acteurspublics.fr

Avec le retard pris par la loi cybersécurité, l'Anssi donne des clés aux administrations pour se conformer sans attendre

Par Victoria Beurnez
5–6 minutes

Alors que la directive européenne NIS 2 tarde à être transposée dans le droit français, le cyber pompier de l'État publie une version de travail de son référentiel, pour inviter les acteurs concernés à se conformer sans attendre. Une publication qui se fait dans la foulée de la présentation, début mars, du panorama de la menace cyber 2026, une menace qui ne décroît pas.

Faut-il attendre que la loi soit promulguée pour la respecter ? Non, selon l'Agence nationale pour la sécurité des systèmes d'information (Anssi). Cette dernière vient de publier sa version de travail du "Référentiel Cyber France". Ce document est destiné à permettre aux entités concernées par la future transposition de la directive européenne NIS 2, sous la forme des lois Résilience et Cybersécurité, de se conformer aux exigences de ces nouvelles règlementations en matière de cyber.

"*Élaboré dans la perspective de NIS 2, ce document a été co-construit avec de nombreuses organisations professionnelles, associations d'élus et acteurs de l'écosystème pour définir une réponse adaptée, d'une part à la réalité de la menace, et d'autre part à la taille et à la*

maturité des entités qui doivent s'en protéger", a déclaré Vincent Strubel, directeur de l'Anssi, sur Linkedin. Ce dernier, à l'occasion de la présentation du panorama 2026 de la menace cyber, début mars, avait d'ailleurs rappelé que *"le plus tôt sera le mieux"* concernant la transposition de la directive européenne.

Lire aussi : L'éducation, la recherche et la santé particulièrement touchées par la cybermalveillance en 2025

Ainsi, le document s'articule autour de plusieurs points, qui sont en fait les objectifs de sécurité devant être nécessairement atteints par les entités importantes et essentielles concernées par la loi cybersécurité. Pour rappel, les entités essentielles, qui doivent se conformer aux exigences maximales de cette future loi, en opposition aux entités importantes, sont par exemple, pour le secteur public, les administrations publiques, les collectivités, les établissements publics de santé, entre autres.

Formaliser les objectifs de sécurité

Le document reprend donc point par point chaque objectif de sécurité devant être mis en place par ces entités, en proposant un rappel des attendus et des moyens acceptables de conformité pour chacun d'entre eux. "*L'objectif de sécurité est l'obligation fixée par le décret pris en application de l'article 14 du projet de loi à laquelle doit se conformer l'entité*. […] *Son atteinte est obligatoire*, rappelle l'Anssi en préambule du document. Les "*moyens acceptables de conformité*", eux, sont "*les mesures à mettre en œuvre proposées par l'Anssi aux assujettis pour atteindre l'objectif*".

Lire aussi : En commission, le projet de loi cybersécurité repensé pour les établissements médicaux et les collectivités

La liste des objectifs est longue, autant que la loi est ambitieuse : elle a pour vocation, pour vulgariser, de recenser et maîtriser la totalité des services informatiques d'une entité, et de faire en sorte que cette dernière réponde de manière adéquate en cas de cyberattaque. Ainsi, les paramètres vont du recensement à la maîtrise des systèmes d'information, la gestion des identités numériques, les audits de sécurité, en passant par la tenue d'exercices, de tests, d'entraînement, de préparation à réagir aux crises cyber.

L'heure n'est plus à l'attente

Pour l'Anssi, le but de cette publication est aussi d'inciter les entités concernées à intégrer ces paramètres dans leur stratégie de sécurité. "*Le référentiel restera un document de travail jusqu'à la transposition de NIS 2 en droit français, mais il ne faut surtout pas attendre pour le mettre en œuvre*", rappelle Vincent Strubel. L'Anssi invite ainsi les entités concernées à l'intégrer dès maintenant dans leur stratégie de sécurité. "*C'est prendre un coup d'avance sur la conformité qui sera exigée à l'avenir, mais c'est aussi et surtout se protéger d'une menace qui est d'ores et déjà une réalité malheureusement trop concrète pour de nombreuses victimes*", a conclu le directeur général.

Lire aussi : Des parlementaires accusent l'Intérieur de freiner l'adoption de la loi "Résilience et Cybersécurité"

La “conformité qui sera exigée à l’avenir” devra en tout cas attendre : pour l’heure, la transposition de NIS 2 dans le droit français a pris un fort retard, que des parlementaires, dont le très familier du sujet Philippe Latombe, imputent à la présence d’un article, dans le projet de loi, protégeant le chiffrement des messageries instantanées. Un texte qui ne serait, selon le député de la Vendée, pas au goût du gouvernement, qui cherche toujours à traduire dans la loi la possibilité de contourner cette barrière, et a par ailleurs lancé une mission d’information à ce sujet, dont les conclusions devraient être rendues en avril.