www.marsouin.org

ENQUÊTE CYBERSÉCURITÉ DES ENTREPRISES BRETONNES DE PLUS DE 10 SALARIÉS - RÉSUMÉ

Ce rapport présente les résultats d'une enquête qualitative exploratoire menée par le Groupement d'intérêt scientifique (GIS) Marsouin, avec le soutien de la Région Bretagne, sur les perceptions et pratiques des entreprises bretonnes en matière de cybersécurité. L'objectif est de mieux comprendre comment les entreprises de plus de dix salariés se positionnent face à l'augmentation des menaces cyber, dans un contexte de transformation digitale rapide et de renforcement des obligations réglementaires européennes et nationales.

Les systèmes numériques sont aujourd'hui au cœur du fonctionnement des entreprises. Cette dépendance les rend vulnérables à une diversité croissante de menaces : attaques par rançongiciel, exfiltration des données, déni de service, ou encore déstabilisation par des groupes hacktivistes. Les petites et moyennes entreprises (PME) sont particulièrement ciblées, souvent en raison d'une préparation insuffisante. En parallèle, les exigences réglementaires (NIS2, ISO27001, DORA, LOPMJ, etc.,) se renforcent et poussent les entreprises à se mettre en conformité.

L'enquête menée auprès de onze entreprises bretonnes issues de secteurs variés (industrie, numérique, santé, logistique, agriculture, agroalimentaire) met en lumière une diversité de situations, de niveaux de préparation et de maturité en matière de cybersécurité.

L'analyse révèle que la cybersécurité est souvent perçue de manière pragmatique. Pour certaines entreprises, elle constitue un levier stratégique intégré à la gouvernance, notamment dans les services numériques ou très régulés. Ces entreprises ont mis en place une gouvernance dédiée, des certifications (comme ISO27001), des plans de continuité d'activité, et des dispositifs de sensibilisation des collaborateurs.

À l'inverse, d'autres entreprises, notamment les plus petites parmi celles enquêtées et dont l'IT n'est pas le cœur de métier, ont une approche plus minimaliste : elles externalisent la quasi-totalité de leur sécurité numérique à des prestataires. Cette externalisation traduit à la fois un manque de structuration interne, un déficit de compétences en interne et parfois une moindre reconnaissance de la cybersécurité dans la stratégie de l'entreprise. La sécurité numérique est alors traitée comme une fonction isolée, sans vision d'ensemble.

L'enquête fait ressortir plusieurs fragilités partagées par les entreprises interrogées : une dette technique à rattraper, une dépendance accrue aux prestataires externes (externalisation quasi-totale de la cybersécurité dans certaines entreprises, souvent par défaut, multiplication du recours aux prestataires pour toutes les entreprises enquêtées), une structuration de la cybersécurité faible ou absente (absence de structure interne claire pour piloter la sécurité, pas de RSSI, pas de comité dédié, etc.), une pression sectorielle et réglementaire croissante (conformité imposée par des clients ou le secteur, avec peu de marge d'initiative interne), un manque de sensibilisation et de culture cyber en interne (faible implication des collaborateurs, manque de formation et d'appropriation de bonnes pratiques), une préparation encore insuffisante à la gestion d'incident et à la résilience (plans de continuité ou de reprise d'activité peu ou pas formalisés, manque d'exercices de crise), des enjeux émergents liés à l'intelligence artificielle (prise de conscience en cours, mais peu d'intégration des risques liés à l'IA dans les stratégies cyber).

JUIN 2025 | GIS MARSOUIN
AVEC LE SOUTIEN DE LA
RÉGION BRETAGNE
EN PARTENARIAT AVEC
BRETAGNE DÉVELOPPEMENT INNOVATION

Afin de mieux comprendre les logiques d'appropriation de la cybersécurité, l'étude propose une typologie structurée autour de trois profils d'entreprises :

PROFIL 1 - MATURITÉ AVANCÉE : ENTREPRISES AYANT INTÉGRÉ LA CYBERSÉCURITÉ DANS LEUR STRATÉGIE, AVEC UN PILOTAGE AUTONOME, UNE GOUVERNANCE STRUCTURÉE, ET UNE CAPACITÉ D'ANTICIPATION. LA SÉCURITÉ EST ICI UN FACTEUR DE COMPÉTITIVITÉ ET DE CONFIANCE.

PROFIL 2 – MATURITÉ INTERMÉDIAIRE : ENTREPRISES CONSCIENTES DES ENJEUX MAIS ENCORE EN TRANSITION, SOUVENT STIMULÉES PAR DES PRESSIONS EXTERNES (CLIENTS, AUDITS, RÉGLEMENTATION) SANS DISPOSER DE TOUS LES MOYENS OU OUTILS POUR FORMALISER UNE STRATÉGIE COMPLÈTE.

PROFIL 3 – MATURITÉ FAIBLE OU FRAGMENTAIRE : ENTREPRISES POUR LESQUELLES LA CYBERSÉCURITÉ RESTE PÉRIPHÉRIQUE, EXTERNALISÉE, PEU COMPRISE EN INTERNE, ET ABORDÉE AVANT TOUT SOUS L'ANGLE DE LA CONTRAINTE PLUTÔT QUE DE L'OPPORTUNITÉ.

Face à cette diversité de situations, plusieurs pistes d'accompagnement peuvent être envisagées : **1) renforcer** la gouvernance interne en incitant à la désignation de référents cybersécurité, à la mise en place de comités, et à l'élaboration des tableaux de bord ; **2) développer** la culture cyber à travers des programmes de formation et de sensibilisation adaptés aux réalités métiers ; **3) structurer** la résilience en accompagnant les entreprises dans la formalisation et la mise à l'épreuve de plans de continuité d'activité ; **4) cibler** des aides publiques selon les profils de maturité afin de soutenir les investissements nécessaires, tout en valorisant les démarches engagées.

Au final, ce rapport montre que la cybersécurité ne peut plus être pensée comme une simple fonction technique ou un coût à maîtriser. Elle conditionne la continuité d'activité, la confiance des partenaires et la compétitivité sur des marchés de plus en plus régulés. Elle devient **un enjeu stratégique, transversal et collectif**, à intégrer dans les pratiques quotidiennes, la gouvernance et les orientations d'avenir des entreprises. L'approche par la maturité, telle qu'elle ressort des entretiens réalisés, permet non seulement de mieux comprendre les besoins différenciés des entreprises bretonnes, mais aussi d'orienter les politiques publiques ciblées et efficaces.

JUIN 2025 | GIS MARSOUIN
AVEC LE SOUTIEN DE LA
RÉGION BRETAGNE
EN PARTENARIAT AVEC
BRETAGNE DÉVELOPPEMENT INNOVATION