Bulletin consultatif sur la gestion de risques

ASSURANCE CONTRE LES CYBER-RISQUES

L'évolution et le marché de masse de la cybercriminalité

Bien que les marchés de la cybercriminalité aient été inondés de milliards de données personnelles, les malfaiteurs ont amélioré leur modèle opérationnel en faisant appel à la technologie et à l'extorsion. Maintenant, plutôt que de voler et de tenter de vendre les données d'une organisation, les criminels refusent tout simplement l'accès à ces données au moyen de « rançongiciels ».

Au Canada, des cabinets d'avocats, des sociétés comptables, des entreprises de construction, des universités, des collèges, des hôpitaux, des municipalités, des organismes gouvernementaux, etc. ont tous été victimes de ce type d'extorsion en ligne, et les incidents se multiplient à l'échelle mondiale.

Dans certains cas, lorsque les criminels ne reçoivent pas la rançon, ou le montant qu'ils estiment mériter, ils menacent de faire fuiter les données volées dans les médias ou auprès du grand public afin d'entacher la réputation de leurs victimes. Peu importe le scénario, les cybercriminels sont capables de monnayer vos investissements dans des appareils, des données, des applications et l'automatisation de processus.

Comment s'infiltrent les cybercriminels

Si vous prenez le nombre d'employés, de clients, de fournisseurs et de tiers qui interagissent numériquement avec votre organisation sous forme de courriels, d'achats, d'ententes d'approvisionnement, de contrats, de services, de paiements, etc., vous constaterez que chaque communication et chaque point de contact représentent une porte d'entrée que peuvent franchir les cybercriminels. Ces gens savent que vous ne pouvez pas sécuriser chaque appareil, réseau ou interaction en ligne. Ils trouvent les points faibles et les exploitent. Les recherches ont montré que neuf fois sur 10, le point faible était une personne peu méfiante. C'est pourquoi la technologie de sécurité ne peut pas à elle seule résoudre le problème.

Le nombre d'hameçonnages en 2016 était de 1 220 523, soit une augmentation de 65 % par rapport à 2015[1]. Votre équipe de sécurité peut-elle répondre à une croissance de 65 %, sachant en plus qu'il ne s'agit que d'une tactique parmi d'autres? Alors,comment atténuer les risques?

Concentrez-vous sur la cause, et pas sur l'effet

Le nombre de personnes susceptibles d'être victime d'une cyberattaque au sein de votre organisation dépasse largement ce que peut gérer un programme de sécurité axé sur la technologie. Il convient plutôt de procéder avec prudence et de manière stratégique, c'est-à-dire en quantifiant la source et la nature des risques humains inconnus, puis en mesurant, en gérant et en surveillant ces risques.

[1]APWG, « Phishing Activity Trends Report for Q4 2016 », le 23 février 2017, en ligne : https://apwg.org/trendsreports/ (disponible en anglais seulement)

Une fois que les risques humains sont connus, leur gestion doit être prise en compte dans les priorités opérationnelles, les processus et les investissements dans la technologie de sécurité. De plus, comme le dit l'adage : « ce qui peut être mesuré peut être fait ». En somme, les dirigeants s'appuient sur les données sur les risques pour améliorer l'efficacité et l'efficience des processus de sécurité.

Atténuez vos risques

Selon un rapport de recherche commandité par FICO[2], les assurances contre les risques cybernétiques jouent un rôle capital dans la protection contre la cybercriminalité. Le même rapport indique également que les organisations doivent établir une stratégie en matière de cybersécurité qui touche tous les domaines d'activité et que pour renforcer la sécurité informatique, elles doivent mesurer cette dernière de façon objective. Le fait de mesurer, gérer et surveiller les risques est une partie essentielle de la stratégie, car ces trois piliers garantissent que tous les domaines d'activité assument leurs responsabilités concernant les risques cybernétiques, et fournissent les moyens de réduire efficacement ces risques.

[2]FICO, « What the C-Suite Needs to Know About Cyber Readiness », le 3 mai 2017, en ligne : http://www.fico.com/en/blogs/fraud-security/what-do-the-c-suite-think-about-cybersecurity/ (disponible en anglais seulement)

Illustration 1 - Détermination proactive des points sensibles aux risques cybernétiques humains

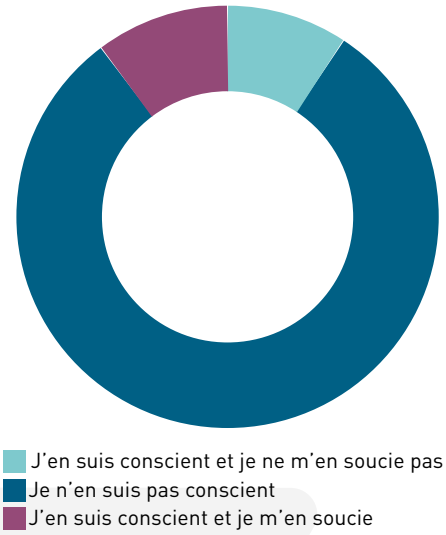
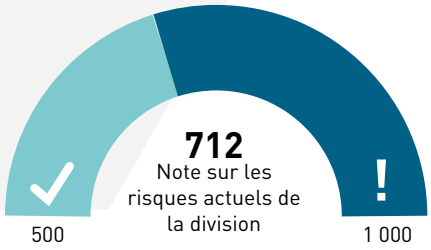


Illustration 2 - Mesures claires pour gérer les risques cybernétiques



Le présent bulletin a été rédigé par David Shipley, chef de la direction de Beauceron Security. Beauceron propose une plateforme en nuage abordable et sûre qui automatise de nombreuses tâches routinières destinées à éduquer les gens et à leur faire prendre conscience des risques cybernétiques, et qui amènent les employés, les gestionnaires et les hauts dirigeants à assumer leur responsabilité en matière de sécurité informatique. Pour obtenir de plus amples renseignements, consultez le site www.beauceronsecurity.com.

Victor propose une couverture contre les risques cybernétiques dans le cadre du produit autonome, Assurance contre les cyber-risques.

Visitez assurancevictor.ca pour en apprendre plus.