Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

5ème édition du baromètre annuel du CESIN
Analyse exclusive de la cybersécurité des grandes entreprises françaises

Le Club des Experts de la Sécurité de l'Information et du Numérique
dévoile les résultats de sa cinquième grande enquête OpinionWay pour le CESIN.

Paris, le 24 janvier 2020 – Afin de mieux cerner l'état de l'art et la perception de la cybersécurité et de ses enjeux au sein des grandes entreprises françaises, le CESIN publie chaque année depuis 2015, son baromètre annuel avec OpinionWay. L'association dévoile aujourd'hui les résultats de cette enquête indépendante et exclusive menée auprès de ses membres, Responsables Sécurité des Systèmes d'Information (RSSI) des grands groupes français.

Le sondage OpinionWay pour le CESIN a ciblé 634 membres de l'association, les résultats de l'étude portent sur un échantillon de 253 répondants. Ils mettent à jour la perception et la réalité concrète de la cybersécurité, avec une évolution des données sur l'impact de la transformation numérique des entreprises.

Cette année le Phishing reste le vecteur d'attaque le plus fréquent, 79% des entreprises en ont été victimes, l'arnaque au Président touche encore 47% d'entre elles, suivi par l'exploitation des vulnérabilités (43%) ou l'ingénierie sociale (35%).

Ces attaques ont pour conséquences principales l'usurpation d'identité (35%), l'infection par un malware (34%), le vol de données personnelles (26%) et l'infection par ransomware (25%).

La prise de conscience des risques entraîne la cyber-résilience et conforte le recours encore plus marqué à la cyber-assurance

91% des entreprises mettent en place un programme de cyber-résilience ou envisagent de le faire. Une tendance forte qui se confirme avec 12 points de plus que l'an passé. En parallèle, 60% des entreprises ont souscrit à une cyber-assurance et 13% sont en cours de souscription, une hausse constante ces trois dernières années ce qui renforce cette perception de prise de conscience des cyber-risques.

Le taux d'entreprises déclarant des cyber-attaques est en baisse 65%, contre 80% en 2019. *(nb : écart de résultat nuancé par l'ajout de la définition de Cyber-attaque pour l'enquête 2020 [1])*

1 Cyber-attaque - Définition donnée pour cette vague 5 : « La cyber-attaque est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information entrainant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise. »

En revanche **57% d'entre elles constatent des conséquences importantes sur le business.** Ces dernières se traduisent principalement par un impact direct sur la production, 9% indiquent une perte du chiffre d'affaires.

Parmi les outils de protection mis en place dans les entreprises, l'enquête révèle une hausse notable des solutions d'authentification multi-facteurs (72%), soit une augmentation de 13 points, et des EDR (34%) avec 14 points de plus qu'en 2019. Concernant **l'approche Zero Trust qui fait son entrée dans le baromètre, avec une défiance non-négligeable, bien que 30 % déclarent étudier la manière dont le modèle va se traduire, 16 % sont réellement engagés ou commence à mettre en œuvre ce concept.** Les offres innovantes issues de start-up sont adoptées par 42% du panel, pour les 58% qui n'y recourent pas le manque de maturité et la pérennité sont en question.

Cloud, IoT et IA : des risques accrus avec la transformation numérique

Le recours massif au cloud, utilisé par 89% des entreprises, dont 55% stockent une partie de leurs données dans des clouds publics, est noté parmi les risques les plus élevés. En tête la non-maîtrise de la chaîne de sous-traitance de l'hébergeur (50%), la difficulté de mener des audits (46%), et la non-maîtrise de l'utilisation du cloud par les salariés (46%). Pour pallier ce manque de sécurité, **91% des entreprises estiment que des outils et/ou dispositifs spécifiques doivent être mis en place.**

Les objets connectés font apparaître de nouvelles typologies de menaces dues à l'absence de chiffrement pouvant porter atteinte à la confidentialité des données, ou l'absence d'authentification avec des accès non protégés... Selon les RSSI les défis majeurs à relever en ce qui concerne l'IoT sont les failles de sécurité présentes dans ces équipement (43%) et le flou dans l'appréciation des risques potentiels (28%).

L'IA reste une technologie embarquée surtout dans les outils de supervision (SIEM), l'acquisition volontaire de solutions utilisant l'IA reste cantonnée à un faible nombre d'entreprises, le frein principal étant le faible niveau de confiance accordé (47%).

Quid de la sensibilisation des salariés ?

Près de la moitié des entreprises (43%) indique que le risque cyber le plus répandu est la négligence des salariés.

Le Shadow IT est massivement répandu, mentionné par 98% des répondants comme étant une menace à traiter. En effet, l'usage notoire des applications et services cloud le plus souvent gratuits, s'est banalisé et échappe toujours au contrôle de la DSI. Cela accroît significativement les risques, comme les fuites de données via les outils de transfert d'information ou de partage de fichiers volumineux. D'autant que l'utilisation même anecdotique d'un service Cloud non sécurisé, peut suffire à compromettre l'intégrité et la sécurité des données de l'entreprise.

Les salariés sont pourtant sensibilisés aux cyber-risques (74%), cependant d'après les RSSI, ils sont seulement la moitié à respecter les recommandations. Pour tenter de mobiliser les salariés plus durablement, **77% des entreprises ont mis en place des procédures pour tester l'application des recommandations par les salariés.**

Les entreprises françaises sont-elles en capacité de défendre leurs infrastructures ?

La confiance des RSSI quant à la capacité de leur entreprise à faire face aux cyber-risques n'a pas progressé en un an, seuls 52% se disent confiants. 4 entreprises sur 10 se disent préparées en cas de cyber-attaque de grande ampleur.

Les enjeux pour l'avenir restent essentiellement humains

La gouvernance est le premier enjeu de demain (70%) soit 10 points de plus que l'année dernière, suivi par celui de la formation et la sensibilisation des usagers (57%). Les ressources humaines sont une demande forte des entreprises : la moitié souhaite augmenter ses effectifs de cybersécurité, mais 90% se heurtent à la pénurie de profils en SSI, en particulier pour les métiers de pilotage, d'organisation et de gestion des risques (34%), suivi par les profils liés au support et à la gestion des incidents.

L'augmentation du budget (50%) est un autre enjeu majeur. La part du budget IT consacré à la sécurité augmente dans les entreprises, et devrait continuer d'augmenter puisque 62% d'entre-elles indiquent vouloir allouer plus de ressources à la cybersécurité et 83% souhaitent acquérir de nouvelles solutions techniques.

« baromètre annuel de la cybersécurité des entreprises »

« Enquête OpinionWay pour le CESIN réalisée en ligne du 2 décembre 2019 au 7 janvier 2020 auprès de 253 membres du CESIN ».

Retrouvez l'intégralité des résultats du sondage OpinionWay pour le CESIN. Disponible sur demande.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN est partenaire de plusieurs organismes et institutions, comme l'ANSSI, la CNIL, la BEFTI, la Gendarmerie Nationale, le Cercle Européen de la sécurité, ACYMA (cybermalveillance.gouv.fr), l'AFAI, l'EBG, le CyberCercle ou encore l'EPITA.

Le CESIN compte plus de 600 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr