Balado sur les villes cybersécurisées

Examen des menaces, de la vulnérabilité et des risques avec Ashley Lukeeram, vice-président international, sécurité ISC/TO chez Tenable

[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 Ashley Lukeeram, vice-président international chez Tenable.

Il est responsable de la stratégie commerciale globale de Tenable au Canada et dirige une équipe d'experts en matière de cybersécurité qui aident les organisations à aborder la cybersécurité et la gestion des risques liés à la cybersécurité grâce aux solutions et aux services de Tenable. Ashley compte plus de 20 années d'expérience dans le secteur informatique. Il a commencé sa carrière dans un rôle de consultant en informatique, infrastructure et sécurité pour des entreprises clientes. Sa passion pour la cybersécurité l'a amené à gérer le programme de sécurité pour les distributeurs de Symantec et de Microsoft pour la région de l'Afrique. Il a poursuivi son parcours dans le domaine de la cybersécurité au sein d'entreprises phares du secteur, telles que Rogers, Symantec et RX. Avant d'entrer chez Tenable, Ashley a obtenu une maîtrise en technologies de l'information à l'Université de Cranfield, au Royaume-Uni. Il est également titulaire de plusieurs certifications reconnues par l'industrie.

Ashley a fait partie du comité consultatif de l'industrie de la conférence Reboot sur la confidentialité et la sécurité et est membre actif de TECHNATION et de l'Échange canadien de menaces cybernétiques. Aujourd'hui, nous discutons avec Ashley de l'examen des menaces, de la vulnérabilité et des risques.

Bienvenue à tous. Nous sommes très heureux d'accueillir aujourd'hui Ashley Lukeeram de Tenable. Parlez-nous un peu de votre travail chez Tenable.

[00:02:12] **Ashley Lukeeram :** Avec plaisir. Comme vous l'avez mentionné, je suis le directeur national de Tenable, donc je travaille avec des gens partout au pays. Notre responsabilité consiste à travailler avec un certain nombre de clients dans différents secteurs verticaux au Canada afin de les aider à aborder la cybersécurité d'un point de vue consultatif afin de les conseiller, au besoin, ou de suggérer des types de solutions qui peuvent les aider à réduire les risques dans leurs environnements.

[00:02:41] **Tenielle Bogdan :** Comment Tenable participe-t-elle à la cybersécurité, avec les municipalités en particulier?

[00:02:46] **Ashley Lukeeram :** Tenable est une entreprise qui a beaucoup investi au Canada depuis trois ans et demi. Une partie du travail que nous avons effectué est en fait pour des organisations comme TECHNATION, Sécurité publique Canada et Échange canadien de menaces cybernétiques. Par l'intermédiaire de ces différentes organisations, nous avons fourni un leadership éclairé aux municipalités. L'année dernière, j'ai participé avec TECHNATION dans la rédaction des meilleures pratiques en matière de cybersécurité municipale.

Outre les éléments clés que je viens de mentionner, nous interagissons également au quotidien avec différentes municipalités partout au pays. Très souvent, la principale raison pour laquelle les clients viennent chez Tenable est pour savoir par où commencer pour leurs besoins en cybersécurité. Dans bien des cas, c'est un grand mot qui a pour effet de désorienter les gens. Les gens ont très peu de ressources, donc ils viennent nous voir pour discuter davantage du programme de cybersécurité. Et c'est donc là que nous intervenons.

[00:04:05] **Tenielle Bogdan :** Alors, nous avons appris au cours des deux dernières années, avec la COVID, que l'environnement de travail a vraiment évolué vers un travail à distance et hybride, et de nombreuses vulnérabilités sont apparues.

Avez-vous vu d'autres raisons qui justifient l'augmentation du risque pour les municipalités?

[00:04:23] Ashley Lukeeram : Le mot clé ici est le risque. Donc quand on en parle, j'y pense sous deux angles principaux. Notre premier constat : les municipalités ont dû accélérer leur rythme de transformation numérique. En tant que citoyens canadiens, nous avons étudié les moyens de fournir de plus en plus de ces services en ligne. Nous recommençons à adopter davantage d'applications Web dans le but de rendre ces services facilement accessibles et aussi rapides que possible pour les citoyens.

Les questions posées portent sur le point de départ. Faut-il exploiter les infrastructures dans le nuage? Nous avons constaté que les différents fournisseurs de services infonuagiques, qu'il s'agisse d'AWS, de Google ou de Microsoft, adoptent de plus en plus souvent cette solution et que les municipalités s'y intéressent de plus en plus.

Le rythme de la transformation s'étant accéléré, il en va malheureusement de même de l'empreinte des attaques pour ces municipalités. Cette situation s'accompagne d'une période tout aussi exploitée avec la pandémie. La charge de travail a augmenté avec une empreinte élargie, et plusieurs n'ont pas nécessairement renforcé leur protection de l'environnement.

[00:08:01] **Tenielle Bogdan :** En discutant du changement de réseau pour les employés à distance, pouvez-vous donner des conseils aux municipalités qui pourraient les aider à atténuer le risque qui accompagne spécifiquement le changement des réseaux?

[00:08:13] **Ashley Lukeeram :** Il y a un certain nombre de mesures qui pourraient être prises, mais il est très important de commencer par la validation de l'identité. Lorsque vous vous connectez à vos appareils, veillez à avoir un mot de passe fort ou une authentification à facteurs multiples. Les municipalités déploient aujourd'hui un certain nombre de capacités.

Ensuite, revenez aux bases et suivez une formation de sensibilisation à la sécurité. Il est important de passer en revue les éléments fondamentaux et d'en être conscient, comme la manière de détecter une attaque par hameçonnage et de la signaler. Une bonne pratique consiste à mettre en place ce type de formation pour l'ensemble de votre personnel afin qu'il sache ce sur quoi il ne faut pas cliquer.

[00:09:20] **Tenielle Bogdan :** Quelles sont les motivations de ces acteurs de menace qui mettent en œuvre des cyberattaques? Pourquoi ciblent-ils davantage les municipalités?

[00:09:35] **Ashley Lukeeram :** Lorsqu'il est question des municipalités, elles font affaire à des citoyens comme vous et moi, et très souvent, nous nous connectons à différentes tablettes et différents appareils. En gros, cela signifie qu'il existe beaucoup de données à caractère personnel (DCP) dans l'environnement que les municipalités ont mis en place aujourd'hui.

Du point de vue d'un pirate informatique, c'est génial. Les données sont d'une importance cruciale dans ce monde. S'ils peuvent avoir accès à vos informations personnelles, il existe de nombreux preneurs de ces informations pour qui est prêt à payer. Il existe une économie souterraine qui exploite les renseignements sur votre identité. Ces acteurs cherchent à savoir comment accéder à ces données et les transformer en argent.

Le deuxième domaine concerne ce qui se passe lorsqu'une attaque touche une organisation. Il s'agit aussi de comprendre l'ampleur de l'impact que cela aura. Dans le cas d'une brèche auprès d'une municipalité, cela a également un impact sur la marque, et pourrait avoir un angle politique. En fin de compte, si une municipalité est victime d'une brèche, il y aura une conversation autour du logiciel de rançon et de la forme que prendra le paiement.

Un autre domaine est la défense autour des municipalités. Il y a une pénurie de main-d'œuvre dans le domaine de la cybersécurité, ce qui signifie qu'il y a moins de personnes qualifiées pour travailler dans ce domaine et protéger les organisations. Les pirates en sont conscients et ces environnements sont de plus en plus sollicités. Avec moins de personnes travaillant dans ce domaine, les pirates n'ont besoin que d'une seule et unique faille pour s'introduire dans ces environnements.

Enfin, il y a le domaine des systèmes de contrôle industriel, que nous appelons aussi techniques opérationnelles. Si vous pensez aux systèmes informatiques, vous pensez aux traitements au sein des municipalités. Ces deux dernières années, nous avons assisté à une convergence entre l'informatique traditionnelle et l'infrastructure TO/ISC. Il peut s'agir de situations de vie ou de mort. Par exemple, si quelqu'un s'introduit dans une usine de traitement de l'eau et modifie légèrement la quantité de chlore ou d'autres produits chimiques entrant dans la composition de l'eau, c'est un gros problème pour les gens. L'accès à ces éléments opérationnels au sein des municipalités a des conséquences très, très sérieuses pour les citoyens.

Et par conséquent, cela en fait une cible très attrayante pour ces personnes très mal intentionnées. Ce sont des attaques ciblées. Ce sont toutes des cibles très connues et les personnes mal intentionnées savent qu'elles peuvent obtenir des rançons potentielles grâce à ces attaques.

[00:14:11] Tenielle Bogdan : Diriez-vous que ces attaques ciblées constituent toujours des crimes de situation?

[00:14:27] **Ashley Lukeeram :** Il est clair que plus la municipalité ou toute autre organisation rend la tâche difficile au pirate, moins elle risque de subir une brèche ou une attaque. Il ne suffit pas d'avoir un seul niveau de sécurité. Il ne suffit pas d'avoir un logiciel antivirus ou un pare-feu. Je pense que ça revient à la taille de l'organisation. Quels sont les points faibles potentiels? Comme tout bon pirate, ils commenceront par effectuer une activité de reconnaissance. Ils vont entrer, balayer l'environnement et le réseau, simplement pour comprendre votre mécanisme de défense.

[00:15:30] **Tenielle Bogdan :** Et je suis certaine que c'est la raison pour laquelle il est très important de connaître et de faire le suivi de ces vulnérabilités potentielles.

[00:15:37] **Ashley Lukeeram :** Absolument. Et plus important encore, il faut intervenir autant que possible en temps réel. Vous ne pouvez pas survivre dans ce monde en faisant une évaluation deux fois par an et penser que vous avez fait preuve de diligence raisonnable. La cybersécurité évolue très rapidement, et nous devons disposer d'évaluations de la vulnérabilité de l'environnement rapprochées du temps réel.

[00:16:03] **Tenielle Bogdan :** Pour une plus petite municipalité qui ne dispose peut-être pas d'une vaste équipe cybernétique ou informatique pour réaliser cette réévaluation constante, qui doit en assumer la responsabilité?

[00:16:18] **Ashley Lukeeram :** C'est là qu'il faut déterminer à qui appartient le risque. Traditionnellement, cette responsabilité incombait au groupe de cybersécurité. En tant que citoyens et membres des municipalités, nous devons nous assurer que tous les membres de l'organisation comprennent la cybernétique et le cyberrisque. Nous devons commencer à introduire la culture du risque dans les organisations. Cela peut se faire par une formation de base et en veillant à ce que votre personnel comprenne que le risque peut avoir un impact considérable sur l'ensemble de la municipalité.

Je dirais que le nombre de mesures que l'on peut prendre sur le plan des évaluations ne couvre pas tous les aspects en ce qui a trait à la technologie dès le premier jour. Vous pourriez commencer par une évaluation très simple de vos processus et flux de travail opérationnels. Vous pouvez commencer à peaufiner certains de vos processus d'entreprise afin de minimiser vos risques.

[00:17:46] **Tenielle Bogdan :** Vous avez abordé brièvement la question des évaluations des risques. Quelles sont les autres évaluations des risques auxquelles les municipalités peuvent se soumettre?

[00:17:52] **Ashley Lukeeram :** Ce que je viens d'évoquer relève davantage d'une évaluation qualitative des risques. Nous pourrions également intervenir pour vous faire répondre à un questionnaire et aborder des questions telles que le déroulement de la sauvegarde. Quel type de contrôles avez-vous mis en place? Vous pouvez également poser ces mêmes questions à vos fournisseurs. Les municipalités, comme plusieurs autres organisations, comptent sur de tierces parties pour fournir différents services. Lorsqu'elles arrivent au sein de l'équipe, il serait bon de disposer d'une liste des contrôles que vous aimeriez voir effectuer par ces tierces parties avant qu'elles vous fournissent le service.

Le deuxième domaine concerne la mesure quantitative de votre risque. Pour bien y parvenir, il est très important que les municipalités mettent en place un programme de gestion de la vulnérabilité. C'est à cet endroit que vous devriez examiner les capacités du secteur à venir, mesurer l'ampleur de votre empreinte totale : vos serveurs traditionnels, vos terminaux, votre nuage, votre infrastructure de travail à distance. Vous aurez ainsi une idée des vulnérabilités professionnelles de votre environnement. En même temps, cela vous permet de mieux comprendre le type d'actifs dont dispose votre organisation. Si vous ne pouvez pas voir ce que vous avez, vous ne serez pas en mesure de vous protéger. C'est également la raison pour laquelle vos examens des actifs et des risques doivent être effectués de manière continue.

De nombreuses organisations avec lesquelles nous avons travaillé, et avec lesquelles nous travaillons encore, font appel à un sous-traitant pour effectuer un test d'intrusion une fois par année ou deux fois par semaine. Oui, c'est un début, mais ce n'est pas suffisant. La question qui revient très souvent est la suivante : quelles nouvelles vulnérabilités existent aujourd'hui? En règle générale, l'entreprise demandera dans quelle mesure elle est protégée contre cette nouvelle vulnérabilité.

Ce que nous voyons souvent, c'est que les organisations sortent leur dernier rapport, déjà vieux de six mois, qui ne contiendra pas la réponse, car il s'agit d'une nouvelle vulnérabilité et d'une nouvelle menace. Il s'agit donc d'évoluer en permanence. Vous devez arriver à ce point où vous comprenez que le risque n'est pas statique. Il change chaque jour, chaque minute. Comme tous les acteurs de menace et toutes les personnes mal intentionnées. Nous devons examiner nos actifs, les renseignements de première ligne, puis l'impact potentiel, et ce, aussi souvent que possible.

[00:21:21] **Tenielle Bogdan :** C'est génial. J'aime beaucoup votre remarque sur le plan de gestion de la vulnérabilité. Pouvez-vous nous parler de la manière dont cela s'intègre dans un plan de préparation aux situations d'urgence ou un plan d'intervention d'urgence (PIU)?

[00:21:34] **Ashley Lukeeram :** Je dirais qu'un plan de gestion des vulnérabilités est un élément fondamental d'un programme de cybersécurité. Lorsque vous examinez les plans d'intervention en matière de TI et d'urgence, il s'agit de votre guide sur la façon dont votre organisation doit réagir. Lorsque nous parlons de plans de gestion des vulnérabilités, il s'agit d'être aussi proactif que possible, en essayant de réduire la probabilité de ces situations et de ces brèches. Ainsi, plus vous en savez sur vos vulnérabilités, plus vous aurez de temps pour travailler avec votre service informatique afin d'appliquer des correctifs et de remédier aux risques, et de réduire le nombre d'interventions d'urgence que vous devrez réaliser. Ceci ne veut pas dire qu'il n'y aura jamais d'incident; toutefois, en étant proactif, vous pouvez espérer en réduire la probabilité.

[00:22:37] **Tenielle Bogdan :** Pouvez-vous partager avec nous une histoire de réussite concernant une organisation avec laquelle vous avez traité ou dont vous avez eu connaissance et qui a éliminé le potentiel d'une cyberattaque ou d'une brèche grâce à une préparation adéquate?

[00:22:50] **Ashley Lukeeram :** Celle à laquelle je pense est en fait une municipalité de l'Ouest canadien. Cela remonte à la fin de 2019. La municipalité était assez petite, avec seulement deux ressources pour le programme de cybersécurité, pour un effectif total d'environ 2 500 employés. À l'époque, ils étaient venus nous voir pour discuter de leurs difficultés en tant qu'entreprise aux ressources limitées. Dans ces conditions, ils étaient seulement en mesure d'obtenir une visibilité de ce qui existait dans leur environnement, mais ils étaient incapables d'aller plus loin dans l'analyse, car à mesure qu'ils analysaient, ils trouvaient de plus en plus de vulnérabilités. Avec un nombre croissant de vulnérabilités, la municipalité se trouvait dans un scénario réactif.

Ils ont décidé d'effectuer des tests de pénétration sur leur système pour aider à diagnostiquer certaines des lacunes. Il s'agit d'un ensemble d'exigences en matière gestion de vulnérabilité en fonction des risques. En faisant appel à nous pour les aider à évaluer la situation, leur équipe de deux employés à temps plein a pu se faire une idée plus précise de la manière de sécuriser leurs principales vulnérabilités sans accroître leur effectif.

De plus, ils ont amélioré la hiérarchisation des vulnérabilités pour définir celles à corriger en premier. Oui, ils en trouvent encore beaucoup, mais grâce aux capacités existantes aujourd'hui, nous disposons de suffisamment d'informations pour les conseiller sur celle à corriger en premier. En même temps, cette organisation commence à réfléchir à la manière d'étendre sa couverture aux systèmes de contrôle industriel, ce que nous étudions pour elle.

[00:25:58] **Tenielle Bogdan :** Et diriez-vous qu'avec davantage de formation et de sensibilisation au sein de cette organisation particulière, la culture de la cybersécurité a changé?

[00:26:08] **Ashley Lukeeram :** Oui. Il y a certainement eu une plus grande prise de conscience du fait qu'il s'agit d'un risque permanent pour eux. Si nous revenons en 2019, ils n'évaluaient que ce dont ils étaient conscients. Maintenant, le fait qu'ils disposent d'une certaine automatisation qui les aide, ils sont indéniablement plus curieux de découvrir tout ce qu'ils peuvent.

[00:26:46] **Tenielle Bogdan :** Si vous pouviez donner un conseil tactique à nos auditeurs, quel serait-il? Que voudriez-vous qu'ils retiennent de notre conversation?

[00:26:58] **Ashley Lukeeram :** L'hygiène informatique est extrêmement importante. Le monde de la cybersécurité offre de nombreuses possibilités. Il y a beaucoup de grands mots, mais quand on parle de s'en tenir aux principes de base, il faut vraiment connaître ses actifs et ses vulnérabilités. À partir de là, vous pouvez déterminer où aller et quels mécanismes de protection mettre en place. C'est comme si vous emménagiez dans une toute nouvelle maison et que vous deviez réfléchir à l'emplacement des caméras de sécurité physique. Vous commencerez par déterminer tous les points d'entrée, fenêtres, portes, accès au sous-sol, etc. Il en va de même de notre approche de la cybersécurité. Ne tentez pas l'impossible, tenez-vous-en aux principes de base.

[00:27:52] Tenielle Bogdan : Je remercie à nouveau Ashley et son équipe de Tenable d'avoir pris le temps de discuter avec nous aujourd'hui. Pour entrer en contact avec Tenable ou pour en savoir plus sur leurs services, rendez-vous sur leur site Web à www.tenable.com. Comme toujours. Si vous souhaitez en savoir plus sur la façon d'améliorer la cybersécurité de votre organisation, rendez-vous sur technationcanada.ca et consultez nos lignes directrices sur les meilleures pratiques en matière de cybersécurité municipale. Je vous remercie de nous avoir écoutés. Soyez cyberprudents.