BELGISCH INSTITUUT VOOR POSTDIENSTEN
EN TELECOMMUNICATIE

BESLUIT VAN DE RAAD VAN HET BIPT VAN 01/04/2014 TOT VASTSTELLING VAN DE HYPOTHESEN WAARIN DE OPERATOREN AAN HET BIPT EEN VEILIGHEIDSINCIDENT MOETEN MELDEN EN VAN DE NADERE BEPALINGEN VAN DEZE KENNISGEVING

INHOUDSOPGAVE

1. DOEL EN JURIDISCHE BASIS

1 De wet van 10 juli 2012 houdende diverse bepalingen inzake elektronische communicatie[1] heeft onder andere een artikel 114/1, § 2, ingevoerd in de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna de WEC). Dat artikel luidt als volgt (wij onderstrepen):

> *"De ondernemingen die openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten aanbieden, stellen het Instituut onverwijld in kennis van elke inbreuk op de veiligheid of elk verlies van integriteit die een belangrijke impact heeft op de exploitatie van netwerken of diensten. Na voorafgaande machtiging van de minister, preciseert het Instituut in welke hypothetische gevallen de inbreuk op de veiligheid of het verlies van integriteit een belangrijke impact heeft in de zin van dit lid."*

2 Dit besluit voert onder andere de laatste zin van de voormelde bepaling uit.

3 Bovendien bepaalt artikel 114/2 van de WEC, zoals ingevoegd in de WEC door de voormelde wet van 10 uli 2012, het volgende:

> *"§ 1. Het Instituut kan de ondernemingen die openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten aanbieden bindende instructies, ook met betrekking tot de termijnen voor de uitvoering, geven met het oog op de uitvoering van de artikelen 114 en 114/1."*

4 Op grond van artikel 114/2 en het voormelde artikel 114/1, § 2, eerste zin, stelt het BIPT bij dit besluit de bindende instructies vast in verband met de verplichting voor de operatoren om het BIPT onverwijld in kennis te stellen van elk risico voor een inbreuk op de veiligheid of verlies van integriteit die een belangrijke impact heeft op de werking van de netwerken of diensten.

5 Dit besluit stelt daarom de praktische regels vast voor de kennisgeving door de operatoren aan het BIPT van veiligheidsincidenten en bepaalt aldus de volgende punten:

- de termijn waarbinnen de kennisgeving moet plaatsvinden;
- de wijze van overzending van de kennisgeving;
- de inhoud van de kennisgeving.

6 Dit besluit heeft echter geen betrekking op de verplichting van de ondernemingen die een openbare elektronische-communicatiedienst aanbieden om de abonnees en het BIPT in te lichten over een risico voor inbreuk op de veiligheid van het netwerk, zoals vermeld in artikel 114/1, § 1, van de WEC:

> *"Indien een bijzonder risico bestaat van inbreuken op de beveiliging van het netwerk, stellen de ondernemingen die een openbare elektronische-communicatiedienst aanbieden de abonnees en het Instituut in kennis van dat risico en, indien het risico tot andere maatregelen noopt dan deze die de ondernemingen die de dienst aanbieden kunnen nemen, van de eventuele middelen om dat risico tegen te gaan, met inbegrip van een indicatie van de verwachte kosten."* (wij onderlijnen)

7 De kennisgeving aan het BIPT van een inbreuk op de veiligheid van een openbare elektronische-communicatiedienst wat persoonsgebonden gegevens betreft, die moet plaatsvinden krachtens artikel 114/1, § 3, van de WEC, komt in dit besluit niet aan bod en zal indien nodig het voorwerp uitmaken van aparte richtlijnen vanwege het BIPT[2].

---

[1] Belgisch Staatsblad van 25 juli 2012, blz. 40969.

[2] Dit besluit behandelt dus evenmin de vergoedingen die de operatoren zouden moeten betalen aan de abonnees in geval van dienstonderbreking conform het koninklijk besluit dat zou kunnen worden aangenomen op basis van artikel 113/2 van de WEC.

2. PROCEDURE

2.1. Openbare raadpleging

8 Van 7 mei 2013 tot 7 juni 2013 heeft het BIPT een openbare raadpleging gehouden over dit ontwerpbesluit, op grond van artikel 14, § 2, 1°, eerste zin, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (hierna de statuutwet).

9 De volgende operatoren hebben op deze raadpleging geantwoord: Belgacom, Mobistar, Plateform, Telenet en Verizon.

10 De samenvatting van de resultaten van de openbare raadpleging vormt bijlage 2 bij dit besluit.

2.2. Raadpleging van de mediaregulatoren

11 Krachtens artikel 3 van het samenwerkingsakkoord van 17 november 2006[3] heeft het BIPT op 3 september 2013 dit ontwerpbesluit verstuurd naar de mediaregulatoren van de gemeenschappen, namelijk de CSA, de Medienrat en de VRM. De Medienrat en de VRM hebben geantwoord dat ze geen opmerkingen hadden. De CSA heeft niet gereageerd.

2.3. Machtiging van de minister

12 Met zijn brief van 21 maart 2014 heeft de heer Johan Vande Lanotte, vice-eersteminister en minister van Economie, Consumenten en Noordzee, de voorafgaande machtiging gegeven, waarvan sprake in artikel 114/1, § 2, van de WEC wat betreft de aspecten van dit besluit die slaan op de hypotheses waarin de inbreuk op de veiligheid of het verlies van integriteit een belangrijke impact heeft op de exploitatie van de netwerken of diensten, hetzij wat punt 4 van dit besluit betreft.

3. EUROPESE CONTEXT

13 Richtlijn 2009/140/EG[4] heeft onder andere de artikelen 13*bis* en 13*ter* ingevoerd in hoofdstuk III*bis*, "Veiligheid en integriteit van netwerken en diensten" van de Kaderrichtlijn uit 2002[5]. De voormelde artikelen 114/1, § 2, en 114/2 van de WEC zijn aangenomen in het kader van de omzetting in Belgisch recht van deze nieuwe artikelen 13*bis* en 13*ter*.

14 Het ENISA (European Network and Information Security Agency) heeft op zijn website[6] een document gepubliceerd getiteld "*Technical Guidelines on Incident Reporting. Technical guidance on the incident reporting in Article 13a. Version 2.0, January 2013"* (hierna de "ENISA-richtlijnen"). Dit document gaat over een reeks aanbevelingen aan de nationale regelgevende instanties (hierna "NRI's") wat betreft de

[3] Samenwerkingsakkoord van 17 november 2006 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franstalige (sic) Gemeenschap en de Duitstalige Gemeenschap betreffende het wederzijds consulteren bij het opstellen van regelgeving inzake elektronische-communicatienetwerken, het uitwisselen van informatie en de uitoefening van de bevoegdheden met betrekking tot elektronische-communicatienetwerken door de regulerende instanties bevoegd voor telecommunicatie of radio-omroep en televisie. Belgisch Staatsblad van 28.12.2006, blz. 75371.

[4] Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronischecommunicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronischecommunicatienetwerken en –diensten.

[5] Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten ("Kaderrichtlijn").

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

uitvoering van artikel 13*bis* van de Kaderrichtlijn en in het bijzonder wat betreft de verplichting vervat in dat artikel 13*bis* voor de NRI's om een keer per jaar aan de Europese Commissie en aan het ENISA een beknopt verslag uit te brengen over de kennisgevingen van inbreuken op de veiligheid die de operatoren ontvangen en over de actie die deze NRI's beogen[7].

15 Dit besluit is geïnspireerd[8] op het document van het ENISA met de bedoeling te zorgen voor een zekere coherentie tussen de kennisgevingen van de operatoren aan het BIPT en het jaarverslag over de veiligheidsdiensten dat het BIPT verstuurt naar het ENISA en naar de Europese Commissie.

4. HYPOTHESES WAARIN DE OPERATOREN AAN HET BIPT EEN VEILIGHEIDSINCIDENT MOETEN MELDEN

4.1 Inleiding

16 Artikel 114/1, § 2, van de WEC bepaalt: "*De ondernemingen die openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten aanbieden, stellen het Instituut onverwijld in kennis van elke inbreuk op de veiligheid of elk verlies van integriteit die een belangrijke impact heeft op de exploitatie van netwerken of diensten.*"

17 De verschillende elementen van deze bepaling worden hieronder nader bekeken.

4.2 Aan kennisgeving onderworpen operatoren

18 Uit deze bepaling vloeit voort dat ze van toepassing is op zowel ondernemingen die openbare communicatienetwerken aanbieden als ondernemingen die openbare elektronische-communicatiediensten aanbieden.

19 Indien verscheidene operatoren betrokken zijn bij eenzelfde incident, zal elk van deze operatoren een kennisgeving doen aan het BIPT, voor zover de drempels vermeld in punt 28 en in de volgende punten zijn bereikt.

4.3 Veiligheidsincident

20 Zoals vermeld in de richtsnoeren van het ENISA, dat overigens verwijst naar de technische literatuur over de netwerken en geïnterconnecteerde netwerken, moet voor de toepassing van dit besluit onder "*integriteit*" worden verstaan "*de capaciteit van het systeem om zijn specifieke karakteristieken te behouden in termen van prestaties en functionaliteit*"[9].

21 Onder "*veiligheidsincident*" of "*incident*" moet voor de toepassing van dit besluit worden verstaan elke inbreuk op de veiligheid of het verlies van integriteit die een impact hebben op de goede werking van een openbaar elektronische-communicatienetwerk (hierna "netwerk") of op de verstrekking van een openbare elektronische-communicatiedienst (hierna "dienst")[10].

22 Onder "inbreuk op de veiligheid" dient te worden verstaan elke fysieke of softwarematige inbreuk (software - virus - via internet - via het netwerk - kabelbreuk - overstroming - kortsluiting, enz.), op een netwerk of op de uitbating van een dienst, die een impact heeft op de fysieke of softwarematige veiligheid van de werking, of de werking zelf van dat netwerk of die dienst. Dit is dus een heel breed begrip.

23 Onder "verlies van integriteit" dient te worden verstaan een verminderd vermogen van het systeem om zijn specifieke karakteristieken te behouden in termen van prestatie en functionaliteit.

---

[7] Zie artikel 13*bis.3*, derde lid, van de Kaderrichtlijn.
[8] Dit in het bijzonder wat de inhoud van de kennisgevingen betreft.
[9] Vrije vertaling van "*the ability of the system to retain its specified attributes in terms of performance and functionality*" Zie richtsnoeren van het ENISA, blz. 5.
[10] Deze definitie is geïnspireerd op de ENISA-richtsnoeren, blz. 5.

4.4 Incident en risico van een incident

24 Het eenvoudige vermoeden dat zich een incident heeft voorgedaan, genereert geen verplichting om het BIPT in kennis te stellen van dat incident krachtens artikel 114/1, § 2, eerste lid, van de WEC[11]. De vaststelling van een incident wordt beschouwd als een feit en het incident moet worden gemeld aan het BIPT zodra de operator over voldoende elementen beschikt die erop wijzen dat zich een veiligheidsincident heeft voorgedaan.

4.5 Betrokken netwerken en diensten

25 De term "*elektronische-communicatienetwerk*" wordt gedefinieerd in artikel 2, 3°, van de WEC. De term "*elektronische-communicatiedienst*" wordt dan weer gedefinieerd in artikel 2, 5°, van de WEC.

26 De lijst van de te beschouwen netwerken en diensten is de volgende[12]:

- Netwerken: vast, mobiel
- Telefoniedienst (spraak)
- Huurlijnendienst
- Datatransmissiediensten Internettoegangsdienst, sms
- Diensten voor gedeelde toegang of ontbundelde toegang tot het aansluitnet en wholesalediensten voor breedbandtoegang.

Deze lijst is niet volledig.

4.6 Impactdrempels

4.6.1 Principes

27 Een incident moet aan het BIPT worden gemeld indien een van de volgende drempels wordt bereikt (niet-cumulatieve criteria).
Deze criteria zijn gebaseerd op deze van ENISA, rekening houdend met het aantal eindgebruikers in België.

28 Het incident heeft invloed op een aantal van meer dan 700 000 (vaste spraaktelefonie), 1 900 000 (mobiele spraaktelefonie en sms), 540 000 (vaste internettoegang), 310 000 (mobiele internettoegang) of 2000 (huurlijnen) eindgebruikers gedurende 1 uur of meer ("drempel 1").

29 Het incident heeft invloed op een aantal van meer dan 460 000 (vaste spraaktelefonie), 1 250 000 (mobiele spraaktelefonie en sms), 350 000 (vaste internettoegang), 210 000 (mobiele internettoegang) of 1330 (huurlijnen) eindgebruikers gedurende 2 uur of meer ("drempel 2").

30 Het incident heeft invloed op een aantal van meer dan 230 000 (vaste spraaktelefonie), 625 000 (mobiele spraaktelefonie en sms), 175 000 (vaste internettoegang), 105 000 (mobiele internettoegang) of 670 (huurlijnen) eindgebruikers gedurende 4 uur of meer ("drempel 3").

31 Het incident heeft invloed op een aantal van meer dan 95 000 (vaste spraaktelefonie), 250 000 (mobiele spraaktelefonie en sms), 70 000 (vaste internettoegang), 41 000 (mobiele internettoegang) of 270 (huurlijnen) eindgebruikers gedurende 6 uur of meer ("drempel 4").

32 Het incident heeft invloed op een aantal van meer dan 48 000 (vaste spraaktelefonie), 125 000 (mobiele spraaktelefonie en sms), 35 000 (vaste internettoegang), 21000 (mobiele internettoegang) of 130 (huurlijnen) eindgebruikers gedurende 8 uur of meer ("drempel 5").

33 Het incident heeft invloed op een aantal van 160 of meer vaste of tijdelijke basisstations, ongeacht het aantal getroffen eindgebruikers of de duur van dat incident ("drempel 6").

---

[11] We herinneren er echter aan dat artikel 114/1, § 1, van de WEC de verplichting oplegt om de abonnees en het BIPT in te lichten in geval van een bijzonder gevaar voor aantasting van de veiligheid van het netwerk (zie hierboven).

[12] Zie p. 9 van de ENISA-richtlijnen.

4.6.2 Uitleg

34 Elke operator is verplicht de impact van het incident op zijn eindgebruikers te onderzoeken en niet op de eindgebruikers van andere operatoren. De drempels een tot vijf worden dus berekend per operator en niet rekening houdende met de eindgebruikers van verschillende operatoren die door het incident getroffen zouden zijn[13].

35 Een eindgebruiker wordt door een incident getroffen wanneer het zo'n effect heeft dat de beschikbaarheid of de continuïteit van het netwerk of de dienst niet langer gegarandeerd kan worden.

36 Elke lijn, elk oproepnummer of elke simkaart die door een incident wordt getroffen, stemt overeen met een eindgebruiker.

37 Worden beschouwd als getroffen door een incident niet alleen de eindgebruikers die de bij het incident betrokken dienst hebben gebruikt en die daadwerkelijk werden getroffen door het incident maar ook de eindgebruikers die door het incident zouden getroffen zijn als ze hadden besloten om de betrokken dienst te gebruiken.

38 Voor de drempels 1 tot 5 kan het gebeuren dat het incident verschillende keren de cijfers overschrijdt (bijvoorbeeld de 700.000 voor vaste spraaktelefonie) die worden vermeld voor deze drempels, telkens gedurende een periode korter dan de duur (1, 2, 4, 6 en 8 uur) die wordt vastgelegd voor deze drempels. In dat geval moeten de verschillende periodes waarin deze cijfers werden overschreden, worden opgeteld om te bepalen of een drempel werd bereikt. Ter illustratie: wat betreft drempel 1, indien het cijfer van 700.000 (vaste spraaktelefonie) vier keer werd overschreden gedurende een kwartier, moet het incident worden gemeld aan het BIPT.

39 Voor de berekening van drempel 6 dient te worden bepaald welke de basisstations waren die werden getroffen door het incident gedurende de hele periode.

40 Elk incident dat niet beantwoordt aan de voormelde criteria mag worden gemeld aan het BIPT op initiatief van de operator indien deze laatste vaststelt dat de impact van het incident zodanig is dat het moet worden gemeld aan het BIPT.

5. TERMIJN WAARBINNEN DE KENNISGEVING MOET PLAATSVINDEN

41 Artikel 114/1, § 2, van de WEC bepaalt: "*De ondernemingen die openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten aanbieden, stellen het Instituut onverwijld in kennis van elke inbreuk op de veiligheid of elk verlies van integriteit die een belangrijke impact heeft op de exploitatie van netwerken of diensten.*" (door ons onderstreept)

42 Om te bepalen wanneer een veiligheidsincident aan het BIPT moet worden gemeld, zullen de operatoren de volgende principes naleven:

1) De kennisgeving moet worden gericht aan het BIPT volgens de hieronder vastgelegde transmissiemethode, zodra de operator over alle inlichtingen bedoeld in deel 7 beschikt, of in elk geval binnen 72 uur na het begin van het incident of vanaf het ogenblik dat een van de drempels werd bereikt. Voor de berekening van de termijn van 72 u, worden enkel de werkdagen beschouwd.

2) Als de naar het BIPT opgestuurde kennisgeving onvolledig is of elementen bevat die gewijzigd zijn, moet binnen 15 dagen een aanvulling op de kennisgeving worden gericht aan het BIPT.

6. WIJZE VAN OVERZENDING VAN DE KENNISGEVING

43 De operatoren mogen tussen de volgende werkwijzen kiezen om de kennisgeving aan het BIPT te bezorgen:

[13] Eenzelfde incident kan invloed hebben op de netwerken of diensten van verschillende operatoren.

- brief via besteller;
- aangetekende postzending;
- fax;
- elektronisch platform ter beschikking gesteld van het BIPT en aangevuld door deze laatste.

44 In hun keuze tussen verschillende manieren, zullen de operatoren rekening houden met eventuele hoogdringendheid.

45 In het geval van een melding via aangetekend schrijven en per besteller, wordt de kennisgeving verstuurd naar:

BIPT
Ter attentie van de voorzitter van de Raad
Kennisgeving "security incident report"
Ellipse Building - Gebouw C
Koning Albert II-laan 35
1030 Brussel

7. INHOUD VAN DE KENNISGEVING

46 De inlichtingen die in het kader van de kennisgeving moeten worden meegedeeld, worden gedetailleerd in bijlage 1.

8. INWERKINGTREDING

47 Dit besluit treedt in werking drie maanden na de publicatie ervan op de website van het BIPT.

9. BEROEPSMOGELIJKHEDEN

48 Overeenkomstig artikel 2, § 1, van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector hebt u de mogelijkheid om tegen dit besluit beroep in te stellen bij het hof van beroep van Brussel, Poelaertplein 1, B-1000 Brussel. Het beroep wordt, op straffe van nietigheid die ambtshalve wordt uitgesproken, ingesteld door middel van een ondertekend verzoekschrift dat wordt ingediend ter griffie van het hof van beroep van Brussel binnen een termijn van zestig dagen vanaf de kennisgeving van het besluit of bij gebreke aan een kennisgeving, vanaf de publicatie van de beslissing of bij gebreke aan een publicatie, vanaf de kennisname van het besluit.

49 Het verzoekschrift bevat op straffe van nietigheid de vermeldingen vereist door artikel 2, §2 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector. Indien het verzoekschrift elementen bevat die u als vertrouwelijk beschouwt, dan moet u dat uitdrukkelijk aangeven en op straffe van nietigheid, een niet-vertrouwelijke versie van dat verzoekschrift indienen. Het Instituut publiceert op zijn website het verzoekschrift dat door de griffie van de rechtbank genotificeerd is. Elke belanghebbende partij kan in de zaak tussenkomen binnen dertig dagen na deze publicatie.

Charles Cuvelliez
Raadslid

Axel Desmedt
Raadslid

Luc Vanfleteren
Raadslid

Jack Hamande
Voorzitter van de Raad

BIJLAGE 1: KENNISGEVINGSFORMULIER

Informatie	Beschrijving
DATUM EN UUR	
Startdatum	Datum en tijdstip waarop het incident heeft plaatsgevonden (in nationale tijd). Deze tijdaanduidingen kunnen worden beschouwd als het ogenblik waarop het incident werd ontdekt. Het tijdstip moet worden uitgedrukt in zowel CET-tijdzone als in lokale tijd.
IMPACT VAN HET INCIDENT EN BRON VAN HET PROBLEEM	
Getroffen diensten: - **Vaste telefonie** - **Mobiele telefonie** - **Berichtendiensten (korte)** - **Vast internet** - **Mobiel internet** - **Huurlijnen**	De dienst of diensten die getroffen is/zijn door het incident.
Parameters van de impact: - **Aantal getroffen lijnen, oproepnummers of simkaarten** - **Aantal lijnen, oproepnummers of simkaarten die worden verstrekt dankzij de dienst of het netwerk die door het incident zijn getroffen**	Totaal aantal lijnen, oproepnummers of simkaarten die getroffen zijn wanneer het incident plaatsvindt. Dat aantal moet worden uitgedrukt in absolute waarde (bijv. "250 000 eindgebruikers" wordt aanvaard) en niet relatief (bijv. "75% prepaid kaarten" wordt geweigerd).
Duur	De duur van het incident. Dit is de periode waarin de drempel werd overschreden[14]. De totale duur van het incident moet ook worden vermeld, indien dat gegeven bekend is. De totale duur van het incident is de verstreken tijd tussen het begin van het incident en het moment waarop het incident volledig was verholpen.
Impact op de noodoproepen	Indien beschikbaar, de nooddienst die is getroffen door het incident.
Details over de impact	[*Facultatief*] Details over de impact van het incident.
Bron van het probleem[15]: - **Ramp of natuurfenomeen** - **Menselijke fout** - **Aanvallen of kwaadwillige acties** - **Hardwarematig of softwarematig defect** - **Tekortkoming van een derde of externe partij**	De oorzaak van het incident
Details over de bron van het probleem	[*Vrijblijvend*] De te melden incidenten moeten gericht zijn op de netwerkintegriteit en de continuïteit van de dienst. Het zou kunnen gaan om subcategorieën van bronnen van het probleem, opgetekend in het relevante deel.
ANDERE INFORMATIE OVER HET INCIDENT	
Algemene beschrijving	Samenvatting van het incident
Beheer van het incident en interventieplannen[16]	Alle interventies die plaatsvinden na de ontdekking van het incident en maatregelen aangenomen om de voorwaarden/het oorspronkelijke niveau van dienstverlening te herstellen.
Acties na het incident	Omschrijving van elke bepaling genomen om het risiconiveau tot een minimum te beperken.

[14] Zie richtsnoeren van het ENISA, blz. 12.

[15] ENISA-richtsnoeren, blz. 13 en 14. Los van het feit of deze oorzaak of bron een veiligheidsinbreuk of verlies van integriteit is.

[16] Maatregelen voor interventie en herstel getroffen door de aanbieders zowel tijdens als na het incident.

Getroffen nationale interconnecties	Indien de getroffen dienst schade/wijzigingen kan teweegbrengen aan een goed (of een dienst) van een andere operator of aanbieder, wordt een interconnectie getroffen. (voorbeelden: interconnectielinks tussen netwerken, huurlijnen, enz.) Indien van toepassing, details over de betrokken Belgische operatoren.
Getroffen internationale interconnecties	In het geval van grensoverschrijdende incidenten, kan een inbreuk op de veiligheid in een lidstaat de goederen van een "geïnterconnecteerde" lidstaat raken. Bepaalde concentraties van infrastructuur zijn kwetsbaar en beduidende storingen kunnen ook worden veroorzaakt door een lokale tekortkoming; de geïnterconnecteerde systemen kunnen het voorwerp uitmaken van de ene technische storing na de andere. Indien van toepassing, details over de betrokken operatoren uit andere lidstaten.
Geografische reikwijdte/getroffen regio	Indien beschikbaar de door het incident getroffen regio (gemeente, stad, provincie, deel van het grondgebied, enz.).
Getrokken lering	Alle interventies uitgevoerd na het incident omschrijven om de veiligheid van het goed te verbeteren en de procedures (of de getroffen maatregelen) die zullen worden gevolgd vanaf dat moment beschrijven. Het verschil tussen dat veld en het veld "Acties genomen na het incident" is dat we in dit veld verwijzen naar langetermijnacties.
Andere vaststellingen	Aan te vullen inlichtingen over het incident of de kennisgeving van het incident

BIJLAGE 2: RESULTATEN VAN DE OPENBARE RAADPLEGING

1. Van 7 mei 2013 tot 7 juni 2013 heeft het BIPT een openbare raadpleging gehouden over dit ontwerpbesluit, op grond van artikel 14, § 2, 1°, eerste zin, van de statuutwet.

2. De volgende operatoren hebben op deze raadpleging geantwoord: Belgacom, Mobistar, Plateform, Telenet en Verizon.

3. Deze synthese vermeldt enkel de niet-vertrouwelijke delen van de ontvangen antwoorden.

4. Voor het goede begrip van deze bijlage wordt gepreciseerd dat het BIPT naar aanleiding van de openbare raadpleging heeft besloten om drempel 1 uit het ter raadpleging voorgelegde ontwerpbesluit niet te behouden. Deze drempel was: "Het incident heeft invloed op een dienst (bijvoorbeeld een huurlijn, een wholesalebreedbandtoegang of een ontbundelde toegang tot het aansluitnet) die door een operator wordt verstrekt aan een of meer gebruikers, die geen eindgebruiker zijn, voor zover een van de drempels hieronder (drempels 2 tot 6) is bereikt."

5. Twee respondenten vestigen de aandacht op het feit dat in de Nederlandse tekst in punt 5 wordt gevraagd aan de operatoren om aan het BIPT elk risico van inbreuk op de veiligheid of verlies van integriteit te melden. Deze respondent uit ernstige bezwaren met betrekking tot de daadwerkelijke en uniforme evaluatie van dit begrip van risico. Er dient te worden opgemerkt dat het een vertaalfout betreft in de Nederlandse versie en dat dit begrip van risico niet is opgenomen in punt 5 van de Franse versie van de tekst.

6. Een respondent gaat akkoord met de impactdrempels 2 tot 6 (momenteel drempels 1 tot 5) maar maakt een voorbehoud bij impactdrempel nr. 1 (die momenteel is geschrapt). Deze respondent alsook een andere, vermeldt dat een wholesaleoperator niet weet hoeveel klanten van zijn klant worden getroffen.

7. Wat betreft impactdrempel nr. 7 (momenteel drempel 6), vermelden drie respondenten dat het gekozen aantal basisstations te laag ligt en dat de impactdrempel nr. 7 minder hoog is dan de drempels 2 tot 6 (momenteel drempels 1 tot 5). Deze respondenten stellen dan ook voor om deze impactdrempel te schrappen ofwel het aantal basisstations te verhogen van 150 naar 200. Wat dit betreft, merkt een andere respondent op dat hij als MVNO geen informatie heeft over deze drempel.

8. Een respondent merkt op dat deze kennisgevingen niet de e-maildiensten of de kabeldistributiediensten beogen.

9. Een respondent is van mening dat de verplichting tot informatieverstrekking binnen de 24 u vanaf het begin van het incident te snel is ten opzichte van het daadwerkelijke gebruik van deze informatie door het BIPT, des te meer aangezien er niet wordt voorzien in een onderscheid tussen werkdagen, weekends en feestdagen. Deze respondent is van mening dat een termijn van een week of zelfs een maand voldoende is, en vraagt met nadruk dat een termijn van minstens 72 werkuren (business hours) wordt toegepast. Indien deze termijn van 24 u zou worden behouden, vraagt deze respondent dat enkel een minimum van informatie moet worden verstrekt binnen deze termijn en dat de rest binnen de week mag volgen.

10. Drie respondenten vragen om een termijn van minstens drie maanden voor de toepassing van het besluit, om zich intern te kunnen organiseren.

11. Twee respondenten vragen ervoor te zorgen dat de informatie mag worden verstuurd naar een beveiligde e-mail van het BIPT. Een respondent meent dat het gebruik van de site zoals aanbevolen door het BIPT te complex en te traag is. Bovendien vormt het een probleem wanneer verschillende personen vanaf verschillende plaatsen proberen toegang te krijgen. Een andere respondent wijst op het probleem van flexibiliteit wat betreft het gebruik van de website van het BIPT.

12. Een respondent vermeldt een duidelijke tegenstrijdigheid tussen het feit dat elke operator verantwoordelijk is om de verplichte kennisgevingen te identificeren en impactdrempel nr. 1 (momenteel geschrapt). Er wordt verduidelijking gevraagd.

13. Een respondent stelt dat hij begrijpt dat alle operatoren op de markt betrokken zijn en vraagt aan het BIPT om dit punt te controleren.

14. Een respondent vermeldt dat noch de richtsnoeren van het ENISA noch het ontwerpbesluit het begrip van inbreuk op de veiligheid definiëren en vraagt duidelijkheid over dit begrip.

15. Een respondent stelt vast dat het BIPT de dienst van de huurlijnen en de diensten voor gedeelde of ontbundelde toegang tot het aansluitnetwerk en wholesalediensten voor breedbandtoegang heeft toegevoegd ten opzichte van wat is vastgelegd in de lijst van het ENISA. Deze respondent verklaart zich akkoord met de toevoeging van de huurlijnendienst maar staat sceptisch tegenover de toevoeging van de diensten voor gedeelde of ontbundelde toegang tot het aansluitnet en wholesalediensten voor breedbandtoegang. Indien deze laatste diensten zouden worden opgenomen in het besluit, vraagt deze respondent dat de doorverkoopdienst voor breedbandtoegang ook in beschouwing wordt genomen.

16. Een respondent maakt voorbehoud bij impactdrempel nr. 1 (momenteel geschrapt). Deze respondent stelt dat een operator niet weet hoeveel (eind)gebruikers van zijn klant worden getroffen, in het bijzonder wanneer het een huurlijn betreft. Deze respondent vermeldt de complexiteit van drempel nr. 1 en wijst op een tegenstrijdigheid met punt 4.2 van het ontwerpbesluit. Deze respondent vraagt ook hoe deze bepaling moet worden toegepast in het geval van "mobiel" en van de MVNO in het bijzonder. Deze respondent vraagt dat drempel nr. 1 wordt geschrapt of, bij gebrek daaraan, dat meer gedetailleerde en volledige uitleg wordt gegeven door het BIPT.

17. Wat betreft de impactdrempels 2 tot 6 (momenteel drempels 1 tot 5), verzoekt een respondent het BIPT om het begrip van getroffen gebruikers beter af te bakenen en vraagt hij dat enkel rekening wordt gehouden met de werkelijk getroffen gebruikers en niet met de mogelijk getroffen gebruikers. In het geval van mobiele diensten, vermeldt deze respondent interpretatieproblemen wat roaming betreft. In het geval van mobiele diensten stelt deze respondent voor om rekening te houden met de eindgebruikers die de dienst kunnen gebruiken, door zich te baseren op de historische gegevens. In het geval van vaste diensten, is de situatie nog steeds niet duidelijk.

18. Een respondent vermeldt een probleem met de interpretatie van impactdrempels in geval van een impact die varieert in de tijd. Indien het aantal getroffen gebruikers afneemt met de tijd, kan het zijn dat geen kennisgeving meer nodig is.

19. Een respondent is van mening dat de termijn van 24 u om de kennisgeving te doen, te kort is en de operator niet de mogelijkheid laat om de diverse inlichtingen te vergaren en de nodige controles uit te voeren. Wat dit betreft, wordt een termijn van 72 uur voorgesteld, waarbij deze

termijn begint te lopen vanaf het ogenblik waarop de operator de nodige informatie heeft vergaard om te bepalen of een kennisgeving al dan niet nodig is.

20. Een respondent stelt dat het gebruik van een site zoals aanbevolen door het BIPT ingewikkeld is, en dat het feit dat de kennisgeving schriftelijk moet worden bevestigd via een schrijven ondertekend door een persoon die verbintenissen kan aangaan jegens de operator, de procedure nog bemoeilijkt. Deze respondent vraagt of kennisgevingsmethodes mogen worden gebruikt die kunnen worden geautomatiseerd (via e-mail of XML).

21. Wat betreft bijlage 1 van het ontwerpbesluit formuleert een respondent diverse detailopmerkingen, met het verzoek om verduidelijkingen. Hij vraagt ook om te voorzien in een referentieveld teneinde te kunnen preciseren om welke kennisgeving het gaat wanneer deze kennisgeving het voorwerp uitmaakt van latere preciseringen.

22. Een respondent stelt voor om te voorzien in een overgangsperiode om het besluit tot uitvoer te kunnen brengen. Deze periode is nodig om zich ten aanzien van het BIPT te kunnen vergewissen van het goede begrip van het besluit en om intern de technische oplossingen te kunnen ontwikkelen om het besluit tot uitvoer te brengen.

23. Een andere respondent is van mening dat de termijn van 24 u om de kennisgeving te doen, te kort is en de operator niet de mogelijkheid laat om de diverse inlichtingen te vergaren en de nodige controles uit te voeren. Een termijn van een maand wordt aanbevolen. Indien deze termijn van 24 u zou worden behouden, vraagt deze respondent dat enkel een minimum van informatie moet worden verstrekt binnen deze termijn en dat de rest binnen de week mag volgen.

24. Een andere respondent vermeldt dat het feit dat de kennisgeving moet worden bevestigd via een schrijven ondertekend door een persoon die verbintenissen kan aangaan jegens de operator, de procedure nog bemoeilijkt. Hij vraagt of dit aan de hand van een e-mail kan.

25. Wat betreft de impactdrempels 2 tot 6 (momenteel drempels 1 tot 5), verzoekt een andere respondent het BIPT om het begrip van getroffen gebruikers beter af te bakenen en vraagt hij dat enkel rekening wordt gehouden met de werkelijk getroffen gebruikers en niet met de mogelijk getroffen gebruikers. Deze respondent benadrukt ook dat hij enkel de cijfers betreffende zijn eigen gebruikers kan geven.

26. Een respondent vermeldt dat hij reeds specifieke, voor Europa geharmoniseerde maatregelen heeft ingevoerd, en dat deze maatregelen verschillen van deze voorgesteld in het hier beoogde ontwerpbesluit. Toch meent deze respondent te voldoen aan zijn wettelijke verplichtingen in België. Hij benadrukt het feit dat het voor een pan-Europese operator belangrijk is om geharmoniseerde pan-Europese procedures te kunnen invoeren.