

CYBERSÉCURITÉ

Une vigilance qui ne peut plus attendre la loi

Le retard de transposition de la directive européenne NIS2 laisse les collectivités et les hôpitaux dans un flou juridique persistant, face à une menace qui s'accélère. Ils n'ont pourtant plus le luxe d'attendre un cadre légal stabilisé pour agir.

Rédaction : Jérémy Paradis

La cybercriminalité contre les services publics a changé d'échelle. Ce qui relevait, il y a encore quelques années, d'un risque lointain et abstrait s'est transformé en une réalité statistique tangible… L'ANSSI a ainsi traité 4 386 événements de sécurité en 2024, soit 15 % de plus qu'en 2023. Sur ce total, 219 concernaient directement des collectivités territoriales, sans distinction de taille ni de strate, des petites communes rurales aux régions.

Le secteur hospitalier a lui aussi appris, à ses dépens, qu'aucun lieu n'est à l'abri : le CH de Dax en février 2021, le CHSF de Corbeil-Essonnes en août 2022, plus récemment les hôpitaux d'Armentières et de Cannes. Chacune de ces attaques a fait tomber un peu plus l'idée qu'un établissement de soin serait naturellement épargné par les cybercriminels.

Derrière ces chiffres, ce sont également des services locaux très concrets qui basculent du jour au lendemain. Dans les mairies, l'état civil, la paie des agents, la facturation, les portails usagers peuvent s'arrêter net. Côté santé, c'est l'accès aux dossiers médicaux et le suivi des patients qui se retrouvent suspendus. Dans les situations les plus sévères, des collectivités entières reviennent, du jour au lendemain, au papier et au crayon, parfois pendant plusieurs semaines, parfois pendant plusieurs mois.

NIS2, le texte qui traîne

Sur le papier, tout était censé être réglé depuis le 17 octobre 2024, date butoir fixée par Bruxelles pour transposer la directive européenne NIS2 en droit français. Dans les faits, le texte navigue toujours entre les bancs du Parlement, ballotté d'une lecture à l'autre. Il a, en effet, été adopté au Sénat en mars 2025, puis retravaillé en commission spéciale à l'Assemblée nationale en septembre de la même année, sans qu'un vote définitif soit intervenu depuis.

La Commission européenne a fini par s'impatienter, engageant en mai 2025 une procédure d'infraction contre la France, avec en toile de fond la menace d'une saisine de la Cour de justice de l'Union européenne.

Ce flottement législatif place les collectivités dans une position inconfortable. Comment se préparer sérieusement à des obligations dont le contenu exact et le calendrier restent, à ce stade, mouvants ? L'ANSSI a apporté un début de réponse en mars 2026, en publiant son référentiel ReCyF. Sans préjuger du texte final, ce document trace une feuille de route opérationnelle pour les collectivités qui préfèrent structurer leur sécurité numérique dès maintenant,

La Suite territoriale, le nouveau socle numérique de l'ANCT

Lancée officiellement le 27 avril 2026, la Suite territoriale est une offre de services numériques opérée par l'Agence nationale de la cohésion des territoires (ANCT), pensée pour les communes les moins armées face au risque cyber.

Le constat de départ. Près de 10 000 communes françaises ne disposent toujours pas de nom de domaine institutionnel. Près de 20 000 utilisent encore des adresses de messagerie non professionnelles pour leurs communications officielles, une fragilité qui expose directement leurs échanges avec l'État et leurs administrés.

Qui est concerné ? Le dispositif cible en priorité les communes de moins de 3 500 habitants et les établissements publics de coopération intercommunale (EPCI) de moins de 15 000 habitants.

Ce que ça contient. La Suite territoriale propose :

- **une identité numérique professionnelle sécurisée, permettant l'authentification des agents et des élus via ProConnect ;**
- **Un socle de services numériques essentiels, avec en particulier une messagerie professionnelle garantissant l'authenticité des communications officielles ;**
- **Un écosystème d'applications interopérables, mises à disposition par les services de l'État (ANSSI, IGN), des opérateurs locaux et des partenaires privés.**

Comment y accéder. Les collectivités éligibles sont invitées à se renseigner sur suiteterritoriale.anct.gouv.fr, puis à se rapprocher de leur opérateur public de services numériques, partenaire de proximité chargé du déploiement sur le terrain.

plutôt que d'attendre un cadre qui tarde à se stabiliser.

Les petites communes, premières fragilisées

Le rapport de force entre la menace et les moyens disponibles n'est pas le même partout. Plus une collectivité est petite, plus elle cumule les fragilités (personnel technique restreint, budgets contraints, et souvent une dépendance presque totale à des prestataires informatiques extérieurs). Face à ce déséquilibre, plusieurs modèles de mutualisation gagnent du terrain, qu'il s'agisse d'un RSSI partagé au sein d'un centre de gestion, d'un syndicat mixte numérique, ou d'un opérateur public de services numériques (OPSN).
Le territoire des Yvelines en offre une illustration concrète. Après une série de cyberattaques qui a frappé plusieurs communes ainsi que l'hôpital André-Mignot de Versailles, le syndicat mixte Seine-et-Yvelines Numérique a réagi en juin 2023, lors de ses assises de la cybersécurité, en déployant une offre pensée pour les petites communes (sensibilisation des agents, suivi individuel de leur niveau de maturité cyber, outils de formation contre l'hameçonnage). Pierre Bédier, président du conseil départemental des Yvelines, s'était rendu au chevet de l'hôpital juste après l'attaque. Il avait résumé, en une phrase, l'ampleur du choc. *« En quelques heures, ils sont revenus à l'âge de pierre ! »* (Banque des Territoires/ Localtis, juin 2023)
À une autre échelle, la Suite territoriale répond à ce même constat d'urgence. Lancée le 27 avril 2026 par l'Agence nationale de la cohésion des territoires (ANCT), elle vise spécifiquement les communes de moins de 3 500 habitants et les EPCI de moins de 15 000 habitants, là où les fragilités numériques sont les plus criantes. Le diagnostic de départ donne la mesure du problème. Près de 10 000 communes françaises n'ont toujours pas de nom de domaine institutionnel, et près de 20 000 utilisent encore des adresses de messagerie non professionnelles pour leurs échanges officiels. Le dispositif propose une identité numérique sécurisée via ProConnect, une messagerie professionnelle, et un écosystème d'applications interopérables développées par l'État, ses opérateurs et des partenaires privés.
Loi qui tarde, mutualisations locales, outil national. Trois réponses différentes à un même problème, celui d'un maillage territorial encore trop inégal face au risque cyber.

POUR ALLER PLUS LOIN SUR WEKA.FR

Fiches

Fiche 14113 - La cybersécurité en établissements de santé, sociaux, et médico-sociaux

Fiche 14305 - La cybersécurité dans les collectivités et leurs établissements

Actualités

Cybersécurité : les collectivités sous surveillance de la Cnil en 2025

Cybersécurité : un MOOC du COMCYBER-MI comme un « kit de crise » à destination **des collectivités**

Masterclasse

Numérique et IA : quels impacts pour les RH ?



PAROLE D'EXPERT

« Les collectivités ne doivent pas attendre la loi Résilience pour agir »

Lionel Pérès, conseiller technique national cybersécurité du SNDGCT

La menace cyber a-t-elle vraiment changé de nature ces dernières années ?
La menace cyber s'est nettement accélérée ces dernières années pour les collectivités, avec une hausse des incidents, une professionnalisation des attaquants et des attaques plus fréquentes, plus rapides, plus difficiles à contenir.
Les attaques ne visent plus seulement les grands acteurs. Les petites structures sont aussi touchées, parce qu'elles ont moins de moyens, moins d'expertise et souvent des systèmes moins bien protégés.

Concrètement, que se passe-t-il le jour où une collectivité est touchée ?
Une cyberattaque peut arrêter l'état civil dont le funéraire, la paie des agents, les e-mails, la facturation, les portails usagers, les billetteries, les accès aux piscines ou musées. Les services passent au papier et au crayon pendant plusieurs semaines, parfois plusieurs mois.

La loi NIS2 tarde à être transposée. Que doivent faire les collectivités en attendant ?
La transposition de la directive européenne NIS2 en droit français a pris du retard, donc les collectivités ne doivent pas attendre la loi Résilience pour agir. Elles doivent déjà préparer leur gouvernance sécurité numérique, les responsabilités, les sauvegardes, le Plan de continuité d'activité (PCA) et la gestion des prestataires.

Les petites communes sont-elles vraiment les plus exposées ?
Oui, les petites communes sont souvent les plus vulnérables, parce qu'elles ont moins de budget, moins de personnel spécialisé et une dépendance plus forte aux prestataires.
La bonne réponse, ce n'est pas l'isolement, c'est la mutualisation : intercommunalités, centres de gestion, syndicats mixtes, les opérateurs publics de services numériques avec une vraie chaîne de responsabilité.

Vous avez suivi de près plusieurs cyberattaques marquantes. Laquelle vous a le plus marqué ?
L'attaque d'Angers, en janvier 2021, est un bon exemple parce qu'elle a montré, très concrètement, qu'une cyberattaque municipale ne vise pas seulement des serveurs, mais peut désorganiser durablement toute une ville. Les services d'Angers et d'Angers Loire Métropole ont été perturbés pendant plusieurs semaines, avec un retour à la normale étalé sur près de quatre mois et un coût estimé à environ 500 000 euros.

Vous avez écrit un guide sur le PCA-cyber en 100 jours. Par où commencer, très concrètement ?
Les premières étapes d'un PCA cyber sont d'identifier les missions essentielles du service public, puis de distinguer celles qui reposent sur l'outil informatique pour être assurées. Pour chacune d'elles, il faut anticiper un mode dégradé, c'est-à-dire une manière de continuer à servir les usagers même sans informatique.

Un dernier conseil pour un DGS ou un maire qui n'a encore rien mis en place ?
Le seul vrai conseil, c'est de sortir du triptyque de la croyance collective : « nous sommes trop petits pour être attaqués », « nous n'avons rien à voler », « la cybersécurité n'est qu'une affaire de techniciens ».