Mars 2019

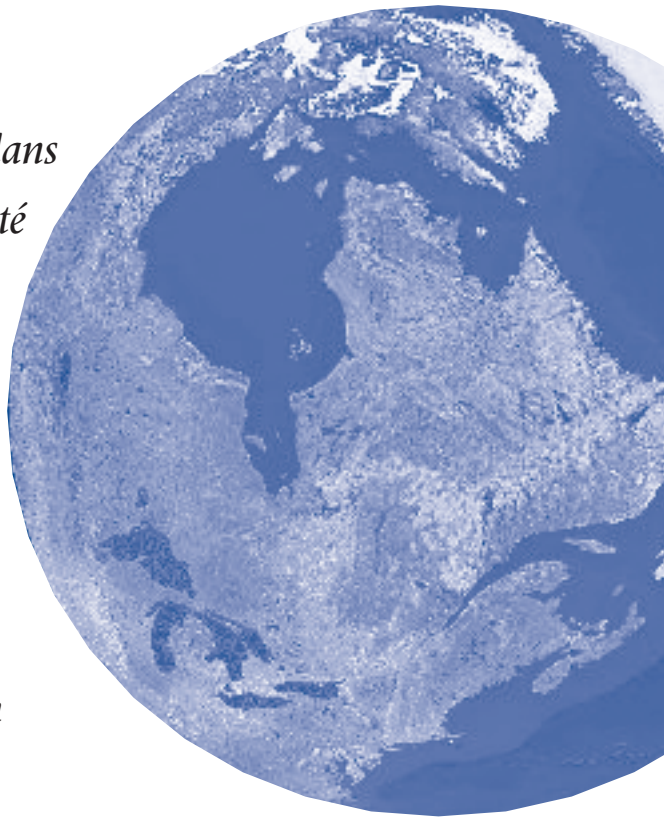
Infotélécom

CCT
Communauté des consultants en télécommunications

Kinessor

Sommaire

Dans ce numéro :



À ne pas *manquer*

Fusion de i3vision et LOEM

Amazon compte investir 1 milliard de dollars au Québec sur 10 ans

Une réforme importante au Gouvernement du Québec pour le stockage de données

Somum Solutions : l'automatisation de la prise de rendez-vous par appel ainsi que par SMS

82

Un antivirus sur votre téléphone intelligent ou sur votre tablette?

Il est plus difficile d'attraper des virus sur un téléphone intelligent et une tablette qu'un ordinateur. Cependant, il suffit de naviguer sur une page Internet malveillante, ou de télécharger une pièce contaminée que votre téléphone peut être affecté par un virus. Vos données personnelles sont alors à risque. Elles peuvent être partagées sans que vous le sachiez et ça peut se rendre jusqu'à un vol d'identité. Votre téléphone peut aussi appeler des gens dans vos contacts au hasard pour une technique d'hameçonnage vers certains produits en vente. Aujourd'hui, il existe plusieurs logiciels de protection pour vos tablettes et téléphones intelligents: ESET, AVG, Avast, Avira, McAfee et Kaspersky.

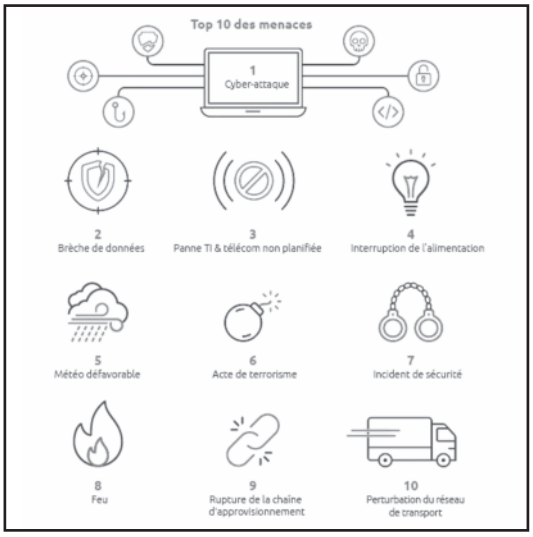
LA CONTINUITÉ DES AFFAIRES : *un allié dans la gestion des menaces de cybersécurité*

MARIE-HÉLÈNE PRIMEAU

Marie-Hélène Primeau, CPA, CA, MBCI
Consultante en continuité des affaires
ISO 22301 Lead Auditor Instructrice pour le Business Continuity Institute Membre du comité technique des normes ISO concernant la continuité (TC 292) et de la norme canadienne en gestion des urgences et de la continuité (CSA Z1600). Vous pouvez la contacter à mhprimeau@premiercontinuum.com.

L'Infotélécom de décembre 2018 mentionnait un rapport de Statistiques Canada soulignant que plus d'une entreprise sur cinq a été victime d'une cyberattaque en 2017[i]. Ce rapport dévoilait également que « plus de la moitié (58 %) des entreprises ont connu un certain temps d'arrêt à la suite d'un incident. En moyenne, le temps d'arrêt total des entreprises en 2017 était de 23 heures et comprenait les appareils mobiles, les ordinateurs de bureau et les réseaux[ii] ». Ceci souligne qu'une cyberattaque ou un rançongiciel, en plus d'affecter la réputation de l'organisation et de mettre à risque les données de ses clients, elle interrompt de plus en plus les activités courantes des organisations, représentant une menace commerciale nécessitant la collaboration des responsables de la continuité des affaires.

D'ailleurs, le rapport « Horizon Scan 2018 » publié par le Business Continuity Institute, institut mondial basé au Royaume-Uni, place la cyberattaque au premier rang des menaces d'interruption des affaires.



On n'a qu'à penser à la cyberattaque NotPetya, qui a bouleversé la chaîne d'approvisionnement mondiale en paralysant le transporteur Maersk en 2017, ou au rançongiciel SamSam, qui a forcé la Ville d'Atlanta en 2018 à opérer en mode manuel pendant plusieurs jours.

Comme le relatait la revue Wired[iii], Maersk, qui représente 1/5 de la capacité maritime mondiale (76 ports, 800 bateaux), a vu tous ses terminaux portuaires affectés par l'attaque. Ainsi, au jour 1, des centaines de camions ont été bloqués aux barrières d'entrée puisque celles-ci ne répondaient plus aux commandes d'ouverture. Ce trouble a causé des files interminables sur plusieurs kilomètres, forçant les clients à trouver des mesures alternatives pour soit faire déplacer leur cargo ou encore trouver un endroit pour l'entreposer. Certains ont même dû réorganiser le transport de leur cargo par voies aériennes pour éviter des pénalités de plusieurs centaines de milliers de dollars prévues en cas d'interruption d'une chaîne d'approvisionnement. Ce casse-tête comportait d'autres dangers, nécessitant des mesures extraordinaires afin d'assurer la température requise pour des centaines de conteneurs réfrigérés remplis de denrées périssables qui risquaient d'être perdues. Les grues étaient immobilisées, tout comme les guides permettant de charger et vider chaque bateau. Les systèmes de réservation ainsi que tous les systèmes opérationnels permettant de savoir ce que contenait chaque cargo étaient inutilisables. Pendant plusieurs jours, un des piliers de l'économie mondiale semblait s'écrouler. Des mesures de secours ont dû être rapidement mises en place pour reprendre les activités, telles que l'utilisation de Gmail et Whatsapp pour prendre les commandes et celle des papiers d'inventaires collés à la main sur chaque conteneur. Selon son ancien PDG, il a fallu 10 jours à Maersk pour reprendre l'essentiel de ses activités, à un coût évalué entre 250 et 300 millions de dollars.

La Ville d'Atlanta, pour sa part, a été infectée en mars 2018 par le rançongiciel SamSam et a immédiatement activé son plan de continuité des activités[iv]. La sécurité publique (y compris la police, le service de protection des incendies et le 911), le service de l'eau et l'aéroport n'ont pas été affectés. La cour municipale a limité ses activités au traitement des accusés ayant été arrêtés et placés en détention, et ce, à l'aide de processus manuels. Pendant près d'une semaine, les autres activités de la Ville ont dû être traitées manuellement et en personne, ou être reportées afin de permettre aux ressources de la Ville de concentrer leurs efforts sur les activités critiques.

Des attaques se produisent également plus près de chez nous, si l'on pense à la MRC de Mékinac, en Mauricie au Québec. La municipalité a versé 30 000 $ aux pirates après que ses données furent prises en otage par un rançongiciel,[v] puisqu'elle n'avait pas la possibilité de continuer ses activités sans payer.

> La continuité des affaires, telle que définie dans la norme ISO 22301, est « la capacité d'une organisation à poursuivre, après une perturbation, la livraison ou la fourniture de produits ou de services à des niveaux prédéfinis acceptables ».

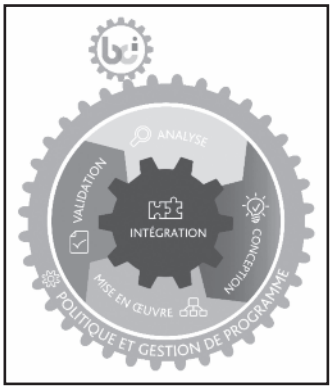
Cette définition ne précise pas les causes signifiant que la démarche devrait nous préparer à faire face à différents types de conséquences. D'ailleurs, la démarche de continuité des affaires fournit un cadre pour construire la résilience de l'organisation, celle-ci

étant la **« capacité d'assimilation et d'adaptation dans un environnement changeant »**[vi], ce qui est tout à fait le lot de la cybersécurité.

Tout comme un feu ou inondation affectant la propriété, l'incident n'est pas seulement l'affaire du gestionnaire d'immeuble, mais de toutes les activités qui y ont lieu qui seront affectées. Dans le cadre de la continuité des affaires, les gestionnaires de ces activités ont peut-être déjà des solutions disponibles et savent quelles sont les activités prioritaires et lesquelles peuvent être mises de côté sans conséquences graves pour l'organisation ainsi qu'une structure de réponse et d'escalade pour communiquer les actions à décisions à prendre. En collaborant avec l'équipe de continuité des affaires de votre organisation, vous pourrez ensemble mieux identifier les systèmes et données qui sont critiques pour l'organisation.

Démarche de continuité en lien avec la cybersécurité

La préparation et la réponse adéquates aux incidents de cybersécurité bénéficient de la démarche de continuité, basée sur les bonnes pratiques du Business Continuity Institute. Si une telle démarche n'existe pas au sein de votre organisation, il peut être un bon temps d'en mettre une en place et de collaborer avec la cybersécurité pour bénéficier de synergies.



Au niveau **politique et gestion de programme** (gouvernance), il est souhaitable qu'un comité de pilotage de la gestion de la continuité soit mis en place, celui-ci étant normalement composé des hauts dirigeants des divisions clés. On retrouve au sein de ce comité une grande écoute et une sensibilité aux différentes menaces. On y fait le suivi des différents indicateurs de performance, y compris le nombre d'incidents, le délai de résolution de chaque incident, les impacts financiers, le plan d'action et les budgets. Lors de l'**analyse**, on évalue les produits et services critiques afin de mieux comprendre la tolérance de l'organisation à l'interruption. Le niveau de service minimum est également entendu, les besoins en services TI ainsi que le nombre d'employés et d'équipements nécessaires à leur prestation sont communiqués. Les responsables des services TI et Télécom peuvent ensuite élaborer le schéma des dépendances pour mieux connaître les vulnérabilités et établir le niveau de protection ou de ségrégation souhaité entre services.

Cela permettra de déterminer, en phase de **conception**, les solutions alternatives qui pourront pallier aux interruptions en pensant au-delà de la traditionnelle relève TI, qui se concentre sur le rétablissement des systèmes d'entreprise critiques. Il est fort possible que le réseau de communication ou les postes de travail soient aussi affectés durant une attaque de rançongiciel, demandant plus de créativité pour poursuivre les activités. Ainsi, l'exploration des alternatives à l'avance, jumelée à la détection et au confinement (en isolant des portions de réseau ou des postes de travail du réseau, par exemple), diminueront l'impact de l'attaque sur les opérations et la nécessité de payer une rançon.

Lors de la réponse (**mise en œuvre**), l'équipe d'experts en cybersécurité et TI / Télécom bénéficiera d'une équipe de gestion de crise mise en place dans le contexte de continuité pour l'appuyer (et éviter le dédoublement de structure). Cette équipe de gestion de crise est exercée à évaluer les impacts d'un incident sur l'ensemble de l'organisation, y compris ses opérations commerciales (en utilisant des grilles d'impact similaires) ainsi qu'à prendre des décisions stratégiques et à gérer les aspects concernant la réputation. C'est elle qui, par exemple, décidera si l'on devra effectivement payer une rançon. Le partage de responsabilité vise à accélérer à la fois la réponse technique et celle de gestion.

Il est important d'exercer et de maintenir à jour les plans et les structures ainsi que faire une revue critique pour s'assurer que les mesures en place sont fiables, à jour et appropriées (**validation**). Les exercices de table permettent à tous les membres de mieux comprendre de façon concrète les enjeux techniques et les implications d'affaires des décisions prises. D'ailleurs, Premier Continuum a eu l'opportunité de réaliser récemmenta quelques exercices avec ses clients sur le thème d'une cyberattaque. Ceux-ci ont été très appréciés puisqu'ils soulevaient des enjeux qui n'avaient pas été préalablement identifiés.

Au niveau de l'**intégration**, la continuité des affaires, par son programme de formation et de sensibilisation, peut collaborer avec les responsables de la cybersécurité pour renforcer le message de prévention en cybersécurité afin de réduire le risque humain (hameçonnage et autres) en soulignant l'impact sur la continuité des services si une cyberattaque survient.

Prochaines étapes

Dépendamment de votre niveau de maturité en continuité des affaires, les étapes à mettre en place seront différentes.

Si une démarche de continuité des affaires existe au sein de votre organisation, il est important d'engager la conversation, car la continuité recèle des informations utiles à la cybersécurité et facilitera la réponse lors d'un incident.

Si une démarche de continuité n'est pas entamée dans votre organisation, faites-en sorte qu'elle soit mise en place. Elle permettra un alignement stratégique, une appropriation « affaires » et mettra en commun les différents intervenants, dont les responsables de la cybersécurité et de la relève TI.

La collaboration accroîtra la résilience de l'organisation!

i https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm

ii https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm

iii https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

iv https://www.wabe.org/know-atlanta-ransomware-attack/
https://blog.barkly.com/atlanta-ransomware-attack-2018-samsam
https://twitter.com/Cityofatlanta/status/976920585434423296

v https://www.lenouvelliste.ca/actualites/cyberattaque-contre-la-mrc-de-mekinac-une-rancon-de-30-000--payee-ad8524e5c841ffddac57c7f027b6a13d

vi ISO 22300:2018(fr) Sécurité et résilience — Vocabulaire

Fusion de i3vision et LOEM

Après 12 années de services, Marie-Hélène Savard et son équipe ont décidé de joindre les rangs de i3vision ainsi que son président Hugo de Bellefeuille. LOEM se spécialise dans les applications de gestion des effectifs et de gestion de la qualité alors que i3vision se spécialise dans le domaine des technologies et des solutions personnalisées évoluées. La synergie et la culture des deux entreprises sont très similaires. Cette alliance permettra d'offrir un excellent service avec encore plus de possibilités pour les centres de contacts clients.