MAIRE info

Cybersécurité : la transposition de la directive « NIS 2 » devra se faire avec les collectivités

12/03/2024
Numérique

La directive du 14 décembre 2022 dite « NIS 2 » visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union doit être transposée en France avant le 17 octobre 2024. Le périmètre d'application de la directive pour les collectivités n'est pas encore défini. Les associations d'élus appellent à une « transposition intelligente ».

Entre janvier 2022 et juin 2023, l'Agence de sécurité des systèmes d'information (Anssi) a enregistré et traité 187 cyberattaques visant les collectivités territoriales. Depuis plusieurs années, toutes les collectivités, même les petites communes plus vulnérables, sont particulièrement touchées par des cyberattaques. *« Une collectivité sur 10 déclare avoir déjà été victime d'une ou plusieurs attaques au cours des 12 derniers mois, notamment d'hameçonnage à 46 % »,* selon Cybermalveillance.gouv.fr.

C'est dans ce contexte que la directive du 14 décembre 2022 dite « NIS 2 » doit être transposée en France avant le 17 octobre 2024.

Pour mémoire, la première réglementation européenne en matière de cybersécurité a été publiée en 2016 et concernait 300 entités *« Opérateurs de services essentiels ».* Les communes et les EPCI n'étaient pas concernés jusqu'à maintenant. *« La directive NIS 2, qui s'appuie sur les acquis de la directive NIS 1, marque un changement de paradigme »*, peut-on lire sur le site de l'Anssi. En effet, les administrations publiques seront désormais concernées par la mise en place de nouvelles pratiques en faveur d'une meilleure cybersécurité. Ainsi, certaines mesures seront applicables aux collectivités.

Mais pour le moment, les informations sur le cadrage de la directive et son périmètre d'application ne sont pas encore fixées. L'Agence nationale de la sécurité des systèmes d'information (Anssi) a lancé une consultation auprès des associations d'élus dont l'AMF. Dans un communiqué diffusé hier, Intercommunalités de France, France urbaine et Les Interconnectés demandent *« que les principes d'adaptabilité, de progressivité et de soutiens financiers et en ingénierie président à la transposition de la directive ».*

Les collectivités appellent à une transposition intelligente de la directive

La directive NIS2, qui vise à collectivement atteindre une immunité cyber nationale, distingue deux types d'acteurs qui vont être soumis à des obligations différentes : les entités essentielles et celles dites importantes (les essentielles auront davantage d'objectif à remplir).

Comme l'indique le trio d'associations dans un communiqué, *« si 77 % des communautés d'agglomération, urbaines et métropoles mettent en place des actions en termes de cybersécurité, c'est le cas de seulement 33 % des communautés de communes, selon le baromètre de la maturité numérique des territoires »*.

« Ainsi, en fonction de leur nombre d'habitants, de leur statut et de leurs compétences, toutes les intercommunalités ne disposent pas des mêmes leviers et ne sont pas exposées à des risques de la même intensité. La catégorisation des intercommunalités en entités dites "essentielles" et "importantes", soumises à des niveaux d'obligations distincts, doivent donc tenir compte des compétences et services publics effectivement exercés par les collectivités. » Les trois

associations demandent donc à ce que le nombre d'habitants ne soit pas le seul critère du degré d'obligations imposées.

Intercommunalités de France, France urbaine et Les Interconnectés demandent *« une mise en conformité par étape, claire et progressive dans le temps »* **mais aussi un** *« accompagnement technique et financier dédié et adapté, en particulier pour les communautés de communes et d'agglomération »*. **Afin de renforcer le soutien de l'Anssi aux collectivités, elles demandent** *« un renforcement du rôle et des moyens alloués aux centres de réponse aux incidents cyber (CSIRT) en uniformisant les modalités de leur financement, aujourd'hui inéquitables »* **(lire article** *Maires de France***) et** *« proposent la mise en place effective d'un numéro "17-cyber" unique et simple à destination des collectivités en cas d'urgence, afin de mieux coordonner les réponses lors d'une attaque informatique ».*

De son côté, l'AMF travaille en lien avec l'Anssi pour que l'impact soit équilibré entre l'ambition légitime d'une meilleure cybersécurité des communes, l'investissement financier qui doit être raisonnable pour les collectivités, la progressivité de la mise en place des obligations, et le niveau de maturité de chaque collectivité.

Vers un seuil de 30 000 habitants ?

Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale, a été auditionné mercredi dernier à l'Assemblée nationale. Il a indiqué, en évoquant le futur projet de loi visant à intégrer la directive européenne, *« qu'un certain nombre de dispositifs sont prévus pour amener ce qu'on appelle les entités essentielles (départements, régions et communes et intercommunalités de plus de 30 000 habitants) à pouvoir avancer là-dessus. On ne va pas imposer aux petites communes ou aux communautés de communes de moins de 30 000 habitants des choses impossibles, donc elles seront appelées entités importantes et on leur demandera simplement de veiller à des actions d'hygiène ».*

Il est possible que lorsque le projet de loi sera étudié par les parlementaires, le seuil des 30 000 habitants évolue pour distinguer les entités « *essentielles* **» des «** *importantes* **». En attendant le début des travaux législatifs, les associations d'élus rappellent que** *« pour que le futur texte de loi atteigne sa cible, et qu'il ait des effets concrets localement, il devra être élaboré en lien étroit avec les associations de collectivités ».*
