



LETTRÉ INFORMATION CYBER – JANVIER 2025

ETUDE SUR LA MATURETE CYBER DES COLLECTIVITES

À l'occasion de sa participation au Salon des Maires et des Collectivités locales, Cybermalveillance.gouv.fr publie sa troisième étude sur la maturité des collectivités en matière de cybersécurité. Alors qu'elles restent des cibles majeures, et ce peu importe leur taille, le dispositif national d'assistance aux victimes de cybermalveillance a souhaité réitérer son enquête avec OpinionWay pour mieux connaître leur degré de considération face aux risques cyber mais également pour approfondir l'étude des freins qu'elles rencontrent.

1. Des collectivités toujours autant victimes

1 collectivité sur 10 déclare avoir été victime d'une ou de plusieurs cyberattaques au cours des 12 derniers mois. L'hameçonnage reste la cause principale dans 30 % des cas. Arrivent en deuxième place le téléchargement d'un virus ainsi que la consultation d'un site infecté, tous deux à 12 %. La faille de sécurité non corrigée prend la troisième place (10% +5pts vs 2023). Mais 45 % des collectivités attaquées n'en connaissent pas la cause. Et ce qui concerne les conséquences, les collectivités touchées ont principalement déploré :

- une interruption d'activité et de service pour 37% d'entre elles,
- une destruction ou un vol de données pour 24%,
- une perte financière 10 %,
- une atteinte à leur réputation 10%.

2. Une prise en compte des risques encore insuffisante

La considération des risques reste limitée, notamment pour les petites collectivités. Un chiffre qui s'explique par le fait qu'elles pensent ne pas être vulnérables et qui les amène à surestimer l'efficacité de leur niveau de protection et à insuffisamment se préparer face aux cyberattaques. En effet, elles sont 44% à s'estimer faiblement exposées aux risques (+6pts vs l'étude 2023) et 18 % ne savent pas l'évaluer. Un sentiment de sous exposition aux risques encore plus important pour 1 collectivité sur 2 de moins de 300 habitants (49%). De plus, 53 % des collectivités déclarent bénéficier d'un bon niveau de protection. Un niveau perçu qui semble s'être renforcé d'une année sur l'autre (+6pts), même pour les petites collectivités de moins de 300 habitants et ce malgré un faible taux d'équipement en dispositifs de sécurité pour ces dernières.

Cependant, si les collectivités s'estiment globalement mieux protégées, elles ne sont pour autant pas mieux préparées en cas de cyberattaque. En effet, elles ne sont en moyenne que 14 % à se sentir bien préparées, principalement les collectivités de plus de 5.000 habitants (24%).

Et parmi celles qui considèrent être bien préparées, 78 % ne disposent pas ou ne savent pas si elles disposent d'une procédure de réaction en cas d'attaque.

3. Le manque de budget, de compétences et d'accompagnement restent des freins pour progresser

Des budgets qui restent majoritairement restreints surtout pour les plus petites collectivités

On ne constate pas d'évolution majeure des budgets consacrés à l'informatique et à la sécurité des systèmes d'une année sur l'autre. 73 % des petites et moyennes collectivités ont un budget informatique annuel de moins de 5.000 euros et 66 % n'envisagent pas d'évolution à la hausse pour l'année à venir même pour les collectivités qui considèrent être fortement exposées aux risques. Quant au budget consacré à la cybersécurité, 77 % des élus et agents indiquent dépenser moins de 2.000€. Seules 10% des collectivités déclarent revoir à la hausse leur budget dédié à la sécurité informatique. Une situation encore plus contrastée selon la taille des collectivités puisque cette hausse ne concernerait que 5% des communes de moins de 1.000 contre 23% des plus de 1.000.

Une nécessité d'accompagnement et de sensibilisation

Parmi les principaux freins leurs permettant d'atteindre un bon niveau en sécurité informatique, ces collectivités pointent du doigt le manque de connaissances sur le sujet (47%), de compétences (36%) et de budget (36 %). Mais également, elles ne se sentent pas en capacité de juger les solutions de cybersécurité proposées aujourd'hui. 70% d'entre elles ne sont pas en mesure d'évaluer si les offres sont adaptées à leurs besoins.

62 % des collectivités appellent à une sensibilisation accrue des élus et agents. La mise en place d'outils de sécurisation (54%) et un accompagnement financier (45%) sont également au cœur des attentes, afin d'aider les territoires à mieux se préparer pour faire face aux menaces numériques en les aidant à se sécuriser en amont.

Enfin, pour s'informer ou se faire aider sur le sujet de la sécurité informatique, les petites et moyennes collectivités se tournent principalement vers leur prestataire informatique (66%) et les services territoriaux (29%). Cybermalveillance.gouv.fr reste un acteur bien identifié en particulier dans les collectivités de plus de 1.000 habitants (seules 9 % des collectivités de – de 1.000 habitants se tournent vers Cybermalveillance.gouv.fr contre 46 % des collectivités de plus de 10.000 habitants).

LA SECURITE EST L'AFFAIRE DE TOUS.