INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS

AVIS DU CONSEIL DE L'IBPT DU 15 MAI 2019 CONCERNANT LE PROJET D'ARRÊTÉ ROYAL PORTANT EXÉCUTION DE LA LOI NIS, AINSI QUE DE CERTAINES DISPOSITIONS DE LA LOI « INFRASTRUCTURES CRITIQUES »

Institut belge des services postaux et des télécommunications
Ellipse Building - Bâtiment C - Boulevard du Roi Albert II 35 - 1030 Bruxelles
Tél. 02 226 88 88 Fax 02 226 88 77 http://www.ibpt.be

TABLE DES MATIÈRES

1. Objet

1. Par une lettre du 2 mai 2019, le Centre pour la Cybersécurité Belgique (ci-après CCB) a demandé à l'IBPT, en sa qualité d'autorité sectorielle pour le secteur des infrastructures numériques, de rendre un avis pour le 17 mai 2019 au plus tard concernant l'article 11 du projet d'arrêté royal (ci-après le projet d'arrêté royal) portant exécution de la loi NIS ainsi que de certaines dispositions de la loi « infrastructures critiques » (voir annexe) [1].

2. Conformément à l'article 14, § 1er, 1°, de la loi IBPT-statut[2], l'IBPT rend un avis au ministre[3] ou à la Chambre des représentants. Etant donné que la loi NIS[4] ne prévoit pas que l'avis de l'IBPT sur le projet d'arrêté royal doit être rendu au CCB, le présent avis est rendu à Monsieur le ministre Philippe De Backer, ministre de l'Agenda numérique et des Télécommunications. Une copie du présent avis est envoyée au CCB. L'IBPT rappelle que le présent avis sera publié sur son site internet.

3. Dans sa lettre, le CCB demande un avis à l'IBPT uniquement sur l'article 11 du projet d'arrêté royal, vu qu'en vertu de la loi NIS les autorités sectorielles doivent rendre un avis sur cet article 11 mais pas sur les autres dispositions du projet d'arrêté royal. Néanmois, l'IBPT formule quelques remarques sur les autres articles du projet d'arrêté royal sur base de la possibilité que lui confère l'article 14, § 1er, 1°, de la loi IBPT-statut de donner un avis d'initiative au Ministre[5].

4. L'IBPT estime qu'une consultation publique concernant le projet d'arrêté royal et le formulaire de notification des incidents de sécurité aurait été fort utile mais comprend également la nécessité d'adopter rapidement l'arrêté royal, afin de compléter la transposition de la directive NIS[6].

2. Résumé du projet d'arrêté royal

5. Le projet d'arrêté royal fixe les règles suivantes :
   5.1. Le chapitre 1er comprend des définitions ;

---

[1] Le titre complet du projet d'arrêté royal est le suivant : « projet d'arrêté royal portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de certaines dispositions de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ».

[2] Voir article 14, § 1er, 1°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges : « § 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes :
1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants ; ».

[3] Selon l'article 2, 4°, de la loi IBPT-statut, il faut entendre par « Ministre », « le ministre ou secrétaire d'Etat qui a les services postaux ou les télécommunications dans ses attributions. »

[4] Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

[5] Voir note de bas de page n° 2.

[6] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

5.2. Le chapitre 2 et les annexes 1 et 2 déterminent les autorités compétentes, à savoir le CCB, la Direction Générale Centre de Crise (DGCC), les autorités sectorielles et les services d'inspection[7] ;
5.3. Le chapitre 3 contient des règles relatives à la notification et le traitement des incidents ;
5.4. Le chapitre 4 contient des règles relatives aux notifications volontaires ;
5.5. Le chapitre 5 contient des règles concernant l'acréditation des organismes d'évaluation de la conformité.

3. Remarques de l'IBPT sur le contenu du projet d'arrêté royal

3.1. Préambule

6. Le préambule du projet d'arrêté royal indique qu'il est pris « vu l'avis des autorités sectorielles sur l'article 11 de la loi du 7 avril 2019 ». L'IBPT suppose que ce considérant vise en réalité l'article 11 du projet d'arrêté et non l'article 11 de la loi NIS. Comme indiqué ci-dessus, l'IBPT rend son avis sur l'ensemble du projet d'arrêté royal et non uniquement sur son article 11.

3.2. Titres des chapitres 3 et 4

7. Les titres des chapitres 3 et 4 devraient être revus, car les notifications volontaires (d'incidents) visées au chapitre 4 sont une forme de notification d'incidents au sens du chapitre 3.

3.3. Article 5. Plate-forme sécurisée de notification

8. L'article 5 du projet d'arrêté royal prévoit ce qui suit :

« Art. 5. Une plate-forme sécurisée de notification est créée afin de faciliter :

1°) l'envoi par les opérateurs de services essentiels et les fournisseurs de service numérique au CSIRT national, à l'autorité sectorielle ou son CSIRT sectoriel, et à la DGCC, des notifications d'incidents de sécurité effectuées en vertu de la loi du 7 avril 2019 ;

2°) la possibilité d'envoi, par les opérateurs de services essentiels et les fournisseurs de service numérique, d'une notification de violations de données à caractère personnel à une autorité de contrôle des données à caractère personnel, telle que prévue par l'article 31, § 1er, al. 2 de la loi. »

9. Il convient de préciser qu'il s'agit de tâches minimum de la plate-forme de notification, vu qu'il est envisagé que cette plate-forme permette aussi la notification des incidents de sécurité des opérateurs télécom envers l'IBPT. Il pourrait également être envisagé que cette plate-forme soit utilisée pour certaines notifications volontaires d'incident de sécurité, s'il apparaît dans la pratique que cela facilite l'envoi ou le traitement de ces notifications.

3.4. Articles 6 et 7. Notification des incidents

10. Les articles 6 et 7 du projet d'arrêté royal prévoient ce qui suit :

[7] L'IBPT n'est pas cité dans l'arrêté royal, ce qui s'explique par le fait que c'est la loi elle-même qui confère la qualité d'autorité sectorielle et de service d'inspection de l'IBPT pour le secteur des infrastructures numériques.

« Art. 6. § 1er. La notification est réalisée via la plate-forme de notification et moyennant l'utilisation du formulaire de notification d'incident déterminé par le CSIRT national. […]

Art. 7. Le CSIRT national détermine les modalités de notification à utiliser par les opérateurs de services essentiels et les fournisseurs de service numérique, en cas d'indisponibilité de la plate-forme de notification visée à l'article 6. »

11. La notification d'incidents de sécurité constitue une source d'information essentielle pour l'exercice de la compétence de l'IBPT. Dès lors, ce dernier estime que c'est en concertation avec les autorités sectorielles, dont l'IBPT, que le CSIRT national devrait fixer le contenu du formulaire de notification d'incident ainsi que les modalités de notification à utiliser par les opérateurs de services essentiels et les fournisseurs de service numérique, en cas d'indisponibilité de la plate-forme de notification.

3.5. Article 9. Protocole d'accord

12. L'article 9 du projet d'arrêté royal prévoit ce qui suit :

« Le CSIRT national, les autorités sectorielles et la DGCC concluent un protocole d'accord pour fixer entre autres :

1° les modalités de gestion de la plate-forme de notification ;
2° les modalités du traitement des notifications visées à l'article 8, § 3 ;
3° les modalités relatives aux demandes d'information complémentaire à l'opérateur de services essentiels ou au fournisseur de service numérique visées à l'article 6, § 4. »

13. L'IBPT estime que ce protocole devrait non seulement fixer « les modalités relatives aux demandes d'information complémentaire à l'opérateur de services essentiels ou au fournisseur de service numérique visées à l'article 6, § 4. » (3°) mais aussi ces modalités pour l'article 8, § 1er, qui prévoit ce qui suit :

« Art. 8. § 1er. Le CSIRT national, l'autorité sectorielle ou son CSIRT sectoriel ou la DGCC peuvent demander à l'opérateur de services essentiels ou au fournisseur de service numérique des informations complémentaires sur les notifications qu'il a effectuées. »

14. En effet, tout comme pour l'article 6, § 4, il existe un risque que la mise en œuvre de l'article 8, § 1er, mène à des demandes parallèles d'informations complémentaires des autorités envers un opérateur de service essentiel.

3.6. Article 10. Notifications volontaires

15. L'article 10, § 3, du projet d'arrêté royal prévoit ce qui suit : « Le CSIRT national transmet les informations relatives à ces notifications à la DGCC et aux autorités sectorielles ou CSIRT sectoriels potentiellement intéressés. »

16. Vu que la notification d'incident de sécurité est essentielle pour l'IBPT, ce dernier souhaiterait recevoir la notification volontaire et non uniquement des informations relatives à cette notification.

3.7. Article 11. Accréditation des organismes d'évaluation de la conformité

17. La loi NIS vise une accréditation des organismes d'évaluation de la conformité dans les deux articles suivants :

17.1. L'article 22, § 2 : « Le respect des exigences visées au paragraphe 1er [à savoir le fait que la politique de sécurité de l'information de l'opérateur de service essentiel réponde aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi] est établi par un certificat délivré par un organisme d'évaluation de la conformité accrédité selon la norme ISO/IEC 17021 ou ISO/IEC 17065 par l'autorité d'accréditation ou par une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation". (c'est nous qui soulignons)

17.2. L'article 38, § 2 : « L'opérateur de services essentiels fait réaliser, au moins tous les trois ans et à ses frais, un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par l'autorité nationale d'accréditation, ou par une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation".[…] » (c'est nous qui soulignons)

18. En pratique, un « organisme d'évaluation de la conformité » visé dans ces deux articles est un « organisme qui effectue des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection »[8] et l' « autorité nationale d'accréditation » visée à l'article 38, § 2[9], est BELAC, qui est constitué au sein du SPF Economie, P.M.E., Classes moyennes et Energie[10].

19. L'article 39, § 1er, de la loi NIS prévoit ce qui suit : « Après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er [en pratique le CCB], le Roi fixe: 1° les conditions générales d'accréditation sur base des exigences des normes ISO/IEC 17021 ou ISO/IEC 17065 […] ».

20. Cette disposition est exécutée dans l'article 11 du projet d'arrêté royal comme suit :

« Les organismes d'évaluation de la conformité qui souhaitent être accrédités pour l'audit externe d'opérateurs de services essentiels, visés à l'article 38, § 2 de la loi, ou de fournisseurs

---

[8] L'article 6, 5°, de la loi NIS définit un organisme d'évaluation de la conformité comme suit : « organisme visé à l'article I.9 du Code de droit économique ». L'article I. 9 contient les définitions suivantes :
4° " Accréditation " : attestation formelle délivrée par l'organisme national d'accréditation selon laquelle un organisme d'évaluation de la conformité satisfait aux critères définis par les normes harmonisées et, si d'application, à toute autre exigence supplémentaire, notamment celles fixées dans les programmes sectoriels pertinents, requis pour effectuer une opération spécifique d'évaluation de la conformité;
5° " Système d'accréditation " : système ayant ses propres règles de gestion et destiné à permettre la mise en oeuvre de la procédure d'accréditation;
6° " Evaluation de la conformité " : processus évaluant s'il est démontré que des exigences définies relatives à un produit, processus, service, système, personne ou organisme ont été respectées;
7° " Organisme d'évaluation de la conformité " : organisme qui effectue des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection; »

[9] L'article 22, § 2, vise « l'autorité d'accréditation » mais l'IBPT suppose qu'il s'agit en réalité de l'autorité nationale d'accréditation.

[10] L'article 6, 7°, de la loi NIS définit une "autorité nationale d'accréditation" comme un « organisme créé par le Roi en exécution de l'article VIII.30 du Code de droit économique ». Cet article VIII.30 prévoit ce qui suit : « § 1er. Le Roi peut, par arrêté délibéré en Conseil des Ministres, prendre toutes les mesures utiles en vue de créer un système d'accréditation. Il créera notamment, à cet effet, un organisme national d'accréditation unique et un Conseil national d'accréditation.
§ 2. L'organisme national d'accréditation est responsable de la gestion de la procédure pour obtenir l'accréditation, y compris la délivrance et le retrait des accréditations. […]
§ 4. Le Roi fixe, après consultation du Conseil national d'Accréditation, par arrêté délibéré en Conseil des ministres, les critères d'accréditation des organismes d'évaluation de la conformité.
§ 5. Les certificats et rapports d'évaluation de la conformité qui ont été délivrés par les organismes accrédités en vertu du présent Titre sont reconnus par l'Etat belge. »

de service numérique doivent introduire une demande auprès de l'autorité d'accréditation nationale ou d'un organisme officiel d'accréditation d'un autre pays.

Les conditions auxquelles l'organisme d'évaluation de la conformité doit répondre pour être accrédité à cette fin sont les suivantes :

1° satisfaire, à tout moment, aux critères d'accréditation concernant à la fois l'opérationnalité du système de gestion appliqué et les aspects techniques spécifiques mentionnés dans la norme ISO/CEI 17021 ou ISO/CEI 17065 concernée;
2° satisfaire aux procédures de fonctionnement du système d'accréditation qui sont applicables aux organismes accrédités. »

21. Tout d'abord, l'article 11 du projet d'arrêté royal ne devrait pas uniquement se référer aux audits externes visés à l'article 38, § 2, de la loi NIS mais aussi à la conformité de la politique de sécurité de l'information (PSI) dont il est question à l'article 22, § 2, de cette même loi, vu que les règles que l'article 11 énonce sont pertinentes pour ces deux articles.

22. Ensuite, pour assurer une conformité entre les articles 22, § 2 et 38, § 2, de la loi NIS d'une part et l'article 11 du projet d'arrêté royal d'autre part, il convient de viser dans cet article « une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation" » comme prévu aux articles 22, § 2 et 38, § 2, et non « un organisme officiel d'accréditation d'un autre pays »[11].

23. Finalement, les éléments suivants contenus dans l'article 11 ne sont pas clairs pour l'IBPT :

- Que faut-il comprendre par les « critères d'accréditation concernant à la fois l'opérationnalité du système de gestion appliqué et les aspects techniques spécifiques mentionnés dans la norme ISO/CEI 17021 ou ISO/CEI 17065 concernée » ? En particulier, de quel « système de gestion appliqué » s'agit-il et que vise-t-on par les « aspects techniques spécifiques » ? Existe-t-il des aspects techniques qui ne sont pas spécifiques ?
- Quelles sont les « procédures de fonctionnement du système d'accréditation qui sont applicables aux organismes accrédités » ? En vertu de quoi sont-elles applicables ?

24. L'IBPT constate que le rapport au Roi n'apporte pas de réponse à ces différentes questions.

25. L'IBPT conseille d'associer BELAC pour la clarification du texte.

4. Annexe

26. En annexe se trouve le projet d'arrêté royal sur lequel l'avis est rendu.

[11] L'article 11 du projet d'arrêté royal vise « l'autorité d'accréditation nationale » mais il s'agit selon l'article 6, 7°, de la loi NIS, de l'autorité nationale d'accréditation.

Axel Desmedt
Membre du Conseil

Jack Hamande
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil