Balado sur les villes cybersécurisées

Préparation à la réponse aux incidents avec Wadeed Mian, vice-président, Criminalistique numérique et réponse aux incidents chez ISA Cybersecurity

[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.

Je suis votre hôte, Tenielle Bogdan. Aujourd'hui, nous discutons avec Wadeed Mian, vice-président, Criminalistique numérique et réponse aux incidents chez ISA Cybersecurity.

Wadeed est un professionnel de la cybersécurité incroyablement passionné, comptant plus de 19 années d'expérience en gestion informatique, en gestion de la sécurité informatique et en architecture d'entreprise informatique. Tout au long de sa carrière, il a mis en œuvre des programmes et des pratiques de grande envergure en matière de sécurité de l'information. Il est très efficace dans la gestion des risques et des activités. Wadeed réussit à prendre des décisions cruciales pour protéger la disponibilité, l'intégrité et la confidentialité de systèmes commerciaux et d'information essentiels. S'il est reconnu pour son expérience et ses connaissances techniques, Wadeed incarne le concept de cadre en ressources humaines; il est toujours là pour son équipe dans ses temps libres.

Il aime passer du temps avec sa famille, manger des plats chinois avec ses amis et conquérir le monde des jeux vidéo. Aujourd'hui, Wadeed nous présente son point de vue et son expérience en matière de planification de la préparation aux incidents.

Bienvenue Wadeed! Avant de commencer, parlez-nous un peu de votre rôle au sein d'ISA.

[00:01:50] **Wadeed Mian :** Certainement. Je suis le vice-président de la criminalistique numérique et de la réponse aux incidents. Donc, en gros, tout ce qui relève de ce domaine fait partie de mon travail.

[00:01:57] **Tenielle Bogdan :** Depuis combien de temps travaillez-vous dans l'industrie? Quelle est votre expérience avec les municipalités?

[00:02:02] **Wadeed Mian :** J'œuvre au sein de l'industrie technologique depuis environ 20 ans. Et notre expérience avec les municipalités va de l'aide à la mise en place de solutions de sécurité et à leur architecture jusqu'à la réponse aux incidents.

[00:02:16] **Tenielle Bogdan :** Nous avons beaucoup entendu parler de l'évolution du contexte des cybermenaces, non seulement pour les municipalités, mais aussi pour de nombreuses autres organisations, l'un des principaux facteurs étant le passage à un environnement de travail à distance. Pourquoi le contexte des cybermenaces évolue-t-il pour les municipalités en dehors de cela?

[00:02:29] **Wadeed Mian :** Vous l'avez bien dit : le contexte évolue très rapidement, et ce, depuis longtemps, mais cette évolution s'est en quelque sorte accélérée ces derniers temps, et le travail à domicile l'a exacerbée. Les municipalités font face à un défi particulier, car de nombreux acteurs de menace ont réalisé qu'elles détiennent un grand nombre

d'informations, très, très sensibles. Il y a les informations d'entreprise et l'espionnage industriel. Le cyberactivisme est utile pour ce genre de choses, mais si vous parlez vraiment d'information sensible en ce qui a trait aux dossiers, les municipalités sont des mines d'or. Malheureusement, les municipalités ont une certaine réputation : leurs contrôles ne sont pas nécessairement à la hauteur et elles n'ont pas les budgets des entreprises Fortune 500.

Ainsi, pour ce qui est de la capacité à investir les ressources, l'infrastructure, elles ont tendance à être un peu en retard sur les objectifs.

[00:03:23] **Tenielle Bogdan :** Je suis certaine que la préparation est un facteur clé dans ce domaine. Comment joue-t-elle un rôle dans la sécurisation des municipalités?

[00:03:30] **Wadeed Mian :** Il y a une variété de domaines en particulier, mais en étant capable de construire un plan d'intervention en cas d'incident et un tel plan qui s'appuie sur votre stratégie, vous êtes mieux positionné pour faire face à une brèche ou à une cyberattaque. Vous devez être en mesure de les établir, ce qui nécessite évidemment un investissement assez important, mais vous devez également les maintenir à jour et les tester continuellement. En effet, au fur et à mesure que les organisations évoluent, les personnes et les rôles changent, inévitablement, et en cours d'évolution, les gens oublient qui faisait partie du plan d'intervention en cas d'incident (PII). Le fait de tester constamment vos plans et de les tenir à jour permet de cerner les domaines à améliorer, car votre infrastructure change et évolue, tout comme votre PII.

[00:04:25] **Tenielle Bogdan :** Je suis sûre qu'un élément clé de ce processus est la reconnaissance des incidents, c'est-à-dire le fait de savoir quand vous avez été attaqué ou quand il y a eu une brèche. Pouvez-vous nous en parler un peu?

[00:04:32] **Wadeed Mian :** C'est l'élément essentiel d'un PII. La première chose à faire est de comprendre qui prend les décisions. Quels en sont les critères? Une des choses à éviter : prendre des décisions ad hoc en temps de crise. Vous n'avez pas le temps d'évaluer correctement tous les risques, les réponses potentielles et tout ce qui s'en suit.

Donc, moins vous prenez de décisions à ce stade, mieux c'est. Vous voulez établir vos propres critères. Vous devez faire en sorte qu'ils portent sur ce qui est considéré comme une crise, un désastre ou un incident, et la façon dont vous les catégorisez. Et en fonction de cette catégorisation, comment invoquer la bonne stratégie? Comment faire participer les bonnes personnes? J'entends, il pourrait simplement s'agir de payer une rançon. Je viens de terminer un dossier au cours duquel le client a perdu l'équivalent de dix jours de données. Il nous a répondu qu'une perte de données importante est une perte financière importante. Nous avons posé des questions comme celles-ci : « quels sont vos critères pour payer la rançon? », « qui prendra cette décision? », « devons-nous faire appel à votre conseiller juridique? », « avez-vous un expert-conseil en gestion des cyberattaques à qui faire appel? ». Plus vous aurez de réponses à ces questions, ainsi qu'une liste de contrôle pour la situation, mieux vous vous porterez. Ainsi, l'identification d'une crise devient beaucoup plus simple. Il ne s'agit pas de demander à une personne de prendre une décision ad hoc pour déterminer s'il s'agit d'une catastrophe ou non.

[00:06:12] **Tenielle Bogdan :** Selon vous, qui pourrait être un bon leader en matière de cybersécurité au sein des municipalités?

[00:06:24] **Wadeed Mian:** Cela dépend vraiment des municipalités, mais nous recommandons toujours les experts-conseils en gestion des cyberattaques. Je ne saurais trop les recommander. La principale raison en est que ce sont des professionnels qui ont vécu cette expérience. Ils connaissent le contexte des cybermenaces, les acteurs de menace, les tactiques, les techniques et les procédures. Ils seront en mesure de vous guider, car, bien souvent, votre réponse en termes de décision concernant la rançon dépend aussi de la menace. Sont-ils les acteurs de menace? S'agit-il des affiliés qui veillent à la distribution? S'agit-il de personnes menaçantes qui se contentent de faire circuler l'information? Est-elle récente? Ce sont tous des paramètres qui doivent être pris en compte.

Je pense qu'il doit y avoir un décideur et c'est généralement, comme je l'ai dit, un expert-conseil en gestion des cyberattaques, un conseiller juridique, etc. qui prend la décision; mais il doit y avoir un effort de collaboration pour leur fournir les renseignements. Vous voulez leur fournir l'information dont ils ont besoin pour prendre une décision éclairée.

Qui est le concepteur de ce logiciel de rançon en particulier? Quel est l'impact? Par ailleurs, il pourrait s'agir d'un logiciel de rançon très sophistiqué, mais heureusement, il a été isolé dans un secteur de l'entreprise ou une zone de

ressources où les répercussions sont relativement faibles. Si tel est le cas, vous serez probablement beaucoup moins pressé de déclarer une urgence ou de payer la rançon.

Plusieurs de ces paramètres doivent être évalués. Et une fois que nous aurons fourni les bons outils aux bonnes personnes, elles pourront prendre une décision éclairée.

[00:08:00] **Tenielle Bogdan :** Donnez un peu plus de précisions sur ce qu'est un expert-conseil en gestion des cyberattaques. Pourrait-il s'agir d'un membre de l'équipe de la municipalité ou d'une tierce partie?

[00:08:09] **Wadeed Mian :** Je pense que tout ce qui précède dépend de la taille de la municipalité. Vous pouvez dépenser tout l'argent du monde et ne pas être sécurisé à cent pour cent. Il faut donc trouver un équilibre entre le budget et la sécurité effective, entre le risque et la récompense. Je pense que certaines municipalités voudront compter un expert-conseil en gestion des cyberattaques à temps plein dans leur équipe, car leur exposition est beaucoup plus importante. Et puis, il y a les petites municipalités, par exemple, qui ne sont peut-être pas en mesure d'avoir quelqu'un à temps plein. Maintenant, on peut faire appel à une tierce partie lorsque le besoin survient ou les municipalités peuvent se regrouper pour retenir les services d'un seul expert-conseil en gestion des cyberattaques.

Je pense que les municipalités devront évaluer le risque par rapport à la récompense lorsqu'il est question de déterminer la meilleure manière d'embaucher un tel professionnel.

[00:09:10] **Tenielle Bogdan :** Quand faut-il faire appel à un expert-conseil en gestion des cyberattaques? À quel moment les municipalités doivent-elles faire appel à un expert-conseil en gestion des cyberattaques?

[00:09:16] **Wadeed Mian :** Dès que possible. Et je suppose que vous le saviez déjà, mais oui, dès que possible. La raison en est que plusieurs personnes qui n'ont jamais fait face à un logiciel de rançon ont tendance à paniquer et à réagir de manière impulsive. Ces décisions rapides et irrationnelles peuvent nuire à votre capacité à vous rétablir rapidement ou à vous rétablir tout court.

Vous voulez engager votre expert-conseil en gestion des cyberattaques le plus tôt possible, parce qu'il est déjà passé par là. Il a été témoin de ces situations des dizaines de fois. L'une des premières choses que nous faisons lorsque nous entrons en relation avec un client est de le calmer. La première chose que je leur dis, c'est que je sais que chaque instinct, chaque fibre de votre être vous dit de paniquer et d'appuyer sur toutes les alarmes et de pousser les boutons, mais je vous en prie : ne le faites pas. La meilleure façon d'aborder cette question est de prendre du recul, de garder la tête froide et de tout évaluer. Vous devez être capable d'évaluer qui fait quoi, quelle est la meilleure approche et quel est le meilleur plan et de valider ce dernier. Parce que si nous nous contentons d'exécuter un plan, nous pouvons finir par aggraver les choses.

Généralement, la première attaque, surtout s'il s'agit d'une attaque sophistiquée, n'est que la première étape. Il y a plusieurs événements qui surviennent par la suite et il y a beaucoup de planification qui a déjà eu lieu avant cela. Un expert-conseil en gestion des cyberattaques apporte ces conseils à une organisation qui n'a pas vécu cette situation à plusieurs reprises et l'aide à comprendre le meilleur plan d'action.

En fait, notre directeur général utilise cet exemple et j'adore ça : quand vous voulez aller quelque part où vous n'êtes jamais allé, vous voulez amener quelqu'un qui y est déjà allé. C'est encore plus vrai dans le domaine de la criminalistique numérique et de la réponse aux incidents.

[00:11:51] **Tenielle Bogdan :** Pouvez-vous nous en dire plus sur la communication en cas de crise et sur la manière dont elle s'inscrit dans le cadre d'un PII?

[00:12:13] **Wadeed Mian :** L'une des premières choses que nous essayons de faire pour aider nos clients en matière de communication est de comprendre qu'il y a deux directions pour le comité. Il y a la communication interne puis la communication externe. Tout d'abord, la réaction instinctive est de commencer à envoyer toutes ces notes de service en interne, alors que nous insistons sur le fait de ne pas partager trop d'information lorsqu'une enquête est en cours. En effet, vous ne savez pas de quel type d'accès disposent les acteurs de menace. Là encore, un expert-conseil en gestion des cyberattaques pourra les guider dans cette démarche.

Vous devez également être conscient de ce que vous communiquez à l'extérieur de votre organisation, car vous pouvez être soumis à des lois en matière d'avis de divulgation. Votre conseiller juridique vous dira ce que vous pouvez et ne pouvez pas partager immédiatement, car cela pourrait mettre en danger certains de vos clients, consommateurs ou patients. Il est essentiel de comprendre ce qu'il faut communiquer et le moment auquel il faut le faire, et il est essentiel d'avoir ces deux critères distincts, car les objectifs diffèrent selon ce que vous communiquez en interne et à l'externe.

[00:14:08] **Tenielle Bogdan :** Nous avons parlé du plan d'intervention en cas d'incident et des stratégies. Comment ces décisions sont-elles prises? Comment sont-elles élaborées?

[00:14:24] **Wadeed Mian :** Le plan d'intervention en cas d'incident et la stratégie fonctionnent ensemble. Le plan d'intervention en cas d'incident est l'approche globale et complète, tandis que la stratégie comprend les outils qui fonctionnent selon l'incident.

Lorsque j'arrive dans une organisation et que j'ai l'occasion de l'aider à créer ces deux éléments, cela aide vraiment à préparer le terrain. C'est à ce moment que vous déterminez votre équipe d'intervention, avec des représentants de chacun des différents services. Ensuite, le PII tient également compte de la structure particulière de votre organisation.

La stratégie, voilà où ça devient technique. Et c'est un domaine qui me passionne. Elle est beaucoup plus précise à l'égard de la menace elle-même. Par exemple, nous enregistrons actuellement une forte hausse de la demande de création de stratégies portant sur les logiciels de rançon pour nos clients. Elles analysent la crise, les contrôles en place et la manière de les exploiter. Vous voudrez examiner vos fichiers et vos solutions de surveillance de l'intégrité pour découvrir où se trouvent vos points de terminaison et quels contrôles vous exercez sur eux. Et également voir s'il y a eu exfiltration de données. La stratégie vous indiquera exactement où aller. C'est très précis et méthodique.

[00:17:06] **Tenielle Bogdan :** Les logiciels de rançon sont un sujet dont on entend de plus en plus parler. Pourquoi ce type d'attaques augmente-t-il?

[00:17:13] **Wadeed Mian :** Je suis très franc, c'est parce que ce type a été efficace. Plusieurs statistiques vous montreront combien d'argent est versé et à quel point ces attaques sont prolifiques. Évidemment, le fait que la majeure partie de la main-d'œuvre travaille désormais à distance a également élargi l'empreinte, car vous n'êtes plus derrière un pare-feu d'entreprise et ces contrôles connexes. Plusieurs organisations ont été contraintes de travailler à distance et n'étaient pas équipées pour cela à l'époque. Avec la diminution des contrôles sur les appareils personnels et ceux auxquels on accède pour un certain nombre de raisons, associée aux résultats positifs que les acteurs de menace ont obtenus avec les logiciels de rançon, cela devient de plus en plus courant. Je déteste le dire comme ça, mais pour les acteurs de menace, ce n'est pas personnel ou émotionnel. C'est purement commercial.

[00:19:56] **Tenielle Bogdan :** Le principal élément que nous constatons est que la plus grande menace est le manque de sensibilisation aux solutions simples et aux mesures qui peuvent être prises pour protéger les municipalités et les organisations. Selon votre expérience, quelle est l'une des plus grandes lacunes que vous constatez dans les plans des clients ou, plus précisément, des municipalités au moment de leur exécution?

[00:20:12] **Wadeed Mian :** Dernièrement, l'un des défis auxquels nous avons fait face est que les organisations ont soit un PII qui est très spécifique à cette activité particulière, par opposition à un PII complet. Ainsi, lorsque quelque chose se produit en dehors de cette unité commerciale, il y a beaucoup de confusion et de retard. En réalité, vous voulez réduire au minimum le temps d'invocation et d'exécution. Lorsqu'on passe beaucoup de temps à essayer de savoir ce que l'on fera et qui en sera responsable, cette perte de temps devient un problème important.

Par exemple, l'enregistrement et la conservation centralisés sont l'une des choses qui vous aident vraiment à suivre ce qu'un acteur de menace a fait du point de vue des tactiques et procédures de base. Malheureusement, une fois de plus, nous avons eu affaire à un client qui ne disposait pas d'un enregistrement centralisé, ce qui a permis à l'acteur de menace de supprimer tous les enregistrements. Dans ce cas, nous avons dû nous lancer à l'aveuglette sans disposer de cette information clé.

[00:21:55] **Tenielle Bogdan :** Donc, les enregistrements centralisés et les sauvegardes sont les deux éléments dont il faut être conscient. Mais si vous pouvez donner à nos auditeurs un autre conseil tactique qu'ils peuvent prendre et mettre en œuvre dans leurs organisations, demain ou la semaine prochaine, quel serait-il?

[00:22:09] **Wadeed Mian :** Il faut absolument faire appel à une organisation qui répond aux incidents. L'un des points essentiels est que vous ne voulez pas être en train de négocier des contrats ou d'essayer de faire l'évaluation nécessaire pour engager un tiers en cas d'incident. Vous voulez que les personnes avec lesquelles vous avez déjà établi une relation et qui connaissent votre environnement soient prêtes à intervenir.

[00:22:34] **Tenielle Bogdan :** Comment les auditeurs peuvent-ils entrer en contact avec vous et avec ISA?

[00:22:37] **Wadeed Mian :** Les auditeurs peuvent toujours se rendre à www.ISAcybersecurity.com ou nous trouver sur LinkedIn pour découvrir un grand nombre de blogues très instructifs.

[00:22:46] **Tenielle Bogdan :** Et n'oubliez pas de consulter nos lignes directrices sur les meilleures pratiques en matière de cybersécurité municipale en direct sur le site Web des techniciens www.technationcanada.ca. Un grand merci encore à Wadeed et à toute l'équipe d'ISA Cybersecurity. Pour entrer en contact avec eux, rendez-vous sur leur site Web, www.isacybersecurity.com, ou consultez les articles et les messages de leur blogue sur leur page LinkedIn. Encore une fois, merci de nous avoir écoutés.