Bulletin consultatif sur la gestion de risques

ASSURANCE CONTRE LES CYBER-RISQUES

Une nouvelle perspective sur les risques cybernétiques

Trop souvent, lorsque nous réfléchissons à la cybersécurité et aux risques cybernétiques, nous ne pensons qu'à la technologie. Or, la vérité, c'est que seule la technologie ne suffit pas à nous protéger. Les connaissances des employés, les processus, la culture et la technologie sont autant de facteurs qui contribuent à construire une défense solide contre la perte de données et les conséquences financières inattendues qui en découlent.

Dans la majorité des cas, un incident de cybersécurité se produit parce qu'une personne aura été dupée par un courriel frauduleux ou parce qu'elle aura navigué sur le Web sur un appareil non sécurisé ou non protégé. La plupart de ces incidents peuvent être évités, à condition que les organisations adoptent une approche proactive.

Tout le monde est une cible

Les risques cybernétiques constituent un problème croissant et important pour les entreprises canadiennes de toute taille, qu'il s'agisse de grandes sociétés, de moyennes entreprises de plusieurs centaines d'employés ou encore d'entreprises comptant moins de 100 employés, et dans tous les domaines (de la fabrication, de la technologie, de la vente au détail, des services financiers, etc.)

La raison en est que la cybercriminalité est devenue un modèle d'affaires rentable pour les groupes du crime organisé du monde entier, et que les outils permettant d'orchestrer des crimes en ligne sont à la disposition de tous : ils ne coûtent pas cher et ils s'accompagnent de services de soutien complets.

Les chercheurs estiment que les conséquences économiques de la cybercriminalité passeront, à l'échelle mondiale, de 500 milliards de dollars en 2017 à plus de 2 billions de dollars d'ici la fin de 2021. Entre temps, les dépenses consacrées aux approches traditionnelles de cybersécurité devraient passer de 80 milliards de dollars à plus d'un billion de dollars au cours de la même période.[1]

Selon les experts, les entreprises de partout dans le monde dépenseront plus que jamais dans le domaine de la cybersécurité, tout en subissant des pertes encore plus lourdes aux mains de cybercriminels et d'autres fraudeurs.

Les dépenses liées à la cybersécurité dépasseront le billion de dollars en 20212. Pour régler un problème, l'argent ne suffira pas. Les dommages réglementaires et causés aux marques, ainsi que les conséquences financières inattendues des rançongiciels, des maliciels avancés et des attaques ciblées, autant de circonstances causées par un employé peu méfiant, montrent qu'il faut adopter un mode de gestion proactif et stratégique pour se protéger.

[1,2]CSO, juin 2017, en ligne : http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html (disponible en anglais seulement)

VICTOR

Que peuvent faire les organisations pour éviter les pertes?

S'il est important d'investir dans la technologie comme un antivirus ou un pare-feu, il faut aussi tâcher de créer une culture de sécurité pour réduire les risques de manière tangible.

- Sensibilisez vos employés aux risques cybernétiques.
- Informez régulièrement la haute direction et les conseils d'administration et discutez des risques cybernétiques.
- Consacrez le temps et l'argent nécessaires pour améliorer les politiques, les processus et la technologie.

Pour créer une culture de sécurité et réduire les risques cybernétiques, votre organisation devra prendre vraiment conscience du problème, puis revoir ses processus et ses politiques en conséquence. L'une des premières choses que vous devriez faire est de voir à ce que chaque employé possède les connaissances de base sur les risques cybernétiques, qu'il comprenne qu'il pourrait, par inadvertance, ouvrir la porte à un cybercriminel, et qu'il saisisse bien l'importance pour votre organisation de se protéger contre les attaques informatiques.

Par exemple, vous pourriez faire appel à un expert en cybersécurité ou à une société spécialisée pour faire créer et mettre en place un programme efficace de cybersécurité, mais une telle mesure peut être coûteuse. Une autre solution s'offre à vous : les technologies de sensibilisation à la sécurité. Elles servent à éduquer les employés en mettant les connaissances de ces derniers à l'épreuve lors de cours en ligne et d'attaques simulées. Elles permettent également de vérifier que les employés se préoccupent en permanence de la question et qu'ils se comportent en conséquence, et ce, en mobilisant très peu les équipes et les ressources technologiques.

Pourquoi une telle approche? Eh bien parce que les rapports de cyberattaques sont clairs : L'écrasante majorité des cyberattaques qui fonctionnent sont le fruit de l'ingénierie sociale (c'est-à-dire le hameçonnage ou autres arnaques électroniques) qui exploitent des personnes peu méfiantes – employés, entrepreneurs ou autres. Autrement dit, les cybercriminels savent qu'il est bien plus facile de manipuler les émotions humaines – la peur, l'avidité, le désir, la colère et la curiosité – que de pirater des systèmes informatiques.

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.