Balado sur les villes cybersécurisées

Collaborer avec les forces d'application de la loi avec le sergent-détective Vern Crowley, Police provinciale de l'Ontario

[00:00:00] **Tenielle Bogdan :** Bienvenue au balado sur les villes cybersécurisées. Il vous est offert par l'Initiative des meilleures pratiques en matière de cybersécurité municipale, dirigée par TECHNATION Canada et financée en partie par Sécurité publique Canada dans le cadre de son programme de coopération en matière de cybersécurité. Ce balado examine les moyens dont disposent les municipalités canadiennes pour garantir leur cybersécurité. Pour en savoir plus, rendez-vous sur technationcanada.com et consultez nos lignes directrices sur les meilleures pratiques en matière de cybersécurité municipale.

Merci d'être à l'écoute. Je suis votre hôte, Tenielle Bogdan, et aujourd'hui nous discutons avec le sergent-détective Vern Crowley de la Police provinciale de l'Ontario.

Le sergent-détective Crowley est membre de l'équipe d'enquête sur la cybercriminalité de la Police provinciale de l'Ontario, équipe composée d'enquêteurs de police et d'experts techniques civils. L'équipe a pour mandat d'enquêter sur les cybercrimes où la technologie est la cible du crime, d'aider dans les enquêtes criminelles complexes où la technologie a été utilisée comme outil pour commettre le crime, et de collaborer avec les forces d'application de la loi, les gouvernements, les universités et le secteur privé pour améliorer le secteur du cyberrenseignement.

Le sergent-détective Crowley nous parle aujourd'hui de la manière dont les municipalités peuvent collaborer avec leurs services d'application de la loi lorsqu'elles sont victimes d'une cyberattaque.

Bonjour Vern! Merci de vous joindre à nous aujourd'hui. Parlez-nous un peu de votre rôle au sein de l'OPP.

[00:01:44] **SD Vern Crowley :** Je suis un membre assermenté de la police provinciale depuis plus de 30 ans. Pendant 25 ans, j'ai consacré la majeure partie de mon temps à des enquêtes fondées sur une preuve numérique.

Actuellement, je suis affecté à l'équipe des enquêtes sur la cybercriminalité de l'OPP en tant que responsable de la sensibilisation. Ma responsabilité consiste à établir ces partenariats avec les secteurs privé et public afin de partager les renseignements sur la menace et d'aider à renforcer les réseaux informatiques de l'Ontario dans le but de réduire la victimisation causée par la cybercriminalité dans la province.

[00:02:16] **Tenielle Bogdan :** À quel titre avez-vous été impliqué dans les municipalités et leur cybersécurité?

[00:02:22] **SD Vern Crowley :** Je fais ce métier depuis très longtemps, je suis presque un dinosaure, si vous voulez, en ce qui concerne la technologie numérique et les enquêtes criminelles. J'ai commencé à enquêter sur les infractions criminelles en 1995, en tant qu'enquêteur judiciaire en informatique. En 2015, j'ai aidé l'OPP dans sa cyberstratégie, qui était un regard holistique sur notre organisation et la façon dont nous traitons la technologie et les preuves fondées sur le numérique.

Un des éléments que nous avons constaté, c'est le besoin et les capacités de la Police provinciale de l'Ontario à enquêter sur les cybercrimes. C'est ainsi que je suis devenu membre de l'équipe. Je suis le responsable de la sensibilisation, car nous avons rapidement constaté que nous ne pouvons pas y arriver seuls, surtout en matière de cybercrimes. Nous devons établir des relations de travail positives pour aider à cibler et à renforcer l'Ontario, et à remplir notre rôle, qui est d'attraper les personnes mal intentionnées qui commettent des cybercrimes.

[00:03:22] Tenielle Bogdan : Nous savons que les cybercrimes et les attaques se produisent en permanence et que les municipalités font face à un nombre croissant de menaces. Mais une chose que nos auditeurs ne savent peut-être pas, c'est qu'il y existe un protocole pour mobiliser les forces locales d'application de la loi.

À quel moment une municipalité doit-elle donc faire appel aux forces d'application de la loi pour faire face à un cyberattaquant?

[00:03:40] **SD Vern Crowley :** C'est une excellente question. Et je suis content que cela fasse partie de ce balado. La meilleure pratique, à mon avis, serait d'entrer en contact avec les forces locales d'application de la loi avant même qu'un incident ne se produise afin de découvrir les protocoles de signalement et d'établir une relation positive de sorte que, lorsqu'un incident se produit, toutes les parties se connaissent. Si les forces locales d'application de la loi n'ont pas les moyens ou la capacité d'intervenir correctement à ce cyberincident, elles s'adresseront à notre service de police provinciale, notre équipe d'enquête sur la cybercriminalité, qui collaborera avec les forces locales d'application de la loi pour obtenir l'intervention et les ressources appropriées, quel que soit l'endroit où se trouve la victime dans la province.

L'une des questions clés est que nous devons obtenir le plus rapidement possible les détails du cyberincident ou de la cyberattaque et son impact sur l'organisation. Si nous pouvons obtenir ces détails, dans un délai assez rapide, cela nous permettra de mieux évaluer la situation et de collaborer au sein de notre comité d'application de la loi. S'il y a une chose que je peux dire, c'est qu'en 30 ans de carrière dans la police, je n'ai jamais vu une aussi grande collaboration entre les services d'application de la loi. Lorsqu'il est question de cybercriminalité, nous faisons un excellent travail.

Je peux vous dire que je suis au téléphone chaque semaine avec nos nouveaux partenaires municipaux, fédéraux et internationaux, que ce soit le Federal Bureau of Investigation (FBI), le département de la Sécurité intérieure (DHS) ou la National Crime Agency (NCA). Nous discutons des différentes cybermenaces et des différents cybercrimes qui se produisent. Ainsi, une notification rapide et opportune permet aux forces d'application de la loi d'obtenir les ressources nécessaires à une intervention efficace.

Cela nous permet également de recueillir ces renseignements qui nous permettraient d'établir des liens avec d'autres enquêtes éventuelles. Soyez assuré que, en tant que victime, vous n'êtes pas seul. L'enjeu est mondial. Un signalement rapide nous permettra d'établir des liens avec d'autres enquêtes et les leçons apprises de ces incidents pourront être partagées afin d'accélérer les efforts d'atténuation et de remédiation appropriés pour l'organisation victime, ici, en Ontario.

[00:06:01] **Tenielle Bogdan :** Sachant que vous vous concentrez sur l'Ontario, pouvez-vous nous dire si le processus est similaire ou non pour les autres provinces et territoires à l'échelle du Canada?

[00:06:12] **SD Vern Crowley :** Nous avons la chance d'avoir cette entité provinciale, mais en travaillant vraiment partout dans la province, comme je l'ai dit, nous ne pouvons pas le faire seuls.

Nous sommes en contact avec nos partenaires d'application de la loi d'un océan à l'autre, ainsi qu'avec la GRC qui a une responsabilité fédérale. Ainsi, pour tous les services de réseau du gouvernement et les infrastructures essentielles, la GRC sera la force policière compétente, celle avec laquelle nous travaillerons également localement avec la communauté de l'application de la loi.

Certains services de police locaux sont un peu plus matures que d'autres. Mais nous apprenons tous et nous nous soutenons mutuellement. Encore une fois, la chose la plus importante est d'établir un contact en amont, de découvrir les capacités et les protocoles de rapport, de sorte que si un événement se produit, vous connaissez les mesures à prendre.

[00:07:21] Tenielle Bogdan : Vous avez évoqué la manière dont l'organisme d'application de la loi peut contribuer à établir des ponts et des liens entre les cyberincidents qui se produisent à l'échelle mondiale et nationale. Que peut-il faire d'autre pour aider à lutter contre ce type d'attaques?

[00:07:34] **SD Vern Crowley :** En tant qu'organisme d'application de la loi, notre principale responsabilité est de trouver l'auteur du crime, les mesures d'atténuation ou correctives et les effets négatifs de l'événement. L'organisation victime,

quant à elle, est responsable de remettre les systèmes informatiques dans l'état où ils étaient avant l'attaque. La rapidité du signalement est très importante pour l'organisme d'application de la loi.

Nous pourrons peut-être vous présenter certaines des leçons apprises auprès de ces autres organisations victimes. Si nous sommes en mesure de présenter ces meilleures pratiques grâce auxquelles nous avons pu atténuer un autre événement, cela peut aider votre processus de remédiation à se dérouler plus efficacement. Il est presque garanti que si vous êtes une organisation victime et que vous passez par là, vous ne voudrez pas que cela arrive à votre municipalité ou organisation voisine. C'est une chose horrible à vivre.

Ces cybercriminels, malheureusement, gagnent beaucoup d'argent en le faisant et ils continuent à le faire pour deux raisons principales. Premièrement, il n'y a pas de signalement. Deuxièmement, ils gagnent beaucoup d'argent lorsqu'il s'agit de logiciel de rançon ou de prise d'otage de vos données. Il y a donc peu de risques pour eux. Ils gagnent beaucoup d'argent : gains élevés, risques réduits. Pourquoi s'arrêteraient-ils? Et c'est la principale raison pour laquelle ça arrive et c'est si répandu aujourd'hui.

[00:09:16] **Tenielle Bogdan :** Quels éléments d'information les municipalités doivent-elles avoir à portée de main lorsqu'elles travaillent avec les forces d'application de la loi?

[00:09:28] **SD Vern Crowley :** Veillez à ce que la personne qui va signaler l'incident aux forces d'application de la loi soit bien consciente de ce qui s'est passé, des effets et du niveau de danger auquel l'organisation fait face.

Le caractère d'actualité de ces éléments d'information essentiels est très important. La personne qui rapporte l'événement doit avoir une connaissance de première main de l'incident et de son effet sur l'ensemble de l'organisation.

En fait, un cybercrime n'est pas différent de n'importe quel autre crime. Si vous vous mettiez dans la peau d'un policier, vous cherchez la réponse à cinq questions : qui, quoi, où, pourquoi et quand.

Ce que nous voudrons savoir en premier lieu, comme je l'ai déjà mentionné, c'est ce qui s'est passé, ce qui est touché et le niveau de danger. Le type d'éléments que nous voudrions connaître dans le cas d'un chiffrement serait le type d'extension du fichier. Parce que ça nous donne une meilleure idée de ce qu'ils recherchent. C'est donc également crucial. Nous voudrions également connaître les mesures qui ont été prises. Parfois, il s'agit du service informatique et d'une société de sécurité tierce qui sont intervenus. Parfois, il peut s'agir d'un tiers totalement indépendant intégré dans le cadre de la cyberassurance.

Soyez assuré que nous travaillerons avec le service informatique ou la société de sécurité tierce. Nous ne sommes pas là pour interférer : nous sommes là pour aider.

Nous voulons aussi savoir s'il y a une menace ou une préoccupation permanente. Si l'incident est terminé et stable, c'est génial. Mais si cela dure depuis deux ou trois semaines après les faits, nous devons savoir s'il y a des conséquences sur les activités ou la sécurité publique, parce que c'est ce qui nous préoccupe.

Donc, une fois que l'incident est signalé, comment pouvez-vous compléter au mieux le signalement? De quels éléments d'information disposons-nous? Nous avons besoin des détails de base concernant l'incident. Les forces d'application de la loi voudront préserver et rassembler dès que possible toute preuve numérique potentielle liée à ce cyberincident. Il s'agit donc de fichiers journaux, de connexions suspectes, d'adresses IP, d'applications ou de processus suspects en cours d'exécution, ainsi que de tout identifiant des acteurs de la menace. Donc ça pourrait être des surnoms, des adresses électroniques. Les personnes mal intentionnées utilisent ces adresses électroniques anonymes. Il pourrait s'agir de ProtonMail ou de différents domaines, portefeuille Bitcoin, identifiants. S'il s'agit d'un logiciel de rançon, ce sera absolument important. Toutes les communications qu'ils ont pu avoir, qu'il s'agisse de la note de rançon, si elle était affichée sur l'écran, ou s'ils vous avaient envoyé un courriel ou même effectué des appels téléphoniques, ils doivent noter le numéro de téléphone d'origine. Le contenu de ces communications serait formidable, en plus de tout fichier suspect.

Nous poserons probablement toujours la question : qui a pu faire ça, à votre avis? L'incident peut sembler provenir d'un acteur de menace extérieur. On ne peut jamais vraiment exclure qu'un travailleur en place ait pu jouer un rôle dans une

certaine mesure; encore une fois, notre travail consiste à faire en sorte d'acquérir une connaissance complète de l'incident, du mieux que nous pouvons.

[00:13:56] **Tenielle Bogdan :** Selon vous, quels sont les autres services avec lesquels vous collaborez le plus étroitement dans le traitement des incidents?

[00:14:11] **SD Vern Crowley :** Avant tout, nous travaillons avec la victime et nous collaborons avec ses services informatiques. Souvent, il règne beaucoup de crainte. Et c'est peut-être l'une des raisons pour lesquelles les forces d'application de la loi ne sont pas forcément prévenues tout de suite.

L'une de leurs craintes est peut-être d'intervenir et d'entraver les efforts d'atténuation et de réparation, ce qui est faux. Nous voulons réduire le niveau de victimisation qui en découle. Nous collaborerons donc avec l'organisation. Une autre crainte est que certains renseignements puissent être divulgués aux médias ou que les médias soient informés de l'incident. Ce n'est pas vrai non plus. Comme il s'agit d'une enquête criminelle, nous ne ferons jamais de commentaires ni ne divulguerons des informations. Certains peuvent également craindre que la police voie des informations sensibles ou des données de tiers et remette l'information que nous recueillons. Comme indiqué précédemment, les services d'application de la loi s'occupent de l'incident lui-même, des métadonnées et, bien entendu, du contenu de la base de données ou de toute information financière.

Une autre opinion préconçue consiste à penser qu'il n'y a aucun avantage à signaler l'incident à la police. Des équipes comme l'équipe d'enquête sur la cybercriminalité de la Police provinciale de l'Ontario ont renforcé leur capacité et font des progrès pour attraper les personnes mal intentionnées. Il est donc très pertinent de signaler l'incident à la police.

D'autres organismes apportent leur soutien, comme le Centre canadien pour la cybersécurité (CCCS), qui ne fait pas partie des forces d'application de la loi. En raison de la place qu'ils occupent au sein du gouvernement canadien, ils ne sont pas vraiment autorisés à partager quoi que ce soit. Ainsi, si quelqu'un fait un rapport au CCCS, les renseignements ne sont pas nécessairement partagés directement avec les forces d'application de la loi. Il est plus que probable que le CCCS vous encourage à signaler l'incident à votre police locale, il est donc important que vous le fassiez.

Je dirais que la mesure proactive pour les personnes qui écoutent le balado est de trouver ces ressources et cela vous aidera à mettre en place votre plan d'intervention en cas d'incident.

[00:16:51] **Tenielle Bogdan :** Est-ce que d'autres partenaires externes ou fournisseurs tiers devraient participer au processus de collaboration avec les forces d'application de la loi?

[00:16:59] **SD Vern Crowley :** Nous compterons probablement une cyberassurance sous une forme ou une autre. Lorsqu'un incident se produit, la compagnie d'assurance déploie les entreprises et les ressources qu'elle a retenues pour intervenir rapidement. Nous avons des entreprises de réponse aux incidents, de criminalistique numérique, de conseil juridique, de marketing ou de soutien à la réputation. Et elles seront toutes prêtes à intervenir. Dirigées par la compagnie d'assurance, elles travailleront avec chacune d'entre elles. Encore une fois, il s'agit de travailler en collaboration pour permettre le partage d'information.

L'une des mises en garde, ou l'une des remarques que je veux faire à tous est que, souvent, un expert-conseil en gestion des cyberattaques ou un représentant juridique peut vous demander, à vous, la victime, de retarder ou même d'éviter l'implication des forces d'application de la loi pour protéger les intérêts de votre organisation. Mais l'ajout à cette réticence à signaler est vraiment un geste nuisible. Vous avez le droit de signaler un tel incident comme vous le feriez pour une introduction par effraction. Si la police n'est pas au courant, le phénomène devient très répandu et se poursuit sans cesse.

[00:18:16] **Tenielle Bogdan :** Vous avez mentionné le Centre canadien pour la cybersécurité et les différences entre vos deux organisations, mais comment travaillez-vous ensemble pour lutter contre la cybercriminalité?

[00:18:24] **SD Vern Crowley :** Nous travaillons avec eux. Leur principal mandat est de soutenir les infrastructures essentielles, notamment les municipalités du Canada, d'accroître la cyberrésilience, de promouvoir le signalement et, si possible, de fournir des conseils pour les aider à prendre les mesures d'atténuation ou de correction appropriées.

C’est là que nous nous complétons. Nous travaillons ensemble pour essayer de réduire la victimisation causée par la cybercriminalité. Ainsi, il arrive souvent que le CCCS soit invité à participer à des webinaires et qu’on nous demande le point de vue des forces d’application de la loi, et vice versa.

[00:19:33] **Tenielle Bogdan :** Nous savons que le contexte des cybermenaces s’élargit rapidement. Diriez-vous que vous avez observé des tendances au cours des deux dernières années?

[00:19:42] **SD Vern Crowley :** Les logiciels de rançon ont été le fléau des municipalités en particulier, mais aussi du secteur des soins de santé. Les groupes criminels sont de plus en plus habiles à utiliser ces logiciels. Ils ne sont pas discriminatoires. Partout où ils peuvent obtenir de l’argent, ils y utiliseront leurs logiciels malveillants dans les systèmes et vous demanderont une rançon. Les logiciels de rançon présentent probablement l’un des niveaux de risque les plus élevés, dans la mesure où ils pénètrent dans le réseau, que ce soit par le biais d’un protocole RDP, d’un courriel d’hameçonnage, d’une pièce jointe ou d’un lien malveillant.

Une fois que les criminels ont l’accès, ils se déplacent latéralement et parcourent toutes vos données pertinentes. D’abord, ils essaieront de les voler, puis ils les chiffreront, exigent alors d’être payés en Bitcoins, fort probablement. Ils exerceront une pression supplémentaire sur le paiement qu’ils divulgueront, soit sur un site de fuite de données, soit en informant littéralement vos parties prenantes ou vos clients des dossiers qu’ils ont obtenus et en leur disant qu’ils ont vos données et qu’elles seront divulguées.

L’entreprise, l’organisation ou la municipalité victime se retrouve donc avec des membres du public ou des parties prenantes qui font pression sur elle pour qu’elle agisse, car on ne veut pas que ces données soient publiées.

Au cours des 12 à 18 derniers mois, nous avons constaté que nos infrastructures critiques sont de plus en plus sondées. Il y a eu quelques incidents — vous avez entendu parler de Colonial Pipeline aux États-Unis, de JBS, le distributeur œuvrant au sein de l’industrie de la viande, qui a en fait affecté la chaîne d’approvisionnement au Canada également.

Nous constatons que ces piliers clés de notre économie, qu’ils soient sous contrôle municipal ou autre, sont désormais sondés par les cybercriminels. Nous devons faire attention et faire preuve de diligence raisonnable afin de garantir, au mieux de nos efforts, la sécurité de ceux-ci.

[00:22:07] **Tenielle Bogdan :** Et nous avons beaucoup entendu parler des crimes de situation. Constatez-vous que ce phénomène est toujours aussi répandu chez les cybercriminels? Constatez-vous que les cybercriminels font plus d’efforts pour s’introduire dans les systèmes ou qu’ils se contentent de saisir les occasions les plus faciles?

[00:22:20] **SD Vern Crowley :** C’est une combinaison des deux. Ils sont très opportunistes. Donc, à tous les auditeurs, soyez sensibles au caractère opportun de ce balado au Canada alors que nous entrons dans une autre période d’isolement.

Soyez prêts. Les cybercriminels vont appliquer leur technique d’ingénierie sociale pour vous inciter à cliquer sur un lien ou à obtenir plus d’information. En mars 2020, nous avons vu les cybercriminels changer de cible. Nous venions d’avoir une catastrophe en Haïti. Donc, chaque fois qu’il y a une opération de secours, ils utilisent leurs compétences en ingénierie sociale et intensifient leurs opérations.

La campagne du Centre antifraude du Canada, « Réfléchissez avant de cliquer », est une excellente campagne.

Si vous n’en avez pas déjà un, le moment est venu de créer un plan d’intervention en cas d’incident et de faire en sorte qu’il indique, en premier lieu, d’informer les forces d’application de la loi. Contactez votre agence locale d’application de la loi et découvrez les protocoles de signalement afin d’établir cette relation positive avant que l’incident ne se produise.

[00:24:17] **Tenielle Bogdan :** C’est fantastique. Merci, Vern.

Je remercie à nouveau le sergent-détective Crowley d’avoir partagé son point de vue et son expertise sur les cyberattaques et sur ce dont les municipalités doivent être conscientes lorsqu’elles travaillent avec les forces d’application de la loi.