Cybersécurité : comment les cyberattaques impactent l'activité des entreprises

Le Cesin (Club des experts de la sécurité de l'information et du numérique) publie la 4e édition de son baromètre de la cybersécurité des entreprises en France. 174 membres, dont 84% de RSSI de grandes sociétés et administrations, ont été interrogés.

Selon le sondage OpinionWay pour le Cesin, 80% des organisations ont été la cible d'une ou plusieurs cyberattaques au cours des douze derniers mois. Malgré ce taux élevé, le nombre d'attaques est resté stable par rapport à l'an dernier pour une majorité (53%).

En revanche, la proportion d'entreprises déclarant un impact négatif sur leur activité a augmenté de 10 points à 59%. Le ralentissement de la production (pour 26% des organisations visées) et l'indisponibilité temporaire d'un site web (23%) sont les effets des cyberattaques sur « le business » les plus souvent cités.

Les retards de livraison (12%), la perte de chiffre d'affaires (11%) et l'arrêt de la prodution « pendant une période significative » (9%) arrivent ensuite.

Harponnage et ingénierie sociale

Les entreprises visées ont été la cible de cinq types différents d'attaques en moyenne en douze mois. Le phishing (hameçonnage) ou spear phishing (harponnage) est le type d'attaque le plus souvent constaté (73%). Les cyber-escrocs utilisent donc encore largement l'email ou tout site web contrefait pour obtenir et détourner des données personnelles à l'insu d'individus et de corporations.

Les escrocs peuvent également cibler spécifiquement des personnes dans l'entreprise et se faire passer pour un dirigeant afin d'obtenir un virement bancaire. Cette « arnaque au président » est citée par 50% du panel.

Elle devance ainsi les attaques par logiciels malveillants (malwares) et rançongiciels (ransomwares) (44% des reponses respectivement). Suivent les techniques d'ingénierie sociale utilisées pour tromper le chaland (40%).

Cloud, IA, IoT

Le partage accidentel ou intentionnel de données sensibles n'est pas le seul gros risque à gérer pour les RSSI. Le Shadow IT l'est aussi. Ainsi, les professionnels de la sécurité des systèmes d'information s'inquiètent également de la diffusion de services cloud hors contrôle de l'IT et de l'utilisation d'applications non approuvées (64%).

En outre, 80% des RSSI estiment que la sécurisation des données stockées dans le cloud requiert des solutions spécifiques en plus des outils fournis par des prestataires. Ils s'intéressent aussi aux

solutions de protection ou de détection basées sur l'intelligence artificielle (IA).

56% déclarent que de telles solutions sont déjà déployées et en production. 33% envisagent de le faire. Toutefois, lorsqu'il est question de décision et de remédiation, 55% des répondants estiment que l'IA ne doit pas décider à la place de l'humain.

Les RSSI qui redoutent de nouvelles failles liées à l'Internet des objets (IoT) en entreprise, veulent donc garder le contrôle.

5% du budget IT

Qu'en est-il des budgets alloués pour gérer le risque ? Dans 59% des entreprises interrogées, la sécurité représente moins de 5% du budget IT.

Toutefois, près de 6 organisations sur 10 prévoient d'augmenter les budgets alloués à la protection des cyber risques dans les mois à venir. Par ailleurs, 84% des entreprises souhaitent acquérir de nouvelles solutions techniques (84%) dans ce domaine.

Enfin, une entreprise sur deux envisage d'augmenter les effectifs dédiés. Mais la pénurie de profils en sécurité freine les recrutements pour 91% des répondants.

(crédit photo : Ecole polytechnique / Paris / France on Visual hunt / CC BY-SA)