DÉCIDEURS MAGAZINE

ACTUALITÉS | CLASSEMENTS | ÉVÉNEMENTS . 12 MARS 2026

NIS 2 : les collectivités territoriales à la peine face aux risques cyber

IMMOBILIER, PUBLIC & ENVIRONNEMENT

Les cyberattaques n'arrivent pas qu'aux autres. Un principe dont les collectivités territoriales, devenues des cibles privilégiées des hackers, peinent encore à prendre la pleine mesure. Pour contrer les attaques toujours plus sophistiquées, la directive NIS 2 entend renforcer le niveau de cybersécurité de nombreuses entités publiques.

La transposition de la directive NIS 2 n'en finit pas de piétiner. Pourtant son objectif demeure essentiel. En proposant une harmonisation des règles à l'échelle européenne, le texte entend relever le niveau de cybersécurité et de résilience de nombreuses organisations économiques et administratives. Il élargit ainsi le champ d'application de la première directive, NIS 1, à de nouveaux acteurs, à l'image des structures publiques locales ou de grands établissements publics. Une évolution majeure pour les collectivités territoriales qui gèrent de multiples services et données d'administrés. En 2024, une collectivité sur dix déclarait avoir subi au moins un incident de sécurité informatique, selon la plateforme Cybermalveillance.gouv.fr.

Dette technologique… ou culturelle ?

Manque de moyens financiers, d'outils technologiques, de temps ou encore de formation, autant d'éléments qui expliquent les lacunes de protection numérique des collectivités territoriales. À moins que les points d'attention soient mal identifiés. « *Globalement, les dirigeants du secteur public considèrent encore, à tort, que le risque cyber relève principalement d'une protection technique* », observe Lionel Pérès, directeur général des services de Vaison-la-Romaine, commune du Sud de la France. « *Pour eux, les solutions se résument à s'appuyer sur un cabinet d'audit ou s'équiper de logiciels spécialisés. Deux options inefficaces si elles ne s'accompagnent pas d'une réflexion sur les pratiques et la gouvernance.* » Également conseiller technique national cybersécurité au sein du Syndicat national des directeurs généraux des collectivités territoriales (SNDGCT), il consacre une grande partie de son activité à ces enjeux. Et pour cause, il y a deux ans, 44 % des collectivités territoriales se considéraient faiblement exposées aux risques de cyberattaques, soit six points de plus qu'en 2023. Cet excès de confiance touche tout particulièrement les plus petites communes et celles qui n'ont encore jamais été confrontées à une attaque.

> « ***Globalement, les dirigeants du secteur public considèrent encore, à tort, que le risque cyber relève principalement d'une protection technique*** » - **Lionel Pérès**

Depuis dix ans, Élodie Grisé, responsable de la practice Cybersécurité au sein de Claranet, spécialiste du cloud et de la transformation digitale, entend le même refrain en boucle : *« Tant qu'on ne s'est pas fait hacker, tout va bien »* ou encore, *« nous sommes la petite ville du coin, pas la NSA ».* La fracture s'amplifie d'autant plus que le calendrier politique nourrit « *une forme d'attentisme des collectivités face aux élections municipales à venir* » constate Élodie Grisé. Une actualité parmi tant d'autres pour justifier de reléguer les sujets cyber au second plan. « *Les dirigeants sont assaillis d'une quantité astronomique de contraintes réglementaires, normes ou protocoles qui les force à arbitrer et fixer des priorités* », rappelle Lionel Pérès. Qualité de l'air dans les écoles, type de revêtement des trottoirs, puissance d'éclairage des lampadaires, les contraintes sont innombrables.

Changement de paradigme

Pour Lionel Pérès, renforcer la sécurité numérique relève moins un défi technique que d'un enjeu d'organisation et de gouvernance. Un constat partagé par Pierre-Alain Raphan, en charge des relations institutionnelles pour Claranet et vice-président de la French tech corporate community. « *Nous n'avons pas assez investi dans la prise de conscience des dirigeants, y compris politiques, sur les sujets du numérique. Il en résulte une forte immaturité* », estime-t-il. Cette « dette culturelle » pèse d'autant plus sur les responsables de la sécurité des systèmes d'information (RSSI) qu'ils peinent à « *convaincre les dirigeants lorsqu'il s'agit de prendre des décisions stratégiques* », poursuit Pierre-Alain Raphan. Les relations avec les directions des systèmes d'information peuvent s'avérer complexes. L'un des enjeux de NIS 2 consiste justement à faire prendre conscience que la cybersécurité est l'affaire de tous et pas des seuls experts techniques. Pour amorcer un changement de paradigme, la nouvelle directive impose aux dirigeants de s'impliquer davantage, notamment à travers la formation. À eux désormais d'indiquer aux équipes techniques le périmètre à sécuriser et d'allouer les budgets nécessaires tout en s'assurant de la bonne mise en œuvre de ces mesures de protection. En cas de défaillance grave, la responsabilité personnelle du dirigeant peut même être engagée.

> **Le calendrier politique nourrit « *une forme d'attentisme des collectivités face aux élections municipales à venir* » - Élodie Grisé**

Pour les collectivités – actives sur les plans social, territorial mais aussi économique – il faut choisir ses combats. Lionel Pérès insiste : « *au lieu de vouloir sécuriser l'ensemble d'un serveur hébergeant 70 % de fichiers publics, il faut agir sur les documents critiques, tels que les avis d'imposition* ». Un arbitrage qui commence par un inventaire des données et des systèmes pour une gouvernance optimale de la sécurité. Prévenir et détecter les risques, gérer les crises ou assurer la continuité d'activité constituent le cœur des objectifs. C'est précisément sur ces volets que les équipes cyber de Claranet interviennent au quotidien, en déployant des solutions concrètes comme l'authentification renforcée, la surveillance des alertes de sécurité en continu, ou encore des sauvegardes isolées pour pouvoir redémarrer rapidement après une attaque. Pour accompagner ses pairs dans cette démarche, Lionel Pérès a consigné sa méthode dans son ouvrage *Cyberattaques : assurer la continuité des services publics locaux*. Une publication inédite pour ces acteurs. Selon lui, les dirigeants publics doivent changer de perspective, et adopter une approche « secure by design », qui consiste à intégrer la cybersécurité dès la conception des projets numériques.

Paradoxe financier

Au-delà des améliorations attendues en matière de gouvernance et de techniques, la question des coûts demeure centrale. Parler d'argent et d'investissements publics peut s'avérer un sujet sensible. À ce stade, aucune sanction financière n'est prévue pour les structures publiques en cas de non-conformité. Un choix quelque peu audacieux. Considérer la conformité comme un levier de performance suffira-t-il à impliquer les décideurs concernés ? C'est l'avis d'Élodie Grisé, qui se refuse à la voir comme un simple « *coup de tampon* ». Pour autant, des sanctions devraient éclore, selon Pierre-Alain Raphan qui souligne que *« prévoir des sanctions pour le secteur privé et non pour le public représente un problème constitutionnel* ». D'autant plus que l'Agence nationale de la sécurité des systèmes d'information (Anssi) pourrait intervenir auprès des collectivités sans les sanctionner financièrement, mais en se limitant à les mettre en demeure de se conformer aux obligations, glisse Lionel Pérès.

> **« *Pour tester les organisations, rien de plus simple que laisser une clé USB par terre dans un parking* » - Pierre-Alain Raphan**

Sens commun

« *Les bons réflexes en matière d'hygiène numérique devraient être inculqués dès le plus jeune âge* », estime Pierre-Alain Raphan. À titre de comparaison, les exercices de sécurité incendie font leurs preuves depuis plus de 40 ans. Mais, dans le domaine du numérique, le chantier de la formation reste considérable. « *Pour tester les organisations, rien de plus simple que laisser une clé USB par terre dans un parking* », illustre-t-il. La curiosité humaine fera le reste. Connectez cette clé à votre PC et le hameçonnage est lancé. Malgré le traumatisme associé à l'expérience d'un incident cyber, les risques potentiels restent présents. « *De la même façon qu'il y a toujours des accidents malgré le code de la route, les incidents cyber se poursuivront. D'où le rôle essentiel de la prévention afin de les minimiser* », tempère Élodie Grisé. « *Pour l'ensemble des acteurs, NIS 2 doit s'intégrer à une conformité holistique* », complète-t-elle. Plus d'un an après l'échéance européenne pour transposer le texte en droit français, la directive NIS 2 attend encore une inscription à l'ordre du jour de l'Assemblée nationale. Une attente qui ne doit pas empêcher les collectivités de lancer les premiers chantiers associés à la sécurisation de leurs services et de leurs données.

Léa Pierre-Joseph