Les voiles au vent

Compte rendu de l'initiative Pleines voiles de la Commission des services financiers et des services aux consommateurs visant à favoriser la croissance des marchés financiers

NUMÉRO SPÉCIAL

La cybersécurité au Nouveau-Brunswick

COMMISSION DES SERVICES FINANCIERS ET DES SERVICES AUX CONSOMMATEURS

Mars 2018

La cybersécurité, à la fois casse-tête et source de possibilités

Il y a quelques années, j'ai assisté à une conférence de l'ISACA (Information Systems Audit and Control Association) où Mike Rogers était le conférencier d'honneur. À l'époque, il venait de terminer son mandat au sein du Permanent Select Committee on Intelligence des États-Unis; sa conférence portait sur l'importance grandissante de la cybersécurité dans un contexte commercial caractérisé par l'emploi de la technologie. Elle comprenait de nombreux exemples de risques cybernétiques touchant pour la première fois l'infrastructure d'affaires. Mike Rogers y évoqua aussi l'importance de gérer ces risques selon une approche systémique de large portée. Il termina sa conférence en affirmant que désormais, la gestion des risques cybernétiques n'était plus un coût d'exploitation, mais bien un coût de pérennisation des activités. Aujourd'hui, ses paroles sont plus vraies que jamais. Pas une semaine ne passe sans que nous entendions parler d'une nouvelle menace ou attaque cybernétique. Il ne fait aucun doute que la cybersécurité doit être prise au sérieux.

Mais il y a aussi de bonnes nouvelles. Grâce à l'adoption de nouvelles normes, de pratiques exemplaires et d'outils novateurs, nous sommes maintenant mieux en mesure de gérer efficacement les risques cybernétiques. Au Nouveau-Brunswick, nous avançons dans la bonne direction, en appuyant et en encourageant les initiatives porteuses de résultats concrets qui aideront les entreprises à mieux gérer les menaces cybernétiques. Les chercheurs et les entrepreneurs sont encouragés à trouver de nouvelles solutions innovatrices non seulement pour les grandes entreprises, mais également pour les PME qui semblent se trouver de plus en plus dans le point de mire des cybercriminels.

Le secteur public et le milieu universitaire sont sur la même longueur d'onde, car ces secteurs cherchent eux aussi à faire du Nouveau-Brunswick un centre d'excellence et d'innovation en matière de cybersécurité. Le présent numéro du magazine *Pleines voiles* s'inscrit résolument dans cette poussée.

JAKE VAN DER LAAN

Jake est le directeur de l'informatique et le directeur de la division de l'Application de la loi de la Commission des services financiers et des services aux consommateurs. Depuis 2015, il est responsable du développement et de l'exécution du plan et de la stratégie de cybersécurité. Son approche s'inspire du cadre du National Institute of Standards and Technology (NIST) des États-Unis.

FCNB

ENVOYEZ-NOUS VOS COMMENTAIRES

Dites-nous ce que vous aimeriez lire dans notre prochaine édition de *Les voiles au vent.* Soumettez-nous votre histoire ou faites-nous parvenir un courriel à propos d'un évènement important qui touche les marchés financiers du Nouveau-Brunswick.

COMMISSION DES SERVICES FINANCIERS ET DES SERVICES AUX CONSOMMATEURS
85, rue Charlotte, bureau 300
Saint John (N.-B.)
E2L 2J2

Sans frais : 1 866 933-2222
Courriel : info@fcnb.ca
Site Web : FCNB.ca

NE MANQUEZ PLUS JAMAIS QUOI QUE CE SOIT

Abonnez-vous en ligne

Suivez-nous pour en savoir plus sur ce que nous faisons pour favoriser les marchés financiers du Nouveau-Brunswick, ainsi que pour vous tenir à jour en matière de réglementation, d'application de la loi, de programmes d'éducation et d'activités de liaison externe.

FCNB.CA
@FCNB_
FCNB CA
FCNB.CA
FR.FCNB.CA/souscrire

Des brigands sur l'autoroute de l'information

Selon David Shipley, personne n'avait songé au brigandage de l'autoroute de l'information, mais c'est malheureusement devenu une réalité.

« Le réseau Internet n'a pas été conçu à l'origine pour assurer des communications sécurisées. Même aujourd'hui, la cybersécurité est le plus souvent une préoccupation secondaire dans le développement de nouvelles technologies, affirme le directeur général de la société Beauceron Security Inc. Malgré ces risques, nombreuses sont les personnes qui persistent à croire que la technologie est la seule façon de contrer la cybercriminalité, faisant fi de l'élément humain. »

Une récente étude menée par IBM révèle que dans 95 p. cent des cas, le succès des cyberattaques est attribuable à l'erreur humaine – des employés qui auraient cliqué sur un lien dans un courriel d'hameçonnage, par exemple. Ce sont des erreurs qui coûtent cher. Selon une étude menée en 2015 par un assureur britannique, la cybercriminalité coûterait 400 milliards de dollars par année aux entreprises à l'échelle du globe.

C'est l'élément humain de la cybersécurité au travail qui motive les efforts déployés par Beauceron. L'entreprise, qui en est à sa troisième année d'activité, tire son nom du beauceron, un excellent chien de garde d'origine française. Comme son nom l'évoque, elle aspire à transformer les salariés de ses clients en des sentinelles efficaces aptes à protéger les actifs numériques de leur employeur. Cette approche représente un changement radical de la façon dont les entreprises sont en général protégées, car la plupart d'entre eux comptent sur les services des TI, souvent surchargés de travail.

« Le réseau Internet n'a pas été conçu à l'origine pour assurer des communications sécurisées. »

Aujourd'hui, Beauceron offre une formation en cybersécurité, des cours en ligne, des exercices de simulation et une vaste gamme de services dans le but de faciliter l'apprentissage des salariés et l'adoption de nouveaux comportements face aux vulnérabilités bien réelles des entreprises.

Des brigands sur l'autoroute de l'information – suite

Voici trois conseils de David Shipley pour vous aider à protéger vos appareils contre les cyberattaques.

1. Renseignez-vous.

Il n'est pas nécessaire d'être un spécialiste, mais il faut tout de même être vigilant. Savez-vous combien d'appareils vous avez à la maison? Vos logiciels sont-ils à jour? (Anecdote : L'affaire Equifax est due à la négligence de l'entreprise à maintenir ses serveurs à jour.) Au bureau, informez-vous auprès du gestionnaire des TI pour savoir si votre ordinateur est à jour. Vous pouvez aider à détecter les problèmes.

2. Traitez la cybersécurité et la sécurité physique sur le même pied.

Il est facile d'oublier qu'un mot de passe trop simple est aussi hasardeux que de se promener dans une foule avec un billet de 100 $ dépassant de sa poche. Les deux font de vous une proie facile.

3. Signalez tout courriel suspect ou toute activité inhabituelle à l'équipe des TI.

Lorsque vous signalez un courriel étrange, vous aidez à protéger les autres membres de l'organisme qui auraient pu recevoir le même message, et vous aidez l'équipe des TI à mieux comprendre la nature de l'attaque.

Les prédictions de David Shipley sur ce que nous réserve l'avenir en matière de cybersécurité? Il est probable que la situation va s'empirer avant de s'améliorer, car il existe un grand fossé entre les besoins et les lacunes réglementaires.

« L'exemple le plus pertinent est à mon avis celui du Titanic, dit-il. Le naufrage du navire a été la première grande catastrophe en mer à provoquer le renforcement de la réglementation sur la sécurité maritime, comme le nombre de canots de sauvetage requis à bord de chaque navire. »

« Des réformes importantes à la *Loi sur la protection des renseignements personnels numériques* sont également nécessaires, renchérit David Shipley. À l'heure actuelle, la pénalité maximale pour une infraction est de 100 000 $, un montant infime en comparaison aux sommes colossales volées par les pirates informatiques. »

De plus, il reste difficile de détecter ces pirates, et encore plus de les surprendre en flagrant délit. Au Canada, les suspects ne sont identifiés que dans 6 p. cent des délits cybernétiques rapportés à la police.

« À l'heure actuelle, la pénalité maximale pour une infraction est de 100 000 $, un montant infime en comparaison aux sommes colossales volées par les pirates informatiques. »

David Shipley ne perd toutefois pas espoir. Il estime que la cybersécurité est entre les mains des personnes qui peuvent prendre des mesures concrètes pour se protéger et protéger leur milieu de travail.

« Lorsque nous disposons des bons outils et que nous comprenons les enjeux et notre rôle relativement à la protection d'un organisme, et lorsque nous sommes encouragés à prendre les mesures nécessaires, nous apportons beaucoup plus d'enthousiasme à notre rôle », ajoute David Shipley.

Protéger le Nouveau-Brunswick du World Wild West

Quand on demande au Dr Ali Ghorbani comment coordonner une initiative efficace en cybersécurité au Nouveau-Brunswick, c'est clair qu'il a longuement réfléchi.

« Pour que ces efforts soient efficaces, il faut impliquer tous les paliers du gouvernement, le milieu de l'enseignement et le secteur privé, afin qu'ils travaillent ensemble, affirme le directeur du Canadian Institute for Cybersecurity (CIC), établi à Fredericton. Les atteintes à la cybersécurité nous concernent tous, alors il est crucial de collaborer afin de les prévenir. »

Le Dr Ghorbani entrevoyait une province prémunie contre la cybercriminalité dès 2007, moment de la création du Centre of Excellence in Cybersecurity au campus de Fredericton de l'Université du Nouveau-Brunswick (UNB). « Nous avons constaté qu'une lacune importante en lien avec la cybersécurité était l'aspect interdisciplinaire, rappelle-t-il. Cette question dépasse la science informatique; elle implique les activités commerciales, l'éducation, la psychologie et le développement de produits, et j'en passe. »

En janvier 2017, l'UNB, l'Agence de promotion économique du Canada atlantique (APECA) et le gouvernement provincial ont développé cette vision en créant le CIC. Il s'agit d'un centre interdisciplinaire de formation, de recherche, de développement et d'entrepreneuriat, qui s'appuie sur l'expertise de chercheurs dans les domaines des sciences sociales, des affaires, de l'informatique, de l'ingénierie, du droit et des sciences.

De nos jours, l'établissement d'un programme efficace en cybersécurité est de mise dans tous les secteurs. Les données médicales électroniques servent

Protéger le Nouveau-Brunswick du World Wild West – suite

à l'élaboration de profils, les secteurs de la chimie et des sciences de la vie amassent d'énormes quantités de données biomédicales, et le système juridique produit toujours plus de renseignements sensibles.

« Au bout du compte, ce sont des particuliers qui sont les responsables de la protection des systèmes qui contiennent des renseignements sensibles, note le Dr Ghorbani. La protection de l'infrastructure essentielle du Nouveau-Brunswick est d'une importance capitale. Par exemple, si une intrusion devait compromettre notre réseau électrique, les conséquences logistiques et financières seraient très graves. »

Le maintien de la cybersécurité au Nouveau-Brunswick comporte des défis particuliers.

« La sensibilisation des Néo-Brunswickois est notre principal défi, affirme le Dr Ghorbani. Beaucoup de Néo-Brunswickois n'ont pas les connaissances de base qui les protégeraient dans le cyberespace. Pour y remédier, nous collaborons avec CyberNB afin d'offrir des présentations et des ateliers dans les écoles. J'espère que nous pourrons offrir cette formation aux personnes âgées également. »

Lorsqu'on lui demande des conseils sur la cybersécurité, le Dr Ghorbani affirme que le plus important, c'est de rester vigilant. « Ne vous fiez à personne en ligne – c'est encore l'anarchie, dit-il. Méfiez-vous de l'inconnu. Assurez-vous d'installer les toutes dernières mises à jour de sécurité dans votre système d'exploitation et vos logiciels. »

Le Dr Ghorbani signale que la prudence sera encore plus importante lorsque les risques augmenteront, particulièrement ceux associés à l'intelligence artificielle et à l'automatisation.

« Au bout du compte, ce sont des particuliers qui sont les responsables de la protection des systèmes qui contiennent des renseignements sensibles. La protection de l'infrastructure essentielle du Nouveau-Brunswick est d'une importance capitale. »

« Ne vous fiez à personne en ligne – c'est encore l'anarchie. Méfiez-vous de l'inconnu. »

« Nous ne faisons que commencer à comprendre les risques de l'Internet des objets », avance le Dr Ghorbani. « L'intelligence artificielle et l'apprentissage automatique, bien que très utiles, dévoilent de nouveaux risques que peuvent exploiter les personnes malveillantes. »

Il est désormais évident que l'éducation est d'une grande importance dans l'atténuation des risques cybernétiques. La faculté des sciences informatiques de l'UNB vient tout juste d'autoriser la création d'un programme de Maîtrise en cybersécurité appliquée, lequel se complèterait en un an, et s'ajouterait aux programmes de premier cycle en la matière.

« L'éducation, l'éducation, l'éducation, conclut le Dr Ghorbani. C'est le moyen par excellence de combattre la cybercriminalité. »

L'Internet des objets (IdO) fait référence à des appareils intelligents qui sont connectés entre eux sur ou hors Internet, et dont la connexion peut être interrompue à volonté. Par exemple, cela peut être un téléphone intelligent, une machine à café, une machine à laver, des écouteurs, une lampe et des appareils portables. Cela peut aussi comprendre des composantes de machine, comme un réacteur d'un avion ou la foreuse d'une installation de forage.

Le Nouveau-Brunswick, épicentre de la cybersécurité

Alors qu'un nombre croissant d'activités quotidiennes sont réalisées en ligne, CyberNB s'efforce de jouer un rôle de chef de file au Canada dans le domaine de la cybersécurité.

« Imaginez le Nouveau-Brunswick sous l'attaque de cybercriminels et que nous n'ayons plus accès à l'Internet, lance Allen Dillon, vice-président de CyberNB. Les technologies sont omniprésentes dans nos vies, de la pompe à essence aux services bancaires et à l'approvisionnement alimentaire, et nous en dépendons. D'où l'importance d'avoir le système le mieux sécurisé possible. »

Établi en 2016, CyberNB est un organisme de services spéciaux d'Opportunités NB, elle-même une agence gouvernementale du Nouveau-Brunswick. Sa stratégie en cinq axes vise à protéger la population et l'économie de la cybercriminalité.

Selon la firme Cybersecurity Ventures, le coût global de la cybercriminalité atteindra 6 billions de dollars d'ici 2021. Parallèlement, elle prévoit qu'il y aura 3,5 millions d'emplois vacants dans le domaine de la cybersécurité d'ici 2021.

M. Dillon affirme que dans un monde de plus en plus branché, notre approche repose sur l'acceptation que la cybersécurité fait désormais partie de notre quotidien. Nous ne pouvons protéger la population et l'économie si nous ne disposons pas de ressources appropriées, comme des politiques pour la protection de nos concitoyens, des infrastructures essentielles et l'offre de nouvelles possibilités de formation et d'emploi pour la main-d'œuvre locale.

« Imaginez le Nouveau-Brunswick sous l'attaque de cybercriminels et que nous n'ayons plus accès à l'Internet. Les technologies sont omniprésentes dans nos vies, de la pompe à essence aux services bancaires et à l'approvisionnement alimentaire, et nous en dépendons. »

Leur stratégie à cinq axes s'inspire des contributions des secteurs d'activité, du milieu universitaire et du secteur public. Ces axes sont : constituer une main-d'œuvre qualifiée afin de répondre au besoin croissant de professionnels de cybersécurité; protéger les infrastructures essentielles de la province; promouvoir le développement des technologies de cybersécurité; établir un parc d'entreprises de cybersécurité de renommée internationale; former un partenariat avec le Canadian Institute for Cybersecurity (CIC) basé à l'Université du Nouveau-Brunswick (voir **Protéger le Nouveau-Brunswick du World Wild West**).

CYBERNB

A SPECIAL OPERATING AGENCY OF OPPORTUNITIES NB | UN ORGANISME DE SERVICE SPÉCIAL D'OPPORTUNITÉS NB

ONB Opportunities | OpportunitésNB

Le Nouveau-Brunswick, épicentre de la cybersécurité – suite

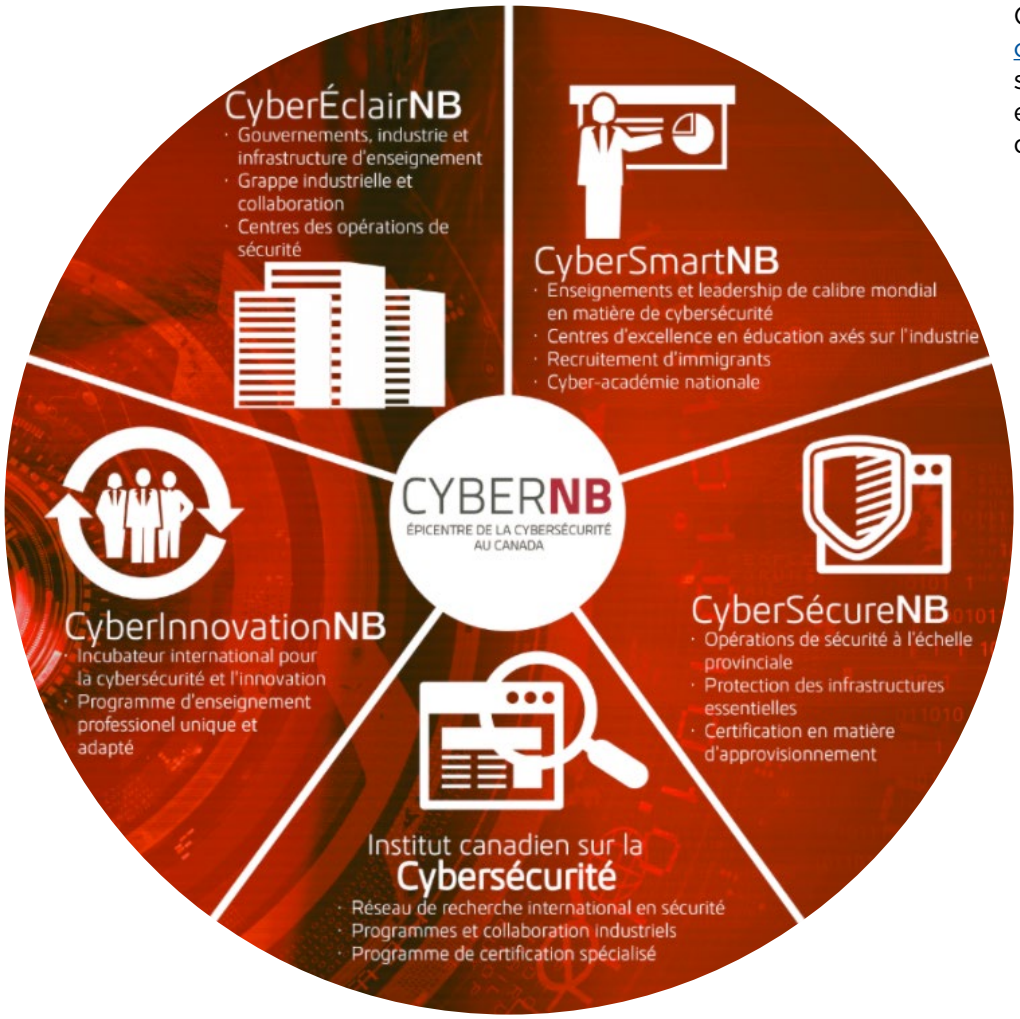
« C'est une approche entièrement intégrée, fondée sur la coopération des secteurs d'activité, du secteur public et du milieu universitaire afin d'assurer la protection de l'économie et de la population à l'aide de renseignements et de ressources appropriés », affirme Allen Dillon.

Depuis son lancement, CyberNB a établi la norme *Cyber Essentials*, une norme sur la cybersécurité dans le cadre de laquelle les organismes peuvent faire l'objet d'une évaluation et peuvent obtenir une certification.

Fruit d'une étroite collaboration avec CyberNB, le Collège communautaire du Nouveau-Brunswick a récemment annoncé qu'il offrira en septembre un nouveau programme d'un an menant à un diplôme au campus de Saint-Jean (N.-B.). Le programme portera sur la mise en place de réseaux sécurisés et l'évaluation des vulnérabilités et des menaces systémiques.

En outre, CyberNB et Blue Spurs ont lancé conjointement un projet pilote de démarrage scolaire grâce auquel les élèves de l'élémentaire au secondaire reçoivent le matériel informatique et les logiciels qui leur permettront de mieux comprendre l'Internet des objets (IdO). Les résultats étant concluants, il s'agit maintenant d'incorporer cette trousse de démarrage dans le programme de cours de toutes les écoles de la province.

Nous sommes un chef de file à bien des égards de dire Allen Dillon. « Nous voulons faire en sorte que le Nouveau-Brunswick soit reconnu comme étant l'épicentre de la cybersécurité au Canada. »



Consultez le site cybernb.ca et sa vidéo[1] pour en apprendre davantage.

1. https://youtu.be/b_KdVfMdPHQ