CYBERSÉCURITÉ
LES ÉLUS DOIVENT GÉRER LE RISQUE AU QUOTIDIEN

Toutes les communes et tous les EPCI doivent se préparer à affronter une cyberattaque. Face à un risque de mise à l'arrêt des services publics, renforcer les systèmes d'information est impératif. Mais l'humain étant souvent le maillon faible des organisations, il faut aussi sensibiliser élus et agents. Panorama des stratégies et dispositifs à disposition des communes. PAR **OLIVIER DEVILLERS**

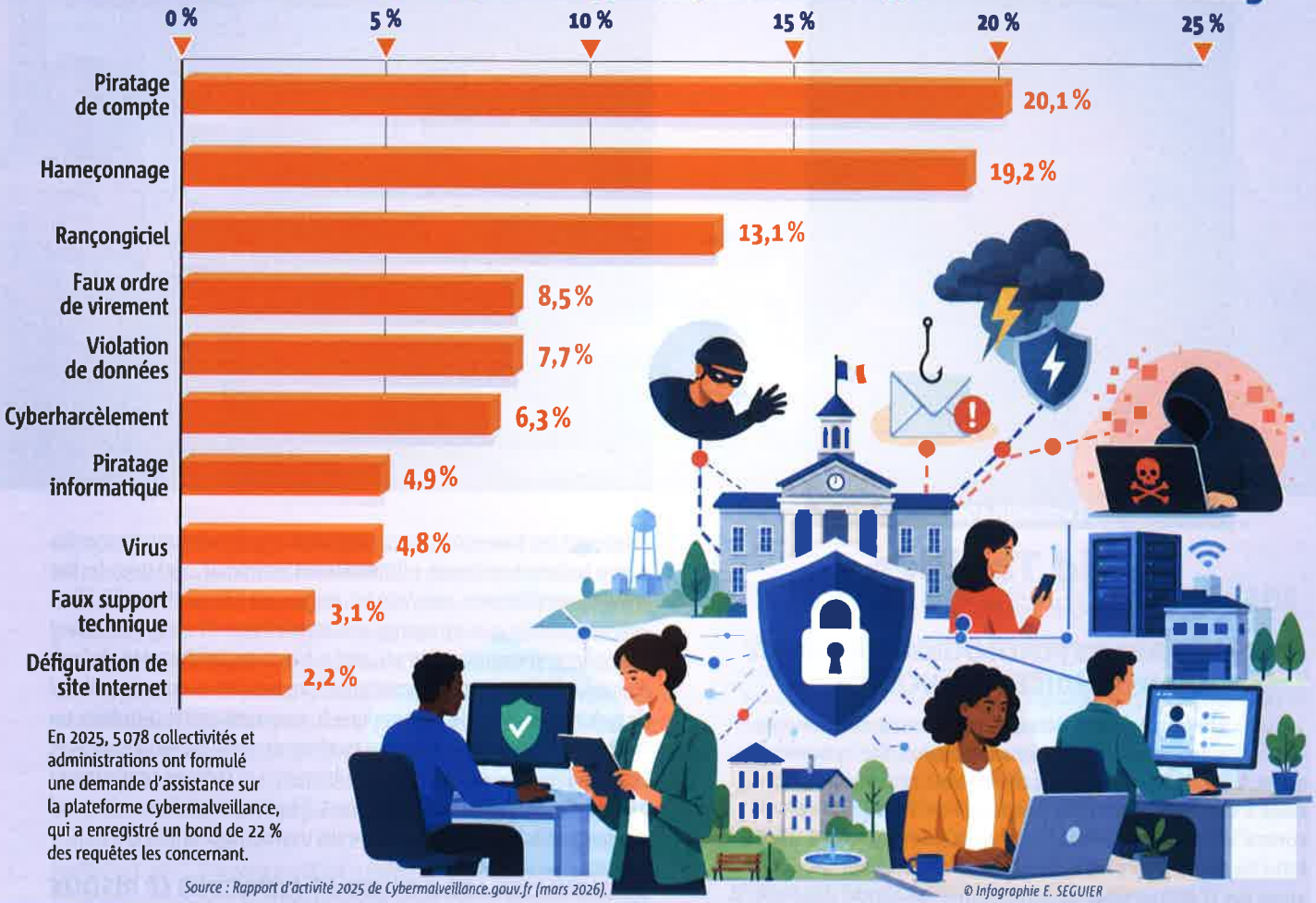
Année après année, la menace cyber ne faiblit pas. Dans son panorama 2025, l'Agence nationale pour la sécurité des systèmes d'information (Anssi, https://cyber.gouv.fr) recense 1 366 incidents, un niveau stable par rapport à 2024 (1 361), année très spécifique avec les Jeux olympiques et paralympiques de Paris (JOP) qui ont généré beaucoup de tentatives de cyberattaques. Les incidents sont surtout en forte progression sur trois ans, 2022 n'en comptant « que » 831. Les ministères et les collectivités concentrent, à eux seuls, 24 % de ces incidents. Et sur les 128 attaques par rançongiciel recensées, les collectivités territoriales représentent 11 % des victimes.

Autre fait marquant : l'irruption de la géopolitique. Les motivations des attaquants ne sont plus uniquement financières. Des États profitent du numérique pour avancer masqués, Russie et Chine en tête. Il s'agit, pour ces puissances étrangères, de mener des opérations de déstabilisation, de collecter du renseignement ou de se prépositionner pour de futures attaques. Le directeur de l'Anssi, Vincent Strubel, évoque un *« risque de sabotage »*, d'attaques coordonnées sur des infrastructures vitales. Le scénario n'est pas théorique : en 2025, la Pologne a déjoué une attaque majeure sur ses réseaux électriques. En Norvège, le barrage de Bremanger a relâché 7 millions de litres d'eau pendant quatre heures après la compromission de son interface de contrôle. En France, des tentatives ont été déjouées sur des stations d'assainissement lors des JOP. Si l'Anssi se concentre sur les attaques majeures, les chiffres de cybermalveillance.gouv.fr, la plateforme d'information et d'orientation des victimes, dressent une photographie plus fine des menaces qui pèsent quotidiennement sur les communes. Premier constat, les collectivités territoriales sont plus exposées au risque que d'autres. *« Pour 1 000 d'entre elles, 141 ont eu recours à l'assistance contre 3 pour 1 000 entreprises »*, explique Jérôme Notin, directeur du GIP Acyma (action contre la cybermalveillance). Plus de 5 000 collectivités territoriales et administrations ont été accompagnées en 2025 (+ 22 %/2024). Le piratage de compte, l'hameçonnage et le rançongiciel forment le trio de tête des menaces (lire ci-contre), mais les progressions les plus marquées concernent la fraude au virement (+ 262 %) et le cyberharcèlement (+ 209 %). *« Historiquement, le cyberharcèlement concernait plutôt les jeunes. Il affecte désormais les élus. Le phénomène a commencé en 2024. Il explose en 2025 avec une multiplication par trois, c'est considérable »*, s'inquiète Jérôme Notin. S'y ajoute une tendance nouvelle : des agressions associant arnaque en ligne et intervention de malfaiteurs pour extorquer, par exemple, une carte bancaire.

LA CYBERATTAQUE, DÉCLENCHEUSE DES DÉCISIONS

La Commission nationale de l'informatique et des libertés (Cnil) complète ce sombre tableau par le prisme des vols de données personnelles. Son rapport annuel 2025 (www.cnil.fr/fr/rapport-annuel-2025) révèle que l'administration publique est le premier secteur touché par les violations de données : elle représente 19 % des notifications reçues en 2025 sur un total de 6 167 violations (+ 9,5 % sur un an). Les administrations cen-

L'assistance aux collectivités territoriales et aux administrations en 2025



En 2025, 5 078 collectivités et administrations ont formulé une demande d'assistance sur la plateforme Cybermalveillance, qui a enregistré un bond de 22 % des requêtes les concernant.

Source : Rapport d'activité 2025 de Cybermalveillance.gouv.fr (mars 2026).

© Infographie E. SEGUIER

trales et grands services publics sont plus touchés (Agence nationale des titres sécurisés, France Travail, DGFiP..., lire *Maire info* du 02/09), mais les contrôles effectués par la Cnil dans plusieurs collectivités territoriales montrent que les règles élémentaires d'hygiène informatique ne sont pas respectées, quelle que soit la taille de la collectivité. Elle note également que la faiblesse des contrôles d'accès aux systèmes d'information publics est à l'origine de la plupart des fuites de données : c'est en se faisant passer pour un utilisateur connu, dont l'identité a été usurpée, que le pirate subtilise des données personnelles. La Cnil recommande aux administrations de généraliser l'authentification multi-facteurs, le login/mot de passe étant complété par un code envoyé par mail ou sur un mobile. Si toutes les collectivités sont invitées à se protéger sans attendre d'être ciblées, force est de constater que les attaques accélèrent les décisions. C'est le cas de Cenon (26 835 habitants, 33), touchée en 2013 par un rançongiciel. L'attaque n'a pas eu de conséquences dramatiques. Le réseau a été coupé à temps, évitant sa propagation. Laissées intactes, les sauvegardes ont permis une restauration des données en deux jours, à l'inverse d'Isbergues (8 650 habitants, 62) où la municipalité a mis quatre mois à retrouver un fonctionnement normal (lire p. 36). Si ses applications métiers ont été épargnées, certaines données, comme les maquettes graphiques utilisées par le service communication, ont été perdues à tout jamais.

À l'issue de la cyberattaque, Cenon s'est dotée d'un programme d'investissement étalé sur le mandat : sortie de Windows XP, antivirus prédictifs, détection des menaces par intelligence artificielle... Si Isbergues a délégué à un tiers la supervision de son système d'information, un prestataire qui « ne fait que ça, 24h/24 et 7j/7 », Cenon a mis l'accent sur le renforcement des équipes internes. La direction informatique est passée de 5 à 12 agents, avec la création d'un poste de responsable de la sécurité des systèmes d'information (RSSI), une fonction assez rare pour cette taille de commune. Côté financement, Cenon a bénéficié du soutien de France 2030 : un audit de sécurité financé à hauteur 40 000 €, assorti de 50 000 € en aides à l'équipement, la commune apportant 20 000 € de sa poche. Isbergues a mobilisé, de son côté, 100 000 €, pris sur sa trésorerie, pour l'achat d'équipements.

APPORTER UNE AIDE AUX PETITES COMMUNES

Dans les deux communes, l'accent a été mis sur la sensibilisation. À Cenon, la direction du service informatique (DSI) a passé la consigne suivante aux agents : *« quand il y a un doute, il n'y a pas de doute, soumettez-le »*, préférant les fausses alertes à la gestion de crise. Isbergues réalise régulièrement des campagnes simulant une tentative d'hameçonnage et des ateliers ludiques pour sensibiliser les agents.

Ces initiatives ne sont pas à la portée de toutes les communes. La cybersécurité exige des moyens financiers, techniques et humains hors de portée des toutes petites communes. Or celles-ci gèrent des données tout aussi sensibles sur les élections, l'état civil ou l'eau. Depuis plusieurs années, l'État réfléchit à la manière d'améliorer le niveau de cybersécurité de l'ensemble des communes. Priorité a été donnée à l'identité numérique des communes, à savoir leur nom de domaine et ce qui va



© Ville d'Isbergues/service communication

Témoignage

David Thellier,

maire d'Isbergues (8 650 habitants, 62)

« UN IMPACT PSYCHOLOGIQUE AU-DELÀ DU PRÉJUDICE FINANCIER »

Un lundi matin de septembre 2024, nous avons découvert que la commune avait été cyberattaquée. Un rançongiciel avait chiffré des années de données à la mairie. On nous proposait de les récupérer contre une rançon : nous ne l'avons pas payée. Il a alors fallu se mettre en ordre de bataille, délocaliser les services sur d'autres sites et fonctionner en mode dégradé. Il nous a fallu trois à quatre mois pour revenir à la normale. Le premier choc a été psychologique. Tant qu'on n'est pas touché, on se dit que ça n'arrive qu'aux autres, comme l'accident de la route. Une petite commune tranquille… on se croit à l'abri. Sauf que non. Pendant quelques semaines, on s'est regardés les uns les autres sans réussir à savoir d'où l'attaque provenait. On se sent presque comme après un cambriolage, pas en sécurité. Des entreprises peu scrupuleuses en ont profité pour tenter de vendre des solutions aux habitants dont ils n'avaient pas forcément besoin. Cette attaque nous a coûté environ 100 000 euros en matériels et accompagnement. Pour une collectivité qui n'a pas la trésorerie, cela peut vite devenir dramatique. Depuis, nous avons changé nos pratiques. Une charte des usages informatiques a été adoptée, les mots de passe ont été renforcés — cela a fait grogner —, et chacun a été sensibilisé aux risques. Nous proposons des formations chaque année. Si on ne le fait pas, on subira de nouveau une attaque car les pirates vont plus vite que nous. On ne sera jamais protégé à 100 %, mais il faut tout faire pour ne pas revivre cela. »

avec : le courrier électronique. Selon l'Agence nationale de la cohésion des territoires (ANCT), près de 11 000 communes ne disposent pas de nom de domaine institutionnel (de type mairie-nom-de-la-commune.fr) et près de 20 000 communes utilisent des adresses mail non professionnelles (Gmail, Orange, Wanadoo…). Or ces adresses grand public



Le commandement cyber de la Gendarmerie nationale sensibilise les collectivités aux menaces numériques (hameçonnage…) et leur expose les solutions pour s'en protéger.

© Olivier Devillers

favorisent les hameçonnages, rançongiciels, fraudes au virement… Avec « La Suite territoriale » (https://suiteterritoriale.anct.gouv.fr ; lire www.mairesdefrance.com/29024), portée par l'Anssi et l'ANCT, l'État entend proposer aux communes une alternative professionnelle, alliant *« simplicité, souveraineté et sécurité »*. Lancé en janvier 2026, il s'agit d'un bouquet de services numériques comprenant un domaine officiel de type mairie-nom-de-la-commune.fr, une messagerie sécurisée, un outil de stockage de fichiers, un système de prise de rendez-vous et un annuaire des administrations publiques. Les services sont adossés à l'outil d'authentification ProConnect, l'équivalent du FranceConnect des particuliers, pour lutter contre les usurpations de comptes.

SENSIBILISER LES AGENTS ET ANTICIPER LE RISQUE

Son déploiement passe par les opérateurs publics de services numériques (OPSN), ces structures, souvent départementales, qui proposent des services numériques aux petites communes (lire www.mairesdefrance.com/28950). En pratique, les OPSN déploient la solution sur leur territoire en offrant un service d'installation et d'accompagnement aux communes. Dans les Pyrénées-Atlantiques, La Fibre 64 (https://lafibre64.fr), qui regroupe 10 EPCI et le département, fait partie de la quinzaine d'OPSN à expérimenter " La Suite territoriale ". Sur 545 communes, 285 n'ont pas de nom de domaine. L'OPSN, qui fait partie de ceux ayant pris la compétence cyber (ce qui n'est pas le cas de tous), a déjà déployé un « bouclier cyber » dans 333 communes (antivirus, antispam, sauvegarde) avec l'aide de l'Anssi. Pour le moment, le syndicat mixte utilise les serveurs de l'ANCT pour des tests. À terme, il aura sa propre « instance », autrement dit une version de « La Suite territoriale » hébergée et maintenue sur ses propres serveurs. Côté modèle économique, le syndicat devrait proposer aux communes une facturation sur la base du gigaoctet stocké, à prix coûtant. *« Sinon, les communes n'ont aucun intérêt à prendre "La Suite territoriale" »*, explique Amalia Martinez, responsable du service solutions numériques à La Fibre64. Le coût n'est cependant qu'un aspect du sujet. Changer d'adresse mail implique de changer le papier à en-tête et d'informer ses contacts, ce qui peut induire des résistances… Priorité est donc donnée à la sensibilisation, le syndicat se plaçant en complémentarité des autres acteurs locaux de la cybersécurité (gendarmes, policiers, associations départementales de maires…). La Fibre64 envoie notamment, deux fois par an, de fausses campagnes de phishing à 5 000 contacts. Environ 5 à 8 %



Le maire de Coublucq (64), Thibaut Moncade (à droite), a choisi de sécuriser la messagerie et les fichiers de la commune *via* « La Suite territoriale », déployée par le syndicat mixte La Fibre64.

des personnes se font piéger à chaque campagne. *« Lors d'une simulation autour des listes électorales, des secrétaires généraux de mairie se sont donné l'alerte* via *une messagerie instantanée. C'est ensuite allé à la préfecture, qui a remonté l'affaire jusqu'aux services de sécurité intérieure. C'est signe d'un bon réflexe, même si "La Fibre64" aurait dû prévenir la préfecture en amont »*, raconte Amalia Martinez. La leçon des cyberattaques intervenues ces dernières années est aussi qu'il faut s'y préparer. Le *« renforcement de la résilience cyber »* est l'un des axes de la stratégie nationale de cybersécurité présentée par l'État, en janvier 2026. Cette stratégie entend préparer tous les acteurs, dont les collectivités, à la gestion de crise par des exercices d'entraînement. Ainsi, en septembre 2025, l'Anssi a organisé « Rempar25 » mobilisant 5 680 professionnels issus de 1 263 organisations publiques et privées, dont des collectivités ou des OPSN. L'exercice national de gestion de crise a été documenté pour être « rejoué » à une échelle locale.

Ces simulations ne doivent cependant pas rester l'affaire de spécialistes, les maires se retrouvant en première ligne sur une crise cyber, comme pour un incendie ou une inondation. C'est ce qui a conduit le ministère de l'Intérieur, plus précisément le commandement dans le cyberespace, à se rapprocher de l'AMF pour concevoir un exercice adapté aux communes. Son nom est CapCyber, crises&collectivités, un dispositif gratuit, en libre accès sur le site de l'AMF (www.amf.asso.fr/page-capcyber brcrises-and-collectivites/43113). CapCyber fournit d'abord une « mallette de crise » : des fiches réflexes par fonction (pilotage, communication, juridique...) et une trame de main courante, car garder trace de tout ce qu'il se passe est essentiel en cas d'attaque. Son originalité tient surtout à un exercice de simulation en ligne, praticable sans préparation ni animateur. Le scénario : un faux mail de l'Agence régionale de santé ouvert par le gestionnaire de la piscine introduit un rançongiciel qui paralyse la commune. Nourri des attaques observées par les cybergendarmes et de l'expérience de gestionnaires de crise, l'exercice balaye des questions clés : à quel moment bascule-t-on de l'incident à la crise ? Qui contacter, et dans quel ordre ? Faut-il éteindre les ordinateurs ou débrancher le réseau ? Les rôles sont distribués autour de la table, chaque choix fait évoluer le scénario et l'équipe reçoit à la fin une évaluation par fonction, sans note. De quoi repérer ses points faibles avant qu'une attaque réelle ne s'en charge.

« Se préparer, c'est se poser toutes ces questions avant que ça nous arrive », résument ses concepteurs qui assument viser d'abord des communes *« peu matures »* sur la question cyber. Pas de solution universelle à l'arrivée : un mémo détaille les avantages et les inconvénients de chaque décision, charge à l'équipe municipale d'en tirer les leçons au regard de ses contraintes locales. Conçu avec une commune et un EPCI témoins et des réservistes gestionnaires de crise dans le civil, l'exercice dure 45 minutes en solo, et deux heures environ en équipe. Un troisième module, réalisé avec le Centre d'analyse et de lutte contre les atteintes aux élus (CALAE), aborde les attaques visant les élus, du cyberharcèlement aux menaces. Enfin, l'AMF et Cybermalveillance.gouv.fr présenteront un Memento sur la cybersécurité dans les communes rurales, lors du 108e Congrès des maires de France, en novembre. Un forum sera aussi consacré à la cybersécurité le 25 novembre. ●

76 %

des 1 366 incidents signalés à l'Anssi en 2025 concernent l'éducation et la recherche (34 %), les ministères et les collectivités territoriales (24 %), la santé (10 %) et les télécommunications (9 %).
(Source : « Panorama de la cybermalveillance en 2025 », Anssi).

Le maquis des acteurs cyber

Anssi, Cybermalveillance, gendarmes, policiers, centres de réponse aux incidents cyber régionaux (Csirt, www.cert.ssi.gouv.fr/csirt/csirt-territoriaux), Recym (réseaux d'experts)... Les interlocuteurs des maires sont pléthoriques et il n'est pas facile de savoir qui fait quoi. La stratégie nationale de cybersécurité, présentée en janvier 2026, prévoit de créer un portail national sur la cybersécurité. L'annonce intervient à peine un an après la création du 17cyber (https://17cyber.gouv.fr), guichet « unique » centré sur l'aide au dépôt de plainte. Ce 17cyber, qui associe policiers et gendarmes, doit se coordonner avec les Csirt régionaux pour assurer une continuité de prise en charge entre les volets judiciaire et la remédiation. Pour ne rien arranger, l'Anssi a annoncé vouloir financer des Csirt thématiques correspondant aux secteurs critiques listés par la directive européenne NIS2. Ce texte, toujours en attente de transposition dans le droit français, impose des contraintes de sécurisation aux collectivités de plus de 30 000 habitants et à leurs groupements.