

Cybercriminalité : un coût élevé pour l'économie mondiale

L'éditeur de solutions McAfee a publié, en partenariat avec le CSIS (Center of Strategic and International Studies)*, son [rapport](#) 2020 sur le coût de la cybercriminalité**.

« La gravité et la fréquence des cyberattaques contre les entreprises continuent d'augmenter à mesure que les techniques évoluent et que le travail à distance s'impose », a déclaré Steve Grobman, vice-président et CTO de McAfee. « L'industrie et les [gouvernements](#) sont conscients des enjeux financiers et de sécurité intérieure. Toutefois les temps d'arrêt imprévus, la baisse de productivité et les investigations sur les intrusions représentent des coûts moins visibles, or ils sont conséquents ».

Selon ce rapport, la cybercriminalité coûte dorénavant à l'économie mondiale 1 000 milliards de dollars (soit 1 trillion \$). Ce montant inclut 945 milliards \$ de pertes financières auxquelles viennent s'ajouter 145 milliards \$ de dépenses de cybersécurité.

Ainsi, le coût de la cybercriminalité a augmenté de plus de 50% en deux ans. Il représente 1% du PIB mondial environ. Par ailleurs, le coût moyen a dépassé les 500 000 dollars par incident majeur et la durée moyenne d'interruption des opérations est de 18 heures.

Espionnage et ransomware

Sans grande surprise, les formes de cybercriminalité les plus coûteuses pour les entreprises qui en sont la cible sont « l'espionnage économique, le vol de propriété intellectuelle, la criminalité financière et, de plus en plus, les [ransomwares](#) ».

Les cyberattaques ciblant des organisations de plus petite taille et des particuliers n'entraînent « généralement pas » de pertes financières majeures, mais elles peuvent impacter « des milliers d'individus », ont souligné les auteurs du rapport.

Une cyberattaque peut également impacter la productivité des équipes, la réputation et la marque employeur. Or, 56% des organisations concernées par l'enquête ne disposent pas encore d'un plan couvrant à la fois la prévention et la réponse à incident.

Parmi les 44% (26% en France) qui disposent effectivement d'un plan d'intervention global, 32% « seulement » considèrent que ce plan est efficace.

* Le CSIS est un groupe de réflexion et d'influence basé à Washington D.C.

** 1500 décideurs IT et Métiers d'entreprises de 1000 collaborateurs et plus ont été interrogés entre avril et juin 2020 par Vanson Bourne pour McAfee. États-Unis, Canada, Royaume-Uni, France, Allemagne, Japon et Australie sont concernés.