Communiqué de Presse

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

10e édition du baromètre annuel du CESIN

une décennie d'éclairage sur la cybersécurité des entreprises françaises

Le Club des Experts de la Sécurité de l'Information et du Numérique
dévoile les résultats de sa 10ème grande enquête OpinionWay pour le CESIN.

Paris, le 27 janvier 2025 – Le CESIN dévoile les résultats de son baromètre annuel réalisé avec OpinionWay, offrant une vue d'ensemble unique sur les enjeux et les tendances du secteur. Cette enquête indépendante et exclusive menée auprès de ses membres, Directeurs Cybersécurité et Responsables Sécurité des Systèmes d'Information (RSSI), analyse les grandes tendances de la cybersécurité en entreprise. Les données issues de 401 répondants révèlent un paysage en mutation, marqué par la résilience des entreprises face à des menaces complexes et un environnement en constante évolution.

Le volume des cyberattaques est stable mais les impacts sont significatifs

47% des entreprises interrogées déclarent avoir subi au moins une cyberattaque[1] significative. Ce chiffre est stable par rapport à l'année précédente, il reflète une maturité croissante des organisations les mieux équipées en ressources et solutions de cybersécurité, malgré une menace toujours plus présente. Cette stabilisation fait suite à une baisse progressive entre 2019 et 2022 (de 65% à 45%), témoignant des bénéfices d'une gestion proactive des risques et d'investissements stratégiques dans la défense cyber.

Le phishing reste le vecteur d'attaque dominant (60%), identique à 2023, suivi par l'exploitation de failles (47%) et les dénis de service (41%). Cependant l'impact des attaques s'intensifie, avec en tête le vol de données en nette augmentation (+11 points à 42%) dont il constitue la principale conséquence. L'impact sur le business pendant une période significative est avéré à 65%, avec une perturbation sur la production dans 23% des cas.

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. »

Vers une sophistication accrue des cybermenaces

Alors que l'année précédente soulignait déjà l'émergence d'attaques hyper-volumétriques, le baromètre 2024 confirme la spécialisation des techniques d'attaques. **Le Deepfake fait une entrée remarquée dans le baromètre**, représentant déjà 9% des vecteurs d'attaques identifiés. Bien que cette proportion puisse sembler modérée, elle souligne l'émergence d'une technologie potentiellement dévastatrice. Ce type d'attaque, basé sur la manipulation réaliste de voix ou d'images, amplifie des stratagèmes existants, notamment l'arnaque au président, qui reste l'une des méthodes d'extorsion favorites des cybercriminels. En facilitant l'usurpation d'identité et en renforçant la crédibilité des attaques par ingénierie sociale par exemple, le Deepfake est aux prémices de nouvelles opportunités pour les acteurs malveillants. Cette menace va évoluer, les technologies de création de Deepfake sont de plus en plus accessibles et leur exploitation dans des scénarios cybercriminels pourrait s'intensifier rapidement. Cette évolution exige une vigilance accrue des entreprises, qui doivent intégrer des stratégies de détection et de sensibilisation spécifiques pour contrer ces nouveaux risques.

En revanche, certaines menaces, comme le chiffrement par ransomware, connaissent une baisse notable (-9 points). La menace reste présente, ici encore il s'agit d'un signe supplémentaire de l'efficacité croissante des outils de défense et des processus de lutte contre la cybercriminalité des entreprises membres.

Avec **37% des entreprises considérant le cyberespionnage comme un risque élevé,** ce type de menace sous haute surveillance continue de représenter un défi majeur. Ce chiffre, constant par rapport à l'année dernière, illustre la persistance des attaques ciblées visant des secteurs stratégiques et des données sensibles. Alors que les acteurs malveillants affinent leurs tactiques pour contourner les défenses, la capacité des entreprises à anticiper et détecter ces incursions devient un enjeu critique. Face à un paysage géopolitique tendu et une sophistication croissante des menaces, le cyberespionnage exige une vigilance spécifique et des réponses renforcées pour protéger les actifs les plus stratégiques. En écho à ce phénomène, les sujets de souveraineté et de cloud de confiance continuent de préoccuper 52% des répondants.

Des défenses plus robustes, et une meilleure maîtrise des assets

Comme l'année précédente, les entreprises continuent au-delà des incontournables pares-feux de plébisciter les solutions EDR (95% d'efficacité perçue, +5 points) et l'authentification multi-facteurs (MFA). Les concepts innovants tels que le Zero Trust et le VOC (Vulnerability Operation Center) poursuivent leur progression, atteignant respectivement 31% (+7 points) et 26% (+9 points) pour les entreprises interrogées.

Porter plainte reste indispensable pour lutter contre la cybercriminalité

En 2024 62% des entreprises ayant subi une cyberattaque ont porté plainte, une proportion stable mais encore insuffisante. Signaler ces incidents est essentiel pour renforcer la lutte collective contre le crime cyber. En collaborant avec les autorités, les organisations contribuent à démanteler les réseaux criminels, tout en bénéficiant d'un accompagnement pour limiter les impacts. Porter plainte, c'est aussi envoyer un signal fort que la cybersécurité est une priorité stratégique et qu'aucune attaque ne doit rester sans réponse.

Du côté des environnements Cloud, la mauvaise visibilité de l'inventaire des assets dans les clouds publics diminue en 2024 (31%, -7 points), en lien avec l'adoption croissante d'outils performants comme les solutions EASM et CAASM. Ces technologies permettent une cartographie plus précise des ressources, qui réduit les angles morts et renforce la posture de sécurité des entreprises. Cette évolution témoigne encore d'une maturité des organisations, bien que des défis subsistent, notamment sur le contrôle des accès administrateurs et des sous-traitants.

Un écosystème en transition avec l'essor de l'IA et la maîtrise des risques liés aux tiers

L'IA s'impose comme un levier de transformation numérique incontournable. En effet, le recours à l'intelligence artificielle fait un bond avec une adoption forte, puisque 69% des entreprises intègrent désormais l'IA dans leurs processus, contre 46% en 2023 (+23 points). Néanmoins, on constate que seulement 35% des organisations l'ont incluse dans leur stratégie de cybersécurité, révélant un potentiel d'amélioration significatif.

Les incidents liés aux tiers restent une préoccupation majeure. 28% des entreprises signalent de mauvaises pratiques, tandis que 85% d'entre elles adoptent des clauses de sécurité dans leurs contrats pour atténuer ces risques. Cette tendance s'inscrit dans la continuité des résultats de 2023, où l'impact des tiers était déjà souligné.

Des priorités en mutation, sur la gouvernance, les budgets et la formation

Le risque cyber se place dans le TOP 3 des risques en entreprise. Malgré des budgets dédiés à la cybersécurité encore stables en 2024, les intentions d'augmenter les effectifs et les solutions techniques diminuent (respectivement -13 points et -15 points), un signe sans doute de tassement dans les moyens accordés à la cybersécurité qu'il conviendra d'observer en 2025.

64% ont intégré des étudiants en alternance cette année. En parallèle, la sensibilisation des collaborateurs reste un levier majeur puisque 85% des utilisateurs sont formés aux risques cyber, un chiffre stable et crucial pour réduire les comportements à risque.

Un lien renforcé entre cybersécurité et RSE

77% des RSSI intègrent désormais les initiatives de responsabilité sociétale des entreprises (RSE), en particulier via la promotion d'une culture de la cybersécurité et la conformité réglementaire. Ce rapprochement illustre la reconnaissance croissante de la cybersécurité comme pilier stratégique et sociétal.

Concernant la réglementation, en 2023 70% des entreprises déclaraient être impactées par au moins une réglementation majeure, telles que NIS2, DORA ou Cyberscore. Cette année, ce chiffre progresse à 79%, dont 52% indiquent un impact fort. La directive NIS2 reste la réglementation la plus citée, touchant 74% des entreprises interrogées. Ces exigences renforcent l'intégration des normes dans les stratégies de cybersécurité, avec des ajustements nécessaires dans les processus et les solutions déployées.

« Baromètre annuel de la cybersécurité des entreprises »
« Sondage OpinionWay pour le CESIN réalisé en ligne de décembre 2024 à janvier 2025 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 compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN rassemble plus de 1 200 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. Pour en savoir plus www.cesin.fr