HarfangLab

LES DÉFIS DE LA CYBERSÉCURITÉ DANS LES COLLECTIVITÉS TERRITORIALES.

Enquête sur la maturité cyber des collectivités territoriales françaises. Quels sont leurs freins ? Quels sont leurs enjeux ? Quelle place pour la cybersécurité dans un environnement en tensions ?

2024

INTRODUCTION :

En 2024, la cybersécurité des collectivités territoriales en France est devenue une priorité nationale. En raison de la numérisation croissante des services publics, allant des systèmes de gestion administrative aux services en ligne pour les citoyens, les collectivités locales sont de plus en plus exposées aux cyberattaques. Selon le rapport de l'ANSSI pour l'année 2023, plusieurs dizaines d'incidents majeurs de cybersécurité ont été rapportés dans les collectivités territoriales, incluant des attaques par ransomware, des vols de données et des dénis de service.

Ce phénomène s'inscrit dans un contexte où les usages et outils numérique se multiplient et se diversifient, impliquant également un accroissement des risques cyber. On pense par exemple à l'adoption rapide, et massive de l'intelligence artificielle générative, qui accroit la surface d'attaque des organisations qui ne l'utilisent pas dans un contexte sécurisé, ou sans précautions de sécurité. Tous les secteurs sont impactés, allant des institutions aux grandes et petites entreprises, sans oublier les collectivités territoriales. Ces dernières, en particulier, rencontrent des difficultés à se protéger en raison de moyens financiers restreints et d'une difficulté à attirer les experts en cybersécurité, qui se font rares à l'échelle mondiale. Les enjeux de la cybersécurité pour les collectivités territoriales sont nombreux et cruciaux.

Premièrement, il s'agit de protéger les données sensibles des citoyens, comme les informations personnelles et les données financières, souvent ciblées par les cybercriminels. Une fuite ou une perte de ces informations peut entraîner des conséquences désastreuses pour les individus concernés et éroder la confiance des citoyens envers leurs administrations locales.

Deuxièmement, la continuité des services publics est en jeu. Une cyberattaque réussie peut paralyser les systèmes informatiques de la collectivité, rendant indisponibles des services essentiels d'eau, la gestion des déchets, ou encore les services de secours et d'urgence. La résilience de ces services est donc primordiale pour assurer le bon fonctionnement de la vie quotidienne des citoyens. Nous avons tous en mémoire des exemples récents de services publics complètement paralysés à la suite d'une cyberattaque, comme la Mairie d'Angers, victime d'un ransomware en 2020. Il lui a fallu plusieurs mois, avant de recouvrir ses données mais surtout de rétablir divers services publics en ligne. Administrés comme employés de la Mairie devaient composer sans le numérique, rallongeant considérablement certains délais de traitement.

Ensuite, le contexte national et international joue également un rôle important dans l'évolution du risque cyber, compte tenu des liens de plus en plus étroits entre l'espace numérique et l'espace cinétique, mais aussi de la montée en compétences et en organisation des groupes d'attaquants. D'opportunistes à hacktivistes en passant par des acteurs sponsorisés par des États, œuvrant à déstabiliser ou soumettre une économie, ou un pays tout entier, l'enjeu de cybersécurité pour les collectivités françaises dépasse aujourd'hui le simple contexte national.

À l'aune des Jeux Olympiques et Paralympiques de Paris 2024, des élections législatives ou encore des conflits internationaux, accompagner les organisations publiques, et privées, du vieux continent dans leur montée en résilience cyber est un enjeu crucial tant l'exposition nous rend vulnérables. Si l'on ajoute à ce contexte tendu, un certain nombre de lois extraterritoriales contraignantes mises en oeuvre par certains États, l'Europe se retrouve prise dans un étau numérique remettant en question son autonomie stratégique d'un point de vue technologique, et sécuritaire. C'est dans ce contexte d'ailleurs que la France a lancé un programme ambitieux, le plan « France 2030 », qui s'inscrit dans la lignée du plan France relance et qui vise à renforcer la protection des infrastructures nationales, à soutenir l'innovation technologique, à combler le déficit de compétences, et à positionner le pays comme un leader mondial en cybersécurité.

Enfin, en réponse à ce contexte international, les collectivités territoriales doivent se conformer à des réglementations de plus en plus strictes en matière de protection des données et de cybersécurité. Cela inclut le Règlement Général sur la Protection des Données (RGPD), en vigueur depuis maintenant 6 ans, et bientôt la directive NIS 2 qui s'appliquera également les établissements publics. Bien qu'ils ne soient pas soumises à des amendes en cas de non- conformité, les sanctions, ajoutent une pression supplémentaire sur les RSSI. Pour autant, ces normes représentent de véritables opportunités pour renforcer la résilience cyber, un réel enjeu face à la réalité des menaces cyber actuelles.

Face à ces défis, les collectivités territoriales doivent adopter des stratégies de cybersécurité robustes et adaptées. Cela inclut la formation du personnel, la mise en place de systèmes de surveillance et de détection des menaces, ainsi que la collaboration avec des experts et d'autres collectivités pour partager les bonnes pratiques et les informations sur les menaces émergentes.

C'est pourquoi, pour comprendre la maturité cyber des collectivités territoriales, les disparités sur le terrain, ainsi que les principaux freins et enjeux qui préoccupent les responsables informatiques du secteur public français, HarfangLab a commissionné InfoPro Digital pour mener une étude auprès de 201 collectivités territoriales à travers la France. Le présent rapport détaille les enseignements de cette étude et apporte des pistes et des conseils pour accompagner les collectivités territoriales vers une montée en maturité, et en résilience, cyber.

NOTE SUR LA MÉTHODOLOGIE

L'étude a été menée par le cabinet Infopro digital avec la méthode d'auto-administration en ligne (CAWI) auprès d'une cible d'élus, DGS/DGA, Directeur de cabinet et Directeur de service des collectivités territoriales. L'étude a été menée du 8 au 24 avril 2024 et compte 201 répondants, répartis à travers la France parmi des collectivités de tailles différentes, à la fois situées en zones urbaines et rurales.

A PROPOS D'HARFANGLAB :

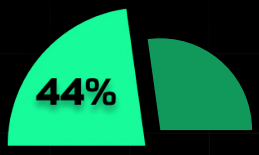
Harfanglab est une entreprise de cybersécurité française, fondée en 2018 et spécialisée dans la sécurité du endpoint. Elle fournit des logiciels EDR et antivirus afin de protéger les organisations contre toutes les menaces cyber, connues et inconnues. Premier EDR certifié par l'ANSSI, Harfanglab protège aujourd'hui plus d'un million de terminaux d'organisations publiques et privées européennes.

Basé à Paris, HarfangLab est un spécialiste européen de la cybersécurité qui aide les organisations à renforcer leur cyber-résilience globale grâce à sa suite logicielle de sécurité des terminaux de pointe, composée de 5 moteurs de détection complémentaires. Disposant d'une expertise technique très avancée, HarfangLab intègre des moteurs comportementaux, d'intelligence artificielle, de signatures, d'indicateurs de compromissions, et spécialisé dans la détection des ransomwares. L'entreprise développe ses propres modèles d'intelligence artificielle, intégrés directement dans l'agent unique, léger, n'affectant pas la productivité et l'efficacité des machines. Depuis 2023, HarfangLab dispose également d'une équipe de recherche en cybersécurité, lui permettant de contribuer à l'effort international de renseignement sur la menace et de lutte contre les attaques les plus avancées.

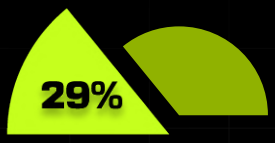
Le logiciel de HarfangLab est l'une des meilleures solutions EDR sur le marché, comme le prouvent ses excellents résultats aux évaluations MITRE ATT&CK de 2023 et les retours de ses clients. L'entreprise offre une option de confiance à ses utilisateurs qui comprennent plusieurs agences gouvernementales, entreprises et organisations internationales opérant dans des secteurs hautement sensibles, mais également un grand nombre d'entités publiques, collectivités territoriales et petites et moyennes entreprises.

HarfangLab

DES COLLECTIVITÉS ENGAGÉES EN MATIÈRE DE CYBERSÉCURITÉ.

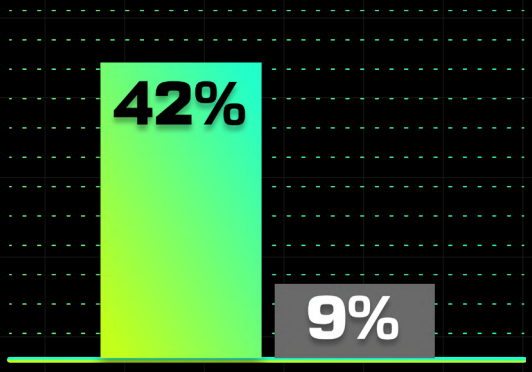


La moitié des collectivités interrogées considère la cybersécurité comme une priorité.

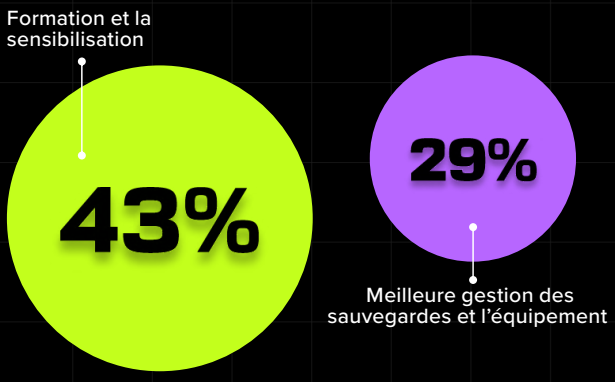


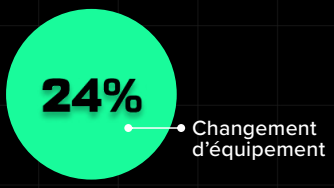
Seul un quart d'entre-elles estime être en avance sur le sujet.

Les élus et agents adhèrent facilement aux problématiques de cybersécurité (42%) mais certains (9%) y sont encore réfractaires.

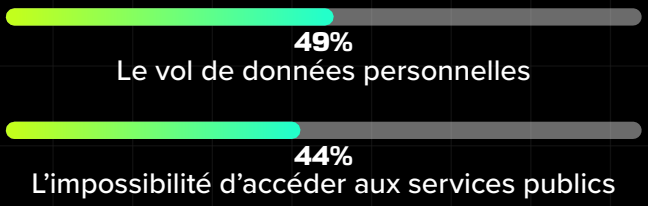


La formation et la sensibilisation, la meilleure gestion des sauvegardes et l'équipement ou le changement d'équipement arrivent dans le top des mesures prises par les collectivités après une cyberattaques.

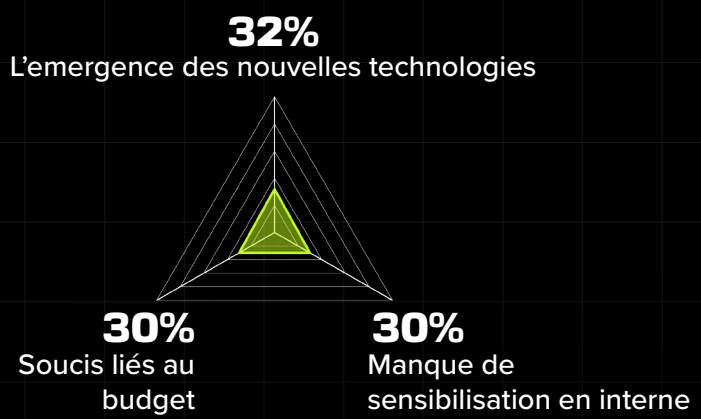


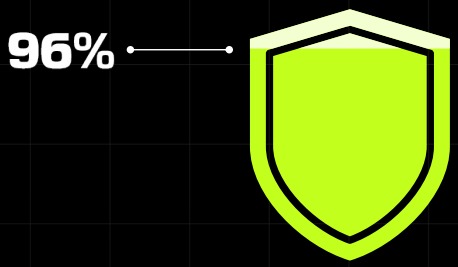


PRINCIPALES CRAINTES CYBER :



FREINS PRINCIPAUX POUR LA CYBERSÉCURITÉ :





PERCEPTION DU RISQUE CYBER & MATURITÉ AU SEIN DES COLLECTIVITES TERRITORIALES

APERÇU DU CONTEXTE INTERNATIONAL ET DES DIFFÉRENTS TYPES DE MENACES CYBER

Alors que les collectivités territoriales sont de plus en plus sensibilisées au risque cyber, et alertes quant à la nécessité de s'y préparer et d'y faire face, la réalité du paysage de ces menaces accroit pourtant leur exposition. En témoigne l'événement annuel, le CoTer, au sein duquel les responsables informatiques des différentes collectivités territoriales se retrouvent pour échanger sur les bonnes pratiques en matière de numérique et de cybersécurité, mais également pour aller à la rencontre des éditeurs et des experts du métier. La numérisation en croissance constante et la dépendance aux services et outils numériques les rend d'autant plus vulnérables. Sans oublier la problématique des ressources, tant financières qu'humaines, qui affecte les organisations du monde entier. Le secteur public, en particulier, peine à rivaliser avec les grandes entreprises privées pour le recrutement des talents et l'investissement, régis par des règles différentes.
Bien que l'ANSSI se soit activement engagée à accompagner et sensibiliser les collectivités territoriales pour renforcer leur maturité et résilience en cybersécurité, la réalité est qu'entre janvier 2022 et juillet 2023, l'agence a traité 187 incidents cyber affectant les collectivités territoriales, soit environ dix incidents par mois. Cela représente approximativement 17 % de l'ensemble des incidents traités par l'ANSSI sur la période, et les conséquences sont souvent très lourdes.

Lors d'un échange dans le cadre d'un enregistrement de podcast avec Antoine Trillard, DSI de la ville de Chelles et Président du CoTer lors d'une interview, il indiquait

« Des retours d'expérience que j'ai pu entendre, des collectivités ont perdu leurs données, voire leurs sauvegardes. Il a également fallu reparamétrer des centaines de logiciels, et parfois même reconstruire toute l'infrastructure. Dans certaines collectivités, les services publics sont bloqués pendant plusieurs mois, le temps de reconstruire le système d'information. Il faut fonctionner en mode dégradé, alors que nous avions justement accéléré la dématérialisation de nos services et procédures. Nous ne sommes pas toujours préparés à fonctionner sans nos services numériques. »

Si l'on se penche sur les risques cyber les plus fréquents auxquels sont exposées les collectivités territoriales, voici un petit palmarès :

1. **LES ATTAQUES PAR RANSOMWARE**, qui bloquent l'accès aux données et aux systèmes, exigeant une rançon pour leur restitution. Actuellement, les attaquants peuvent également exfiltrer les données sensibles et menacer de les divulguer en cas de non-paiement de la rançon, ou détruire l'intégralité des données. Cette menace peut paralyser les services publics essentiels et causer du tort à la collectivité, et ses administrés.

2. **LE PHISHING**, qui est souvent une méthode pour ensuite déployer un ransomware, ou un autre type de malware sur les systèmes d'information. Il s'agit d'une attaque souvent liée à de l'ingénierie sociale, ayant pour objectif de piéger les employés afin qu'ils cliquent sur un lien malveillant ou divulguent des informations sensibles. Le phishing est aujourd'hui de plus en plus crédibles et cela reste l'un des principaux vecteurs d'attaques cyber.

3. **ATTAQUES PAR DÉNI DE SERVICE** (DDoS) qui surchargent les systèmes et les réseaux, rendant les services publics indisponibles. Elles peuvent être particulièrement perturbantes pour les sites web et les services en ligne des collectivités.

4. **L'EXPLOITATION DES FAILLES DE SÉCURITÉ :** les attaquants profitent des failles non corrigées dans les programmes ou les systèmes pour infiltrer les réseaux et voler des données ou installer des logiciels malveillants. C'est une problématique fréquemment rencontrée lorsque le suivi et la gestion du parc informatique n'est pas 100% maitrisé. On peut citer l'exemple de l'exploitation de failles PowerShell qui sont courantes.

5. **CYBER-ESPIONNAGE :** les collectivités, plutôt les plus grandes et les plus exposées peuvent être ciblées pour l'espionnage, visant à obtenir des informations stratégiques ou sensibles.

6. **ATTAQUES SUR LES INFRASTRUCTURES CRITIQUES**, telles que l'eau, l'électricité, et les transports pour des sabotages ou des perturbations. C'est souvent l'œuvre de groupes sponsorisés par des États et l'une des principales menaces à craindre dans le cadre de conflits géopolitiques.

7. **MALVEILLANCE INTERNE :** les employés, actuels ou anciens, peuvent, intentionnellement, causer des incidents de cybersécurité en accédant à des informations sensibles ou en compromettant des systèmes.

A noter également, la multiplication des nouvelles technologies et une rapide adoption, notamment de l'intelligence artificielle qui, utilisée dans un contexte non sécurisé et sans les formations appropriées peut également accroitre l'exposition des collectivités au risque cyber. Pour atténuer ces risques, les collectivités territoriales doivent adopter une approche de cybersécurité robuste incluant la formation du personnel, la mise à jour régulière des systèmes, l'implémentation de politiques de sécurité strictes, et la collaboration avec des experts en cybersécurité.

Intéressons-nous désormais à la perception de la menace dans les collectivités territoriales.

ANALYSE DES RÉSULTATS DE L'ENQUÊTE VIS-À-VIS DE L'EXPOSITION AU RISQUE CYBER ET DE LA MATURITÉ DES ORGANISATIONS SUR LE SUJET DE LA CYBERSÉCURITÉ.

Nous avons souhaité comprendre la perception des collectivités vis-à-vis de l'état de la menace cyber mais également de leur maturité pour faire face à cette réalité.
On constate beaucoup de disparités dans l'évaluation de la maturité d'une collectivité en matière de cybersécurité.

En effet, 29% des répondants s'estiment en avance sur ce point-là tant au niveau de leur stratégie que de leurs investissements. Ces résultats sont particulièrement probants dans les communes urbaines, pour lesquelles ce pourcentage atteint 44% de collectivités en avance. En parallèle, et en opposition, pour les communes rurales, seules 24% s'estiment en avance sur le sujet.

Un peu moins d'un tiers des répondants (31%) s'estiment en retard sur le sujet de la cybersécurité, au regard de leurs investissements, de la sensibilisation ou des actions menées en matière de prévention. C'est particulièrement le cas des plus petites communes et collectivités comptant moins de 5000 administrés, où 40% s'estiment même en retard, voire très en retard sur la question de la cybersécurité. Dans les communes de plus de 100 000 habitants, 20% des participants s'estiment en retard sur les sujets cyber, et 46% plutôt en avance.

36%, soit un peu plus d'un tiers se considèrent à niveau en la matière, ayant déployé outils et méthodes en ligne avec la réalité de leur exposition aux menaces. Nous reviendrons plus tard sur les outils déployés et leur approche de la cybersécurité.

EN MATIÈRE DE CYBERSÉCURITÉ, DIRIEZ-VOUS QUE VOTRE COLLECTIVITÉ EST :

- **7%** Très en avance
- **22%** Plutôt en avance
- **36%** A niveau
- **24%** Plutôt en retard
- **7%** Très en retard
- **3%** Ne sait pas

« La question de la maturité est assez subjective en soit, et il est souvent difficile, excepté dans le cadre de la comparaison, d'évaluer une avance ou un retard en particulier sur le sujet de la cybersécurité. L'idée est de questionner sa résilience : est-ce que l'investissement dans des mesures de cybersécurité est anticipé où est-ce qu'il fait suite à une cyber-attaque ? Est-ce que des plans de sauvegarde et de reprise d'activité sont prévus ? Une cellule de crise est-elle en place en cas d'attaque cyber ? Qui gère la cybersécurité en interne, est-ce que les systèmes sont bien à jour et est-ce qu'on a confiance dans les outils déployés ? Surtout en cas de difficulté pour répondre à toutes ces questions, des ressources de confiance existent et il ne faut pas hésiter à s'appuyer dessus : celles de l'ANSSI, de cybermalveillance.gouv.fr ou encore de partenaires privés experts sur le secteur public et ses enjeux »

Anouck Teiller, Chief Strategy Officer at Harfanglab

Lorsque l'on interroge les collectivités territoriales sur leurs principales craintes en matière de conséquences d'une cyberattaque, beaucoup mettent en avant la sensibilité des données traitées et le risque de vol. En effet, 49% des répondants considèrent cela comme leur principale préoccupation. Viennent ensuite la crainte de la destruction d'un système d'information et de l'inaccessibilité des services publics en ligne (44%), ainsi que la fuite d'information (38%). La demande de rançon (34%), le cyber-espionnage (13%), les attaques ciblées et la fraude externe sont également mentionnés.

QUEL TYPE DE CYBERATTAQUE REDOUTEZ-VOUS LE PLUS POUR VOTRE COLLECTIVITÉ ?

- **49%** Vol de données personnelles
- **44%** Destruction/Inaccessibilité des services publics en ligne
- **38%** Vol/Fuite d'informations
- **34%** Demande de rançon (Ransomware/Rançongiciel)
- **18%** Attaque ciblée
- **15%** Fraude externe
- **13%** Cyber-espionnage
- **8%** Cryptominage (Exploitation de ressources matérielles pour générer des crypto-monnaies)

« La spécificité des collectivités territoriales s'illustre bien dans les problématiques qu'elles rencontrent. A l'inverse des entreprises qui craignent surtout le risque réputationnel et financier, pour les collectivités territoriales, les principales craintes tiennent de la sécurité de leurs administrés et de l'accessibilité des services publics qui peuvent handicaper le fonctionnement de nombreux services publics comme les écoles, les formalités administratives, l'état civil, les infrastructures publiques etc. Pour autant en matière de protection, les mêmes recommandations s'appliquent aux collectivités qu'aux entreprises : gestion des vulnérabilité, déploiement d'outils de protection des terminaux, sensibilisation aux bonnes pratiques, investissement humain & technologique, etc. »

Anouck Teiller, Chief Strategy Officer at Harfanglab

Ce sujet de la protection des données sensibles identifié dans les collectivités, s'illustre aussi dans leurs attentes, en matière d'équipement et d'accompagnement. Lorsqu'on les interroge au sujet de leurs attentes et besoins afin de répondre à ces enjeux, la plupart indiquent qu'ils aimeraient un meilleur soutien financier de l'État, davantage d'aides financières et de moyens de manière générale. Ils attendent aussi de la part de l'État un accompagnement au niveau de la sensibilisation aux bonnes pratiques cyber. Beaucoup souhaitent également plus de confiance, de fiabilité dans les outils et notamment dans les plateformes de sauvegarde, de traitement des données pour permettre plus de sécurité. 29% des répondants attendent des professionnels des solutions pour assurer une meilleure protection des données sensibles.

« Les collectivités territoriales ont des activités très sensibles, tout en disposant souvent de moins de moyens, de plus de contraintes et de réglementations en matière d'investissement et d'équipement que les entreprises de taille équivalente. La cybersécurité ne fait pas exception. Il est donc crucial pour elles de pouvoir collaborer avec des tiers de confiance et de bénéficier du soutien et de l'accompagnement de l'État, des régions, etc., pour améliorer leur cybersécurité. Chez HarfangLab, nous sommes très fiers d'accompagner aujourd'hui un grand nombre de collectivités territoriales et établissements publics dans leurs efforts de sécurisation. »

Anouck Teiller, Chief Strategy Officer at Harfanglab

UN APERÇU DU PLAN FRANCE 2030 LANCÉ PAR L'ÉTAT.

Le plan « France 2030 » est une initiative ambitieuse du gouvernement français visant à renforcer la protection des infrastructures nationales, à soutenir l'innovation technologique, à combler le déficit de compétences, dans le but de positionner la France comme un leader mondial en cybersécurité. En matière de cybersécurité, cela s'illustre notamment par des investissements massifs pour développer les technologies pertinentes, soutenir la recherche et l'innovation, ainsi que renforcer les capacités de détection et réponse aux cybermenaces. Il prévoit aussi des fonds pour former des experts pour palier à terme à la pénurie de talents et de professionnels qualifiés. Ce plan propose, entre autres mesures, des subventions pour aider les infrastructures publiques et les petites et moyennes entreprises à renforcer leur maturité en cybersécurité et s'équiper adéquatement. Il inclut également l'intensification de la coopération internationale, et la modernisation des infrastructures critiques.

QUEL IMPACT CONCRET POUR LES COLLECTIVITÉS ?

Les collectivités territoriales peuvent bénéficier de plusieurs aides et initiatives prévues dans le cadre du plan « France 2030 » pour améliorer leur maturité en cybersécurité. Voici quelques-unes des principales mesures :

FINANCEMENTS ET SUBVENTIONS :
Le plan « France 2030 » prévoit des financements spécifiques pour les collectivités territoriales afin de les aider à investir dans des technologies de cybersécurité avancées et à moderniser leurs infrastructures. Des subventions peuvent également être accordées pour des projets spécifiques visant à renforcer la sécurité informatique.

FORMATIONS ET CERTIFICATIONS :
Des programmes de formation et de certification en cybersécurité peuvent être mis en place pour les agents des collectivités territoriales. Cela inclut des formations continues, des ateliers pratiques et des certifications reconnues pour développer les compétences en cybersécurité au sein des équipes locales.

DES PARTENARIATS PUBLIC-PRIVÉ :
Le plan encourage la création de partenariats entre les collectivités territoriales, les entreprises de cybersécurité, et les instituts de recherche. Ces accords peuvent faciliter l'accès à des expertises, des technologies innovantes et des solutions adaptées aux besoins spécifiques des collectivités locales.

ACCOMPAGNEMENT ET CONSEIL :
Des dispositifs d'accompagnement et de conseil seront disponibles pour aider à évaluer leur niveau de maturité en cybersécurité et à élaborer des plans d'action adaptés. Des audits de sécurité, des analyses de risques et des conseils personnalisés peuvent être fournis par des experts en cybersécurité.

SENSIBILISATION ET CAMPAGNES DE COMMUNICATION:
Des campagnes de sensibilisation seront organisées pour informer les responsables et les agents des collectivités sur l'importance de la cybersécurité et sur les mesures à prendre pour se protéger contre les cybermenaces. Ces campagnes peuvent inclure des séminaires, des conférences et des supports de communication adaptés.

RENFORCEMENT DE LA COOPÉRATION INTERINSTITUTIONNELLE :
Le plan « France 2030 » favorise la coopération entre les différentes collectivités territoriales, les agences gouvernementales et l'autorité nationale de cybersécurité l'ANSSI. Cette coopération permet un partage d'expériences et une mutualisation des ressources pour mieux répondre aux défis de cybersécurité.

QUELLE EXPOSITION RÉELLE AUX MENACES ET QUELLES ACTIONS MISES EN ŒUVRE POUR RÉPONDRE À CES MENACES ?

En matière d'exposition aux cyberattaques, la perception est également assez disparate entre les différentes collectivités. 53% des répondants indiquent se sentir très exposés aux cyberattaques, alors que 42% ne s'estiment pas du tout exposés. Si on regarde la répartition des participants en fonction de la taille et du type de leur collectivités, on peut remarquer d'autres grands écarts.
Si les collectivités de moins de 5 000 habitants répondent à 60% ne pas se sentir exposées, les agglomérations de plus de 100 000 habitants se sentent elles, exposées aux cyberattaques pour plus de 71% d'entre-elles. Si 59% des communes urbaines s'estiment menacées, seules 41% des communes rurales se considèrent comme à risque.

En effet, 29% des répondants s'estiment plutôt en avance sur ce point-là tant au niveau de leur stratégie que de leurs investissements. Ces résultats sont particulièrement probants dans les communes urbaines, pour lesquelles ce pourcentage atteint 44% de collectivités en avance. En parallèle, et en opposition, pour les communes rurales, seules 24% s'estiment en avance sur le sujet.

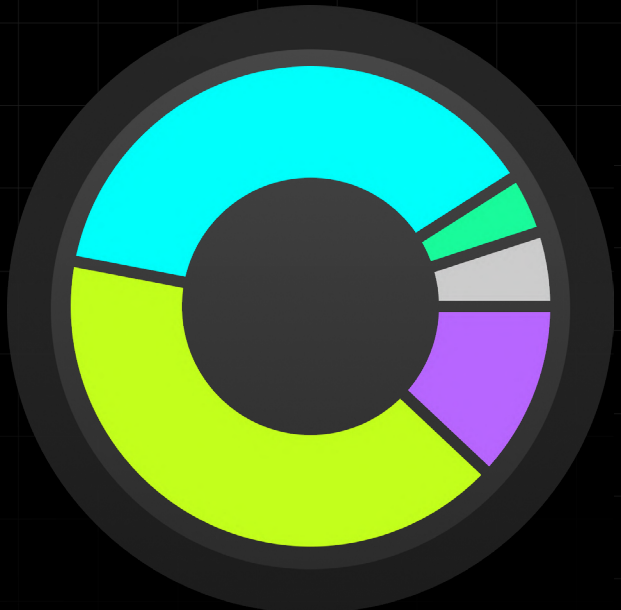
Lorsque l'on interroge notre panel de répondants sur le fait d'avoir déjà été victimes ou non de cyberattaques, 7% indiquent qu'elles n'en ont aucune idée. Cela peut paraitre surprenant, mais rappelons que de nombreuses intrusions peuvent être furtives et passer inaperçues pendant un certain temps. 55% des collectivités indiquent n'avoir jamais été attaquées, 37% estiment avoir déjà subi à minima une cyberattaque : 25% une seule fois, et 17% attestent avoir été attaquées plusieurs fois.

La question qui se pose est celle du lien de causalité entre les cyberattaques, les mesures prises, et la perception de la d'une collectivité en cybersécurité. On observe souvent que les mesures d'équipement en cybersécurité sont mises en place après qu'une attaque ait eu lieu, lorsque les impacts et les dégâts sur le fonctionnement de la collectivité deviennent évidents.

Parmi les principales mesures prises à la suite de cyberattaques, la formation et sensibilisation des salariés des collectivités (43%) suivi par la collaboration avec des entreprises de conseil en cybersécurité (33%) et une meilleure gestion des sauvegardes (29%) arrivent en tête.

Seuls 23% estiment avoir un dispositif de gestion de crise en place dans leur collectivité. 24% ont recruté des profils experts en cybersécurité à la suite d'un incident de sécurité et 24% se sont équipés d'outils (antivirus, EDR) ou ont changé leur équipement après une cyberattaque.

TROUVEZ-VOUS QUE VOTRE COLLECTIVITÉ EST :



- **41%** Assez exposée
- **38%** Peu exposée
- **12%** Fortement exposée
- **4%** Pas du tout exposée
- **5%** Ne sait pas

Antoine Trillard, DSI de la ville de Chelles et Président du CoTer revient sur les transformations réalisées en matière de cybersécurité depuis la cyberattaque vécue en 2019 sur sa commune :

« Avant l'attaque, nous étions moins regardants sur les mises à jour ou les accès aux postes de travail par exemple. Aujourd'hui on ne laisse plus passer les mauvaises pratiques. Nous avons mis en place l'authentification multi-facteurs, un durcissement des politiques de mises à jour, des mots de passe, et des comptes utilisateurs. Personne n'a le droit de se connecter à son PC avec un compte admin par exemple. Que ce soit l'ingénieur sécurité ou moi-même, nous utilisons un compte utilisateur classique. Nous avons également placé nos efforts dans le durcissement de l'Active Directory, et nous avons acquis de nouveaux outils qui nous permettent de nous sentir un peu plus sereins qu'en 2019. Entre la cybersécurité de la ville de Chelles de 2019, et celle de 2024, c'est le jour et la nuit. »

COMMENT SE PRÉPARER À UN INCIDENT CYBER ET Y FAIRE FACE ?

ANTICIPATION : La maîtrise des risques nécessite une parfaite connaissance du système d'information, des actifs et des données critiques, ainsi qu'une compréhension des menaces et du contexte. Un incident de sécurité nécessite également de pouvoir déployer rapidement une cellule de crise pour gérer les sujets techniques et de communication. Les exercices de simulation sont essentiels pour s'y préparer.

DÉTECTION : Une détection efficace nécessite des outils et des ressources adaptés. Plus précisément, le Système d'Information doit être protégé par des solutions pertinentes et performantes qui doivent être mises en place et gérées par un personnel expert – en interne ou par l'intermédiaire de partenaires.

ANALYSE : Une fois qu'un outil a détecté un événement de sécurité, les experts doivent évaluer sa criticité et le documenter, afin de définir les actions à entreprendre.
Cette étape vise également à comprendre la menace et les objectifs des attaquants, afin de limiter sa propagation sur le moment et dans le futur.

RÉPONSE : Après une analyse de la situation, en fonction du contexte, les experts peuvent procéder au blocage de la menace, à l'arrêt des processus, à l'isolation des endpoints, à la mise en quarantaine des fichiers... Dans la perspective d'une récupération du système ou des données. Outre les aspects techniques, la phase de réponse peut également inclure des actions de communication interne et externe.

POST-MORTEM : L'analyse post-incident, ou post-mortem, permet de tirer des enseignements de l'incident, afin de renforcer la protection du Système d'Information et d'améliorer la sensibilisation des collaborateurs... et mieux anticiper les futures attaques.

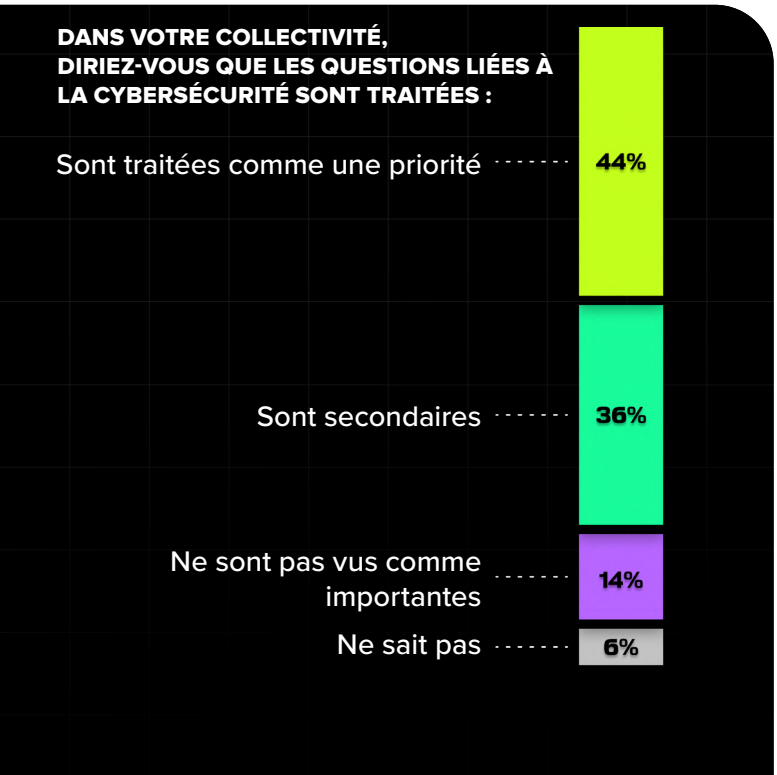
Le conseil d'expert :
Une bonne connaissance de l'infrastructure IT améliorer la détection des menaces et permet de savoir quelles actions et réponses sont nécessaires. Elle offre également une meilleure visibilité sur les actions des attaquants, facilite une réponse efficace et aide à identifier ce qui doit être nettoyé.

LA PLACE DE LA CYBERSÉCURITÉ DANS LES COLLECTIVITÉS TERRITORIALES

LA GOUVERNANCE

À la question « quel niveau de priorité est donné à la cybersécurité dans votre organisation ? », 36% des participants estiment qu'elle a une place secondaire, et 14% répondent même que le sujet est jugé comme « non important » au sein de leur organisation. Si on s'intéresse aux disparités en fonction de la taille et du type de collectivité, là encore, nous constatons quelques différences. Alors que 74% des collectivités de plus de 100 000 habitants mettent la cybersécurité comme une priorité absolue dans leur collectivité, ce n'est le cas que de 27% des collectivités de moins de 5 000 habitants. A l'inverse 22% des collectivités de moins de 5 000 habitants estiment que la cybersécurité n'est pas considérée comme importante.

Il est également intéressant de noter qu'à l'échelle des régions, ou dans les communes urbaines, ces sujets cyber tendent à ressortir comme prioritaires avec 78% des régions, 60% des départements, et 56% des communes urbaines allant dans ce sens. À l'inverse, 28% seulement des communes rurales positionnent la cybersécurité comme prioritaires.



Pour déployer une stratégie de cybersécurité robuste, l'un des meilleurs conseils est de convaincre la direction de s'approprier les bonnes pratiques et de comprendre les enjeux de la cybersécurité. Cela permet d'instaurer une véritable culture de la cybersécurité au sein de l'organisation et de donner la priorité aux actions vivant à renforcer la résilience cyber sécurité. Bien que la situation soit différente dans les collectivités territoriales en raison de leur gouvernance distincte, et de la manière dont les budgets sont souvent votés, il reste crucial pour les DSI et RSSI de se sentir écoutés par leurs élus.

Dans notre étude, 42% des répondants estiment que les élus et agents adhèrent moyennement aux politiques de cybersécurité, et beaucoup de travail pour les convaincre. Ce chiffre est particulièrement élevé dans les collectivités s'estimant en retard sur le sujet de la cybersécurité puisqu'il atteint 56%. 42% considèrent au contraire, que les agents adhèrent facilement à la politique de cybersécurité – ce chiffre atteint 66% parmi les collectivités se jugeant en avance dans la cybersécurité.

« Jusqu'ici c'est plutôt logique et on voit bien que les répondants font le lien entre l'adhésion, l'implication et la formation des collaborateurs aux notions et bonnes pratiques de cybersécurité. Cela fait partie des clés pour développer une plus grande maturité et résilience cyber. L'inverse aurait été inquiétant, puisque les organisations auraient pu être persuadées de mettre en place de bonnes pratiques de cybersécurité, sans que leurs collaborateurs soient réellement impliqués dans cette démarche, où ils jouent pourtant un rôle essentiels. »

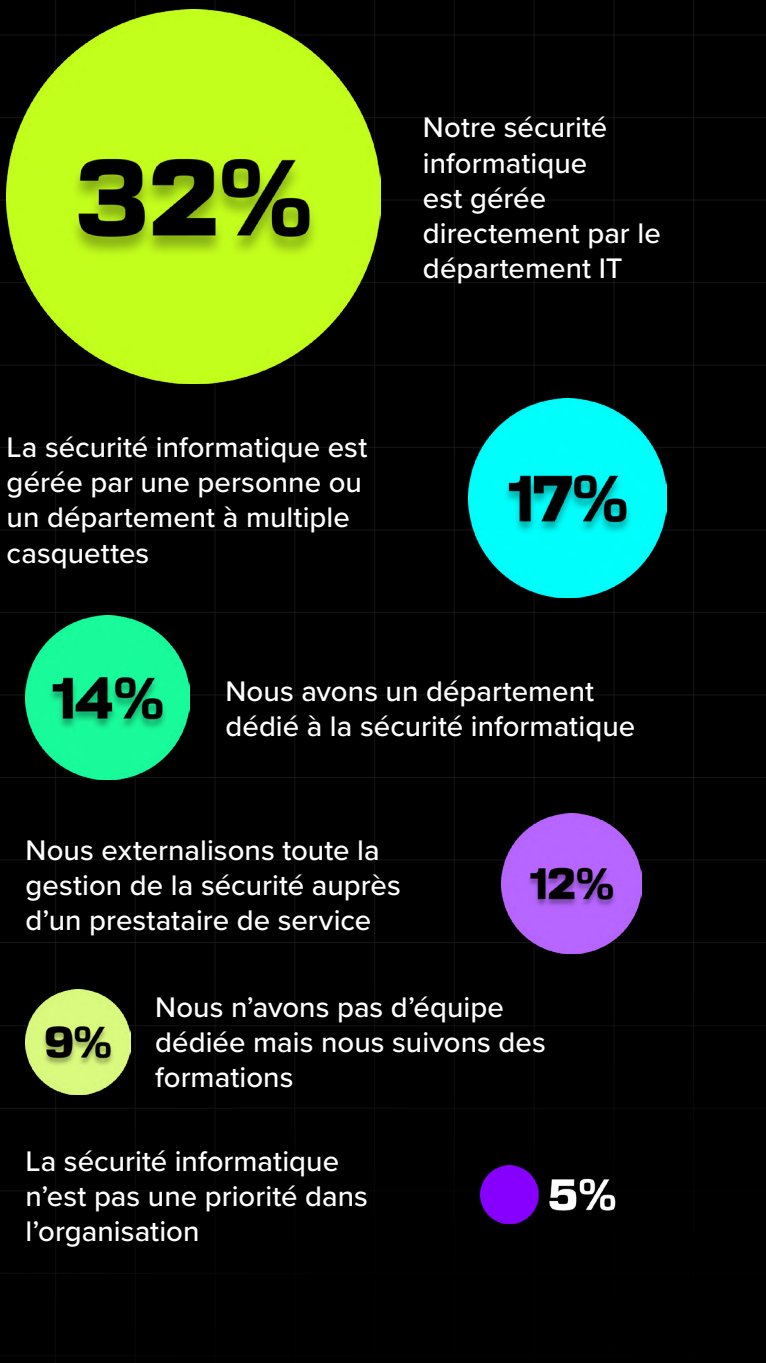
Anouck Teiller, Chief Strategy Officer at Harfanglab

41% des répondants estiment par ailleurs le risque de cyberattaques « élevé » à « très élevé » compte tenu du faible niveau de priorité donné à la cybersécurité dans leur organisation. 10% jugent même ce risque « extrême ». En parallèle, 27% des organisations quant à elles, estiment ce risque très faible. On observe donc de grandes disparités entre les organisations, révélant un manque d'harmonisation et une véritable inégalité entre les différentes collectivités territoriales. Les collectivités de plus de 10 000 administrés jugent ce risque beaucoup plus élevé (moyenne donnée au risque 6,5), que les plus petites collectivités (moyenne donnée au risque 4,7).

Du point de vue de la gouvernance et de l'organisation interne, cette étude a examiné la gestion interne de la cybersécurité. Elle s'est intéressée à savoir s'il existe un département dédié et si les responsables cumulent cette tâche avec d'autres fonctions. Pour 6% des répondants, aucune organisation spécifique n'existe dans leur collectivité. 12% externalisent à 100% la gestion de leur cybersécurité auprès d'experts tiers. 32% des participants révèlent que la question de la cybersécurité est intégrée directement à la direction informatique et 17% indiquent que la personne ou le département pertinent est en charge d'autres sujets en parallèle et qu'il ne s'agit pas d'une responsabilité à part entière. En parallèle, 14% des répondants indiquent avoir un département dédié et 5% confirment que la sécurité informatique n'est pas une priorité et que cela s'illustre aussi au niveau des ressources humaines impliquées dans la gestion de l'opérationnel. 9% admettent également ne pas avoir d'équipe dédiée ou de personnes gérant la question de la cybersécurité en interne mais que les employés suivent des formations à ce sujet pour être plus alertes quant aux bonnes pratiques.

On observe également de grandes disparités entre les différentes collectivités territoriales. Faire de la cybersécurité une priorité implique certes de mobiliser la direction et les salariés pour adopter de bonnes pratiques. Cependant cela nécessite aussi de déployer des d'équipes et des ressources dédiées à la sécurité informatique, quitte à les externaliser (via des MSSP ou MSP par exemple). La gestion du risque cyber nécessite des équipes et outils spécialisés.

COMMENT EST ORGANISÉE LA CYBERSÉCURITÉ DANS VOTRE COLLECTIVITÉ ?



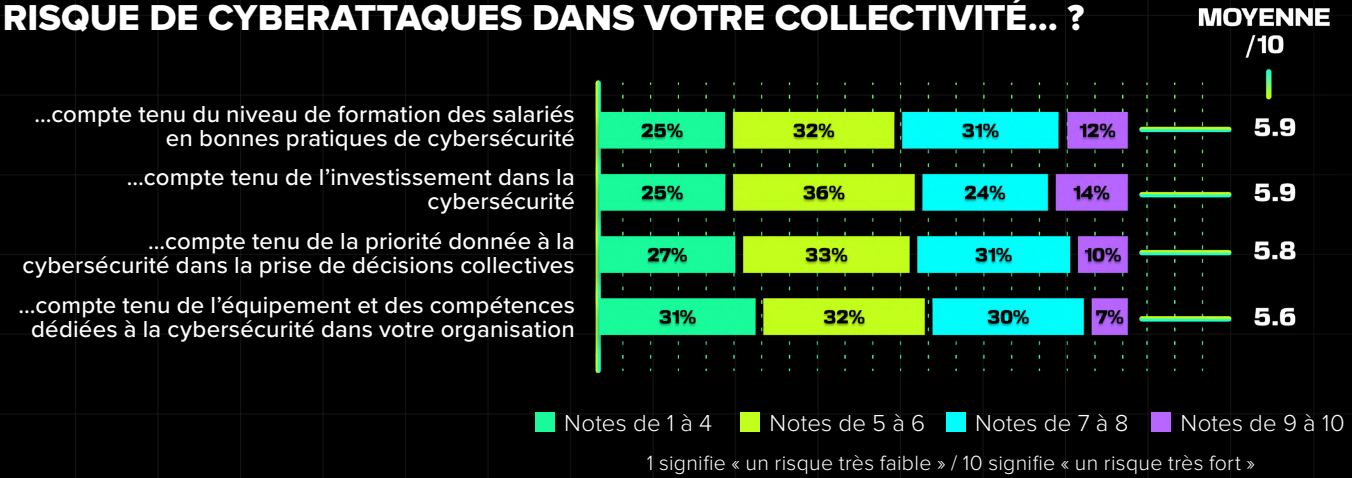
« On constate qu'il n'y a pas d'unanimité ou de procédure standardisée dans la gestion de la cybersécurité dans les collectivités territoriales. On voit bien qu'il reste un travail d'allignement notamment dans la nécessité de gouvernance cyber pour déployer une stratégie et de pratiques quotidiennes avec les recommandations des autorités, et la réalité des menaces. Positionner la cybersécurité comme une priorité, c'est certes impliquer la direction et les salariés dans la mise en œuvre de bonnes pratiques, mais c'est aussi déployer des équipes et ressources dédiées à la sécurité informatique, qui peuvent être internes ou externes. » commente Anouck Teiller.

LE BUDGET

25% des collectivités estiment être très peu exposées aux menaces grâce au budget investi dans la cybersécurité (note donnée de 1 à 4). 38% des répondants jugent le risque très élevé dans leur collectivité (note de 7 à 10, 10 étant un risque extrêmement élevé) notamment à cause d'un manque de budget. Toutefois, ce n'est rien par rapport aux 41% de répondants qui jugent le risque très élevé dans leur entreprise si on s'en réfère au niveau de priorité donné à la cybersécurité dans leur organisation.

Les collectivités s'estiment plutôt bien équipées et dotées de compétences en cybersécurité de haut niveau puisque seules 7% jugent le risque lié au manque de compétences et d'outils extrêmement élevé. Toutefois, on constate une certaine forme de prudence et de modération dans les propos, les notes de 5 à 8 étant les plus fréquemment données dans l'analyse de risque. Ainsi 62% des organisations jugent le risque « possible » voir « probable » en attribuant une note entre 5 et 8 à la menace liée au manque de compétences et d'équipement dans leur organisation.

QUELLE NOTE DE 1 À 10 METTRIEZ-VOUS AU NIVEAU DE RISQUE DE CYBERATTAQUES DANS VOTRE COLLECTIVITÉ... ?



1 signifie « un risque très faible » / 10 signifie « un risque très fort »

ENJEUX CYBER AUJOURD'HUI ET DEMAIN

LES FREINS AU DÉPLOIEMENT D'UNE STRATÉGIE CYBER

Les collectivités territoriales en France font face à plusieurs obstacles dans la mise en place de stratégies de cybersécurité robustes. Voici les principaux obstacles identifiés par les experts spécialisés dans le secteur public :

DES RESSOURCES FINANCIÈRES LIMITÉES :
les budgets des collectivités territoriales sont souvent restreints, ce qui limite les investissements dans des solutions avancées. Les coûts associés à l'acquisition de technologies de pointe, à la mise à jour des infrastructures existantes et à la formation du personnel peuvent être prohibitifs, où à minima sembler l'être.

UN MANQUE DE PERSONNEL QUALIFIÉ :
Dû à une pénurie de talents globale, mais aussi à un manque d'attractivité du secteur public vis-à-vis du privé. Les collectivités locales peinent à attirer et à retenir des experts en raison de la concurrence avec le secteur privé, où les salaires sont souvent plus attractifs.

LA COMPLEXITÉ TECHNOLOGIQUE D'UNE COLLECTIVITÉ TERRITORIALE :
La diversité des systèmes informatiques utilisés par les collectivités territoriales rend la gestion de la cybersécurité plus complexe. Les infrastructures héritées, parfois obsolètes, sont difficiles à sécuriser et à intégrer dans une stratégie cohérente.

LA SENSIBILISATION PARFOIS INSUFFISANTE :
La cybersécurité n'est pas toujours perçue comme une priorité par les décideurs locaux. Pour autant de nombreuses améliorations ont été constatées sur ce plan, en témoigne la popularité d'événements comme le CoTer sur lesquels les spécialistes en informatique des collectivités se retrouvent pour échanger sur les bonnes pratiques et outils ainsi que sur les enjeux. Le travail mené par l'ANSSI est également bénéfique dans l'amélioration de la sensibilisation à ces enjeux dans le secteur public.

LA RÈGLEMENTATION ET LA CONFORMITÉ :
La complexité des régulations, telles que le RGPD, et la nécessité de se conformer à des normes de sécurité peuvent représenter un défi. Les collectivités locales doivent souvent naviguer dans un cadre juridique et réglementaire en constante évolution, en témoignent les nouvelles exigences présentées dans le cadre de NIS 2.

L'INTEROPÉRABILITÉ ET LA COORDINATION :
La coordination entre différentes entités et niveaux de gouvernance peut être difficile. Les collectivités territoriales doivent collaborer avec les autorités nationales, les fournisseurs de services et les autres collectivités pour partager des informations et des ressources, ce qui peut s'avérer complexe.

ÉVOLUTION DES MENACES :
Les cybermenaces évoluent rapidement, rendant difficile la mise en place de mesures de sécurité capables de répondre à des attaques de plus en plus sophistiquées. Les collectivités locales doivent constamment adapter leurs stratégies pour faire face à de nouvelles vulnérabilités.

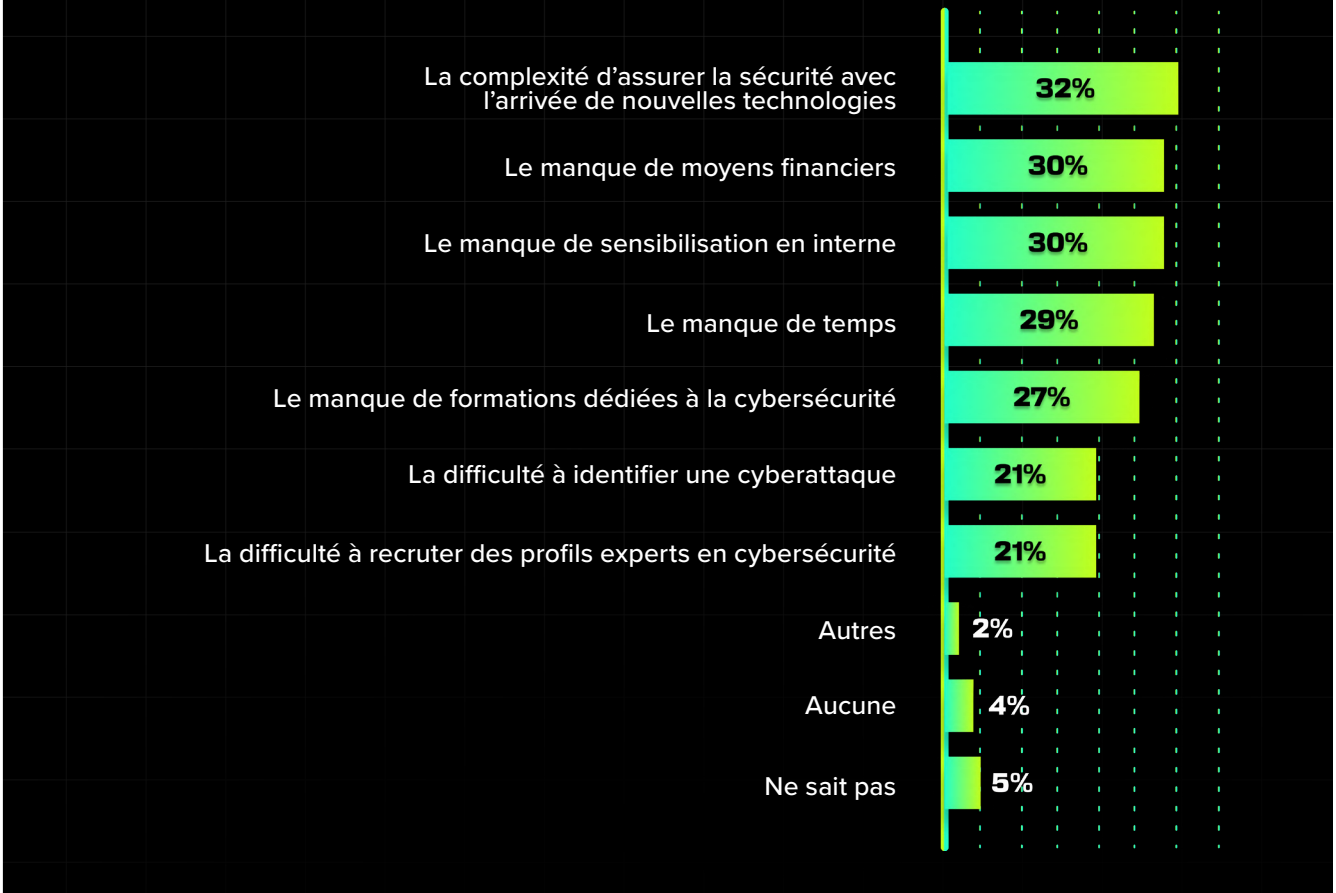
RÉACTIVITÉ ET GESTION DES INCIDENTS :
les capacités de réponse aux incidents de sécurité sont souvent limitées. Un manque de protocoles clairs et de plans d'urgence peut retarder la détection et la réponse aux cyberattaques, aggravant les dommages.

D'après les répondants à l'enquête menée pour ce rapport, les principaux obstacles à l'implémentation d'une stratégie de cybersécurité adaptées aux menaces sont le manque de sensibilisation interne pour plus de 30% d'entre eux, suivi par le manque de moyens financiers pour également 30% des participants. Plus important encore, la complexité de sécuriser les systèmes face à la rapidité de développement des nouvelles technologies complique la tâche pour 32% des interrogés. Sont également mentionnés le manque de temps pour 29% des répondants, et le manque de formations dédiées à la cybersécurité.

43% des collectivités estiment que le bas niveau de formation des salariés aux bonnes pratiques expose davantage leur collectivité au cyber-risque (de 7 à 10). Seuls 25% estiment le niveau suffisamment élevé pour ne pas exposer du tout leur organisation au risque (note de 0 à 4).

« La réduction des budgets de fonctionnement alloués aux collectivités affecte directement les dépenses dans la cybersécurité, notamment en ce qui concerne les logiciels. Les collectivités territoriales, se retrouvent avec l'enjeu colossal de devoir faire face à plus de menaces, plus de risques, plus de règlementations, malgré moins de moyens. C'est aussi aujourd'hui essentiel d'avoir conscience de cet état budgétaire pour proposer des approches en ligne avec ces réalités, tout en restant compétitives malgré tout » précise Anouck Teiller.

QUELLE(S) DIFFICULTÉ(S) RENCONTREZ-VOUS POUR LA MISE EN PLACE D'UNE STRATÉGIE DE CYBERSÉCURITÉ DANS VOTRE COLLECTIVITÉ ?



CONTEXTE ACTUEL ET NIVEAU DE LA MENACE

Pour les collectivités territoriales, ce qui expose le plus leur organisation au risque est surtout lié à des problématiques internes, à leur gestion, dépenses et gouvernance plus qu'à des problématiques externes (Jeux Olympiques, guerre en Ukraine etc.) 34% d'entre elles estiment que les guerres en Ukraine et à Gaza n'exposent pas ou très peu leur organisation au risque. 11% sont en revanche extrêmement inquiètes de l'impact de ces conflits sur leur cybersécurité en mettant des notes d'analyse du risque entre 9 et 10.

31% estiment que les Jeux Olympiques n'exposent pas ou très peu leur organisation au risque cyber (notes de 0 à 4) – en revanche 43% des collectivités estiment que cet événement sportif représentent un risque très élevé voire extrêmement élevé (notes de 7 à 10). Plus les collectivités sont grandes, plus le risque cyber identifié dans le contexte des Jeux est grand. Ainsi les collectivités de 100 à 500 000 habitants sont 64% à donner une note de 7 à 8 au risque contre 16% pour les organisations de 2 500 à 5 000 habitants. 33% des collectivités entre 5 000 et 10 000 habitants et 50% des collectivités comptant entre 10 000 et 50 000 habitants donnent également une note de 7 à 8 au niveau de risque cyber dans ce contexte.

Si l'on s'intéresse à la géographie des collectivités, contre toute attente, l'Ile-de-France qui accueillera une grande partie des Jeux Olympiques, n'est pas la région qui anticipe le plus haut niveau de risque de cyber menaces lors de l'événement avec une note moyenne de 6,3 donnée au risque en Ile de France contre 6,4 dans le Nord de la France. En examinant plus en détails les réponses, on constate que ceux qui attribuent la note la plus élevée correspondante au plus haut niveau de risque sont principalement les collectivités de l'Ile-de-France avec 21% de participants donnant une note entre 9 et 10, contre une moyenne nationale de 13%.

LE RISQUE CYBER PENDANT LES JEUX OLYMPIQUES ET PARALYMPIQUES (ET LES ÉVÉNEMENTS DE GRANDE AMPLEUR), POURQUOI EST-IL CROISSANT ?

A l'aune des Jeux Olympiques et Paralympiques de Paris 2024, la question de la cybersécurité dans les organisations et les collectivités territoriales est d'autant plus critique ; la surexposition de la France pendant cette période accroissant le risque cyber. En effet, cet événement attire l'attention mondiale, ce qui en fait une cible attrayante pour les cybercriminels et les hacktivistes cherchant à gagner en visibilité ou à perturber un événement de grande envergure.

De plus, la gestion des Jeux nécessite une augmentation substantielle des infrastructures numériques pour supporter le flux de données provenant des systèmes de billetterie, des communications, de la sécurité, et des diffusions en direct. Cette augmentation du trafic crée des opportunités pour les cyberattaques, notamment les attaques par déni de service (DDoS).

Les collectivités territoriales doivent coordonner leurs efforts avec divers organismes, y compris les autorités nationales, les services de sécurité, et les fournisseurs de technologies. Cette interconnexion des systèmes expose les collectivités locales à des vulnérabilités supplémentaires. De la même manière, compte tenu de l'aspect essentiel des infrastructures critiques, comme les réseaux de transport, les services de santé et les systèmes de gestion de l'eau pour le bon déroulement des Jeux Olympiques, ces dernières peuvent s'avérer attractives pour quiconque souhaiterait interférer avec le bon déroulement de l'événement. De plus, de par leur médiatisation, les Jeux peuvent attirer des acteurs motivés par des intentions politiques ou économiques, cherchant à collecter des informations sensibles ou à promouvoir une cause par des moyens cyber.

La planification et la gestion d'un tel événement implique de nombreux partenaires et prestataires, ce qui augmente la surface d'attaque. Chaque nouvelle connexion et intégration de système peut introduire des points d'entrée potentiels pour les cyberattaques. Enfin, la préparation des Jeux nécessite des efforts colossaux en matière de cybersécurité. Les collectivités territoriales doivent non seulement mettre en place des mesures préventives robustes mais aussi des plans de réponse aux incidents pour minimiser les impacts en cas d'attaque.

DÉFIS ET PERSPECTIVES DES RÈGLEMENTATIONS

La mise en application de la directive NIS 2 au sein des organisations est source de questionnements et d'incertitudes. Probablement parce qu'elle n'est pas encore retranscrite dans le droit français, 11% des collectivités ne savent pas comment se positionner sur le sujet et ignorent si la directive représente une opportunité ou une contrainte.

En revanche, dans les très grandes communes (de plus de 500 000 habitants), les réponses sont plus unanimes : 48% estiment que la mise en application de NIS 2 est surtout une opportunité pour améliorer son niveau de cybersécurité. L'autre moitié des participants estiment qu'il s'agit à la fois d'une opportunité et d'une contrainte. Bien que conscients des atouts d'une telle directive dans la démarche d'amélioration de la cybersécurité des organisations et collectivités territoriales, ils s'inquiètent toutefois du poids supplémentaire de ces règlementations sur leur organisation au quotidien et du chemin à parcourir pour être conformes. Les collectivités entre 100 000 et 500 000 habitants sont, elles, les plus tranchées : les directives telles que NIS 2 sont une réelle opportunité pour améliorer le niveau cyber global du secteur public en France pour près de 65% des répondants de cette tranche.

Bien que ces règlementations puissent être perçues comme des contraintes supplémentaires, les ambitions européennes visent à augmenter la maturité cyber des organisations publiques et privées à l'échelle de l'Europe et à établir un référentiel commun pour une base de sécurité harmonisée. Il est possible d'anticiper cette mise en conformité en partant du postulat de base que l'objectif initial est la montée en maturité du système d'information et non pas la complexification des processus.

LA DIRECTIVE NIS 2 EST UNE DIRECTIVE QUI TEND À HARMONISER LES RÈGLES DE CYBERSÉCURITÉ EN EUROPE ET NOTAMMENT DANS LES COLLECTIVITÉS. TROUVEZ-VOUS QUE CETTE DERNIÈRE EST :

- Une opportunité : plus de bénéfices à améliorer la cybersécurité dans ma collectivité que de contraintes pour la mise en place des règles.
- Autant une opportunité qu'une contrainte : autant de bénéfices que de contraintes pour améliorer la cybersécurité dans ma collectivité.
- Une contrainte : plus de contraintes pour la mise en place des règles que de bénéfices à améliorer la cybersécurité dans ma collectivité.
- Ne sait pas

CONCLUSION

En définitive, les enjeux de la cybersécurité dans les collectivités sont alignés avec la réalité des menaces et le contexte international. La numérisation croissante des processus et des services entraîne une augmentation des risques liés aux cyberattaques. Le secteur public en France est particulièrement exposé aux risques comme l'actualité a pu le montrer ces dernières années et le contexte international actuel particulièrement tendu accroit encore davantage la menace.

Comme le démontre ce rapport, les collectivités sont plutôt lucides en matière de risque cyber et leur maturité progresse de manière graduelle mais certaine au sein des départements informatiques des entités territoriales. Les principales problématiques rencontrées par ces organisations sont principalement liées au manque de ressources, de budget, et de priorisation accordée à la cybersécurité dans les dépenses. La diminution des budgets publics, combinée à la hausse des risques généraux et à la difficulté de prioriser les questions de cybersécurité, ralentit la montée en résilience cyber des collectivités.

De plus, le secteur pâtit d'une attractivité relative au niveau des professionnels qui préfèrent souvent occuper des missions dans le secteur privé. Pour autant, l'État français, et l'Europe, s'organisent pour garantir un niveau minimal de cybersécurité tant dans le public que dans le privé avec la mise en application de règlementations telles que NIS 2 qui ont pour objectif de constituer un socle de sécurité commun et minimal, pour une large palette d'entités en Europe. De la même manière, en France, des initiatives telles que le plan de relance, « France 2030 », ainsi que les objectifs donnés à l'ANSSI pour améliorer l'équipement, et les pratiques cyber des collectivités permettent de positionner le sujet comme une priorité, et de réduire les écarts entre la réalité des cybermenaces et les capacités de protection des organisations publiques françaises.

2024 avec son lot d'événements stratégiques et ses tensions politiques, tant internationales que nationales, devrait être une année charnière. La cybersécurité n'y fera pas exception. Les éditeurs, les prestataires de service, l'État ainsi que les dirigeants et élus doivent tous collaborer et avancer ensembles pour garantir une meilleure résilience, et sensibilisation en matière de cybersécurité.

harfanglab.io Inside the Lab @harfanglab HarfangLab

CONTACT PRESSE

Noémie Minster
PR & Communications Manager
noemie.minster@harfanglab.fr