Communiqué de Presse

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

7ème édition du baromètre annuel du CESIN

Enquête exclusive sur la cybersécurité des entreprises françaises

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

Paris, le 17 janvier 2022 – Afin de mieux cerner l'état de l'art et la perception de la cybersécurité et de ses enjeux au sein des entreprises françaises, le CESIN publie depuis 2015 son baromètre annuel avec OpinionWay. L'association dévoile aujourd'hui les résultats de cette nouvelle enquête indépendante et exclusive menée auprès de ses membres, Directeurs Cybersécurité et Responsables Sécurité des Systèmes d'Information (RSSI) des entreprises françaises. Ce sondage OpinionWay pour le CESIN porte sur un échantillon de 282 répondants, membres du CESIN.

En 2021 plus d'une entreprise sur deux déclare avoir subi entre une et trois attaques cyber au cours de l'année. Ce chiffre tient compte uniquement des attaques réussies, ayant eu des répercussions flagrantes pour les victimes *(cf : définition de Cyber-attaque pour l'enquête CESIN-OpinionWay [1]).*

Il faut souligner que l'ampleur et la virulence des attaques ne cessent d'augmenter. En effet **6 entreprises sur 10 ont connu un impact sur leur business**, avec pour principaux retentissements une perturbation de la production (21%), et/ou une compromission d'information (14%), et/ou une indisponibilité du site web pendant une période significative.

Le Phishing reste le vecteur d'attaque le plus fréquent. 73% des entreprises déclarent le phishing comme vecteur d'entrée principal pour les attaques subies. Les autres moyens de transmission sont, l'exploitation des failles (53%), et en augmentation, l'attaque par rebond via un prestataire (21%). Ce dernier axe s'est illustré ces derniers mois par des incidents retentissants comme le piratage de SolarWinds ou encore la faille d'Apache, Log4J.

Les attaques par ransomware ont touché 1 entreprise sur 5 parmi les répondants. Face à cette déferlante, on note en corollaire l'augmentation des campagnes de sensibilisation auprès des utilisateurs, le déploiement d'EDR (+16 points) et le durcissement de l'AD (+9 points). Par ailleurs, **4 entreprises sur 10 ont recours à des programmes d'entrainement à la crise cyber**, et 47% déclarent que c'est en projet.

---

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 et/ou des efforts significatifs de défense pour contenir et traiter l'attaque. Nous ne comptons pas les tentatives d'attaques qui ont été arrêtées par les systèmes de prévention. »

De surcroît, les entreprises ont dû revoir massivement leurs dispositifs de sécurité dans le contexte de crise sanitaire et d'intensification du télétravail. 63% d'entre elles ont généralisé le recours à l'authentification multi-facteurs (MFA) et 70% ont mené des campagnes de sensibilisation liées aux risques de ce nouveau mode de travail pour beaucoup de salariés.

Avec l'adoption manifeste du cloud le RSSI doit faire face à des dizaines de sujets qu'il n'avait pas à traiter avec des solutions sur site. **Les principaux facteurs de risques induits par l'adoption du Cloud** concernent la non maîtrise de la chaîne de sous-traitance de l'hébergeur pour 48% des répondants, et des difficultés de contrôle d'accès déclarées par 43%. En outre, 40% indiquent des risques liés à la rareté de l'expertise parmi les architectes et les administrateurs, et une mauvaise visibilité de l'inventaire des ressources dans le cloud pour 38%. **8 RSSI sur 10 estiment encore que la sécurisation des données stockées dans le cloud requiert des outils spécifiques,** et dans la plupart des cas (63%) il est nécessaire d'utiliser d'autres dispositifs que ceux proposés par le fournisseur de cloud.

6 entreprises sur 10 se disent préoccupées par les sujets de souveraineté et de cloud de confiance. Ce qui suppose une attente forte autour des perspectives de potentiels rééquilibrage des forces avec le développement des solutions dites de confiance annoncées en France et en Europe.

La question du cyberespionnage a été abordée pour la première fois lors du précédent baromètre**. Plus d'une entreprise sur deux considère que le niveau de menaces en matière de cyberespionnage est élevé** (55%)**.** Un score édifiant qui corrobore de nombreux rapports et les observations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette menace croissante demande une vigilance accrue car elle devrait encore s'intensifier.

69% des répondants affirment avoir souscrit une cyber-assurance. Après plusieurs années d'engouement, les premiers bilans révèlent un moindre taux de satisfaction pour ceux qui ont eu recours. D'autre part, la majorité des entreprises ont un avis négatif sur l'usage des services d'agences de notation. Lors de récentes réunions des membres du CESIN, nombre d'entreprises se sont déclarées hésitantes à un renouvellement de leur contrat, ce qui pose question sur l'avenir de ce marché. Le CESIN note globalement une hausse exponentielle des tarifs, pour une baisse des couvertures et des niveaux d'exigences de la part des assureurs, quasiment inatteignables.

Les budgets alloués à la cybersécurité sont encore en hausse cette année. 70% des entreprises confirment cette tendance, contre 57% en 2020. Elles sont 56% à vouloir allouer plus de ressources humaines à leur organisation. **84% vont acquérir de nouvelles solutions techniques, tandis que 62% d'entre elles ont recours aux offres innovantes issues de start-up.**

En parallèle la prise en compte des enjeux de cybersécurité au sein du COMEX progresse. **79% des répondants sont confiants sur l'engagement de leur comité exécutif**. Une tendance en adéquation avec une récente étude publiée par le CESIN sur la relation du RSSI avec son Comité Exécutif.

« Baromètre annuel de la cybersécurité des entreprises »

« Enquête OpinionWay pour le CESIN réalisée en ligne en décembre 2021
auprès de 282 membres du CESIN ».

Retrouvez ici l'intégralité des résultats du sondage OpinionWay pour le CESIN.

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