Incidence de la pandémie de maladie à coronavirus sur le cyberrisque

Les préoccupations au sujet de la propagation du nouveau coronavirus ont déclenché la plus importante mobilisation de « télétravailleurs » de l'histoire. Dans cette alerte cyberrisque, Aon décrit les mesures concrètes que les organisations peuvent mettre en place pour demeurer résilientes à travers la situation de crise.

La pandémie de maladie à coronavirus (COVID-19) a provoqué d'importantes perturbations dans le monde des affaires et une certaine panique au sein des employés touchés. Partout au Canada, des entreprises ont activé des plans d'urgence ou de continuité des affaires et ont donné à leurs employés l'autorisation ou l'ordre de travailler à domicile pour limiter la propagation du virus. Face à la nouvelle réalité où des millions de travailleurs se connectent à distance, la sécurité des réseaux informatiques et plus importante que jamais. Afin de demeurer opérationnelles et en sécurité, Aon recommande aux entreprises de suivre les étapes suivantes :

- **Se défendre contre la vague d'hameçonnage**

  Des individus malveillants tireront parti du fait que tous les efforts sont concentrés sur le nouveau coronavirus ainsi que de la peur et de la panique qu'il suscite. Des chercheurs en sécurité de l'information ont déjà pu observer la circulation de courriels d'hameçonnage simulant des alertes concernant la COVID-19.

  Ces courriels renferment généralement des pièces jointes contenant soi-disant de l'information sur la pandémie ou des recommandations à jour sur la façon dont les destinataires peuvent éviter l'infection. Dans un environnement où les gens sont anxieux et à l'affût du moindre renseignement touchant la COVID-19, les bonnes pratiques en matière de sécurité informatique sont oubliées.

  Le moment est bien choisi pour les organisations de rappeler à leur personnel l'importance de demeurer vigilant et les risques associés à l'ouverture de pièces jointes ou l'accès à des liens provenant de sources suspectes. La simulation d'une campagne d'hameçonnage peut aussi démontrer le niveau de résilience à ces attaques. Sur le plan technique, des antivirus à jour et des outils de surveillance des réseaux peuvent limiter l'efficacité des attaques par hameçonnage.

- **Tester l'état de préparation du système**

  Les organisations font face à une quantité sans précédent d'utilisateurs tentant d'accéder au réseau (trafic) à distance. Les entreprises dotées d'une main-d'œuvre agile se sont préparées à cette éventualité depuis un certain temps et seront bien outillées pour maintenir l'intégrité de leur réseau grâce à l'utilisation de réseaux privés virtuels (RPV) et de stratégies d'authentification multifactorielle. Il est recommandé aux équipes de sécurité informatique des entreprises d'intensifier la surveillance des activités provenant des employés en télétravail, sachant que les ordinateurs personnels de ces derniers sont un point faible que les individus malveillants exploiteront pour accéder aux ressources de l'entreprise.

  Pour ceux qui sont moins bien préparés, la COVID-19 présente un défi de taille. Il existe un risque que le volume accru de trafic sur le réseau mette à rude épreuve les systèmes et le personnel informatique, et que les employés accèdent à des données et à des systèmes sensibles en utilisant des réseaux ou des appareils non sécurisés. Nous recommandons à ces organisations de migrer le plus rapidement possible vers un système répondant aux normes du travail à distance et PAP « Prenez vos appareils personnels » (BYOD). Des correctifs doivent être régulièrement apportés aux VPN (par exemple, une vulnérabilité dans le VPN Pulse Secure a été corrigée en avril 2019, mais les entreprises qui n'ont pas effectué de mise à jour ont été la proie de rançongiciels en décembre), et la tolérance des réseaux à la charge des applications doit être testée pour s'assurer que l'augmentation du trafic peut être gérée.

- **Se préparer aux perturbations**

  Il peut être plus difficile pour le personnel des technologies de l'information (TI) de surveiller et de contenir les menaces à la sécurité du réseau avec main-d'œuvre connectée à distance. Dans les bureaux, lorsqu'une menace est détectée, le service des TI peut immédiatement mettre l'appareil en quarantaine en déconnectant le terminal (l'ordinateur compromis) du réseau de l'entreprise pendant qu'il enquête. Lorsque des utilisateurs travaillent à distance, les organisations doivent s'assurer, dans la mesure du possible, que les collègues des services informatiques et de sécurité sont facilement joignables et, idéalement, capables de se présenter en personne pour régler un problème à sa source. Un logiciel de détection et de réponse des terminaux (EDR) sophistiqué peut également être utilisé pour mettre en quarantaine les postes de travail à distance et limiter la possibilité que des individus malveillants s'introduisent dans le réseau.

Alors que le risque s'étend au-delà du département des TI, une approche en gestion du risque doit être adoptée à l'échelle de l'entreprise. Cette approche peut inclure un test des plans de continuité des affaires (PCA) et de la réponse de la haute direction à un cyberincident par le biais d'une simulation de crise axée sur différents scénarios, et sur les effets que les pandémies et autres événements perturbateurs similaires sont susceptibles d'avoir au niveau de l'automatisation, de la connectivité et de la cyberrésilience.

Les entreprises peuvent aussi se prémunir contre le risque accru de perturbations grâce à une assurance cyber robuste qui, en cas de perturbation numérique des systèmes, peut couvrir les pertes liées à l'interruption des affaires et les honoraires de spécialistes judiciaires pour enquêter sur une brèche de sécurité en vue d'y remédier.

La COVID-19 présente de nombreux défis pour les entreprises canadiennes mais les progrès technologiques réalisés depuis l'épidémie de SRAS permettront aux entreprises de demeurer opérationnelles et agiles face à l'incertitude. Il est cependant essentiel de garder un œil sur la menace cybernétique omniprésente dans le contexte de la crise actuelle, car la pérennité de nos entreprises en dépend.