INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS

PROJET DE DÉCISION DU CONSEIL DE L'IBPT DU 03/05/2013 FIXANT LES HYPOTHÈSES DANS LESQUELLES LES OPÉRATEURS DOIVENT NOTIFIER À L'IBPT UN INCIDENT DE SÉCURITÉ ET LES MODALITÉS DE CETTE NOTIFICATION

Modalités d'envoi des réactions au présent document
Délai de réponse : Vendredi 7 juin 2013
Personne de contact : Karel Peeters
Adresse de réponse par e-mail : **consult08@bipt.be** Les réponses sont attendues uniquement par voie électronique.
La réaction doit indiquer clairement ce qui est confidentiel en utilisant le formulaire prévu à cet effet [http://www.ibpt.be/ShowDoc.aspx?levelID=384&objectID=3243].
Si la réaction contient des éléments confidentiels, une version publique de la réaction doit être fournie.

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 ET BASES JURIDIQUES

1 La loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques[1] a introduit entre autres un article 114/1, § 2, dans la loi du 13 juin 2005 relative aux communications électroniques (ci-après la LCE). Cet article se lit comme suit (c'est nous qui soulignons):

«*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*. »

2 La présente décision exécute entre autres la dernière phrase de la disposition précitée.

3 La présente décision ne concerne cependant pas l'obligation des entreprises fournissant un service de communications électroniques accessible au public d'informer les abonnés et l'IBPT d'un risque de violation de la sécurité du réseau comme indiqué dans l'article 114/1, § 1, de la LCE[2] :

« *Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, les entreprises fournissant un service de communications électroniques accessible au public informent les abonnés et l'Institut de ce risque et, si les mesures que peuvent prendre les entreprises fournissant le service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable.* » (c'est nous qui soulignons)

4 Par ailleurs, l'article 114/2 de la LCE, tel qu'inséré dans la LCE par la loi du 10 juillet 2012 susmentionnée, 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.* »

5 Sur base de l'article 114/2 et de l'article 114/1, § 2, première phrase, précité, l'IBPT fixe par la présente décision des instructions contraignantes quant à l'obligation pour les opérateurs de notifier sans délai à l'IBPT toute atteinte à la sécurité ou perte d'intégrité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.

6 La présente décision fixe dès lors les modalités pratiques de la notification par les opérateurs à l'IBPT d'incidents de sécurité et détermine ainsi les points suivants :
- le délai dans lequel la notification doit être faite ;
- le mode de transmission de la notification ;
- le contenu de la notification.

7 La notification à l'IBPT d'une atteinte à la sécurité d'un service de communications électroniques accessible au public en matière de données à caractère personnel qui doit être faite en vertu de l'article 114/1, §3, de la LCE n'est pas traitée dans la présente décision et fera l'objet, si nécessaire, de directives distinctes de l'IBPT.

[1] Moniteur belge du 25 juillet 2012, p. 40969.

[2] La présente décision ne traite pas non plus des indemnités que les opérateurs devraient verser aux abonnés en cas d'interruption du service conformément à l'arrêté royal qui pourrait être pris sur base de l'article 113/2 de la LCE.

2. PROCÉDURE

2.1. Consultation publique

8 Du *[sera complété ultérieurement]* au *[sera complété ultérieurement]*, l'IBPT a organisé une consultation publique concernant le présent projet de décision, sur base de l'article 14, § 2, 1°, 1ière phrase, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (ci-après la loi-statut).

9 Ont répondu à cette consultation les personnes suivantes :

[sera complété ultérieurement]

10 La synthèse des résultats de la consultation publique se trouve en annexe à la présente décision.

2.2. Consultation des régulateurs des médias

11 En vertu de l'article 3 de l'accord de coopération du 17 novembre 2006[3], le *[sera complété ultérieurement]*, l'IBPT a transmis le présent projet de décision aux régulateurs média des communautés, à savoir le CSA, le Medienrat et le VRM. Les régulateurs média des communautés ont réagi en répondant *[sera complété ultérieurement]*.

2.3. Autorisation du ministre

12 Par sa lettre du *[sera complété ultérieurement]*, M. Johan Vande Lanotte, Vice-Premier Ministre et Ministre de l'Economie, des Consommateurs et de la Mer du Nord, a donné l'autorisation préalable visée à l'article 114/1, §2, de la LCE pour ce qui concerne les aspects de la présente décision qui traitent des hypothèses dans lesquelles l'atteinte à la sécurité ou perte d'intégrité a un impact significatif sur le fonctionnement des réseaux ou des services, soit concernant le point 4 de la présente décision.

3. CONTEXTE EUROPÉEN

13 La directive 2009/140/CE[4] a introduit entre autres les articles 13*bis* et 13*ter* dans le chapitre III*bis* « Sécurité et intégrité des réseaux et services » de la directive « cadre » de 2002[5]. Les articles 114/1, § 2, et 114/2 de la LCE susmentionnés ont été adoptés dans le cadre de la transposition en droit belge de ces nouveaux articles 13*bis* et 13*ter*.

14 L'ENISA (European Network and Information Security Agency) a publié sur son site Internet[6] un document intitulé « *Technical Guidelines on Iincident Reporting. Technical guidance on the incident reporting in Article 13a . Version 2.0, January 2013* » (ci-après « les lignes ENISA »). Ce document adresse une série de recommandations aux autorités réglementaires nationales (ci-après « ARN ») en ce qui concerne la mise en œuvre de l'article 13bis de la directive « cadre » et en

[3] Accord de coopération du 17 novembre 2006 entre l'Etat 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'informations et lors de l'exercice des compétences en matière de réseaux de communications électroniques par les autorités de régulation en charge des télécommunications ou de la radiodiffusion et la télévision. Moniteur belge du 28.12.2006, p. 75371.

[4] Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.

[5] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre").

[6] Voir https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

particulier en ce qui concerne l'obligation contenue dans cet article 13bis pour les ARN de fournir une fois par an à la Commission européenne et à l'ENISA un rapport succinct sur les notifications d'incidents de sécurité reçues des opérateurs et sur l'action envisagée par ces ARN[7].

15 La présente décision s'inspire[8] du document de l'ENISA en vue d'assurer une certaine cohérence entre les notifications des opérateurs vers l'IBPT et le rapport annuel sur les incidents de sécurité que l'IBPT envoie l'ENISA et à la Commission européenne.

4. HYPOTHÈSES DANS LESQUELLES LES OPÉRATEURS DOIVENT NOTIFIER À L'IBPT UN INCIDENT DE SÉCURITÉ

4.1 Introduction

16 Selon l'article 114/1, §2, de la LCE, « *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.* »

17 Les différents éléments de cette disposition sont analysés ci-dessous.

4.2 Opérateurs soumis à la notification

18 Il ressort de cette disposition qu'elle s'applique tant aux entreprises fournissant des réseaux publics de communications qu'aux entreprises fournissant des services de communications électroniques accessibles au public.

19 Si plusieurs opérateurs sont concernés par un même incident, chacun de ces opérateurs fera une notification à l'IBPT, pour autant que les seuils indiqués au point 25 et aux points suivants soient atteints.

4.3 Incident de sécurité

20 Comme indiqué dans les lignes directrices ENISA, faisant par ailleurs référence à la littérature technique sur les réseaux et les réseaux interconnectés, il faut entendre, pour l'application de cette décision, par « *intégrité* » comme étant « *the ability of the system to retain its specified attributes in terms of performance and functionality* »[9].

21 Par « *incident de sécurité* » ou par « *incident* », il faut entendre, pour l'application de cette décision, toute atteinte à la sécurité ou à la perte d'intégrité qui a un impact sur le bon fonctionnement d'un réseau public de communications électroniques (ci-après « réseau ») ou sur la fourniture d'un service de communications électroniques accessible au public (ci-après « service »).

4.4 Incident et risque d'incident

22 Le fait de simplement soupçonner qu'un incident s'est produit ne génère pas l'obligation de notifier en vertu de la présente décision[10]. Le constat d'un incident est considéré comme établi dès lors que l'opérateur dispose d'assez d'éléments indiquant qu'il s'est produit un incident de sécurité pour justifier une notification à l'IBPT.

---

[7] Voir l'article 13*bis.3,* alinéa 3, de la directive "cadre".

[8] Ceci en particulier pour ce qui concerne le contenu des notifications.

[9] « *la capacité du système de conserver ses caractéristiques spécifiques en termes de performances et de fonctionnalité* »
Voir document de l'ENISA, p. 5.

[10] On rappellera cependant que l'article 114/1, § 1er, de la LCE impose d'informer les abonnés et l'IBPT en cas de risque particulier de violation de la sécurité du réseau (voir ci-dessus).

4.5 Réseaux et services concernés

23 Le terme « *réseaux de communications électroniques* » est défini à l'article 2, 3°, de la LCE. Le terme « *service de communications électroniques* » est quant à lui défini à l'article 2, 5°, de la LCE.

24 La liste des réseaux et des services à considérer est la suivante[11]:

- Réseaux : fixe, mobile
- Service de téléphonie (voix)
- Service de lignes louées
- Services de transmission de données : Service d'accès à Internet, SMS
- Services d'accès partagé ou dégroupé à la boucle locale et services de gros d'accès à la large bande.

Cette liste n'est pas exhaustive.

4.6 Seuils d'impact

4.6.1 Principes

25 Un incident doit être notifié à l'IBPT si un des seuils suivants est atteint (critères non cumulatifs) ; ces critères s'inspirent de ceux de l'ENISA, en tenant compte du nombre d'utilisateurs finaux en Belgique:

26 L'incident affecte un service (par exemple, une ligne louée, un accès de gros à la large bande ou un accès dégroupé à la boucle locale) que rend un opérateur à un ou plusieurs utilisateurs, qui ne sont pas des utilisateurs finaux, pour autant qu'un des seuils (« seuils 2 à 6 ») ci-dessous soit atteint. (« seuil 1 »)

27 L'incident affecte un nombre supérieur à 700 000 (téléphonie voix fixe), 1 900 000 (téléphonie voix mobile et SMS), 540 000 (accès internet fixe), 310 000 (accès internet mobile) ou 2000 (lignes louées) utilisateurs finals et cet incident ne peut être résolu endéans l'heure. (« seuil 2 »)

28 L'incident affecte un nombre supérieur à 460 000 (téléphonie voix fixe), 1 250 000 (téléphonie voix mobile et SMS), 350 000 (accès internet fixe), 210 000 (accès internet mobile) ou 1330 (lignes louées) utilisateurs finals et cet incident ne peut être résolu endéans les 2 heures. (« seuil 3 »)

29 L'incident affecte un nombre supérieur à 230 000 (téléphonie voix fixe), 625 000 (téléphonie voix mobile et SMS), 175 000 (accès internet fixe), 105 000 (accès internet mobile) ou 670 (lignes louées) utilisateurs finals et cet incident ne peut être résolu endéans les 4 heures. (« seuil 4 »)

30 L'incident affecte un nombre supérieur à 95 000 (téléphonie voix fixe), 250 000 (téléphonie voix mobile et SMS), 70 000 (accès internet fixe), 41 000 (accès internet mobile) ou 270 (lignes louées) utilisateurs finals et cet incident ne peut être résolu endéans les 6 heures. (« seuil 5 »)

31 L'incident affecte un nombre supérieur à 48 000 (téléphonie voix fixe), 125 000 (téléphonie voix mobile et SMS), 35 000 (accès internet fixe), 21000 (accès internet mobile) ou 130 (lignes louées) utilisateurs finals et cet incident ne peut être résolu endéans les 8 heures. (« seuil 6 »)

32 L'incident affecte un nombre supérieur ou égal à 10 stations de base, fixes ou temporaires indépendamment du nombre d'utilisateurs finals affectés ou de la durée de cet incident. (« seuil 7 »)

4.6.2 Explications

4.6.2.1 Premier seuil : l'incident affecte un service rendu à un utilisateur qui n'est pas un utilisateur final

33 L'article 2, 12°, de la LCE définit le terme utilisateur comme « *une personne physique ou morale qui utilise ou demande un service de communications électroniques accessibles au public* ». L'article 2,

[11] Voir page 9 du document de l'ENISA.

3°, définit quant à lui l'utilisateur final comme « *un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public.* »

34 Le premier critère se réfère donc à un service (par exemple un service d'accès partagé ou dégroupé à la boucle locale ou un service d'accès à la large bande) qu'un opérateur rend à un autre opérateur. Pour déterminer si le seuil 2, 3, 4, 5 ou 6 est atteint et si plusieurs utilisateurs autres que des utilisateurs finals sont affectés par l'incident, l'opérateur qui rend le service affecté par l'incident additionnera les utilisateurs finaux affectés des différents utilisateurs concernés. Pour ce faire, il prendra en compte le nombre de lignes, numéros d'appels ou de cartes SIM qui sont potentiellement affectées. Un utilisateur final est affecté lorsque la disponibilité ou la continuité du réseau ou service ne peut plus être assurée.

4.6.2.2 Seuils 2 à 6 : l'incident affecte un certain nombre d'utilisateurs finaux pendant une certaine durée

35 Chaque opérateur est tenu d'examiner l'impact de l'incident sur ses utilisateurs finals et non sur les utilisateurs finals d'autres opérateurs. Les seuils 2 à 6 se calculent donc par opérateur et non en tenant compte des utilisateurs finals de différents opérateurs qui seraient affectés par l'incident[12].

36 Un utilisateur final est affecté par un incident lorsque l'incident a un effet tel que la disponibilité ou la continuité du réseau ou service ne peut plus être assurée.

37 Chaque ligne, numéro d'appel ou carte SIM affecté par un incident correspond à un utilisateur final.

38 La "durée de l' incident" est la durée en temps (en heures) pendant laquelle l'impact sur le fonctionnement des services a été significatif [13].

5. DÉLAI DANS LEQUEL LA NOTIFICATION DOIT ÊTRE FAITE

39 L'article 114/1, § 2, de la LCE prévoit que «*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.* » (c'est nous qui soulignons)

40 Par conséquent, pour déterminer quand un incident de sécurité doit être notifié à l'IBPT, les opérateurs respecteront les principes suivants :

1) La notification doit être adressée à l'IBPT dès que l'opérateur dispose de toutes les informations visées à la section 7, ou en tout cas dans les 24 h 00 à partir du début de l'incident selon le mode de transmission prévu ci-dessous.

2) Si la notification envoyée à l'IBPT n'est pas complète ou contient des éléments ayant changé, un complément de notification doit être adressé à l'IBPT dans les 15 jours.

6. MODE DE TRANSMISSION DE LA NOTIFICATION

41 Il est imposé aux opérateurs d'utiliser le site Internet sécurisé mis en ligne par l'IBPT pour la notification des incidents de sécurité.

42 En cas d'indisponibilité du site et dans tous les cas après avoir notifié un incident par le site susmentionné, l'opérateur adressera cette notification dans un délai raisonnable (maximum 24 h)

[12] Un même incident peut affecter des réseaux ou services de différents opérateurs.
[13] Voir document de l'ENISA, pp. 12 et 13.

à l'IBPT par porteur, courrier ou fax, cette notification devant être signée par une (des) personne(s) pouvant représenter l'opérateur.

7. CONTENU DE LA NOTIFICATION

43 Les informations à communiquer dans le cadre de la notification sont détaillées en annexe 1[14] .

8. VOIES DE RECOURS

44 Conformément à l'article 2, §1 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 d'appel de Bruxelles, 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.

45 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.

Georges Denef
Membre du Conseil

Axel Desmedt
Membre du Conseil

Catherine Rutten
Membre du Conseil

Michel Van Bellinghen
Membre du Conseil

[14] Ces informations sont également reprises sur le site Internet sécurisé de l'IBPT.

ANNEXE 1 : FORMULAIRE DE NOTIFICATION

Information	Description
DATE ET HEURE	
Date de début	Date et heure à laquelle l'incident a eu lieu (en heure nationale). Ces indications temporelles peuvent être considérées comme le moment où l'incident a été découvert. L'heure doit être exprimée tant en zone horaire CET qu'en zone horaire locale.
IMPACT DE L'INCIDENT ET SOURCE DU PROBLEME	
Services touchés: - **Téléphonie fixe** - **Téléphonie mobile** - **Services de messages (courts)** - **Internet fixe** - **Internet mobile** - **Lignes louées**	Le ou les services qui sont touchés par l'incident.
Paramètres d'impact: - **Nombre de lignes, numéros d'appel ou cartes SIM affectés** - **Nombre de lignes, numéros d'appel ou cartes SIM qui sont fournis grâce au service ou réseau affecté par l'incident**	Nombre total de lignes, numéros d'appel ou cartes SIM affectés lorsque l'incident a lieu. Ce nombre doit être exprimé en valeur absolue (p. ex. « 250 000 d'utilisateurs finals » est accepté) et non pas de manière relative (p. ex. « 75% des cartes pre-paid» est refusé).
Durée	La durée de l'incident
Impact sur les appels d'urgence	Si disponible, service d'urgence touché par l'incident.
Détails sur l'impact	[*Facultatif*] Détails sur l'impact de l'incident.
Source du problème[15]: - **Catastrophe ou phénomène naturel** - **Erreur humaine** - **Attaques ou actions malveillantes** - **Défaillance matérielle ou logicielle** - **Défaillance d'une tierce partie ou partie externe**	La cause à l'origine de l'incident
Détails sur la source du problème	[*Facultatif*] Les incidents à rapporter doivent se focaliser sur l'intégrité du réseau et la continuité du service. Il pourrait s'agir de sous-catégories des sources du problème, répertoriées dans la section pertinente.
AUTRES INFORMATIONS SUR L' INCIDENT	
Description générale	Résumé de l'incident
Gestion de l'incident et plans d'intervention[16]	Toutes les interventions effectuées après la découverte de l'incident et des mesures adoptées pour rétablir les conditions/le niveau d'origine du service.
Actions après l'incident	Description de toute disposition prise afin de minimizer le niveau de risque..
Interconnexions nationales touchées	Si le service touché peut causer des dommages/changements à un bien (ou service) appartenant à un autre opérateur ou fournisseur, une interconnexion est touchée.

[15] Document de l'ENISA, pp.. 13 et 14. Indépendamment que cette cause ou origine soit une défaillance de sécurité ou une perte d'intégrité.

[16] Mesures d'intervention et de rétablissement prises par les fournisseurs tant pendant qu'après l'incident.

	Si applicable, détails sur les opérateurs belges concernés.
Interconnexions internationales touchées	En cas d'incidents transfrontaliers, il se peut qu'une brèche de sécurité dans un Etat membre touche les biens d'un autre Etat membre 'interconnecté'. Certaines concentrations d'infrastructure sont vulnérables et des perturbations significatives peuvent être causées par une faille locale; les systèmes interconnectés peuvent faire l'objet de failles techniques en cascade. Si applicable, détails sur les opérateurs concernés des autres Etats Membres.
Portée géographique /région touchée	Si disponible, la region touchée par l'incident.
Enseignements tirés	Décrire toutes les interventions effectuées après l'incident pour améliorer la sécurité du bien et les procédures (ou les mesures prises) qui seront suivies à partir de ce moment-là. La différence entre ce champ et le champ des "Actions après l'incident" est que dans ce champ, nous renvoyons aux actions à long terme.
Autres observations	Informations à compléter sur l'incident ou la notification de l'incident

ANNEXE 2 : RÉSULTATS DE LA CONSULTATION PUBLIQUE

[sera complété ultérieurement]