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 toute l'histoire. Dans la présente alerte au risque, Aon décrit les mesures concrètes que les organisations peuvent prendre pour demeurer résilientes malgré 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 effectifs. Partout en Asie, des entreprises ont activé des plans d'urgence ou de continuité des activités et ont donné à des employés l'autorisation ou l'ordre de travailler à domicile pour limiter la propagation du virus. Face à une nouvelle réalité où des millions de gens travaillent à distance, il est maintenant plus important que jamais de disposer de réseaux sécurisés. Pour assurer la continuité des activités et la sécurité, Aon recommande aux entreprises de suivre les étapes suivantes :

- **Se prémunir 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 des systèmes d'information (SSI) 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 stressés et à l'affût du moindre renseignement, les bonnes pratiques en matière de sécurité informatique sont négligées.
  Le moment est bien choisi pour les organisations de rappeler à leur personnel l'importance de demeurer vigilant et les risques associés au fait d'ouvrir des pièces jointes ou d'accéder à des liens provenant de sources suspectes. La simulation d'une campagne de harponnage peut aussi démontrer le niveau de résilience à ces attaques. Sur le plan technique, des antivirus à jour et des outils de surveillance peuvent limiter l'efficacité des attaques par harponnage.
- **Tester l'état de préparation du système**
  Les organisations feront face à une quantité sans précédent d'utilisateurs tentant d'accéder au réseau (trafic réseau) 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 multifacteur.
  Il est recommandé aux équipes de SSI des entreprises d'intensifier la surveillance des activités en provenance des télétravailleurs, sachant que les ordinateurs personnels de ces employés 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 informatiques, 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 « Prenez vos appareils personnels » (Bring your own devices ou BYOD). Des correctifs doivent être régulièrement apportés aux RPV (par exemple, une vulnérabilité dans le RPV 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 d'une main-d'œuvre éloignée. Dans les bureaux, lorsqu'une menace est détectée, le service informatique 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) perfectionné peut également être utilisé pour mettre en quarantaine les postes de travail à distance et limiter ainsi la possibilité que des individus malveillants s'introduisent dans le réseau. Ce risque s'étendant au-delà du risque technique, une approche de la gestion du risque doit être adoptée à l'échelle de l'entreprise. Cette approche peut inclure des essais des plans de continuité des activités (PCA) et de la réponse de la haute direction au moyen de simulations de crise sur maquette axées sur des cyberscénarios et sur les effets que les pandémies et autres événements perturbateurs similaires sont susceptibles d'exercer sur l'automatisation, la connectivité et la cyberrésilience.
  Les entreprises peuvent aussi se prémunir contre le risque accru de perturbations grâce à une cyberassurance solide qui, en cas de perturbations numériques des systèmes, peut couvrir les pertes liées à l'interruption des activités et les honoraires de spécialistes judiciaires pour enquêter sur une faille en vue d'y remédier.

La COVID-19 soulève de nombreux défis pour les entreprises qui exercent leurs activités en Asie, mais les progrès technologiques réalisés depuis l'épidémie de SRAS permettent aux entreprises de demeurer opérationnelles et souples face à l'incertitude. Il est essentiel de garder un œil sur la menace cybernétique omniprésente dans le contexte de la crise actuelle; il en va de la réussite à long terme des entreprises.