AVIS D'EXPERT

DIRECTIVE EUROPÉENNE NIS2 : QU'EST-CE QUI CHANGE ?

Vincent Nicaise
Responsable des partenariats et de l'écosystème industriels, Stormshield

Adoptée par les institutions européennes en juillet 2016, la directive NIS a pour objectif d'assurer un certain niveau de sécurité pour les réseaux et systèmes d'information des infrastructures critiques et sensibles des pays membres de l'Union européenne. Six ans plus tard, la révision de cette directive s'accélère, avec de premiers accords entre la Commission, le Parlement et le Conseil européen en mai et juin 2022. Pas encore adoptée, cette nouvelle directive NIS2 donne déjà lieu à de nombreuses questions quant à ses implications et son périmètre d'application. Explications.

UN ÉLARGISSEMENT DES ACTEURS CONCERNÉS

L'accroissement des cyberattaques de ces dernières années oblige les États membres de l'UE à augmenter leur niveau de sécurité dans le but de protéger les citoyens, les collectivités territoriales et les entreprises. Pour faire face à ce défi, la directive NIS se réforme, s'harmonise et se renforce en une version 2.0. Selon **Thierry Breton**, Commissaire européen au commerce intérieur, cette réforme doit « *sécuriser davantage les services critiques pour la société et l'économie* ». Et permettre « *de moderniser les règles* ».

Le premier degré d'harmonisation se traduira par une précision des secteurs concernés. Et c'est la première question qui revient sur le sujet : **est-ce que mon entreprise est concernée par la directive NIS2 ?** Précisés dans le Journal officiel de l'Union européenne, **les secteurs concernés sont au nombre de 18, séparés entre secteurs critiques** et hautement critiques. Les secteurs hautement critiques sont au nombre de 11 : énergie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène), transports (transports aériens, ferroviaires, par eau, routiers), secteur bancaire, infrastructures des marchés financiers, santé, eau potable, eaux usées, infrastructure numérique, gestion des services TIC, administration publique et espace. Les secteurs critiques sont, eux, au nombre de 9 : services postaux et d'expédition, gestion des déchets, fabrication, production et distribution de produits chimiques, production, transformation et distribution des denrées alimentaires, fabrication (fabrication de dispositifs médicaux, de produits informatiques, électroniques et optiques, d'équipements électriques, de machines et équipements, de véhicules automobiles ou encore d'autres matériels de transport), fournisseurs numériques et recherche. Pour aller encore plus finement dans la description, une liste d'entité est précisée dans la directive européenne, correspondant à des activités métier. La taille de l'entité est également une dimension à prendre en compte avec la directive NIS2, car le nombre d'employés (supérieur ou égal à 50) ou le chiffre d'affaires (ou bilan annuel, supérieur ou égal à 10 millions d'euros) sont également des critères de sélection.

Cette liste n'est pas exhaustive et certains détails restent à définir dans le cadre des transpositions nationales, par exemple pour intégrer ou exclure unitairement des entités (suite à une analyse de risque national ou une clause de défense et sécurité nationale). Pour le territoire français, **Guillaume Poupard**, l'ancien Directeur Général de l'ANSSI, déclarait en juin 2022, que la directive NIS2 allait étendre considérablement son rayon d'action, ce qui représenterait « *un nombre d'acteurs classés OSE multiplié par 10* ». À ce jour, il n'existe aucun chiffre officiel du nombre d'entreprises concernées, mais les premières communications officielles de l'ANSSI évoquent plusieurs milliers d'organisations françaises impactées par la directive NIS2. **Et pour mieux adapter la réglementation aux spécificités de chaque secteur, l'ANSSI travaille avec les organisations professionnelles et sectorielles (fédérations, syndicats…).** De premières consultations ont déjà été menées depuis début 2023.

Avec le secteur de l'administration publique, les collectivités territoriales sont donc intégrées à cette réforme. D'après une interview d'Yves Verhoeven, le sous-directeur stratégie de l'ANSSI, pour le journal *La Tribune*, « *le NIS révisé donne la possibilité d'aller réguler les collectivités territoriales, et de leur imposer des règles de cybersécurité* ». À noter qu'il ne s'agit que d'une possibilité : comme expliqué plus haut, chaque État membre ayant la main pour élargir, ou non, le périmètre de la nouvelle directive à ses administrations locales.

Oubliés de la première version, les acteurs de la chaîne d'approvisionnement (sous-traitants et prestataires de services) ayant un accès à une infrastructure critique seront également soumis à la directive NIS2. Car les failles dans l'infrastructure d'un prestataire pouvaient mettre à mal la sécurité des OSE pour lesquels il travaille. La cyberattaque ayant touché la société Kaseya en juillet 2021 en est un triste et célèbre exemple de ces s*upply chain attacks*. Dès l'application de NIS 2, la réalité sur le terrain sera bien différente. Par exemple dans le secteur de l'énergie, les producteurs, transporteurs et distributeurs d'électricité ne seront plus seuls à se voir imposer des mesures de sécurité. Et l'ensemble des sous-traitants des infrastructures critiques le seront également. Les sociétés de prestations de services et autres ESN auront notamment l'obligation de prévenir en moins de 72 heures tout incident de sécurité, afin d'endiguer la propagation de l'attaque.

Il faut ainsi s'attendre à ce que les petites et moyennes entreprises recrutent rapidement un profil RSSI pour répondre aux exigences de sécurité et continuer à travailler auprès des grands comptes. De quoi ajouter une tension supplémentaire à un marché de l'emploi qui semble déjà à son point de rupture.

NIS2, VERS LA FIN DES OSE

Point définition avant de parler de leur fin, **c'est quoi un OSE ?** Pensé comme une extension du statut d'OIV établi en France par la Loi de programmation militaire de 2013, un OSE est un opérateur de services essentiels dont l'arrêt du système informatique ou de son infrastructure aurait un impact significatif sur le fonctionnement de l'économie ou de la société française.

Mais avec l'intégration des sous-traitants et prestataires de services en charge d'une infrastructure critique et surtout un mouvement sémantique, **la directive NIS2 signe la fin des OSE. Désormais, le périmètre de ces opérateurs régulés sera divisé en deux typologies d'acteurs : les entités essentielles (EE) et les entités importantes (EI), dont la différenciation se fera par la criticité des secteurs associés.** La directive NIS2 intègre ici une proportionnalité entre les entités au niveau des mesures de sécurité, de la régulation mais aussi des sanctions. Une approche logique tant les entités essentielles auront logiquement un impact plus important en cas de coupure de service que les

entités importantes. La fin des opérateurs de service essentiel (et des fournisseurs de services numériques) ainsi que l'adoption des typologies d'entreprises essentielles et importantes ont pour ambition d'harmoniser l'ensemble des obligations auprès de ces acteurs. Au niveau français, cette logique d'harmonisation ne devrait pas aller jusqu'à remettre en doute l'existence des OIV, tant ils sont encore aujourd'hui l'objet d'une réglementation et d'une surveillance poussée.

Cette volonté d'harmonisation soulève aussi des questions car ce sont bien les entreprises et les opérateurs qui devront… s'autodésigner comme EE ou EI. Pour cela, ils se baseront sur l'un des secteurs d'activité préalablement ciblés et la taille de leur entité (ETI et grande entreprise, moyenne entreprise et petite et micro entreprise). Une règle de base explicite que les entités essentielles seront notamment les grandes entités qui appartiennent aux 11 secteurs hautement critiques. En complément, chaque pays membre pourra désigner, à sa discrétion, certains opérateurs comme essentiels ou importants selon des mécanismes d'ajustement à la marge.

UNE NOUVELLE DIMENSION CONTRAIGNANTE DE LA DIRECTIVE

Toujours selon Thierry Breton, cette réforme de la directive permet de sécuriser davantage les entités « *en mettant en place un régime d'obligations et de sanctions* ». Véritable « *avancée majeure* » selon le commissaire européen, l**a directive NIS2 étend donc son pouvoir coercitif**. Mais quelles sont les obligations des entités essentielles et entités importantes ? Tout d'abord, l'obligation de déclaration de sinistre permet de réagir au plus vite et d'endiguer la cyber-menace. Si la directive précise une notification initiale de l'incident sous 24h, elle laisse une marge de manœuvre dans le cadre de la transposition nationale notamment sur le délai d'implémentation des mesures de sécurité. Au moment de la rédaction de cet article (et de sa mise à jour), les délais de mise en œuvre de la directive pour les entités concernées n'ont pas encore été précisés. En parallèle, les entreprises, sous-traitants et collectivités devront se soumettre à des audits de sécurité dans le but de recevoir des recommandations et ainsi répondre à des normes de sécurité drastiques. Analyse des risques et à la sécurité des systèmes d'information, gestion des incidents, continuité des activités, sécurité de la chaîne d'approvisionnement, sécurité de l'acquisition, du développement et de la maintenance des systèmes d'information, évaluation des mesures de gestion des risques cyber, pratiques de base (comme l'hygiène cyber et formation), sécurité des ressources humaines ou encore utilisation de solutions d'authentification à plusieurs facteurs sont autant de mesures de sécurité prévues par la directive NIS2.

Pour les entreprises non coopérantes ou en faute, la directive NIS2 a également fait évoluer ses sanctions. En cas d'incident de sécurité et de refus de collaboration avec les autorités, NIS 2 dote les États d'un droit d'injonction. Les entreprises devront donc se soumettre à la demande de l'État et peuvent être soumises à des amendes comprises entre 1,4% à 2% du chiffre d'affaires. Comme pour le feu statut d'OSE, la responsabilité du dirigeant peut être engagée.

Mais **si cette réforme a pour but de renforcer la sécurité, elle soulève également des questions budgétaires.** Pour les milliers d'entreprises concernées, les comités exécutifs devront se concentrer sur leurs budgets d'investissement dans les produits de cybersécurité. Et leur accorder plus de souplesse. Et qu'en est-il pour les communes, départements et régions ? Moins souples que leurs homologues privés, ces entités devront faire avec les possibilités qui s'offrent à elles (comme le plan France Relance) avec des budgets restreints et des ressources humaines manquantes. Un retard en termes d'outils et de compétences déjà difficile à combler notamment pour les petites et moyennes collectivités aujourd'hui, et qui risque même de s'aggraver suite à l'application de la direction NIS2.

NIS 2, c'est pour quand ? La réponse n'est pas si simple. Si **le Parlement européen a officiellement adopté la nouvelle directive NIS2 le jeudi 10 novembre 2022, la transposition à l'échelle nationale devra se faire avant le 17 octobre 2024.** Mais des phases de consultation sont prévues pour le second semestre 2023, autour de l'élaboration d'autres textes réglementaires (décrets, arrêtés). La transposition à l'échelle nationale ne devrait donc pas se faire avant la toute fin 2023, début 2024. De quoi laisser le temps à toutes les entités concernées de se préparer à un gros changement face à la menace cyber ?