Communiqué de Presse

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

6ème édition du baromètre annuel du CESIN

Enquête exclusive sur la cybersécurité des grandes entreprises françaises

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

Paris, le 9 février 2021 – 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, Directeurs Cybersécurité et Responsables Sécurité des Systèmes d'Information (RSSI) des grandes entreprises françaises.

Le sondage OpinionWay pour le CESIN a ciblé 704 membres de l'association, les résultats de l'étude portent sur un échantillon de 228 répondants. Cette enquête permet d'obtenir la perception et la réalité concrète de la cybersécurité des grandes entreprises, dans un contexte de transformation numérique pendant une crise sanitaire avec des répercussions économiques et sociales sans précédent.

En 2020 une entreprise sur cinq déclare avoir subi au moins une attaque par Ransomware au cours de l'année, provoquant un chiffrement et/ou un vol de données, assortis d'une demande de rançon pour délivrer une clé de déchiffrement et/ou un chantage à la divulgation de données.

Le Phishing reste le vecteur d'attaque le plus fréquent, 80% des entreprises déclarent que le phishing a été un vecteur d'entrée pour les attaques subies.

Le Shadow IT déjà largement répandu est toujours en forte augmentation. Avec le télétravail généralisé, l'usage d'applications et de services cloud non sécurisés et inconnus de la DSI constituent l'une des causes principales de risques cyber pour 44% des entreprises.

La menace en matière de cyber-espionnage est elle aussi en augmentation. Plus de **56% considèrent que ce niveau de menace est élevé.** Un score inquiétant qui corrobore les observations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) quant aux acteurs des secteurs stratégiques.

58% des cyber-attaques ont eu des conséquences avérées sur le business, avec des perturbations sur la production dans 27% des cas.

(nb : définition de Cyber-attaque pour l'enquête CESIN-OpinionWay [1])

1 Cyber-attaque - Définition donnée pour cette enquête : « 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. »

Seulement 1 entreprise sur 2 est confiante en sa capacité à faire face à une cyberattaque

24% des entreprises ont fait appel à leur cyber assurance après une cyber-attaque. Nous avions observé un engouement notable pour la souscription de couverture aux cyber-risques ces dernières années, or sur ces 24%, 10% déclarent se heurter à des difficultés assurantielles.

47% ont porté plainte auprès des autorités compétentes, mais cela n'a abouti que dans 15% des cas. L'exercice de l'attribution des attaques reste un sujet complexe.

La crise sanitaire apporte de nouveaux risques, 35% d'augmentation des crises lui sont liées, et notamment 37% sont attribués la généralisation du télétravail. En conséquence 43% des entreprises se disent prêtes à augmenter leurs budgets pour affronter ces aléas.

Alors que l'adoption du Cloud est massive, les risques induits restent pourtant bien présents. 51% déclarent un risque fort de non maîtrise de la chaîne de sous-traitance de l'hébergeur, 45% déplorent des difficultés de contrôle d'accès et 44% de non maîtrise de l'utilisation par les salariés. En outre, 86% estiment que la sécurisation des données stockées dans le Cloud requiert une adaptation avec des outils ou dispositifs spécifiques. Tandis que 23% signalent le risque d'attaque par rebond depuis l'hébergeur.

Pour contrer la menace du ransomware, le premier dispositif renforcé est la sensibilisation des salariés pour 83%. A noter le développement du SOC (Security Operation Center) 56%, le durcissement de l'AD (Active Directory) 53%, et le déploiement en hausse des EDR (Endpoint Detection & Response) 48%.

Par ailleurs une dizaine de solutions est mise en place en moyenne par entreprise. Sans surprise le télétravail nécessite le recours massif à l'utilisation de VPN (90%). Avec toujours une forte adoption des solutions d'authentification multi-facteurs (73%). En revanche les solutions de CASB semblent avoir encore du mal à s'imposer (15%).

Le concept Zero Trust, qui a fait son entrée dans le baromètre précédent avec une certaine défiance, progresse avec 29% des entreprises réellement engagées ou en passe de mettre en œuvre ce concept, contre 16% l'année dernière.

L'augmentation des budgets alloués à la cybersécurité a continué et 57% des entreprises prévoient encore de poursuivre cette tendance. Elles sont 52% à vouloir allouer plus de ressources à la cybersécurité. **85% souhaitent acquérir de nouvelles solutions techniques en 2021.** Côté innovation, les responsables de la cybersécurité **sont désormais plus de la moitié à avoir recours aux offres issues de start-up** (55%).

Les enjeux pour l'avenir restent essentiellement humains

La gouvernance est le premier enjeu de demain (60%), suivi par celui de la formation et de la sensibilisation des utilisateurs (56%). Les ressources humaines sont un défi de taille pour les entreprises, la moitié souhaitant augmenter ses effectifs de cybersécurité. La prise en compte des enjeux de cybersécurité par le COMEX s'améliore, en hausse de 8 points par rapport à l'année passée, 72% des répondants sont confiants sur l'engagement de leur comité exécutif sur la cybersécurité.

« Baromètre annuel de la cybersécurité des entreprises »

« Enquête OpinionWay pour le CESIN réalisée en ligne du 7 décembre 2020 au 11 janvier 2021 auprès de 228 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 700 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr