Réponse de Synergrid à la Consultation publique sur l'avant-projet de "Loi NIS2" et le projet d'arrêté royal d'exécution - Centre pour la Cybersécurité Belgique (belgium.be) -

Le 20 décembre 2023

Synergrid, la Fédération belge des gestionnaires de réseaux, remercie le Premier Ministre et son gouvernement, par le biais du Centre pour la Cybersécurité Belgique (CCB), de solliciter son avis et avoir ainsi la possibilité de contribuer à la transposition de la directive NIS 2 en droit belge.

Synergrid constate de belles avancées depuis ses premiers commentaires apportés en juillet à une des premières versions.

À propos de Synergrid, The Voice of the Belgian Energy Networks

Synergrid est le porte-parole des gestionnaires de réseaux de gaz et d'électricité belges (*). À ce titre, elle est l'interlocuteur du secteur auprès des autorités belges et européennes et toute autre instance qui sollicite la Fédération. Synergrid représente 9 entreprises qui ensemble desservent en gaz et en électricité les entreprises et la population sur la totalité du territoire belge. Avec nos membres, et grâce à des projets innovants, nous aidons les clients à œuvrer à une transition énergétique afin d'atteindre les objectifs climatiques et améliorer la qualité de vie de tous. Synergrid élabore aussi des normes sur le plan technique et environnemental afin de garantir des réseaux fiables répondant aux critères les plus stricts en matière de sécurité. Ces normes s'adressent à ses membres mais aussi à des tiers. En fonction du contexte dans lequel elles s'inscrivent, ces normes ont un caractère légalement obligatoire ou sont des règles de l'art à respecter comme telles par leurs destinataires. Synergrid accompagne ses membres et collabore avec eux à la mise en œuvre de nouvelles plateformes dans le domaine de la flexibilité, comme le FlexHub (unique plateforme en Belgique pour la gestion de la flexibilité) et la RTCP ('Real time communication platform'). Enfin, Synergrid est le conseiller de référence de ses membres en matière de droit social, des relations sociales et auprès des organismes de fonds de pensions sectoriels. La Fédération assume également le rôle de porte-parole patronal du secteur au sein des organes de concertation sociale au niveau national.

(*) Gestionnaires de transmission (GRT) : Elia, Fluxys, et de distribution (GRD) : Aieg, Aiesh, Fluvius, ORES, Resa, REW et Sibelga

1 Transposer la directive en droit belge tout en restant proche des réalités

Synergrid et ses membres pointent des améliorations notables des textes en projet qui faciliteront la mise en œuvre de la directive dite « NIS 2», reprise sous NIS 2 ci-après.

1.1 Lex specialis derogat generalis

Les membres de Synergrid, les gestionnaires de réseaux de distribution et de transport d'électricité et de gaz ayant été désignés opérateurs essentiels sous NIS 1 insistent sur l'importance d'une transition qui soit à la fois facilement réalisable sur le plan opérationnel et aussi compatible avec les règles européennes qui leur sont directement applicables comme le Network code on Cyber Security. En effet, ce Code européen, de caractère réglementaire, valable sur le territoire européen pour l'ensemble des gestionnaires de réseaux d'électricité (à l'avenir la parallèle en gaz sera établie), impose ses propres règles à notre secteur. Ce Règlement européen n'ignore pas l'existence de NIS 2 mais est à considérer comme une législation spécifique aux gestionnaires de réseaux d'énergie. Selon le principe *Lex specialis derogat generalis,* comment concilier NIS 2 et le Network Code *?*

1.2 S'assurer que le délai pour répondre aux décisions des autorités réglementaires est réalisable

Art. 51,§2, et art.52,§2 : le délai pour répondre aux projets de décisions des autorités réglementaires est de 15 jours. Ce délai est trop court et devrait être porté au moins à 30 jours.

1.3 Éviter à tout prix d'avoir à notifier le même incident par différents canaux

Nous insistons sur le respect du principe du *one stop shop* selon lequel un incident ne doit déclencher qu'un seul message .

Dans le même ordre d'idées, nos membres réitèrent le besoin d'une grille de lecture homogène et claire sur les éléments à notifier : tout notifier n'est ni soutenable ni opportun. Si le terme « significatif » de l'article 34, §1er, laisse à l'entité essentielle une parfaite autonomie quant aux incidents à notifier ou pas en fonction de ce qu'elle considère être significatif, nous pouvons accepter cette approche libre. Il ne saurait, par conséquent, être reproché à l'entité un quelconque manquement.

1.4 Éviter de créer des risques supplémentaires en exigeant des informations

Art. 58, 7° : Synergrid insiste pour que la publication visée n'ait pas pour effet de divulguer des failles encore existantes ou en cours de remédiation, ce qui serait de nature à créer de nouveaux risques. Il en va de même pour l'article 9 de l'annexe 3 de l'arrêté royal : nous considérons qu'il est dangereux d'envoyer au même endroit toutes les analyses de risques. Nous proposons de tenir à disposition des autorités ces analyses et de les présenter à première demande.

De manière générale, nous tenons à éviter les doubles notifications ainsi que la multiplication des destinataires des notifications.

1.5 Le *gold plating* ne rendra pas la Belgique plus sûre.

L'art. 33 prévoit la possibilité d'imposer des mesures supplémentaires pour gérer les risques de cybersécurité. Dans l'exposé des motifs, le législateur précise à juste titre que des mesures peuvent être prises pour expliquer comment les principes prévus doivent être appliqués à un secteur spécifique. Mais la possibilité d'imposer des mesures supplémentaires est également prévue. La Belgique doit soutenir l'établissement et l'alignement avec des normes internationales comme ISO27001 ou les différentes normes internationales d'effet équivalent.

Nous attirons également votre attention sur le point 3.2 ci-après où le législateur belge dépasse à notre sens inopportunément la lettre et l'esprit de la directive.

2 Une mise en œuvre phasée

Synergrid se félicite de ce que la norme ISO27001 reste un cadre de référence. L'implication des autorités sectorielles est également un élément important. La mise en œuvre progressive, prévoyant un délai de 18 mois et 12 mois supplémentaires pour les entités essentielles prévues, doit être maintenue.

Nous rappelons les éléments à conserver :

- Arrêté royal - art. 22 : Les textes définissent une mise en œuvre progressive à la fois en termes de calendrier, de trajet et de nombre de contrôles. Nous soutenons la direction envisagée.
- Art. 3.2 : Synergrid souligne l'importance de prendre en compte le niveau d'indépendance du réseau et du système d'information, que ce soit par des mesures techniques comme la segmentation du réseau et/ou la séparation contractuelle et donner aux autorités la souplesse nécessaire pour une collaboration optimale.

3 Questions complémentaires importantes à clarifier

3.1 *Comment* s'assurer que le travail réalisé à partir de NIS 1 est adapté à NIS 2 ?

La loi de transposition de « NIS 2 » abroge la loi « NIS 1 ». Pour les entités qui se sont préparées pour la mise en œuvre de NIS 1, des adaptations sont nécessaires quant à leurs nouvelles obligations. Par exemple, la portée de l'applicabilité pour ceux qui sont certifiés ISO27001 ou qui envisagent de le faire, est un point d'attention important pour garantir une transposition opérationnelle efficiente.

3.2 *Sous*-entité visée ou non, à qui s'adresser, définition d'une entité ?

Il nous semble opportun de préciser ce qu'on entend par « sous-entité est concernée ». Les organisations ont des installations de recherche internes, des centres de services partagés, des entités séparées en charge des activités de call center, etc.

Dans le cas où une entité est impliquée dans une activité essentielle et importante du secteur, cela signifie-t-il automatiquement que l'ensemble de l'entité est classé comme entité essentielle ? Cette décision est-elle fondée sur la taille de la sous-entité ?

3.3 *L'article* 8 prévoit une définition large de « réseau et système d'information »

Le réseau est ainsi entendu comme « *tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un* programme*, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; » …*

Cette définition va beaucoup plus loin que la directive. Ceci est-il une volonté de limiter le pouvoir d'appréciation des entités essentielles et importantes quant aux éléments qui devront être ou non considérés comme « sensibles » ?

Pour le cas des distributeurs d'énergie par exemple, la volonté du législateur semble être de couvrir les compteurs digitaux (compteurs communicants). Ne serait-il pas plus opportun de donner la possibilité aux entités essentielles de déterminer elles-mêmes les mesures à mettre en place en fonction de la connaissance critique de leurs assets et des analyses de risques réalisées sur les processus les impliquant sachant que, dans le même temps, ces mêmes entités essentielles deviennent infrastructures critiques au sens de la directive CER 2022/2557 ?

3.4 *Responsabilité* des organes de direction (directeur général, comité de direction, conseil d'administration) à clarifier :

Art. 31 : cet article rend les organes de direction responsables des violations de la loi . L'article 60 peut temporairement interdire aux personnes physiques membres de ces organes d'exercer leurs missions. Ces textes doivent être modifiés pour s'assurer que les personnes visées ne puissent pas être interdits temporairement d'exercer leurs missions. D'autres solutions existent et devraient être privilégiées.

Le manque de clarté de l'article 61 vient ajouter une confusion supplémentaire sur les responsabilités encourues.

3.5 La *présomption* de conformité demeure cruciale

L'article 42 accorde une présomption de conformité aux entités qui font régulièrement l'objet d'évaluations de conformité. La présomption demeure cruciale pour les opérateurs actuels de services essentiels en vertu de la directive NIS 1. Il faut tenir compte du travail accompli depuis des années sur les trajectoires de certification. Nous partons donc du principe que les revues annuelles réalisées dans le cadre de la certification ISO27001 sont conformes aux exigences visées à l'article 42.

Il y a lieu de clarifier la valeur réelle de l'effort de certification. L'article 44 précise clairement que les services d'inspection contrôlent la conformité. Le paragraphe 3 permet que les inspections soient fondées sur une analyse des risques. Il conviendrait de préciser dans quelle mesure l'analyse des risques sera fondée sur les évaluations de conformité régulièrement effectuées. Une entité qui fait l'objet d'une évaluation de conformité est-elle considérée comme une entité à faible risque ? Et partant, peut-elle se concentrer sur la mise en œuvre des résultats de l'évaluation de la conformité externe au lieu de consacrer de l'énergie à la préparation d'une éventuelle inspection supplémentaire ?

3.6 La *supervision* des entités par le service d'inspection

Art. 50,§2 : le mot rétribution nous paraît inapproprié juridiquement.

Contact : Christine Declercq – Email : christine.declercq@synergrid.be