Cyberattaques : la résilience numérique devient un levier stratégique pour les entreprises françaises

La cybersécurité n'est plus une menace ponctuelle : elle est devenue un **enjeu structurant de l'économie française**. La billetterie de l'Olympique de Marseille a récemment été visée par une attaque informatique. La plateforme gouvernementale *Choisir le service public* a annoncé la compromission de centaines de milliers de données personnelles et professionnelles. Un opérateur télécom français a subi une fuite d'informations, et des transactions frauduleuses ont été signalées chez PayPal, liées à l'exposition de données sensibles.

Les dispositifs de cybersécurité opérés par Koesio illustrent cette pression constante. En 2025, près de **10.000 tentatives d'attaques ont été détectées sur les infrastructures de ses clients, soit environ une tentative par mois et par entreprise protégée**.

Dans ce contexte d'instabilité numérique croissante, la cybersécurité ne peut plus être traitée comme un sujet purement informatique. Elle devient un élément stratégique et concurrentiel. Selon les derniers bilans en France, **près de 67 % des entreprises ont été victimes d'au moins une cyberattaque en 2024**, avec plus de 5 600 violations de données déclarées à la CNIL et un coût global estimé à plus de **100 milliards d'euros** pour l'économie française[1]. À l'échelle mondiale, les pertes liées à la cybercriminalité pourraient atteindre 10 500 milliards de dollars par an d'ici 2025[2].

« Nous ne sommes plus dans une logique d'incidents exceptionnels, mais dans un environnement d'exposition permanente qui requiert une réponse structurée », affirme **Piéric Brenier, Président-Fondateur de Koesio**. « La résilience numérique devient un facteur de compétitivité pour les organisations capables d'anticiper plutôt que de subir. »

Transformer le cyber-risque en avantage stratégique

La transformation numérique et l'usage massif d'outils interconnectés ont élargi la surface d'exposition des organisations : cloud, télétravail, chaine de sous-traitance, applications SaaS, etc. Dans le même temps, les attaques se professionnalisent. Un rapport mondial indique que **90 % des cyberattaques exploitent des failles liées à l'identité**, et que 65 % des attaques démarrent par des vecteurs humains tels que le phishing ou le contournement de l'authentification multifacteur[3].

Cette évolution ne relève plus du seul enjeu technique. Elle touche directement la confiance des clients, des partenaires et des citoyens, pilier essentiel de l'économie numérique. À force de répétition, les incidents fragilisent la confiance dans les services dématérialisés, dans le paiement digital et dans l'administration numérique.

Pour aider les organisations à mesurer concrètement leur niveau d'exposition, Koesio met à disposition un simulateur d'audit de cybersécurité en ligne. Cet outil permet aux dirigeants et aux responsables IT d'obtenir une première évaluation de leur maturité cyber et d'identifier les priorités d'action. Une démarche pédagogique qui vise à transformer une prise de conscience souvent tardive en plan d'action structuré.

Les données issues des dispositifs de supervision opérés par Koesio illustrent cette pression permanente :

- **882 entreprises protégées** par l'offre MDR ISI-Crypto
- **Près de 10.000 attaques détectées en 2025**, soit environ **1 tentative par mois et par client**
- **97 % des attaques neutralisées sans impact** grâce aux technologies et aux équipes EMPES
- **301 attaques nécessitant une remédiation**, avec isolement rapide des équipements pour limiter la propagation

Derrière ces chiffres, une réalité : la cyberattaque n'est plus un événement rare, mais une pression continue. Dans un contexte où un rançongiciel peut se propager en moins d'une heure, réduire le temps d'exposition à 30 minutes constitue un avantage opérationnel décisif.

Un impératif de gouvernance pour les dirigeants

Face à cette réalité, la cybersécurité doit être traitée comme un sujet de gouvernance à part entière. L'approche doit s'étendre de la direction informatique aux directions générales et aux conseils d'administration, dans une posture d'anticipation des risques et de renforcement de la résilience.

« Il ne s'agit pas de viser un risque zéro, mais d'intégrer la cybersécurité au cœur de la stratégie », poursuit **Piéric Brenier.** « Les organisations qui relèvent ce défi renforcent leur stabilité, leur performance, et leur attractivité à long terme. Les entreprises doivent partir d'un constat simple : l'attaque n'est plus une éventualité mais une certitude. Sur les infrastructures que nous supervisons, nous avons identifié **près de 9 500 tentatives d'attaques en 2025**, dont **97 % ont été stoppées sans impact pour nos clients** »

Dans une économie où la donnée est devenue une ressource stratégique, la **protéger n'est plus une option technique**, mais bien **une condition de stabilité économique et de compétitivité durable**.

1. *Bilan des cyberattaques en France : près de 5 629 violations de données déclarées, 67 % d'entreprises affectées et plus de 100 milliards EUR de coût économique estimé en 2024 - RM3A Cybersécurité.*
2. *Estimation des pertes mondiales liées à la cybercriminalité : 10 500 milliards USD par an d'ici 2025 - CyberTrustLog.*
3. *Rapport mondial sur les vecteurs d'attaque : 90 % des violations exploitent des failles d'identité, 65 % commencent par des attaques humaines - ITPro.*

Audit Cyber proposé par Koesio : https://koesio.com/questionnaire-audit-cyber/