Près des trois quarts des entreprises canadiennes pensent qu'elles seront victimes d'une intrusion en 2022

Le travail à distance, les applications tierces et les appareils mobiles constituent le principal risque de cybercriminalité pour les entreprises

TORONTO, le 18 avril 2022 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), leader mondial de la cybersécurité, a annoncé aujourd'hui les résultats de son plus récent indice mondial du cyberrisque (en anglais, *Cyber Risk Index* ou CRI) pour le second semestre 2021. Ce dernier se situe à l'échelle mondiale à -0,04, ce qui représente un niveau de risque élevé, en comparaison avec l'Amérique du Nord qui se situe à -0,01. Le Canada a obtenu un résultat de 0,16, ce qui signifie que le pays présente un niveau de cyberrisque modéré par rapport aux organisations mondiales et nord-américaines (NA). L'étude a également révélé que le Canada est mieux préparé que l'ensemble de l'Amérique du Nord à gérer les cyberrisques (avec un pointage de 5,41 contre 5,35 en Amérique du Nord). Toutefois, les réponses ont permis de constater que près des trois quarts (74 %) des entreprises canadiennes pensent être victimes d'une intrusion au cours des 12 prochains mois, et 30 % d'entre elles affirmant qu'il est « très probable » que cela se produise.

Classement de l'indice de cyberrisque	
Échelle	**Interprétation**
5,01 à 10	Risque faible
0,1 à 5,0	Risque modéré
0 à -5,0	Risque élevé
-5,01 à -10	Haut risque

Classement de l'indice de cyberpréparation	
Échelle	**Interprétation**
7,51 à 10	Risque faible
5,01 à 7,50	Risque modéré
2,51 à 5,0	Risque élevé
0 à 2,5	Haut risque

« Les entreprises naviguent constamment dans un paysage de sécurité en constante évolution, et il est essentiel de comprendre ce qui rend leurs activités vulnérables », a déclaré Greg Young, vice-président de la cybersécurité chez Trend Micro Canada. « C'est là que des rapports tels que le CRI peuvent constituer une ressource importante puisqu'ils mettent en évidence les domaines potentiellement préoccupants afin d'aider les entreprises à élaborer une stratégie efficace en matière de cybersécurité. »

Le rapport semestriel du CRI pose des questions précises visant à mesurer l'écart entre la préparation des personnes interrogées aux attaques et leur probabilité d'être attaquées*. Au Canada, 83 % des entreprises ont affirmé avoir été victimes d'une ou plusieurs cyberattaques réussies au cours des 12 derniers mois, et 32 % ont déclaré en avoir subi sept ou plus.

Les rançongiciels, l'hameçonnage/ingénierie sociale, le déni de service (DoS) et les réseaux de zombies figurent en tête de liste des principales préoccupations. Les conséquences négatives d'une intrusion comprennent le vol ou l'endommagement d'équipements, la perte de revenus et les coûts des consultants/experts externes.

Sur le plan de l'infrastructure informatique, les entreprises canadiennes sont les plus préoccupées par les risques de sécurité liés aux employés mobiles ou à distance (note de 7,55/10), aux applications tierces (note de 7,25/10) et aux appareils mobiles/téléphones intelligents (6,55/10).

Si les investissements numériques ont été nécessaires pour soutenir le travail à distance et améliorer l'efficacité de l'entreprise pendant la pandémie, ce rapport met en lumière la multiplication des points de contact des entreprises et les défis permanents auxquels elles sont confrontées pour obtenir de tels investissements.

« Les entreprises sont confrontées chaque jour à des défis de sécurité complexes, qu'il s'agisse de vulnérabilités logicielles, de

« Les entreprises sont confrontées chaque jour à des défis de sécurité complexes, qu'il s'agisse de vulnérabilités logicielles, de fuites de données, d'attaques par rançongiciels ou autres », a déclaré le Dr Larry Ponemon, fondateur et président du Ponemon Institute. « L'enquête semestrielle représente un atout considérable pour évaluer l'évolution rapide du paysage du cyberrisque. Il permet d'aider les organisations à renforcer leur préparation en matière de sécurité et sert de guide pour la planification stratégique. »

Au Canada, les niveaux de risque les plus élevés étaient liés aux déclarations suivantes :

- Le service de sécurité informatique de mon entreprise veille à ce que les infractions aux politiques de sécurité, aux directives opérationnelles standard et aux exigences externes soient strictement sanctionnées.
- Le service de sécurité informatique de mon entreprise soutient la sécurité dans l'environnement DevOps.
- Mon entreprise réalise des investissements appropriés dans des technologies de sécurité de pointe telles que l'apprentissage automatique, l'automatisation, l'orchestration, l'analyse et/ou les outils d'intelligence artificielle.
- Le service de sécurité informatique de mon entreprise respecte les exigences en matière de protection des données et de confidentialité.
- Le responsable de la sécurité informatique de mon entreprise (CISO) dispose d'une autorité et de ressources suffisantes pour assurer un niveau de sécurité élevé.

Cela démontre clairement que davantage de ressources doivent être consacrées aux personnes, aux processus et aux technologies afin d'améliorer la prévention et de réduire les niveaux de risque globaux.

À l'heure où les entreprises et les équipes de sécurité s'efforcent de gérer la complexité croissante introduite par la transformation numérique, la confidentialité des données, la conformité, et autres, il devient essentiel d'adopter une approche basée sur une plateforme.

* Un pointage est calculé à partir de ces informations sur une échelle numérique de -10 à 10, où -10 représente le niveau de risque le plus élevé. Dans ce rapport, le pointage du Canada se situe à 0,16 contre -0,01 pour l'Amérique du Nord et -0,04 pour le monde, ce qui indique un niveau de risque modéré.

À propos de Trend Micro
Trend Micro, leader mondial en matière de cybersécurité, contribue à sécuriser les échanges d'informations numériques à travers le monde. S'appuyant sur des décennies d'expertise en matière de sécurité, de recherche sur les menaces et d'innovation continue, Trend Micro protège des centaines de milliers d'entreprises et des millions d'individus grâce à des solutions de sécurité connectées pour les environnements Cloud, les points de terminaison, les appareils et les réseaux. En tant que leader de la cybersécurité dans le nuage et en entreprise, la plateforme offre une vaste gamme de techniques de défense contre les menaces avancées, optimisées pour des environnements tels que AWS, Microsoft et Google, ainsi qu'une visibilité centrale pour une détection et une réponse qui sont à la fois meilleures et plus rapides. Avec plus de 7 000 employés dans 65 pays, Trend Micro permet aux entreprises de simplifier et sécuriser leur monde connecté www.TrendMicro.com.

---

https://newsroom.trendmicro.ca/2022-04-14-Pres-des-trois-quarts-des-entreprises-canadiennes-pensent-quelles-seront-victimes-dune-intrusion-en-2022