L'engagement de la haute direction doit être renforcé en 2022 pour atténuer les cyberrisques

Une étude Trend Micro révèle une inquiétude généralisée concernant la menace que représentent les rançongiciels

TORONTO, le 2 février 2022 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), leader mondial de la sécurité infonuagique, a publié une nouvelle étude* qui révèle que le manque persistant d'engagement des services informatiques et de la direction peut mettre en péril les investissements et exposer les organisations à un risque accru de cybercriminalité. Au Canada, 93 % des décideurs informatiques et commerciaux interrogés se disent particulièrement préoccupés par les attaques de type rançongiciels.

Pour lire une copie complète du rapport mondial, veuillez visiter le site (en anglais) : https://www.trendmicro.com/explore/en_gb_trendmicro-global-risk-study

Malgré l'inquiétude généralisée suscitée par la montée en flèche des menaces, l'étude révèle que seulement deux équipes TI sur cinq (42 %) discutent des cyberrisques avec la haute direction au moins une fois par semaine.

« Les entreprises de toutes tailles doivent prioriser une communication ouverte, claire et cohérente avec leurs équipes TI, surtout que les organisations doivent continuer à s'adapter à une main-d'œuvre mobile », affirme **Antoine Saikaley, directeur technique chez Trend Micro Canada**. « Bien que les dirigeants comprennent le besoin de transparence et d'être informés, ils se sentent souvent dépassés par l'évolution rapide de l'environnement de la cybersécurité. Par conséquent, il est plus important que jamais pour les équipes TI de communiquer efficacement, en mettant en évidence le potentiel de risque de l'organisation et la meilleure façon de le gérer. »

Heureusement, l'investissement actuel dans les initiatives en matière de cybersécurité n'est pas dangereusement bas. Près de la moitié (46 %) des répondants affirment que leur organisation consacre la majeure partie de ses dépenses aux « cyber-attaques » afin d'atténuer les risques opérationnels. Il s'agit de la réponse la plus populaire, devançant des projets plus typiques comme la transformation numérique (40 %) et la restructuration des effectifs (32 %). En outre, près de la moitié (44 %) ont déclaré avoir récemment augmenté leurs investissements pour atténuer les risques d'attaques par rançongiciels et de violations de la sécurité.

Or, le faible engagement de la haute direction, combiné à l'augmentation des investissements, suggère une tendance à simplement « jeter de l'argent » pour régler le problème plutôt que de comprendre les défis de la cybersécurité et d'investir de manière appropriée. Cette approche pourrait nuire à des stratégies plus efficaces et entraîner des pertes financières plus importantes. Un répondant sur deux (50 %) a déclaré que les cybermenaces étaient un problème informatique, tandis que 34 % seulement ont estimé qu'il s'agissait d'un risque d'affaires. Moins de la moitié (40 %) des personnes interrogées ont affirmé que des concepts tels que « le cyberrisque » et « la gestion du cyberrisque » étaient largement connus dans leur organisation. Plus troublant encore, 8 % des personnes interrogées ont déclaré que leur entreprise n'évaluait pas du tout les cyberrisques.

Les trois quarts des répondants canadiens (75 %) aimeraient qu'un plus grand nombre de personnes au sein de l'organisation soient responsables de la gestion et de l'atténuation de ces risques, ce qui contribuerait à instaurer une culture de « sécurité dès la conception » à l'échelle de l'entreprise. Parmi les autres rôles ne relevant pas des TI, les répondants ont cité les directeurs financiers (26 %) et les directeurs marketing (14 %).

Cette étude succède à de précédentes recherches de Trend Micro qui ont révélé une déconnexion inquiétante en matière de cybersécurité entre les dirigeants d'entreprise et les responsables informatiques, phénomène perpétué par l'autocensure des experts en cybersécurité et les désaccords sur la responsabilité finale.

**Trend Micro a mandaté Sapio Research pour interroger 5321 décideurs informatiques et commerciaux d'entreprises de plus de 250 employés dans 26 pays.*

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/2022-02-02-Lengagement-de-la-haute-direction-doit-etre-renforce-en-2022-pour-attenuer-les-cyberrisques