Communiqué de Presse

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

4ème 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 quatrième grande enquête OpinionWay pour le CESIN.

Paris, le 15 janvier 2019 – 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 la quatrième édition de 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 498 membres de l'association, les résultats de l'étude portent sur un échantillon de 174 répondants. Ils mettent à jour la perception et la réalité concrète de la cybersécurité, avec de nouvelles données sur l'impact de la transformation numérique des entreprises.

L'impact des cyber-attaques est de plus en plus décisif

Si le nombre des cyber-attaques constatées tend à se stabiliser, huit entreprises sur dix continuent d'être impactées, **avec pour 59% d'entre elles des conséquences sur le business** (arrêt de la production, indisponibilité significative du site internet, perte de chiffre d'affaire...) soit 10 points d'augmentation par rapport à l'année dernière.

Le Phishing est le mode d'attaque le plus fréquent, 73% en ont été victimes, étonnamment l'arnaque au Président que l'on croyait en extinction touche encore une entreprise sur deux en 2018. Le Ransomware est au troisième rang avec 44% d'entreprises touchées, suivi par le social engineering (40%).

Le Shadow IT est le risque cyber le plus répandu, mentionné par 64% 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 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, peut suffire à compromettre l'intégrité et la sécurité des données de l'entreprise.

Cloud et IoT : des risques accrus avec la transformation numérique

98% des entreprises estiment que la transformation numérique a une incidence sur la sécurité des systèmes d'information des données. En tête des enjeux : **le recours massif au Cloud, utilisé par 87% des entreprises**, dont 52% dans des clouds publics. Un mode de stockage qui pose des problèmes de non-maîtrise ; que ce soit par rapport à l'accès aux données de l'entreprise par les hébergeurs (via les administrateurs ou autres) ou par rapport à la chaîne de sous-traitance pratiquée par le fournisseur. **Pour 89% des RSSI interrogés ces enjeux impliquent le recours à des 'outils de sécurisation supplémentaires à ceux proposés par le prestataire.**

Dans un même temps, les objets connectés se sont progressivement installés dans le paysage et la course à l'innovation ne va pas de pair avec l'implémentation de la sécurité, faisant apparaître de nouvelles typologies de menaces. Les nombreux cas de piratage témoignent d'une progression de la cybercriminalité via les objets connectés. **Pour l'IoT, la caractéristique la plus marquante reste les failles de sécurité présentes dans ces équipements.** On notera souvent l'absence de chiffrement pouvant porter atteinte à la confidentialité, ou l'absence d'authentification avec des accès non protégés.

Face aux cyber-risques, une cyber-résilience à développer

Pour contrer ces cyber-risques, les RSSI déploient une panoplie de solutions techniques, globalement jugées adaptées à leurs besoins (75%), même si des progrès restent à faire dans leur adaptation à la transformation numérique. À noter l'enjeu de l'IA : **56% des répondants ont mis en place des solutions basées sur l'IA ou envisagent de le faire** ; toutefois 55% estiment que l'IA ne se substituera pas à l'expertise humaine en matière de sécurité.

Pour autant, les entreprises françaises sont-elles en capacité de défendre leurs infrastructures ? Les RSSI se disent moins confiants que l'année dernière quant à la capacité de leur entreprise à faire face aux cyber-risques. 51% sont confiants, soit une baisse de 12 points ; et moins d'un sur deux considère que son entreprise est préparée à gérer une cyber-attaque de grande ampleur. 50% ont désormais souscrit à une cyber-assurance, soit une hausse de 10 points, mais seule une entreprise sur dix a mis en place un véritable programme de cyber-résilience. Si ce n'est pas en projet pour 21%, c'est une tendance avec 33% en cours et 34% qui l'envisagent.

Trois enjeux pour l'avenir, essentiellement humains

D'après les RSSI, l'enjeu principal pour l'avenir de la cyber-sécurité est celui de **la formation et de la sensibilisation des utilisateurs** (61%). Les usages des salariés apportent en effet leur lot de risques, notamment via le shadow IT. Et si les salariés sont sensibilisés, ils restent peu impliqués en ne suivant pas forcément les recommandations. Un important travail de pédagogie reste à faire.

La **gouvernance de la cyber-sécurité** doit également être placée au bon niveau pour 60% des RSSI. Malgré un impact positif de la mise en conformité RGPD sur la gouvernance des entreprises (59%), la confiance en la capacité des COMEX à prendre en compte les enjeux de la cyber-sécurité est très inégale en fonction des secteurs d'activité.

En France comme dans le reste du monde, **la pénurie de ressources humaines en cybersécurité est un défi majeur pour les organisations, constatée par 91% des RSSI**... À l'heure où 50% d'entre eux prévoient d'augmenter les effectifs alloués à la protection contre les cyber-risques.

«baromètre annuel de la cybersécurité des entreprises»

«Enquête OpinionWay pour le CESIN réalisée en ligne du 23 novembre au 26 décembre 2018 auprès de 174 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, l'ARJEL, 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 500 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr