

Plus de la moitié des entreprises canadiennes se sentent plutôt exposées aux cyberrisques tels que l'hameçonnage, les rançongiciels et les attaques de produits IdO

Une étude de Trend Micro révèle une complexité accrue et une confiance réduite

TORONTO, le 4 août 2022 – Une nouvelle étude de la firme mondiale de cybersécurité Trend Micro a révélé que 58 % des entreprises canadiennes estiment qu'elles sont actuellement exposées à un risque de niveau modéré. Toutefois, plus de la moitié (53 %) estiment que leur entreprise est exposée à des menaces de cyberrisque telles que l'hameçonnage (59 %), les attaques par rançongiciels (55 %), la chaîne d'approvisionnement (55 %) et les attaques de produits IdO/Internet des objets (52 %). Les personnes interrogées ont également indiqué que des grappes technologiques trop complexes et un manque d'implication des dirigeants ne font qu'exacerber les problèmes.

En moyenne, les entreprises canadiennes estiment avoir un taux de visibilité de 57 % de leur surface d'attaque totale, et plus d'un quart des répondants évaluent encore leur surface d'attaque en cartographiant leurs systèmes manuellement (27 %). Cela peut expliquer pourquoi seulement environ 37 % d'entre elles sont en mesure de détailler complètement et précisément l'un ou l'autre des éléments suivants en fonction des évaluations des risques :

- Les niveaux de risque pour les actifs individuels
- La fréquence des tentatives d'attaque
- Les tendances en matière de tentatives d'attaque
- Les conséquences d'une intrusion dans un périmètre donné
- Les références de l'industrie
- Des plans d'action préventifs pour des vulnérabilités précises

« En plus de s'inquiéter face à l'expansion rapide de la surface d'attaque numérique avec une visibilité limitée, les entreprises se questionnent sur la meilleure façon de découvrir et gérer les cyberrisques dans un environnement de menaces en constante évolution. En mettant en œuvre une approche fondée sur un modèle de plateforme unique, les entreprises seront en mesure d'améliorer la visibilité, de réduire les coûts et d'identifier les brèches plus rapidement », affirme **Greg Young, vice-président chargé de la cybersécurité chez Trend Micro**

Environ 43 % des décideurs informatiques et des cadres d'entreprise interrogés par Trend Micro déclarent que le fait de se tenir au courant de l'évolution constante de la surface d'attaque est le principal problème auquel ils sont confrontés. En outre, près de la moitié (44 %) considèrent l'hameçonnage ou les attaques par courriel comme le principal moyen de déclencher une cyberattaque contre leur entreprise.

Le fait que les entreprises ne soient pas en mesure d'évaluer avec précision le risque lié à la surface d'attaque maintient également les dirigeants d'entreprise dans l'ignorance. Selon Trend Micro, 11 % des entreprises canadiennes n'ont pas de méthode bien définie pour évaluer l'exposition au risque de leur surface d'attaque numérique, et 69 % des répondants pensent que la haute direction devrait jouer un rôle plus actif dans la promotion de bonnes pratiques de cybersécurité. Un quart (24 %) des personnes interrogées pensent que l'augmentation de la formation ou de l'éducation en matière de cybersécurité aurait le plus grand impact sur la capacité des dirigeants à mieux comprendre les cyberrisques.

Il y a là une occasion évidente pour les entreprises de tirer parti de l'expertise d'un tiers.

Seulement un tiers (36 %) des répondants canadiens ont déjà investi dans une approche de gestion de la surface d'attaque centrée sur une plateforme, tandis que près de la moitié (47 %) des répondants disent qu'ils aimeraient en faire autant. Parmi ceux qui ont déjà fait ce choix, l'amélioration de la visibilité (42 %), la réduction des coûts (40 %) et la détection plus rapide des brèches (35 %) constituent les avantages les plus cités.

Parmi celles qui ne prévoient pas de passer à un modèle de plateforme unique, 37 % des entreprises canadiennes considèrent le temps nécessaire à la transition comme le principal obstacle à l'utilisation d'un tel modèle.

Pour réaliser cette étude, Trend Micro a chargé Satio Research d'interroger 6297 décideurs informatiques et d'entreprise dans 29 pays.

Pour plus d'informations sur les études de Trend Micro portant sur les risques au niveau mondial, cliquez ici :
https://www.trendmicro.com/explore/trend_global_risk_research_2

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 cloud 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/2022-08-04-Plus-de-la-moitie-des-entreprises-canadiennes-se-sentent-plutot-exposees-aux-cyberrisques-tels-que-lhameconnage.-les-rancongiciels-et-les-attaques-de-produits-IdO>