COMPTE-RENDU TABLE RONDE
DÉCRYPTAGE DE LA DIRECTIVE NIS

Animateur

Bénédicte PILLIET, *Directeur*
CyberCercle and Co

Participants

Julien BARNU
ANSSI

Maître Garance MATHIAS, *avocate*

La Directive NIS (*Network and Information Security*) a été adoptée par le Parlement européen le 6 juillet 2016. Cette directive vise à harmoniser à l'échelle de l'UE les pratiques en matière de cybersécurité. Importance vitale.

Julien BARNU
ANSSI

Julien Barnu, chef de cabinet de Guillaume Poupard et chargé de la transposition de la directive NIS à l'ANSSI, commente ainsi sa tâche : «*[L'application de] la directive NIS est vraiment un sujet complexe car il faut faire la distinction entre le pourquoi de la directive, ce qu'elle signifie, sa lettre, et enfin, ce qu'on veut en faire, nous, en tant qu'organisme à la tête de l'application de la directive.* »

« Dans l'esprit [de la directive NIS], il y a la volonté de mettre en place une obligation de moyens de protection pour les infrastructures critiques. »

La directive NIS s'inscrit en effet dans le cadre d'une volonté de sécurisation des OPE (Opérateurs de Services Essentiels) propres à chaque États membres de l'Union européenne.
Dans son esprit, il y a la volonté de mettre en place une obligation de moyens de protection pour les infrastructures critiques. De telles infrastructures comprennent les réseaux de transports, les établissements de santé et l'approvisionnement en eau potable, par exemple…

« Il existe 20 règles de sécurité obligatoires à appliquer : il y a des règles organisationnelles et des règles techniques, qui sont des règles obligatoires, incontournables, et sans aucune dérogation possible. »

Quant à sa lettre, la transposition de cette obligation à partir d'une directive, plutôt que d'un règlement, permet de mieux respecter la coopération entre les États membres. Une telle directive n'étant pas normative en soi, elle n'entraîne aucune obligation dans sa lettre, afin que tout se fasse sur la base du volontariat dans les organes législatifs propres des États.

L'angle de la directive NIS vise le marché intérieur : le tissu « économique et sociétal » des États. Ainsi, la mise en avant des activités « sociétales » permet d'inclure les activités telles que la gestion de l'approvisionnement en eau, activité importante pour la société, et non purement « économique ».

La directive couvre donc le marché intérieur économique et sociétal des États, et dans son annexe, sont spécifiés les secteurs couverts. Il y a une similitude avec ce que la France a mis en place avec la loi de 2006 concernant la protection des SAIP (Secteurs d'Activité d'Importance Vitale).

Le bagage législatif français concernant la protection des OIV (Opérateurs d'Importance Vitale).

Depuis un **arrêté du 2 juin 2006**, douze secteurs d'activité ont été désignés comme d'importance vitale. Si la liste exhaustive des entreprises correspondantes à ces secteurs est tenue secrète, il est certain qu'il s'agit d'entreprises qui réalisent des missions vitales pour l'exercice de la souveraineté du pays.

« L'article 22, permet de fixer des règles de sécurité obligatoires. Un décret d'application est pris pour chaque secteur d'activité. »
La Loi de Programmation Militaire n°2013-1168 du 18 décembre 2013 (codifié dans les articles L.1332-6-1 à L. 1332-6-6 du Code de la Défense) prévoit des articles destinés à protéger les infrastructures vitales nationales contre les attaques informatiques. Le plus important, l'article 22, permet de fixer des règles de sécurité obligatoires. Un décret d'application est pris pour chaque secteur d'activité.

Ces arrêtés fixent les critères à suivre pour que chaque OIV identifie les systèmes d'importance vitale dans leur activité et les déclare à l'ANSSI. Il existe 20 règles de sécurité obligatoires à appliquer à ces systèmes. Il y a des règles organisationnelles (audit régulier à effectuer) ou des règles techniques (avoir des mots de passe, séparer les comptes administrateurs, des règlements techniques). Ce sont des règles obligatoires, incontournables, sans aucune dérogation possible.

« La transposition à partir d'une directive, plutôt que d'un règlement, permet de mieux respecter la coopération entre les États membres. »

Il y a une obligation de notifier à l'ANSSI les incidents de sécurité qui affectent ces secteurs d'importance vitale. Le but premier de l'ANSSI est donc d'accompagner les OIV dans la mise en place de leurs systèmes de sécurité, d'où la possibilité d'envoyer des prestataires de qualité pour assurer des contrôles.

Loi 2006 – Directive NIS : du pareil au même ?

Le système mis en place par la directive NIS ressemble à l'arsenal législatif de la Loi de Programmation Militaire (LPM) avec la protection des opérateurs essentiels. La LPM a un champ d'application plus large que la directive car elle s'applique à la Défense.

« L'ANSSI souhaite profiter de cette directive pour étendre les règles qui s'appliquent aux OIV à des opérateurs qui sont essentiels à l'économie et qui ne sont pas des OIV. »

Pour le moment, la transposition de la directive en est à ses débuts. Deux possibilités sont envisageables. La première est de dire que tout ce qui n'est pas couvert par le dispositif OIV le serait par la directive NIS.
Il est également envisageable d'interpréter strictement la directive puisqu'elle a un périmètre d'application plus restreint que l'OIV. La directive est plus axée préservation des secteurs économique et social.

Qu'en est-il de la vision de l'ANSSI sur cette question ? Le directeur général de l'ANSSI souhaite profiter de cette directive pour étendre les règles qui s'appliquent aux OIV à des opérateurs qui sont essentiels à l'économie et qui ne sont pas des OIV.
On considère que les règles qui s'appliquent aux OIV sont des règles de base d'hygiène informatique. Certains mécanismes sont coûteux, tels que toutes les règles obligeant à utiliser des prestataires qualifiés par le Premier Ministre.

Cette extension se ferait selon deux axes. D'abord, il s'agirait de toucher des acteurs de même type que les OIV, mais pas assez sensible pour être OIV. Ainsi certains aéroports sont OIV quand d'autres, parfois dans la même zone, ne le sont pas. Ensuite, au sein des secteurs d'importance vitale, il s'agirait de diversifier les acteurs touchés par la NIS pour toucher quelques acteurs jusque-là non inclus dans la protection OIV.

La directive NIS - application

Selon Maître Garance Mathias, la directive NIS se traduira légalement, pour les acteurs économiques et sociétaux concernés, par la mise en place de niveaux de sécurité informatique sur leurs systèmes sensibles. Cela se passera via une extension des 20 règles de sécurité informatique déjà présentes dans la loi de 2006, ainsi que d'une procédure de notification des incidents.
A partir de quel degré faut-il notifier l'ANSSI ? Il ressort que, dans la vision de l'ANSSI, le devoir de notification intervient même si l'incident n'a pas eu d'impact sur l'activité de la structure.

Quelques zones d'imprécisions demeurent.
Ainsi, l'évaluation des risques se fera en fonction des impacts des dégâts potentiels, mais ces impacts économiques et sociétaux sont difficiles à appréhender.
De même, dans le cas de recours à des sous-traitants pour l'activité sensible, il sera de la responsabilité de l'acteur en question d'organiser la sécurisation des procès vitaux des sous-traitants.

CE QU'IL FAUT RETENIR

- Volonté de mettre en place une obligation de moyens de protection pour les infrastructures critiques.
- Il existe 20 règles de sécurité obligatoires à appliquer : il y a des règles organisationnelles et des règles techniques, qui sont des règles obligatoires, incontournables, et sans aucune dérogation possible.
- La transposition à partir d'une directive, plutôt que d'un règlement, permet de mieux respecter la coopération entre les États membres.
- L'ANSSI souhaite profiter de cette directive pour étendre les règles qui s'appliquent aux OIV à des opérateurs qui sont essentiels à l'économie et qui ne sont pas des OIV.