Communiqué de Presse

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

9ème 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 neuvième grande enquête OpinionWay pour le CESIN.

Paris, le 29 janvier 2024 – Afin de mieux cerner l'état de l'art et la perception de la cybersécurité et de ses enjeux au sein des organisations, 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). Ce sondage OpinionWay pour le CESIN porte sur un échantillon de 456 répondants, membres du CESIN, dont 40% provenant d'Entreprises de Taille Intermédiaire (ETI) et 48% de grandes entreprises.

L'étude révèle que le nombre des cyberattaques réussies reste stable (49%), moins d'une entreprise sur deux déclare avoir subi au moins une cyberattaque avec un impact significatif. *(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 omniprésente et en constante évolution, cependant les efforts déployés sont probants dans l'anticipation des crises, avec notamment les investissements dans les outils de protection, l'amélioration de la capacité de détection et de gestion des incidents, les campagnes de sensibilisation ou encore les exercices d'entraînement aux situations de crises.

Bien que **le Phishing demeure le principal mode d'attaque, signalé par 60% des entreprises comme vecteur d'entrée principal pour les attaques subies**, il semble que cette méthode devienne plus sophistiquée et plus ciblée, elle engendre une baisse de 14 points. L'arnaque au Président diminue fortement (28%) avec un recul de 13 points.

Parallèlement, **on note une augmentation des attaques en déni de service**, un impact croissant corroboré par plusieurs études alertant notamment sur des attaques DDoS hyper-volumétriques. Cette augmentation peut-être attribuée à divers facteurs. Techniques par exemple, avec l'essor des botnets massifs, ou encore liés aux tensions géopolitiques et pouvant s'intensifier lors de périodes critiques, comme lors d'élections, de manifestations ou d'événements politiques majeurs.

---

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. »

Les cyberattaques opportunistes perdurent et sont fréquentes (39%), toutefois, l'édition 2024 du baromètre confirme à nouveau la complexité croissante du paysage de la cybersécurité, avec des attaquants qui ajustent leurs tactiques. Les demandes de rançons se stabilisent autour de 10% d'entreprises victimes de cyberattaques. **Le cyberespionnage représente quant à lui un risque élevé pour 2 entreprises sur 5**, toutes industries confondues, un résultat qui revêt une importance particulière étant donné que certaines organisations, en raison de leur domaine d'activité, ne sont pas très exposées à ce type de menace. Enfin, l'enquête met en lumière la persistance de mauvaises pratiques comme sources d'incidents. A l'exception des risques induits par le télétravail, les responsables cyber voient une hausse des usages numériques à risque qui échappent au contrôle de l'entreprise (shadow IT), on note aussi les vulnérabilités résiduelles permanentes, la négligence ou encore les erreurs de configuration.

65% déclarent que les attaques ont eu des impacts sur le business, avec perturbation de la production pour 24% d'entre eux. 22% indiquent une indisponibilité du site web pendant une période significative, un impact en hausse dû à l'augmentation des attaques en déni de service.

La confiance envers les solutions et services de sécurité du marché reste élevée, avec 87% des répondants qui jugent ces offres adaptées. Au global, on compte une moyenne de plus de 15 solutions ou services par entreprise. Le couple MFA (Authentification multi-facteurs) et EDR (Système de détection et réponse pour endpoints) est vu comme très efficace. Cependant, l'analyse souligne aussi une sous-utilisation de solutions éprouvées, malgré leur efficacité avérée. L'EDR progresse de 9 points, en tête des solutions déployées (90%), le concept Zero Trust gagne en maturité, déployé par 76% des entreprises. Le VOC (Vulnerability Operation Center) est désormais utilisé par 50% d'entres elles, tandis que le CAASM (Cyber Asset Attack Surface Management) émerge (34%).

Les entreprises privilégient généralement le traitement interne de la gestion des vulnérabilités, du VOC et de la gestion de la surface d'attaque. Les audits, Pentests, la Threat Intelligence et les CERT-CSIRT sont bien sûr davantage externalisés. À noter qu'une part significative des EDR et des SOC est gérée de manière hybride.

L'écosystème de la cybersécurité est réceptif aux innovations, la moitié des entreprises adopte des offres émanant de startups, témoignant ainsi d'une disposition à prendre des risques mesurés.

Le Cloud occupe une place significative dans les systèmes d'information, avec un tiers à un quart des entreprises ayant plus de 50% de leur SI en IaaS/PaaS et SaaS. Les responsables cyber notent des risques persistants liés au contrôle des sous-traitants et aux accès administrateurs, bien que le niveau d'expertise global s'améliore dans ce domaine.
La souveraineté et le Cloud de Confiance présentent intérêt significatif puisqu'une entreprise sur deux (55%) montre un attrait marqué pour ces initiatives.

Concernant les normes, une majorité écrasante d'entreprises les intègre régulièrement dans leurs pratiques quotidiennes. 88% estiment que les normes sont une composante essentielle du paysage cyber, et recherchent activement des certifications pour l'interne, comme pour leurs partenaires.

La Cyberassurance a séduit 7 entreprises sur 10 et la plupart envisage de renouveler ses contrats, signalant une stabilisation dans le champ des entreprises assurées. Le recours à l'assurance n'est pas systématique, malgré une moyenne de trois incidents par an et par entreprise, trois quarts d'entre elles n'ont pas recours à la cyberassurance. Cette observation suggère que deux incidents sur trois en moyenne ne font pas l'objet de déclarations d'assurance, laissant supposer que l'impact de ces incidents est inférieur aux montants des franchises. Cette

situation pourrait être expliquée par la capacité des entreprises à gérer ces incidents sans supporter des coûts significatifs. En outre, la confiance a baissé envers les agences de notation dont il est estimé que les résultats sont très partiels.

La réglementation et l'impact de l'IA incitent les entreprises à prendre des mesures. Actuellement, 7 entreprises sur 10 déclarent être impactées par au moins une réglementation, telle que NIS2, DORA, ou Cyberscore.

En ce qui concerne **l'Intelligence Artificielle** (IA), près de la moitié des RSSI, soit 46%, observent son utilisation en interne. Cependant, seuls 16% l'ont intégré dans leur stratégie de cybersécurité. Cette adoption modérée incite les RSSI à considérer l'adaptation des solutions à la transformation numérique de l'entreprise comme leur principal défi à venir, avec un taux de 52%.

Bien que les inquiétudes quant à la capacité à faire face aux cyberattaques diminuent légèrement, passant de 43% à 38%, la proportion de ceux qui se disent « très inquiets » chute de 9% à 5%.

Enfin, plus de la moitié des entreprises a l'intention d'accroître ses effectifs dédiés, et la grande majorité (78%) envisage d'acquérir de nouvelles solutions techniques. Les budgets pour faire face aux risques cyber restent stables.

« Baromètre annuel de la cybersécurité des entreprises »
« Enquête OpinionWay pour le CESIN réalisée en ligne de novembre 2023 à janvier 2024 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, Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.
Le CESIN compte plus de 900 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.
Pour en savoir plus www.cesin.fr