Cybersécurité : comment les entreprises françaises gèrent le risque

Le Cesin (Club des experts de la sécurité de l'information et du numérique) a livré la 5e édition de son baromètre de la cybersécurité en France. L'enquête a été menée auprès de 253 des 634 membres de l'organisation présidée par Mylène Jarossay, RSSI* du groupe LVMH.

Selon le **sondage OpinionWay pour le Cesin, le taux de sociétés qui déclarent avoir été la cible de cyberattaques dans les douze derniers mois a baissé de 15 points en un an. Elles étaient 80% à le signaler en janvier 2019, contre 65% début janvier 2020.

En revanche, la proportion d'entreprises qui soulignent un impact négatif sur leur activité a peu évolué (57% cette année, contre 59% l'an dernier). Pour les firmes touchées, le ralentissement de la production est l'impact des cyberattaques sur « le business » le plus souvent cité (27%). L'indisponibilité d'un site web visible par les clients arrive ensuite (17%), devant la perte de chiffre d'affaires (9%) et les retards de livraison (8%), entre autres soucis.

Au-delà du phishing…

Les entreprises visées ont été la cible de 4 types d'attaques cyber en moyenne en douze mois (contre 5 l'an dernier). Le phishing (hameçonnage) est à nouveau le type d'attaque le plus souvent constaté (79%). Il devance « l'arnaque au président » (47% la mentionnent), l'exploitation à des fins lucratives d'une vulnérabilité (43%) et les tentatives frauduleuses de connexion (40%).

Les conséquences les plus fréquentes de ces attaques étant : l'usurpation d'identité (exprimée par 35% des organisations concernées), l'infection par malware (34%), le vol de données personnelles (26%), le blocage par ransomware (rançongiciel) (25%) et le déni de service (DoS) (19%).

Outre la menace externe, le partage de données sensibles par des initiés ou des employés « négligents » est un risque à ne pas sous-estimer. Or, le déploiement et l'usage d'applications et services hors du contrôle des équipes informatiques (le Shadow IT) sont largement répandus (pour 98% des répondants).

Face à l'extension de la surface d'attaque

Avec ou sans le contrôle de l'IT, l'usage du cloud progresse dans les entreprises. Ainsi 89% des répondants déclarent que leur société utilise le cloud pour stocker des données. 55% dans le cloud public, 42% dans le cloud hybride (public et privé).

La migration de données dans le cloud n'est pas sans risques. Les RSSI redoutent en priorité la non maîtrise de la chaîne de sous-traitance de l'hébergeur (citée par 50% de l'échantillon), la difficulté de mener des audits (46%) et, enfin, l'utilisation à risque du cloud par les salariés (46%).

En réaction, 91% des répondants (contre 80% l'an dernier) estiment que des solutions spécifiques

doivent être déployées en plus des outils de fournisseurs cloud pour sécuriser l'ensemble. Avec ou sans intelligence artificielle (IA). 15% seulement déclarant que la présence d'IA est un critère « déterminant » dans le choix de solutions. Pourtant, 47% disent être prêts à laisser une IA prendre des décisions en matière de détection et/ou remédiation.

Quels types de solutions sont utilisées ?

S'équiper en solutions techniques

Pour faire face, les organisations utilisent en priorité, outre les antivirus et les firewalls, les passerelles de sécurité mail, les VPN, le filtrage d'URL (tous trois cités par 85% des répondants) et l'authentification multi-facteurs (+13 points à 72%).

L'usage d'autres outils et approches de la sécurité (SSO, SIEM, IAM, chiffrement…) arrivent ensuite. L'usage de solutions de détection des menaces et d'intervention pour les terminaux (EDR ou Endpoint detection and response) progresse aussi (+14 points à 34%).

Quant à l'approche zero trust (ou la confiance zéro en matière de sécurité informatique), elle fait une entrée discrète dans le baromètre du Cesin. Ainsi, 16% déclarent avoir initié (11%) ou pleinement engagé (5%) le processus. 30% envisagent de le faire.

S'assurer contre le risque cyber

Davantage sensibilisées au cyber-risque, 91% des organisations (contre 79% l'an dernier) ont mis en place ou envisagent de le faire un programme de cyber-résilience. De surcroît, 60% (+10 points) ont souscrit une cyber-assurance et 13% sont en cours de souscription.

Malgré tout, une entreprise sur deux s'inquiète de sa capacité à faire face aux cyber-risques. Aussi, 61% des répondants estiment que leur entreprise n'est plutôt pas (47%) ou pas du tout préparée (14%) à gérer une cyber-attaque d'ampleur.

Pour mieux gérer le risque, les organisations sont prêtes à investir.

Investir et recruter (un peu)

Dans 79% des entreprises interrogées, la sécurité représente entre moins de 5% (pour 50% des organisations) et de 5% à 10% (pour 29% des répondants) du budget IT.

Au cours des douze prochains mois, 62% des organisations prévoient d'augmenter la part du budget consacré à la sécurité informatique. Elles sont plus nombreuses encore (83%) à anticiper l'achat de nouvelles solutions techniques de protection.

En revanche, seule une firme sur deux (51%) prévoit d'augmenter les effectifs dédiés à la sécurité de systèmes d'information (SSI). Lorqu'il est question de recrutement, 9 sur 10 parlent d'une pénurie de profils qualifiés et de difficultés de recrutement.

*Responsable de la sécurité des systèmes d'information ou RSSI (en anglais, Chief security information officer ou CISO).

**L'enquête a été menée par OpinionWay pour le Cesin entre le 2 décembre 2019 et le 7 janvier 2020.

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