NIS 2 consacre l'obligation des plans de lutte cyber

Les États membres de l'UE avaient jusqu'au 17 octobre 2024 pour transposer la directive « NIS 2 ». Bien que le projet de loi ait enfin été présenté en Conseil des ministres, un tel calendrier laisse en réalité peu de temps aux acteurs pour s'adapter.

La directive (UE) 2022/2555 du 14 décembre 2022, dite directive «NIS 2», pour «Network and Information Security», entrée en vigueur le 16 janvier 2023, a fait l'objet d'un projet de transposition préparé par l'Anssi et remis au gouvernement en mars 2024. Son adoption ne devait être qu'une formalité, d'autant que les États membres n'avaient que jusqu'au 17 octobre pour s'exécuter. Mais les récents événements politiques en ont décidé autrement. Et si un projet de loi a bien été présenté en Conseil des ministres le 15 octobre, le temps parlementaire ainsi que la place laissée par le projet de loi à des décrets d'application supposent que la transposition effective de la directive ne sera pas immédiate.

Il n'en demeure pas moins que les entreprises doivent entreprendre dès maintenant leur mise en conformité. Ce n'est certes pas le spectre de l'«applicabilité directe» de la directive que doivent craindre les entreprises concernées, mais peut-être davantage le contrecoup de la transposition par certains pays européens ayant respecté les délais (à ce jour, Belgique, Croatie et Hongrie, liste qui est appelée à grossir rapidement). En effet, pour les entreprises ayant des relations avec ces derniers, la primeur ira aux prestataires qui pourront, à date, leur garantir le meilleur niveau de conformité.

La directive affiche l'ambition d'établir des mesures qui ont pour but «*d'obtenir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur.*» En cela, sa vocation est de mettre à jour les acquis de la directive (UE) 2016/1148 dite «NIS 1» ou «SRI», d'harmoniser les pratiques cyber et de renforcer la coopération européenne, notamment via l'instauration d'un réseau des centres nationaux de réponse à incident (les CSIRT).

Pour ce faire, la directive NIS 2 étend la liste des secteurs concernés par les exigences qu'elle met en place pour la porter à 31 secteurs clés (contre 12 sous l'égide de la directive NIS 1), parmi lesquels ceux de l'énergie, des transports, de la banque, des marchés financiers, de la santé, qui subsistent, et, nouvellement, de la fourniture de services numériques (à savoir les fournisseurs de services d'informatique en nuage, de places de marché en ligne, de réseaux sociaux) ou encore du spatial.

La checklist du DSI se trouve dans la directive !

Plus encore, le texte introduit renforce, compte tenu de leur importance sociale, les obligations des entités dites «essentielles» lesquelles exercent dans les secteurs dits «hautement critiques», notamment cités ci-dessus (banques, marchés financiers, santé, certaines infrastructures numériques...) et qui dépassent les plafonds des PME tels que définis par l'Union européenne (moins de 250 employés et un CA inférieur à 50 M€ ou un bilan annuel inférieur à 43 M€). Le projet de loi français y ajoute un certain nombre d'administrations.

Seront réputées «importantes», les entités exerçant dans les secteurs en question sans dépasser ces seuils, ainsi que dans les «autres secteurs critiques» (constructeurs automobiles, fournisseurs de services numériques). Le projet de loi français de transposition de la directive précise qu'il s'agira de celles qui emploient au moins 50 personnes ou dont le CA et le total du bilan annuel excèdent chacun 10 M€.

Selon une technique législative désormais en vogue, la directive NIS 2 impose aux entités essentielles et importantes de prendre les «*mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information*» qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services.

Concrètement, ces mesures, qui devront être approuvées par leurs organes de direction (ce dont le projet de loi en France ne dit mot), sont censées permettre de maîtriser les risques par une approche ordonnée et méthodique. Elles sont d'ailleurs détaillées dans la directive : elles viseront notamment à cartographier les risques cyber, imposeront de mettre en œuvre une politique interne ou encore des dispositifs élémentaires tels que l'authentification multi-facteurs. Seules les entités «essentielles» pourront cependant faire l'objet d'inspections et de sanctions de l'autorité compétente hors de toute incident de sécurité.

De l'urgence de réaliser un audit « Cyber » de son SI

Les dirigeants accompagnés de leur DSI ont tout intérêt à prendre à bras le corps ces nouveautés règlementaires dont la Cnil a déjà démontré qu'elles convergeaient avec ses propres standards de sécurité, s'agissant notamment de l'authentification, sur laquelle le guide des TPE/PME de l'Anssi insiste également. Notre expérience des dossiers traités montre que les failles des systèmes d'authentification et de gestion des droits (absence de politique du «moindre privilège») sont à l'origine de nombreuses cyberattaques. Et nous remarquons bien souvent dans les dossiers contentieux que les audits de cybersécurité, lorsqu'ils sont disponibles, avaient permis d'identifier des vulnérabilités qui se sont révélées exploitées par les attaquants.

François-Pierre Lani,
avocat associé du cabinet Derriennic