Deloitte.

Bâtir une communauté d'échange avisée

L'échange de renseignements pour contrer les cybermenaces est devenu un impératif

La complexité des cybermenaces évolue rapidement ces dernières années. En effet, des réseaux criminels, politiques et gouvernementaux très spécialisés supplantent les pirates informatiques et les criminels qui sévissent à petite échelle et de manière aléatoire, pour s'imposer comme la principale menace des organisations.

Ces réseaux spécialisés sont les auteurs d'un savant mélange de cybermenaces qui peuvent cibler des organisations, des régions et des profils clients précis, grâce à un ensemble ingénieux de logiciels malveillants et de systèmes d'anonymisation.

Les dirigeants d'entreprise comprennent de mieux en mieux que la nouvelle cyberréalité engendre des menaces, plus nombreuses et plus complexes, et qu'à mesure que ces menaces s'amplifient, le renforcement des capacités des cybercriminels s'intensifie également. En outre, ils se rendent compte peu à peu qu'il ne suffit pas de modifier les politiques en matière de sécurité et d'apporter des correctifs techniques pour contrer ces nouvelles menaces.

Pour combattre les nouveaux cyberguerriers, les entreprises ont besoin d'un renseignement d'un nouveau genre. Elles doivent se doter de solides capacités en matière de renseignements sur les cybermenaces (RCM) et pouvoir communiquer l'information sur les cybermenaces aux personnes et systèmes appropriés afin de prendre des décisions de manière proactive. Pour relever ce défi, les entreprises devront élargir leur vision, compter sur des dirigeants avertis et créer de nouveaux modèles de collaboration au sein des secteurs et entre ceux-ci.

Les cybercriminels savent à quel point le renseignement est important. Ils profilent activement les organisations afin de mettre au point un code malveillant et des techniques d'attaque très personnalisées dans le but d'exploiter des failles précises en matière de sécurité. Ils ne se bornent pas à recueillir des renseignements : ils se les échangent, s'entraidant pour exploiter les vulnérabilités des organisations.

Les entreprises canadiennes font donc face à un bataillon de cyberadversaires tenaces, motivés et agiles qui échangent et emploient diverses tactiques, techniques et procédures (TTP) destinées à infecter les systèmes, à perturber les services, à commettre des actes de fraude financière, à exposer des renseignements de nature délicate et à voler la propriété intellectuelle.

Les entreprises auraient intérêt à s'inspirer du mode opératoire des cybercriminels d'aujourd'hui. Si les cyberattaquants consacrent des ressources pour mettre à profit les renseignements provenant de leur communauté afin de faire avancer leurs travaux, qu'est-ce qui empêche les entreprises d'en faire autant?

En quoi consistent les renseignements sur les cybermenaces (RCM)?

Les RCM correspondent à une capacité organisationnelle, et non à un ensemble de données. Il s'agit d'une approche fondée sur le renseignement visant à gérer les cyberrisques et à bâtir une cyberrésilience. Elle nécessite une sensibilisation constante aux menaces actuelles, pertinentes et émergentes qui pèsent sur l'organisation afin de déceler et d'atténuer les attaques à venir de façon proactive.

Des avantages pour les organisations

Bien que les cyberattaquants se transmettent depuis longtemps des renseignements sur la sécurité dans leur intérêt mutuel, les entreprises mettent beaucoup de temps à collaborer. Les dirigeants d'entreprise commencent à peine à reconnaître pleinement l'utilité d'échanger des renseignements sur les cybermenaces pour lutter contre ce phénomène.

Le besoin est urgent, car les activités cybercriminelles continuent de proliférer. Selon un rapport conjoint entre McAfee et le Center for Strategic and International Studies publié en juin 2014, le coût de la cybercriminalité au Canada est estimé à 0,17 % du produit intérieur brut du pays[1], et selon le Ponemon Institute, le coût de la cybercriminalité s'élevait en moyenne à 7,6 M$ par entreprise en 2014, ce qui représente une variation nette de 10,4 % par rapport aux résultats de l'étude menée l'année précédente par cet organisme[2].

L'intensification des cyberattaques alimente le débat entourant l'échange de renseignements entre tous les secteurs et sous-secteurs d'activité. De nombreuses organisations n'ont cependant pas dépassé l'étape des pourparlers. Selon les résultats d'un sondage, la majorité des chefs d'entreprise se disent disposés à échanger des renseignements sur la cybersécurité et le feraient volontairement. Néanmoins, plus de 40 % ne communiquent aucune information, invoquant essentiellement des motifs juridiques ou des impératifs opérationnels.

La nécessité d'échanger des RCM devient toutefois de plus en plus évidente, et des organisations telles que le U.S. National Institute of Standards and Technology (NIST) proclament haut et fort que « pour renforcer les moyens d'intervention en cas d'incident et raffermir les mécanismes de cyberdéfense, les organisations doivent tirer parti de la sagesse collective de leurs pairs en échangeant des renseignements et en coordonnant les interventions en cas d'incident[3] ».

Les organisations ont encore de la difficulté à aller de l'avant dans le domaine de l'échange de RCM. Pour surmonter leur réticence, elles doivent mieux comprendre la manière exacte dont elles peuvent se transmettre des renseignements de façon sûre et efficace, protéger leur confidentialité et tirer des avantages globaux importants de leurs échanges.

La création de communautés d'échange de renseignements est un pas en avant, et cela peut améliorer la capacité de déjouer les menaces durables et ingénieuses qui pèsent sur les entreprises, les secteurs d'activité et les régions tout en renforçant la cyberrésilience aux attaques ciblées. Pour mettre à profit l'échange de RCM, il faut comprendre les principales conditions préalables, c'est-à-dire les caractéristiques d'une plate-forme ou d'une infrastructure technologique habilitante et la nature du cycle de vie d'une initiative d'échange de RCM.

Une nécessité reconnue

Reconnaissant l'utilité et la nécessité d'une communauté d'échange de renseignements sur les cybermenaces, Deloitte a participé à la création du centre d'Échange canadien de menaces cybernétiques (ECMC). En tirant parti de notre savoir et de notre expertise en renseignements sur les menaces et du partage de renseignements sectoriels à l'échelle mondiale, nous avons contribué à définir les exigences et les éléments constitutifs du centre ECMC en plus de développer un modèle de gouvernance qui explique son fonctionnement et la façon dont les entreprises peuvent en bénéficier.

Création d'une communauté d'échange de RCM

Les menaces actuelles peuvent être un facteur de motivation décisif qui incitera les entreprises à collaborer à la création d'une solide communauté d'échange de RCM au Canada. Avant qu'une communauté de ce type ne puisse fonctionner, les milieux d'affaires canadiens doivent, dès le départ, tenir compte de certaines considérations. Voici une liste de mesures qui comprend les meilleures pratiques pour créer une communauté d'échange de RCM efficace :

Élaborer des structures de supervision et de gouvernance

Des structures claires peuvent contribuer à orienter la vision de la communauté d'échange de renseignements et garantir la mise en place de procédures pour résoudre les problèmes. Cette communauté doit se doter d'un conseil de surveillance vigoureux, assujetti à des règles claires. Au-delà du conseil, elle devra disposer d'un code de conduite, de procédures et de sanctions capables de régler les différends ou les manquements de ses adhérents. Une surveillance stricte procure aux adhérents la certitude que leurs droits et obligations sont régis par des règles claires et que des mesures de sécurité ont été mises en place pour empêcher l'échange non autorisé ou la fuite de données.

Mettre en application des critères d'adhésion à la communauté d'échange

L'établissement d'un processus et de critères définis peut aider à assurer que les nouveaux adhérents sont évalués en fonction de leur volonté d'échanger des renseignements, des meilleures pratiques, leur savoir-faire et leur expérience. Pour bâtir une communauté d'échange de RCM forte, il faudrait un processus défini d'intégration des renseignements des adhérents selon lequel les analystes peuvent obtenir une information essentielle et pertinente auprès de l'organisation membre. Ce processus permettrait également aux membres de recevoir des rapports personnalisés sur les menaces qui pèsent sur des actifs précis.

Donner priorité aux échanges intersectoriels

Les cyberattaquants ne s'en prennent pas toujours à un secteur d'activité en particulier lorsqu'ils cherchent de nouvelles cibles. Bien que le fait de se fier au renseignement de leur secteur d'activité, comme au Financial Services – Information Sharing and Analysis Centre (FS-ISAC), soit d'une grande valeur pour les communautés d'échange de RCM, celles-ci auraient intérêt à se fier également à l'échange intersectoriel dans le cadre du plan d'action des communautés d'échange de RCM, et des contrôles et des accords adéquats devraient être mis en place.

Mettre à profit les connaissances en matière de cybersécurité

La collecte et l'analyse des renseignements de la communauté d'échange doivent être confiées à des spécialistes qui peuvent produire des rapports et dégager des tendances. Les communautés d'échange de RCM requièrent également un personnel spécialisé dans l'exploitation courante, qui collaborera à la gestion et à l'administration du programme.

Encourager des discussions ouvertes relatives aux renseignements sur les menaces

Des discussions de groupe ouvertes et périodiques peuvent aider les membres de la communauté à échanger des meilleures pratiques, des points de vue et des perspectives d'une manière motivante et enrichissante, et les aider aussi à créer un climat de confiance au sein du groupe.

Respecter les exigences juridiques et réglementaires de conformité et de confidentialité

Le respect des exigences juridiques er réglementaires de conformité et de confidentialité en matière d'échange de renseignements demeure fondamental. Cela permet aux organisations de définir, de publier et de diffuser les responsabilités en matière de droit civil ou pénal pour que tous les membres comprennent leurs obligations.

Toutefois, comprendre le contexte réglementaire ne fournit que les bases. Si les renseignements personnels de clients sont recueillis, utilisés ou divulgués, des mesures pour vérifier que des contrôles de confidentialité appropriés sont intégrés dans la conception de la technologie et dans l'infrastructure de confidentialité doivent être prises. Selon le type et la quantité d'information divulguée ou compromise, des questions de responsabilité pourraient se poser compte tenu de la hausse du nombre de recours collectifs et de poursuites judiciaires au Canada.

Un avantage concurrentiel consiste à choisir une approche de gestion des risques proactive en ce qui a trait à la confidentialité. Il convient d'adopter une démarche de protection intégrée de la vie privée pour que les pratiques liées au renseignement et les normes de confidentialité ne soient pas seulement conformes aux exigences réglementaires, mais également aux meilleures pratiques en matière de confidentialité. Deloitte offre un programme[4] d'attestation de protection intégrée de la vie privée visant à démontrer que les processus, les solutions et les programmes respectent les meilleures pratiques en matière de confidentialité, minimisant ainsi le risque de compromission et d'atteinte à la réputation.

Élaborer un cadre de financement de la communauté d'échange

L'acquisition de technologies, de plateformes et de ressources adéquates pour produire un renseignement utile nécessite que les membres prennent des engagements en matière d'affectation de fonds. Il importe d'explorer les méthodologies de partage des coûts pour déterminer celles qui conviennent à la communauté d'échange.

Par exemple, l'imposition de droits d'adhésion par catégorie plutôt que celle de contributions fixes pourrait être efficace dans certaines communautés d'échange. Les affectations de fonds devraient couvrir non seulement les coûts d'exploitation et de technologie, mais également les coûts de recherche et de développement.

Établir des relations avec les pouvoirs publics

Les communautés d'échange du secteur privé devraient commencer immédiatement à établir des relations de réciprocité avec les organismes gouvernementaux afin d'émettre et de recevoir des avis d'atteinte à la sécurité, qui peuvent aider à prévenir et à détecter les menaces et à intervenir en cas d'incident.

Que faut-il échanger?

Les entreprises désireuses de collaborer pour combattre et prévenir les cyberattaques peuvent échanger une foule de renseignements. En voici des exemples :

- les renseignements sur les cibles et les attaquants potentiels;
- les vecteurs utilisés par un attaquant connu;
- les méthodes d'attaque et les répercussions d'une attaque réussie;
- les leçons retenues et les lignes directrices pour se protéger.

Les principaux paramètres pour l'établissement d'une communauté d'échange de RCM réussie sont les suivants :

1. Disposer d'un outil centralisé et sécurisé **d'échange de renseignements;**
2. Établir une relation de **confiance** entre les membres de la communauté composée de sociétés publiques et privées de divers secteurs;
3. **Échanger des meilleures pratiques, des préoccupations et des sujets de discussion entre les membres;**
4. **Consigner les résultats** auxquels on pourra avoir recours pour favoriser une sensibilisation interne aux RCM.

Le pouvoir de l'échange

Une communauté d'échange dans laquelle les organisations peuvent communiquer des renseignements en temps réel sur les menaces constamment en évolution peut retirer des avantages généraux de ces échanges, notamment :

- l'accès à des renseignements utilisables et pertinents;
- une meilleure compréhension des menaces;
- des économies de coûts en raison de l'élimination du chevauchement des tâches;
- des évaluations des risques plus justes;
- la mise en œuvre de modèles d'échange sans la nécessité d'adopter de nouvelles lois;
- la détermination de tendances et l'établissement d'indicateurs de compromission;
- la hiérarchisation des menaces et des vulnérabilités par ordre d'importance et d'imminence;
- l'amélioration de la sécurité par l'adoption de meilleures pratiques communes;
- l'acquisition d'une connaissance contextuelle commune des menaces;
- la mise en corrélation d'indicateurs qui, en apparence, ne sont pas liés;
- une meilleure souplesse défensive en passant des stratégies réactives aux stratégies proactives;
- l'amélioration et l'accélération du processus décisionnel par le recours à une information en temps réel commune;
- le signalement plus rapide aux clients des incidents susceptibles d'avoir des répercussions.

Établir une plate-forme d'échange de RCM

Une fois en place les éléments de base d'une communauté d'échange de RCM, l'étape suivante consiste à établir une plate-forme technologique appropriée. Les travaux à accomplir porteront sur les systèmes, les outils et les contrôles permettant d'échanger rapidement des connaissances sur les menaces tout en protégeant les renseignements exclusifs de l'organisation.

Tout comme la création d'une communauté générale d'échange de RCM, l'établissement de plates-formes efficaces d'échange de RCM comporte des mesures et des meilleures pratiques essentielles :

Créer une taxonomie des communautés d'échange de renseignements

Une taxonomie explicite aidera à assurer que tous les participants utilisent et comprennent un langage et des termes communs. Cette taxonomie devrait comporter des normes de classement des renseignements selon leur degré de crédibilité, telles que le Traffic Light Protocol (protocole par feu de signalisation). Les communautés d'échange devraient délimiter des frontières pour déterminer les niveaux d'information auxquels les membres et les secteurs ont accès. Enfin, il conviendrait d'établir des cotes de confiance et de les inclure dans les rapports destinés aux membres pour qu'ils sachent à quel point ils peuvent se fier à une certaine source d'information.

Opérationnaliser la plate-forme

Si une communauté d'échange décide de créer sa propre plate-forme, elle devra mettre au point des applications de même qu'une infrastructure. Une telle approche requiert l'élaboration d'une solide interface d'applications largement fonctionnelles, ainsi que l'acquisition et la mise en œuvre d'éléments infrastructuraux qui assureront son accessibilité en tout temps.

Plutôt que de créer sa propre plate-forme, une communauté d'échange préférera peut-être s'épargner du temps et des ressources en mettant à profit des partenariats avec des spécialistes des RCM et en ayant recours aux technologies existantes. Une telle approche pourrait comporter, par exemple, la mise en œuvre d'une plate-forme d'échange d'information sur les logiciels malveillants (MISP), c'est-à-dire une plate-forme en libre accès pour l'échange, le stockage et la mise en corrélation « d'indicateurs de compromission » pour des attaques ciblées ou une plate-forme d'échange de renseignements sur les cybermenaces reconnue dans le secteur (Soltra Edge).

Mettre en place des capacités d'anonymisation

Une plate-forme devrait permettre aux membres d'échanger ouvertement ou anonymement des renseignements. Pour soutenir l'anonymisation, la communauté d'échange devrait créer une définition consensuelle et mettre au point les contrôles nécessaires. Tous les membres devraient connaître les aspects du processus d'échange qui sont, ou peuvent être, anonymisés sans risque de causer des erreurs d'interprétation.

Contrôler le volume des renseignements échangés

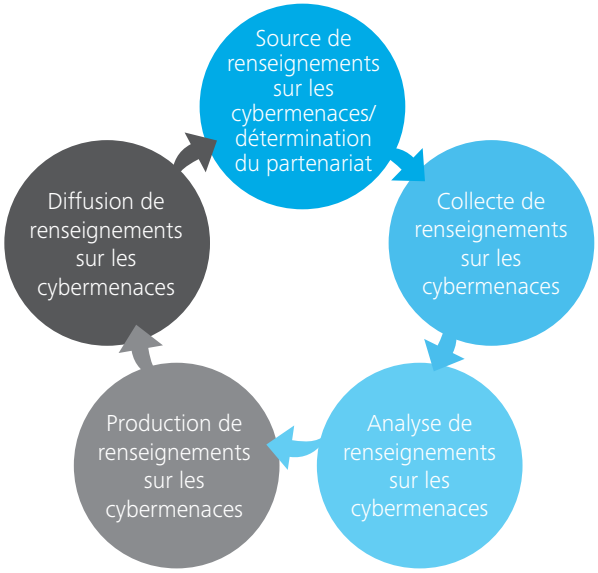
La mise au point de processus clairs de tri et d'analyse des renseignements contribue à assurer que l'information névralgique est échangée en priorité tout en limitant la quantité de renseignements échangés. Un excès d'information peut consommer de précieuses ressources et pourrait retarder le traitement de renseignements vitaux.

Produire des renseignements utilisables

L'échange de renseignements présente une valeur limitée si les rapports et les discussions ne font pas ressortir les mesures possibles que les membres devraient prendre pour protéger leurs activités contre les menaces ou les vulnérabilités décelées.

Le cycle de vie de l'échange de RMC

Une fois la plate-forme nécessaire mise en place, le processus permanent d'échange de renseignements sur les cybermenaces peut commencer. Dans sa forme la plus efficace, ce processus est une initiative de bout en bout qui comporte l'acquisition, l'évaluation, la diffusion et l'application de connaissances sur les cyberadversaires dans le but de produire des « renseignements utilisables ». L'objectif est de maximiser la valeur générée pour chacune des entreprises membres et pour l'ensemble de la communauté d'échange.



Un pouvoir protecteur

Les communautés d'échange de RCM qui ont une portée intersectorielle et ont accès aux renseignements en temps réel peuvent aider les entreprises à réagir plus efficacement aux menaces et à mieux protéger leurs actifs.

La mise en place et l'opérationnalisation d'une communauté d'échange exigent une approche graduelle, dont la première véritable étape consiste à rassembler un groupe de leaders engagés et visionnaires et à établir une structure directrice. Une fois que les leaders ont défini les exigences et les résultats escomptés de base, ils peuvent commencer à établir un programme pilote et à adopter une stratégie véritablement révolutionnaire en matière de cybersécurité.

En somme, l'adoption de meilleures pratiques établies pour l'échange de RCM peut fournir de solides principes aux organisations qui veulent non seulement créer une communauté d'échange de renseignements sur les cybermenaces, mais aussi permettre à cette dernière de devenir un mécanisme collectif de protection actif, efficace et durable contre les cybermenaces.

La véritable première étape consiste à rassembler un groupe de leaders engagés et visionnaires et à établir une structure directrice.

Transmettre ce que nous savons

Deloitte possède l'expérience qui lui permet d'aider les organisations à faire face aux cybermenaces à l'aide de divers outils, processus et tactiques, dont des projets d'échange de RCM. Nous sommes heureux de transmettre ce que nous savons. Pour en savoir plus au sujet de notre approche à l'égard des RCM et discuter de la marche à suivre pour créer une communauté d'échange de RCM, n'hésitez pas à nous joindre.

Dina Kamal

Associée
Leader nationale, Cyber Intelligence et Services d'analytique
dkamal@deloitte.ca
+1 416-775-7414

[1] McAfee et Center for Strategic and International Studies. Net Losses: *Estimating the Global Cost of Cybercrime,* [En ligne], page consultée le 20 août 2015, http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.

[2] Ponemon Institute. *2014 Global Report on the Cost of Cyber Crime,* [En ligne], page consultée le 31 mai 2015, http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime.

[3] National Institute of Standards and Technology. *Guide to Cyber Threat Information Sharing (Draft),* [En ligne], page consultée le 9 juillet 2015, http://csrc.nist.gov/publications/drafts/800-150/sp800_150_dr05pdf.

[4] Deloitte LLP, Université Ryerson, Cavoukian Dre Ann et Kingsmill S. *Privacy by Deisgn – Setting a news standard for privacy certification.*

www.deloitte.ca

Deloitte, l'un des cabinets de services professionnels les plus importants au Canada, offre des services dans les domaines de la certification, de la fiscalité, de la consultation et des conseils financiers. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 15-3128H