Communiqué de Presse

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

8ème 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 huitième grande enquête OpinionWay pour le CESIN.

Paris, le 30 janvier 2023 – 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 328 répondants, membres du CESIN.

L'étude révèle que les cyberattaques sont en baisse. Elles concernent désormais moins d'une entreprise sondée sur deux. *(le baromètre tient compte uniquement des attaques réussies, ayant eu des répercussions significatives pour les victimes - cf : définition de Cyberattaque pour l'enquête CESIN-OpinionWay [1]).*

La menace est toujours très présente, néanmoins l'anticipation semble porter ses fruits à mesure des politiques de sensibilisation, de l'investissement dans les outils de protection, de la capacité de détection et de gestion des incidents, ou de l'entraînement aux situations de crises.

Les attaques par ransomware ont touché moins d'1 entreprise sur 5. Cependant, si pour 64% des répondants le nombre d'attaques abouties est resté stable, cela ne signifie pas que l'activité soit moins dense, 24% des entreprises ayant déclaré au moins une attaque en 2022 estiment toujours que le phénomène est en augmentation.

Le Phishing reste le vecteur d'attaque le plus fréquent. 74% des entreprises déclarent le Phishing comme vecteur d'entrée principal pour les attaques subies. Parmi les autres moyens de transmission, en tête du classement l'exploitation des failles (45%) et nous savons que le nombre

1 Cyberattaque - Définition donnée pour cette enquête : « La cyberattaque 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 entraînant 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 vulnérabilités, mais aussi la surface d'attaque publique sont en constante augmentation, ou encore l'attaque par rebond via un prestataire (24%). Sur ce point, notons que la gestion des risques liés aux tiers prend une place de plus en plus importante dans les activités des responsables cybersécurité.

Dans 60% des cas, les attaques impactent fortement le business des entreprises, avec pour effet de perturber significativement la production pour 24% des sondés. Dans 7% des cas on constate un déficit du chiffre d'affaires. Au nombre des préjudices, le vol de données (35%), l'usurpation d'identités (33%), et les données chiffrées par ransomware (22%).

Plus d'une entreprise sur deux considère toujours que le niveau de menaces en matière de cyberespionnage est élevé (50%)**.** Ces opérations visent le plus souvent des cibles d'intérêts stratégiques. Une dynamique à nouveau confirmée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui rappelle que le ciblage des victimes peut affecter les fournisseurs d'opérateurs stratégiques, leurs prestataires et parfois leurs autorités de tutelle.

A propos du Cloud, qui représente moins de 50% du SI en moyenne chez les répondants, les principaux facteurs de risques induits concernent toujours la non maîtrise de la chaîne de sous-traitance de l'hébergeur et la difficulté de contrôle des accès par les administrateurs de l'hébergeur. **La surveillance de la sécurité des clouds requiert des outils spécifiques** et dans la grande majorité des cas (89%) il est jugé nécessaire d'utiliser d'autres dispositifs que ceux proposés nativement par les fournisseurs de cloud.

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

L'axe sensibilisation est au rang des mesures qui progressent pour faire face aux défis de la cyber. **8 entreprises sur 10 mènent des campagnes de sensibilisation auprès des collaborateurs**. La culture de la cybersécurité n'est pourtant toujours pas suffisamment ancrée dans les organisations, seuls 2/3 des utilisateurs respectent les recommandations. D'autant que la négligence et les erreurs de manipulation constituent la principale cause d'incidents (38%). Alors que tous les collaborateurs ont un rôle à jouer en matière de cybersécurité, on déplore encore un manque d'expertise sécurité pour les administrateurs, architectes ou développeurs, une compétence qui permettrait un progrès significatif dans la contribution de chacun de ces métiers à réduire les risques.

Les outils sont au cœur de la politique de protection avec une moyenne d'adoption de 15 solutions et services par organisation. On constate un bon niveau de confiance dans les solutions puisque 88% des répondants jugent les solutions du marché plutôt adaptées. Une place prépondérante est donnée aux outils de détection et de réponse aux incidents. L'authentification multi-facteurs concerne 81% des entreprises et est réputée performante. C'est d'autant plus important que 33% des attaques ont conduit à des usurpations d'identités. On note une forte hausse du déploiement des EDR, devenu une réalité dans 81% des entreprises. Les outils de gestion des vulnérabilités ainsi que les services de SOC comptent parmi les dispositifs jugés les plus efficaces. Enfin, on peut noter que **6 entreprises sur 10 ont recours à des offres innovantes issues de start-up**.

Les budgets alloués à la cybersécurité augmentent encore légèrement cette année. Ils dépassent majoritairement 5% du budget IT global. 63% prévoient une augmentation allouée aux dispositifs de protection, et 54% attribuée à l'augmentation des effectifs.

82% prévoient d'acquérir de nouvelles solutions. In fine 77% estiment avoir les moyens de se prémunir d'une cyberattaque de grande ampleur, mais plus de la moitié se déclare limitée dans son aptitude à répondre et reconstruire. La résilience des SI face à des cyberattaques reste un maillon important à améliorer dans la stratégie de défense.

Près de 2/3 des répondants ont souscrit une cyberassurance. Les premiers bilans révélaient un moindre taux de satisfaction pour ceux qui avaient eu recours à l'assurance, tandis que 76% d'entre elles ne l'ont pas utilisée. Cette année, 1 répondant sur 10 se déclare hésitant pour renouveler son contrat, et 2% y ont déjà renoncé. En outre, une majorité d'entreprises émet un avis négatif sur le recours aux services d'agences de notation par les assureurs. De son côté Le CESIN note toujours une forte hausse des tarifs, pour une baisse des couvertures, avec toujours plus d'exclusions, et des niveaux d'exigences de la part des assureurs, quasiment inatteignables.

En parallèle la prise en compte des enjeux de cybersécurité au sein du COMEX est stable. Le sujet cybersécurité est bien présent dans les COMEX. **75% des répondants sont confiants sur l'engagement de leur comité exécutif**. Placer la gouvernance de la cybersécurité au bon niveau dans l'entreprise est au premier rang des objectifs d'avenir.

« Baromètre annuel de la cybersécurité des entreprises »
« Enquête OpinionWay pour le CESIN réalisée en ligne de décembre 2022 à janvier 2023 auprès des 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 cybersécurité.

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, Gimelec, le CyberCercle ou encore l'EPITA.

Le CESIN compte plus de 900 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr