Sécurité IT : la France affronte des « cyberattaques pros », selon PwC

Les **cyber-attaques** s'amplifient et elles coûtent de plus en plus chères aux entreprises françaises.

Selon l'étude mondiale « **The Global State of Information Security Survey 2018** » du cabinet de conseil **PwC** qui vient de sortir, les pertes financières liées aux cyber-assauts ont augmenté de 50% sur un an. Comptez 2,25 millions d'euros en moyenne sur douze mois.

Les entreprises françaises prennent des mesures pour endiguer ce fléau. Mais est-ce suffisant ? En un an, elles déclarent avoir consenti un investissement moyen de 4,3 millions d'euros dans la sécurité de leurs systèmes d'information. Ce qui correspond à une hausse de 10,2% par rapport à 2016 (à taux de change constant).

Un volume de 4550 incidents ont été repérés en un an, soit une hausse de 9% par rapport à l'année dernière.

70% des entreprises françaises interrogées affirment avoir défini ou être en cours de définition d'une stratégie globale en matière de sécurité et d'information (contre 67% des entreprises du panel monde).

Quelles sont les conséquences principales de ses cyberassauts en France ? L'interruption des opérations et la mise en danger de données sensibles sont évoquées en premier (36% des répondants), puis vient les menaces portant sur la qualité des produits (32%) et un risque pour la vie humaine (25%).

Comparons par rapport à la situation internationale (en raisonnant toujours en impact moyen) : les entreprises ayant répondu à l'étude ont consacré 4,4 millions d'euros dans la protection contre la cybercriminalité. 3458 attaques ont été détectées. Le montant des pertes financières est estimé à 1,7 million d'euros.

En constatant des attaques plus ciblées et mieux préparées, Philippe Trouchaud, associé responsable du département cybersécurité de PwC, évoque « une réelle professionnalisation des hackers » aux motivations essentiellement mercantiles.

Des lacunes sur la sensibilisation à la sécurité IT

Mais il reste du chemin à parcourir sur la sensibilisation et la vigilance accrue. « La transformation numérique ne se fera pas sans confiance », aime rappeler Guillaume Poupard, Directeur général de l'ANSSI (agence nationale de la sécurité informatique). « La sécurité du numérique est maintenant un gage pour les entreprises et les citoyens. »

L'étude PWC confirme que la pédagogie reste de mise. Trois entreprises françaises sur quatre affirment avoir défini une stratégie de surveillance et de gestion des cyberattaques mais une entreprise sur deux en France n'a pas de programme de formation et sensibilisation à la sécurité

pour ses collaborateurs.

« Il faut garder à l'esprit que, même avec ce type de sensibilisation, le risque résiduel reste important car près de 30 % des personnes ayant reçu un phishing ciblé ouvre quand même la pièce jointe malveillante », évoque Philippe Baumgart, associé expert en cybersécurité chez PwC, également cité dans le communiqué.

Le cabinet de conseil dresse aussi un bilan d'étape de l'application du Règlement Général européen sur la Protection des Données (GDPR en anglais), qui entrera en vigueur à l'échéance de mai 2018 et qui s'ancre dans une « logique de protection des données unifiée » dans toute l'Europe.

Plus d'une entreprise sur dix dans le monde (14%) déclarent encore n'avoir engagé aucune démarche de mise en conformité à ce nouveau règlement.

Mais les entreprises françaises semblent plus aguerries : seule une proportion de 9% d'entre elles déclarent ne pas avoir encore entrepris de changement dans leur processus. Mais on aura l'occasion d'en reparler dans les prochains mois…

L'étude PwC a été réalisée par Internet auprès de 9500 dirigeants et responsables informatiques (CEO, CFO, CIO, RSSI, OSC, vice-présidents et directeurs de l'information et des pratiques de sécurité) dans 122 pays. 29% des répondants proviennent de l"Europe.

(Crédit photo : Pixabay)