux modèles d'interaction entre les différents éléments du réseau afin de garantir l'interopérabilité, la satisfaction des accords sur les niveaux de service et une interaction sécurisée.

Avènement de technologies de réseau sans risque quantique. Les capacités des ordinateurs quantiques évoluent rapidement, ce qui augmente les chances de briser les algorithmes de cryptographie axés sur l'infrastructure à clés publiques (ICP). Les exploitants de réseaux de télécommunications sont confrontés à un défi potentiel pour leurs systèmes de sécurité, car ils s'appuient sur l'ICP pour un grand nombre de fonctions, notamment l'authentification des utilisateurs, la sécurité des données et la sécurité des protocoles de routage. Les technologies à résistance quantique répondent au risque croissant que les algorithmes de cryptage existants soient compromis par des ordinateurs quantiques. Plusieurs solutions sont proposées pour renforcer la sécurité des réseaux de télécommunications. Par exemple, la distribution quantique des clés permet l'échange de clés de chiffrement

à l'aide de techniques quantiques résistantes aux interceptions. Un autre exemple est celui des mécanismes de chiffrement et d'échange de clés post-quantiques ou à résistance quantique, tels que les algorithmes que le National Institute of Standards and Technology (NIST) est en train de normaliser (le NIST a sélectionné quatre algorithmes de ce type avant 2023). Quelques grands exploitants de télécommunications ont mis à l'essai des solutions quantiques dans le cadre de vrais déploiements commerciaux. Certains organismes de réglementation cherchent à rendre obligatoire la sécurité post-quantique pour les communications de nature délicates. L'évolution vers une architecture de sécurité basée sur la quantique serait un élément clé des exigences en matière de résilience des réseaux au cours des prochaines années. Le fait de ne pas s'attaquer aux menaces de cybersécurité et de ne pas adapter les protocoles et les processus de sécurité aux menaces de l'informatique quantique mettrait en péril la résilience des réseaux de télécommunications en cas d'attaques contre la sécurité.

8.3. Recommandations pour améliorer la résilience

Les tendances technologiques susmentionnées ont une incidence sur l'architecture, la conception, la mise en œuvre et l'exploitation des réseaux de télécommunications. En conséquence, les exploitants de réseaux devraient faire évoluer leurs processus et leurs capacités techniques. Les organismes de réglementation devront eux aussi faire évoluer le paysage réglementaire pour tenir compte de ces tendances dans les années à venir.

Nous présentons ci-dessous d'autres recommandations tournées vers l'avenir, compte tenu de l'évolution des réseaux et services de télécommunications. Ces recommandations sont de nature générale et s'appliquent à tous les exploitants de réseaux. Nous les regroupons en recommandations technologiques et en recommandations relatives au processus. Cependant, nous ne présentons pas les détails dans le présent rapport, étant donné les implications complexes de ces évolutions technologiques.

8.3.1. Recommandations technologiques pour les FST

Réseaux de satellites en orbite non géostationnaire. Les avancées récentes en matière de constellations de satellites en orbite basse et en orbite moyenne, ainsi que leur propre écosystème d'appareils, renforcent la connectivité des satellites en orbite géosynchrone et constituent un bon moyen de compléter la connexion des équipes d'assistance pendant les pannes majeures, tout en fournissant une redondance supplémentaire pour la gestion hors bande.

Connectivité directe du satellite à l'appareil. L'émergence d'exploitants de constellations de satellites en orbite basse à l'échelle mondiale a incité les vendeurs d'appareils et les fournisseurs de services à élaborer des solutions pour connecter les téléphones mobiles directement aux satellites. Un exemple est le service Urgence SOS par satellite d'Apple lancé sur l'iPhone 14 en 2022, qui fournit un service de messagerie texte bidirectionnel à faible débit binaire et à faible capacité

pour les situations d'urgence. D'autres modèles de connexion directe aux appareils sont plus ambitieux et visent à fournir des débits de quelques mégabits par seconde. Ces solutions viendraient compléter les services terrestres d'appels 9-1-1 et d'alertes en cas d'urgence dans certaines situations de panne.

Futures normes d'itinérance en cas de catastrophe de 3GPP. Les organismes de réglementation du monde entier commencent à réclamer une mise en œuvre plus large de l'itinérance en cas de catastrophe[19] auprès des fournisseurs de services, en raison de l'omniprésence des réseaux de télécommunications et du risque de pannes plus fréquentes et plus étendues. Le secteur de la téléphonie mobile est conscient de l'importance de l'itinérance d'urgence dans les situations de reprise après catastrophe et de pannes majeures. L'organisme de normalisation 3GPP a commencé à travailler sur l'itinérance en cas de catastrophe dans la version 17, et il promet de nouvelles mises à jour et un élargissement des scénarios d'itinérance dans les versions ultérieures [17]. Les exploitants de réseaux mobiles devraient envisager ces nouvelles solutions pour les futures mises à niveau de leurs réseaux. Les exploitants de réseaux mobiles doivent travailler en étroite collaboration avec leurs fournisseurs pour garantir la conformité, planifier la mise en œuvre potentielle de ces nouvelles spécifications dans leurs réseaux 5G et s'aligner avec leurs partenaires de réseaux d'itinérance en conséquence.

Messagerie par contournement. Les défaillances de certains systèmes critiques, tels que le système multimédia IP, ont entraîné des pannes de services de téléphonie, de messagerie et de vidéo, alors que les services Internet restaient disponibles. Dans de tels cas, les applications de messagerie en ligne offrent un autre moyen de communication, notamment pour les services d'urgence.

Technologies SIM dynamiques axées sur les logiciels. Les technologies SIM axées sur les logiciels offrent différents niveaux de programmabilité et permettent de nouveaux modèles d'itinérance vers d'autres fournisseurs en cas de pannes majeures. Cela nécessiterait que les exploitants concluent des accords au sujet de solutions d'itinérance dynamique appropriées qui tirent parti de la programmabilité dynamique de la carte SIM.

Partage du spectre et de la capacité en cas d'urgence. Différents modèles d'attribution du spectre sont possibles et pourraient avoir des avantages directs lors de pannes majeures, par exemple lorsque les utilisateurs d'un exploitant sont transférés vers d'autres fournisseurs de services pendant une panne. Le partage du spectre est un exemple de ces mécanismes, où les exploitants partagent dynamiquement le spectre pour augmenter temporairement la capacité du réseau afin d'accueillir les utilisateurs itinérants. La mise en œuvre de ces techniques nécessite des accords commerciaux et techniques entre les exploitants, et

[19] Dans ce cas, l'itinérance en cas de catastrophe comprend l'itinérance d'urgence (par exemple, la possibilité de composer le 9-1-1 en utilisant les services d'un exploitant d'un réseau mobile tiers en itinérance) ainsi que d'autres services d'itinérance, y compris la voix, les données et la messagerie texte.

éventuellement la normalisation de mécanismes précis. Le partage de la capacité s'applique également aux exploitants de réseaux filaires pour le partage dynamique de la bande passante et de la capacité entre les réseaux d'accès, les installations de raccordement et les réseaux centraux. Les exploitants devraient normaliser les mécanismes et les interactions, notamment en déterminant clairement les scénarios de défaillance et la procédure à suivre pour y remédier.

Interaction avec les réseaux de diffusion de contenu et les applications par contournement. Les fournisseurs de services de télécommunication pourraient collaborer avec les fournisseurs d'applications et de contenus par contournement pour définir des modèles d'interaction précis en cas d'urgence. Par exemple, la gestion dynamique du trafic (p. ex. le ralentissement artificiel du trafic, le contrôle, l'élaboration, etc.) permet au trafic de sortie des caches et des serveurs des fournisseurs de contenu et des fournisseurs d'applications par contournement de s'adapter dynamiquement en fonction de la rétroaction des exploitants de réseaux de télécommunications.

Connectivité redondante pour les fournisseurs de services d'infrastructures essentielles. La panne de juillet 2022 a mis en évidence l'importance de disposer d'une connectivité secondaire ou de secours pour maintenir les services d'infrastructures essentielles opérationnels (p. ex., la sécurité publique, les soins de santé, les services financiers, les services publics, etc.) Les FST pourraient mieux servir cette catégorie de clients en leur conseillant d'envisager des options de connectivité secondaire auprès d'autres fournisseurs afin d'améliorer la disponibilité de leurs propres services. Les FST pourraient proposer des services tiers loués auprès d'un autre fournisseur de services qui disposent d'une infrastructure de réseau indépendante afin de réduire la probabilité d'une interruption de service.

8.3.2. Recommandations relatives au processus

Formation et simulations de réponse aux incidents. Il est essentiel que les fournisseurs de services organisent régulièrement des formations et des simulations de différents scénarios de panne et d'urgence. La formation permettra au personnel d'être plus à l'aise et prêt à faire face aux urgences et aux pannes, et d'avoir une connaissance claire de son rôle et de ses responsabilités. Les exercices aideront le fournisseur de services à déceler les lacunes dans le processus de réponse aux pannes, l'architecture du réseau et l'état de préparation général.

IRC pour la réponse à la gestion des incidents. Les IRC pour la réponse aux incidents aident les organisations à évaluer l'efficacité de leurs processus et à s'assurer que les incidents, comme les pannes de réseau ou de service, sont gérés efficacement. La mise en place d'IRC pour la gestion des incidents présente plusieurs avantages : une meilleure responsabilisation, une attribution efficace des ressources, une prise de décision fondée sur des données et une réduction des risques. Les IRC communs pourraient être alignés sur ceux définis par les cadres de l'Information Technology Infrastructure Library et du Control Objectives for Information Technologies pour la gestion des incidents ou des problèmes. Plus

précisément, nous constatons que l'évolution des technologies de réseau et des modèles de déploiement nécessite l'adaptation des IRC existants pour inclure de nouveaux aspects, par exemple la virtualisation, les modèles de télécommunications en nuage, l'automatisation, l'utilisation de modèles d'apprentissage de l'IA, etc.

Rôles et responsabilités définis. Les fournisseurs de services gagneraient à ce que certains membres du personnel aient des rôles et des responsabilités clairement définis en cas d'urgence et de panne. L'une de ces responsabilités consisterait à informer les ESLT et l'administrateur de l'ADNA, entre autres, de la panne. Ces rôles ne doivent pas entrer en conflit avec les rôles liés à la résolution de la panne (p. ex. un rôle d'ingénieur pour la recherche des causes profondes de la panne).

Calcul du coût de la panne. Les exploitants auraient intérêt à calculer les répercussions financières d'une panne de réseau, qui est un élément essentiel de la gestion des risques et de la planification de la continuité des activités. Le calcul des coûts d'une panne fournit des informations exploitables en vue de faciliter la prise de décisions financières. Il aide le fournisseur de services à atténuer les conséquences des incidents en prenant des décisions relatives à l'affectation des ressources et à la communication avec les intervenants afin de préserver l'image de marque et la stabilité financière.

Communication à propos des services d'urgence. Les fournisseurs de services devraient rappeler au public comment accéder aux services d'appel d'urgence et d'alerte au public pendant une panne. Il serait souhaitable que les fournisseurs de services tiennent à jour une page Web contenant des informations pertinentes sur l'accès aux services d'urgence pendant les pannes.

9. Références

[1] Cloudflare Blog, « Cloudflare's view of the Rogers Communications outage in Canada » [en anglais seulement], 8 juillet 2022, https://blog.cloudflare.com/cloudflares-view-of-the-rogers-communications-outage-in-canada/ (dernière consultation : 1er août 2023).

[2] Rogers Communications Inc, « Résultats pour le deuxième trimestre de 2022 », 27 juillet 2022, https://about.rogers.com/wp-content/uploads/Rogers-Q2-2022-Press-Release_FRE.pdf (dernière consultation : 1er août 2023).

[3] CRTC, *Groupe de travail Services d'urgence du Comité directeur du CRTC sur l'interconnexion*, *Rapport de consensus ESRE0076 – Procédures en matière d'avis de panne du service 9-1-1*, Décision de télécom CRTC 2017-389, 27 octobre 2017.

[4] Groupe de travail Services d'urgence du Comité directeur du CRTC sur l'interconnexion, « 9-1-1 Service Outage Notification Processes » (Procédures en matière d'avis de panne du service 9-1-1) [en anglais seulement], numéro de rapport : ESRE0076, 25 mai 2017.

[5] Commission fédérale des communications, *Improving 911 Reliability* [en anglais seulement], FCC 22-88, 18 novembre 2022.

[6] Rogers Communications, *Réponse à une demande de renseignements : Panne de service de Rogers dans tout le Canada en juillet 2022*, document 4215437, 22 juillet 2022.

[7] Rogers Communications, *Réponse à une demande de renseignements : Panne de service de Rogers dans tout le Canada en juillet 2022*, document 4229639, 22 août 2022.

[8] Rogers Communications, « Groupe de soumission 1 : Événements du 8 juillet, RCA et facteur contributif », réponses à la demande de renseignements du CRTC, 17 juillet 2023.

[9] Rogers Communications, « Groupe de soumission 2 : Architecture et gestion d'entreprise », réponses à la demande de renseignements du CRTC, 18 juillet 2023.

[10] Rogers Communications, « Groupe de soumission 4 : Événements du 8 juillet, RCA et facteur contributif », réponses à la demande de renseignements du CRTC, 14 juillet 2023.

[11] Rogers Communications, « Groupe de soumission 5 : Événements du 8 juillet, RCA et facteur contributif », réponses à la demande de renseignements du CRTC, 20 juillet 2023.

[12] Rogers Communications, « Groupe de soumission 6 », réponses à la demande de renseignements du CRTC, 31 juillet 2023.

[13] Rogers Communications, « Groupe de soumission 7 », réponses à la demande de renseignements du CRTC, 4 août 2023.

[14] Rogers Communications, « *Réponse à une demande de renseignements : Panne de service de Rogers dans tout le Canada en juillet 2022* », document 4215439, CONFIDENTIEL Rogers (CRTC) 11 juillet 2022-1_ix_Annexe.

[15] Rogers Communications, « Groupe de soumission 8 », réponses à la demande de renseignements du CRTC, 30 août 2023.

[16] Innovation, Sciences et Développement économique Canada, « *Protocole d'entente sur la fiabilité des télécommunications* », 9 septembre 2022, https://ised-isde.canada.ca/site/isde/fr/protocole-dentente-fiabilite-telecommunications (dernière consultation : 23 août 2023).

[17] 3GPP, « *System architecture for the 5G System*", TS 23.501, v18.2.2, 7 July 2023.

[18] Rogers Communications, « Groupe de soumission 9 », réponses à la demande de renseignements du CRTC, 13 septembre 2023.

[19] Rogers Communications, « Groupe de soumission 10 », réponses à la demande de renseignements du CRTC, 6 octobre 2023.

[20] Rogers Communications, « Rogers Responses to CRTC Questions dated 22 February 2023 », Contribution nº NTCO0746 préparée en réponse à la tâche nº NTFF044 aux fins de discussion au sein du sous-groupe de travail sur le formulaire d'identification de la tâche 44 du Groupe de travail Réseau, 11 août 2023.

[21] CRTC, *Appel aux observations – Élaboration d'un cadre réglementaire pour améliorer la fiabilité et la résistance des réseaux – Obligations en matière de transmission d'avis et de production de rapports lors d'interruptions de services de télécommunication majeures, Avis de consultation de télécom CRTC 2023-39*, 22 février 2023.

Annexe 1 : Chronologie de la panne

Le tableau suivant présente les étapes critiques de la chronologie de la panne de juillet 2022 qui sont importantes dans le cadre du présent rapport.

Date (2022)	Heure (HAE)	Temps écoulé depuis le début de la panne (h : min)	Détails
8 juillet	2 h 27		[caviardé]
8 juillet	4 h 43	0 h	Rogers effectue la première modification sur le premier routeur de distribution concerné, en supprimant un filtre de gestion, ce qui s'avère être l'élément déclencheur de l'événement. [caviardé]
8 juillet	4 h 58	0 h 15	Les routeurs de distribution ont inondé tous les routeurs centraux avec des routes qui dépassaient leur limite de mémoire et les ont donc empêchés de traiter le trafic. [caviardé]
8 juillet	6 h 28	1 h 45	[caviardé]
8 juillet	8 h 39	3 h 56	Rogers a informé les fournisseurs de réseaux 9-1-1 [également appelés ESLT : Bell, TELUS, SaskTel] de la panne du réseau et leur a demandé de transmettre le message en cascade aux CASP.
8 juillet	8 h 54	4 h 11	Rogers a envoyé un premier message à ses clients sur Twitter pour les informer de la panne de réseau. Rogers a ensuite diffusé des messages similaires sur différentes plateformes (réponse vocale interactive, médias sociaux).
8 juillet	9 h 25	4 h 42	Pelmorex, qui exploite l'ADNA, a d'abord communiqué avec Rogers pour obtenir des informations sur l'incidence que la panne aurait sur la distribution des alertes d'urgence, après avoir pris connaissance de la panne de service par l'entremise des médias et des perturbations personnelles.
8 juillet	9 h 38	4 h 55	[caviardé]
8 juillet	10 h 21	5 h 38	[caviardé]
8 juillet	11 h 10	6 h 27	[caviardé]
8 juillet	11 h 19	6 h 36	Rogers a informé le CRTC et Pelmorex de la panne nationale et les a avertis que toute agence qui tenterait de diffuser des

Date (2022)	Heure (HAE)	Temps écoulé depuis le début de la panne (h : min)	Détails
			alertes d'urgence aux clients de Rogers sur les réseaux de Rogers n'y parviendrait pas.
8 juillet	17 h 1	12 h 18	[caviardé]
8 juillet	17 h 45	13 h 2	[caviardé]
8 juillet	18 h 48	14 h 5	[caviardé]
8 juillet	19 h	14 h 17	[caviardé]
8 juillet	20 h 32	15 h 49	Rogers a rétabli les services pour un peu plus de [caviardé] abonnés dans les régions [caviardé].
8 juillet	21 h 50	17 h 7	[caviardé]
8 juillet	22 h 3	17 h 20	Rogers a rétabli les services à plus de [caviardé] abonnés dans toutes les régions [caviardé]
8 juillet	23 h 13	18 h 30	[caviardé]
8 juillet	23 h 43	19 h	L'accès VPN filaire de Rogers est rétabli.
9 juillet	0 h 50	20 h 7	[caviardé]
9 juillet	1 h 34	20 h 51	Au Canada, environ [caviardé] abonnés sont connectés avec succès. [caviardé]
9 juillet	3 h	22 h 17	[caviardé]
9 juillet	4 h 50	24 h 7	[caviardé] Environ [caviardé] abonnés sont connectés avec succès. [caviardé]
9 juillet	7 h	26 h 17	[caviardé]
9 juillet	10 h 51	30 h 08	Rogers informe les fournisseurs des réseaux 9-1-1 que le réseau a été rétabli.
9 juillet	16 h 25	36 h 42	Rogers diffuse avec succès la première alerte émise par Pelmorex depuis le début de la panne.