INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS

PROJET DE DÉCISION DU CONSEIL DE L'IBPT DU XX/XX/XXXX CONCERNANT LES SEUILS ET LES MODALITÉS DE NOTIFICATION D'INCIDENTS DE SÉCURITÉ DANS LE SECTEUR DES COMMUNICATIONS ELECTRONIQUES

MÉTHODE D'ENVOI DES RÉACTIONS AU PRÉSENT DOCUMENT

Délai de réponse :	Jusqu'au 15/09/2017
Méthode pour répondre :	À : consultation.sg@ibpt.be Objet: « CONSULT-2017-C2 »
Personne de contact :	Tim Masy, Ingénieur-conseiller (+32 (0)2 226 89 74)

Les réponses sont attendues uniquement par voie électronique.

Vous êtes prié d'utiliser le Formulaire de couverture à joindre à la réponse à une consultation publique organisée par l'IBPT.

L'IBPT demande également que les commentaires se réfèrent aux paragraphes et/ou parties dont ils traitent. Le document doit indiquer clairement ce qui est confidentiel.

TABLE DES MATIÈRES

1 Contexte

1.1 Objet

1 La présente décision remplace la décision du Conseil de l'IBPT du 1er avril 2014 fixant les hypothèses dans lesquelles les opérateurs doivent notifier un incident de sécurité à l'IBPT et les modalités de cette notification.

1.2 Objectifs

2 Après évaluation des notifications d'incident de sécurité (ci-après « *notifications* ») reçues depuis la décision du 1er avril 2014 , un abaissement et une simplification des des seuils de notification s'avère nécessaire pour que l'IBPT ait une meilleure connaissance des incidents de sécurité (ci-après « incidents ») ayant un impact significatif. En outre, la modification des modalités de notification est nécessaire pour une collecte automatisée et un stockage structuré des notifications.

3 Les modifications proposées contribueront à un monitoring efficace de la sécurité des réseaux et des services. Sur cette base, une analyse plus détaillée des risques pour le secteur peut être réalisée afin de pouvoir adapter en conséquence les mesures de sécurité minimales pour le secteur.

4 La présente décision est basée sur les lignes directrices techniques les plus récentes d'ENISA en la matière[1] et a pour but d'assurer la cohérence entre les notifications des opérateurs à l'IBPT et le rapport succinct de l'IBPT à l'ENISA et la Commission européenne. Comme recommandé dans les ligne directrices[2], des seuils plus sévères et un champ d'application plus large sont appliqués dans la présente décision par rapport à ceux repris dans les lignes directrices.

1.3 Base juridique

5 L'article 114/1, §2, de la de la loi du 13 juin 2005 relative aux communications électroniques (ci-après la « LCE »)prévoit :

> *« Les entreprises fournissant des réseaux publics de communications ou des services de communications électroniques accessibles au public notifient sans délai à l'Institut toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services. Après autorisation préalable du ministre, l'Institut précise dans quelles hypothèses l'atteinte à la sécurité ou perte d'intégrité a un impact significatif au sens du présent alinéa. »*

6 Pour ce qui concerne les aspects de la présente décision qui ne concernent pas les hypothèses dans lesquelles l'atteinte à la sécurité ou perte d'intégrité a un impact significatif, la présente décision s'appuie sur l'article 114/2, §1er, de la LCE, qui prévoit ce qui suit :

> *« § 1er. « L'Institut a le pouvoir de donner des instructions contraignantes, y compris concernant les dates limites de mise en œuvre, aux entreprises fournissant des réseaux publics de communications électroniques ou des services de communications électroniques accessibles au public, en vue de l'application des articles 114 et 114/1. ».*

---

[1] ENISA Technical Guideline on Incident Reporting in Article 13a Version 2.1, October 2014. https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

[2] Citation du chapitre 6 Annual summary reporting :
« Dans cette section, nous définissons la portée et les seuils du reportage annuel succinct par les ARN à l'ENISA et la CE. Nous tenons à souligner que cette section ne doit pas être considérée comme une recommandation concernant les incidents à considérer comme significatifs (au niveau national) ni sur les incidents à notifier au niveau national. Les ARN devraient utiliser une portée plus large et des seuils plus stricts en tenant compte, le cas échéant, des circonstances et exigences nationales. » (traduction libre).

1.4 Procédure

1.4.1 Consultation publique

7 Du XX/XX/2017 au XX/XX/2017, l'IBPT a organisé une consultation publique concernant le projet de la présente décision, sur la base de l'article 14, § 2, 1°, première phrase, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.

1.4.2 Consultation des régulateurs médias

8 En vertu de l'article 3 de l'accord de coopération du 17 novembre 2016[3], l'IBPT a transmis le projet de la présente décision aux régulateurs médias des communautés, à savoir le CSA, le Medienrat et le VRM, en date du XX/XX/2017.

1.4.3 Autorisation du ministre

9 Par courrier du XX/XX/2017, monsieur Alexander De Croo, Vice-Premier ministre et ministre de la Coopération au développement, de l'Agenda numérique, des Télécommunications et de la Poste, a donné l'autorisation préalable visée à l'article 114/1, § 2, de la LCE.

2 Hypothèses pour la notification d'incidents

2.1 Champ d'application

10 L'obligation de notification prévue dans la présente décision, en vertu de l'article 114/1, § 2, de la LCE, s'applique tant aux entreprises fournissant des réseaux publics de communications électroniques[4] (ci-après « *réseaux* ») qu'aux entreprises fournissant des services de communications électroniques accessibles au public[5] (ci-après « *services* »), ces entreprises étant dénommées ci-après les opérateurs.

11 La présente décision s'applique à tous les réseaux et services[6].

12 Pour l'application de la présente décision, il faut entendre par « *incident* », une atteinte à la sécurité ou une perte d'intégrité ayant un impact sur le bon fonctionnement ou la sécurité des réseaux et des services[7].

13 La « *sécurité des réseaux et des services* » est définie[8] comme la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou traitées ou des services connexes offerts par ou rendus accessibles via ces réseaux ou services.

---

3 Accord de coopération du 17 novembre 2006 entre l'État fédéral, la communauté flamande, la communauté française et la communauté germanophone, relatif à la consultation mutuelle lors de l'élaboration d'une législation en matière de réseaux de communications électroniques, lors de l'échange d'information et lors de l'exercice de compétences en matière de réseaux de communications électroniques par les autorités de régulation en charge des télécommunications ou de la radiodiffusion et de la télévision. Moniteur belge du 28.12.2006, p. 75371.

4 Le terme « *réseau de communications électroniques* » est défini à l'article 2, 3°, de la LCE.

5 Le terme « *service de communications électroniques* » est défini à l'article 2, 5°, de la LCE.

6 Les services concernés comprennent entre autres les services suivants : téléphonie fixe, Internet fixe, téléphonie mobile, Internet mobile, lignes louées, SMS, MMS, itinérance internationale, Wi-Fi public, services vocaux via Internet, services de messagerie via Internet, e-mails publics.

7 Sur la base de la définition des lignes directrices techniques d'ENISA, chapitre 3.3.

8 Définition extraite de la proposition 2016/2088(COD) de la Commission européenne de Directive du Parlement européen et du Conseil fixant le Code européen pour les communications électroniques.

2.2 Seuils

14 L'obligation de notification s'applique à tout incident ayant un impact significatif sur le fonctionnement ou la sécurité des réseaux et de services. L'impact d'un incident est considéré comme significatif lorsqu'au moins un des seuils suivants a été atteint ou dépassé :

1) l'incident dure au moins 1 heure et affecte au moins 25 000 utilisateurs finals[9] ;

2) l'incident a un impact sur le réseau affectant ainsi l'accès aux services d'urgence[10] via ce réseau ;

3) l'incident a un impact sur des interconnexions[11] affectant ainsi d'autres opérateurs en Belgique ou à l'étranger ;

4) l'incident a un impact sur un élément de réseau que l'opérateur considère comme critique pour le fonctionnement de ses réseaux ou services.

15 Si un opérateur le juge utile, il peut notifier chaque incident, même si celui-ci ne répond pas aux seuils précités.

16 Chaque abonné, chaque ligne, chaque numéro d'appel ou carte SIM active affecté(e) par un incident, correspond à un utilisateur final.

17 Lorsque le nombre d'utilisateurs finals affectés ne peut être déterminé avec exactitude[12], le fournisseur procède autant que possible à une estimation du nombre d'utilisateurs finals affectés en tenant compte de l'utilisation normale des installations affectées.

18 Dans de nombreux incidents, plusieurs services sont affectés simultanément. Le nombre d'utilisateurs affectés peut différer selon le service affecté. Dans ces cas-là, l'opérateur mentionne les chiffres séparément par service affecté dans la même notification.

19 La présente section ne porte pas préjudice à la possibilité pour l'IBPT de demander à un ou plusieurs opérateurs, sur base de l'article 114/2, § 2, de la LCE, de lui rapporter un type d'incident spécifique. Ce rapportage s'effectuera également conformément à la section 3 ci-dessous.

3 Modalités pour la notification d'incidents

20 Sans délai après avoir constaté l'incident, une notification écrite succincte doit être transmise à l'adresse électronique « incident@ibpt.be », contenant uniquement des informations de base sur l'incident et l'impact[13] Une nouvelle notification succincte sera effectuée si de nouvelles informations sont connues ou lorsque des développements importants surviennent.

21 Dans les 3 jours qui suivent le constat de l'incident, une notification complète est envoyée à l'IBPT via le formulaire mis à disposition par l'IBPT sur la plateforme de notification électronique[14]. Ce formulaire comprendra au moins les éléments essentiels

---

9 Ce seuil est basé sur les limites inférieures prévues dans les lignes directrices techniques d'ENISA pour les seuils concernant le nombre d'utilisateurs finals affectés et la durée de l'incident : « Sont exclus, les très petits incidents affectant moins de 25 000 connexions utilisateurs, ainsi que les incidents très courts, d'une durée inférieure à 1 heure » (traduction libre).

10 Le terme « *service d'urgence* » est défini à l'article 2, 58°, de la LCE.

11 Le terme « *interconnexion* » est défini à l'article 2, 19°, de la LCE.

12 Par exemple, pour les utilisateurs de communications électroniques mobiles ou parce que des services sont fournis à d'autres opérateurs (MVNO...) ou à des tiers et donc pas directement à l'utilisateur final.

13 Entre autres les informations déjà disponibles sur les services, réseaux, nombre d'utilisateurs et zone géographique affecté.

14 www.incident.ibpt.be

d'information, tels que repris au point 7 « Incident Report Template » des lignes directrices techniques d'ENISA précitées.

4 Entrée en vigueur et voies de recours

4.1 Entrée en vigueur

22 La présente décision entrera en vigueur le 1er janvier 2018 et remplacera ce jour-là la décision du Conseil de l'IBPT du 1er avril 2014 fixant les hypothèses dans lesquelles les opérateurs doivent notifier à l'IBPT un incident de sécurité et les modalités de cette notification.

4.2 Voies de recours

23 Conformément à l'article 2, §1er de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges, vous avez la possibilité d'introduire un recours contre cette décision devant la Cour des marchés, Place Poelaert 1, B-1000 Bruxelles. Les recours sont formés, à peine de nullité prononcée d'office, par requête signée et déposée au greffe de la Cour d'appel de Bruxelles dans un délai de soixante jours à partir de la notification de la décision ou à défaut de notification, après la publication de la décision ou à défaut de publication, après la prise de connaissance de la décision.

24 La requête contient, à peine de nullité, les mentions requises par l'article 2, §2 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges. Si la requête contient des éléments que vous considérez comme confidentiels, vous devez l'indiquer de manière explicite et déposer, à peine de nullité, une version non-confidentielle de celle-ci. L'Institut publie sur son site Internet la requête notifiée par le Greffe de la juridiction. Toute partie intéressée peut intervenir à la cause dans les trente jours qui suivent cette publication.

Axel Desmedt
Membre du Conseil

Jack Hamande
Membre du Conseil

Luc Vanfleteren
Membre du Conseil

Michel Van Bellinghen
Président du Conseil