BELGISCH INSTITUUT VOOR POSTDIENSTEN EN TELECOMMUNICATIE

ONTWERPBESLUIT VAN DE RAAD VAN HET BIPT VAN 03/05/2013 TOT VASTSTELLING VAN DE HYPOTHESEN WAARIN DE OPERATOREN AAN HET BIPT EEN VEILIGHEIDSINCIDENT MOETEN MELDEN EN VAN DE NADERE BEPALINGEN VAN DEZE KENNISGEVING

Hoe kunt u reageren op dit document?
Antwoordtermijn: Vrijdag 7 juni 2013
Aanspreekpunt: Karel Peeters
Antwoordadres per e-mail: consult08@bipt.be
Antwoorden dienen elektronisch te worden verzonden.
In de reactie moet duidelijk worden vermeld wat vertrouwelijk is door het desbetreffende formulier te gebruiken [http://www.bipt.be/ShowDoc.aspx?levelID=384&objectID=3243]. Bevat de reactie vertrouwelijke elementen, dan moet een openbare versie van de reactie worden verstrekt.

INHOUDSOPGAVE

INHOUDSOPGAVE **2**

1. DOEL EN JURIDISCHE BASIS **3**

2. PROCEDURE **4**

2.1. OPENBARE RAADPLEGING 4
2.2. RAADPLEGING VAN DE MEDIAREGULATOREN 4
2.3. MACHTIGING VAN DE MINISTER 4

3. EUROPESE CONTEXT **4**

4. HYPOTHESES WAARIN DE OPERATOREN AAN HET BIPT EEN VEILIGHEIDSINCIDENT MOETEN MELDEN **5**

4.1. INLEIDING 5
4.2. AAN KENNISGEVING ONDERWORPEN OPERATOREN 5
4.3. VEILIGHEIDSINCIDENT 5
4.4. INCIDENT EN RISICO VOOR EEN INCIDENT 6
4.5. BETROKKEN NETWERKEN EN DIENSTEN 6
4.6. IMPACTDREMPELS 6
4.6.1. Principes *6*
4.6.2. Uitleg *7*

5. TERMIJN WAARBINNEN DE KENNISGEVING MOET PLAATSVINDEN **7**

6. WIJZE VAN OVERZENDING VAN DE KENNISGEVING **8**

7. INHOUD VAN DE KENNISGEVING **8**

8. BEROEPSMOGELIJKHEDEN **8**

BIJLAGE 1: KENNISGEVINGSFORMULIER **9**

BIJLAGE 2: RESULTATEN VAN DE OPENBARE RAADPLEGING **10**

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 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[2] :

"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." (door ons onderstreept).

4 Bovendien bepaalt artikel 114/2 van de WEC, zoals ingevoegd in de WEC door de voormelde wet van 10 juli 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. "

5 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.

6 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.

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.

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

[2] Dit besluit behandelt ook niet de vergoedingen die de operatoren zouden moeten betalen aan de abonnees in geval van een onderbreking van de dienst zoals beschreven in een koninklijk besluit die zou kunnen genomen worden op basis van het artikel 113/2 van de WEC.

2. PROCEDURE

2.1. Openbare raadpleging

8 Van [wordt later ingevuld] tot [wordt later ingevuld] 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 personen hebben op deze raadpleging geantwoord:

[zal later worden aangevuld]

10 De samenvatting van de resultaten van de openbare raadpleging vormt een bijlage 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 [zal later worden ingevuld] dit ontwerpbesluit overgezonden naar de mediaregulatoren van de gemeenschappen, namelijk de CSA, de Medienrat en de VRM. De mediaregulatoren van de gemeenschappen hebben als reactie het volgende geantwoord: [zal later worden aangevuld].

2.3. Machtiging van de minister

12 Met zijn brief van [zal later worden aangevuld] 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*

[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

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 uitvoering van artikel 13bis van de Kaderrichtlijn en in het bijzonder wat betreft de verplichting vervat in dat artikel 13bis 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 26 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 "*the ability of the system to retain its specified attributes in terms of performance and functionality"*[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").

---

[7] Zie artikel 13*bis.3*, derde lid, van de Kaderrichtlijn.

[8] Dit in het bijzonder wat de inhoud van de kennisgevingen betreft.

[9] "*het vermogen van het systeem om zijn gespecificeerde eigenschappen in termen van prestatievermogen en functionaliteit te behouden*"
Zie ENISA-document, blz. 5.

4.4. Incident en risico voor een incident

22 Het zuivere vermoeden dat er zich een incident heeft voorgedaan, leidt niet tot de verplichting om krachtens dit besluit een kennisgeving te doen[10]. De vaststelling van een incident wordt beschouwd als vaststaand wanneer de operator over genoeg elementen beschikt die erop wijzen dat er zich een veiligheidsincident heeft voorgedaan om een kennisgeving aan het BIPT te rechtvaardigen.

4.5. Betrokken netwerken en diensten

23 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.

24 De lijst van de te beschouwen netwerken en diensten is de volgende[11]:
- Netwerken: vast, mobiel
- (Spraak)telefoniedienst
- 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

26. Een incident moet worden gemeld aan het BIPT indien een van de volgende drempels wordt bereikt (niet-cumulatieve criteria); deze criteria zijn geïnspireerd op die van het ENISA, rekening houdende met het aantal eindgebruikers in België:

27. 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 vastgesteld in de punten 2 tot 6 hieronder is bereikt. ("drempel 1")

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 en dat incident kan niet binnen een uur worden opgelost. ("drempel 2")

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 en dat incident kan niet binnen 2 uur worden opgelost. ("drempel 3")

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 en dat incident kan niet binnen 4 uur worden opgelost. ("drempel 4")

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

[10] 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).

[11] Zie bladzijde 9 van het document van het ENISA.

internettoegang) of 270 (huurlijnen) eindgebruikers en dat incident kan niet binnen 6 uur worden opgelost. ("drempel 5")

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), 21 000 (mobiele internettoegang) of 130 (huurlijnen) eindgebruikers en dat incident kan niet binnen 8 uur worden opgelost. ("drempel 6")

33. Het incident heeft invloed op een aantal van 10 of meer vaste of tijdelijke basisstations, ongeacht het aantal getroffen eindgebruikers of de duur van dat incident. ("drempel 7")

4.6.2. Uitleg

4.6.2.1 Eerste drempel: het incident treft een dienst verstrekt aan een gebruiker die geen eindgebruiker is

33 Artikel 2, 12°, van de WEC definieert het begrip gebruiker als "*een natuurlijke of rechtspersoon die gebruik maakt van of verzoekt om een openbare elektronische-communicatiedienst*". Artikel 2, 13° definieert dan weer een eindgebruiker als "e*en gebruiker die geen openbaar elektronische-communicatienetwerk of openbare elektronische-communicatiediensten aanbiedt.*"

34 Het eerste criterium verwijst dus naar een dienst (bijvoorbeeld een dienst voor gedeelde of ontbundelde toegang tot het aansluitnet of een dienst voor breedbandtoegang) die een operator aan een andere operator verstrekt. Om te bepalen of de drempel twee, drie, vier, vijf of zes is bereikt en of verschillende gebruikers buiten eindgebruikers door het incident getroffen zijn, zal de operator die de door het incident getroffen dienst verstrekt de getroffen eindgebruikers optellen bij de verschillende getroffen gebruikers. Daartoe zal hij rekening houden met het aantal lijnen, oproepnummers of simkaarten die mogelijks getroffen zijn. Een eindgebruiker is getroffen wanneer de beschikbaarheid of de continuïteit van het netwerk of de dienst niet kan worden gegarandeerd.

4.6.2.2. Drempels twee, drie, vier, vijf en zes: het incident treft een aantal eindgebruikers voor een bepaalde duur

35 Elke operator is verplicht de impact van het incident op zijn eindgebruikers te onderzoeken en niet op de eindgebruikers van andere operatoren. De drempels twee tot zes worden dus berekend per operator en niet rekening houdende met de eindgebruikers van verschillende operatoren die door het incident getroffen zouden zijn[12].

36 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 meer gegarandeerd kan worden.

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

38 De "duur van het incident" is de tijd (in uren) gedurende dewelke er een beduidende impact was op de exploitatie van de diensten[13].

5. TERMIJN WAARBINNEN DE KENNISGEVING MOET PLAATSVINDEN

39 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)

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

[12] Eenzelfde incident kan invloed hebben op de netwerken of diensten van verschillende operatoren.
[13] Zie ENISA-document, blz. 12 en 13.

1) De kennisgeving moet worden gericht aan het BIPT zodra de operator over alle inlichtingen bedoeld in deel 7 beschikt, of in elk geval binnen 24 uur na het begin van het incident volgens de hieronder vastgestelde wijze van verzending.

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

41 De operatoren worden verplicht de beveiligde website te gebruiken die door het BIPT online is gezet voor de kennisgeving van veiligheidsincidenten.

42 Wanneer de site onbeschikbaar is en telkens nadat er via de voormelde site een incident is gemeld, zal de operator deze kennisgeving binnen een redelijke termijn (maximaal 24 uur) aan het BIPT doen via drager, brief of fax, waarbij deze kennisgeving moet worden ondertekend door een of meer personen die de operator mogen vertegenwoordigen.

7. INHOUD VAN DE KENNISGEVING

43 De inlichtingen die in het kader van de kennisgeving moet worden meegedeeld worden gedetailleerd in bijlage 1[14].

8. BEROEPSMOGELIJKHEDEN

44 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 na de kennisgeving van het besluit of bij gebreke aan een kennisgeving, na de publicatie van het besluit of bij gebreke aan een publicatie, na de kennisname van het besluit.

45 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 het door de griffie van de rechtbank betekende verzoekschrift op zijn website. Elke belanghebbende partij kan in de zaak tussenkomen binnen dertig dagen na deze publicatie.

Georges Denef
Lid van de Raad

Axel Desmedt
Lid van de Raad

Catherine Rutten
Lid van de Raad

Michel Van Bellinghen
Lid van de Raad

[14] Deze inlichtingen worden ook vermeld op de beveiligde website van het BIPT.

BIJLAGE 1: KENNISGEVINGSFORMULIER

Informatie	Beschrijving
DATUM EN TIJD	
Aanvangsdatum	Details over de datum en het tijdstip waarop het incident heeft plaatsgevonden (in nationale tijd). Het kan worden geïnterpreteerd als het tijdstip waarop het incident is vastgesteld. Het tijdstip moet worden uitgedrukt in zowel MET en plaatselijke tijd.
IMPACT EN GRONDOORZAAK VAN HET INCIDENT	
Getroffen diensten: - **Vaste telefonie** - **Mobiele telefonie** - **(Short) Message Services (tekstberichten)** - **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
Impact op noodoproepen	Indien beschikbaar, nooddienst die door het incident getroffen is
Meer details over de impact	[*Facultatief*] Details over de impact van het incident
Grondoorzaak[15]: - **Natuurramp of -fenomeen** - **Menselijke fout** - **Kwaadwillige aanval of acties** - **Hardware- of softwarefout** - **Fout bij een derde of een externe partij**	De aanvankelijke oorzaak van het incident
Meer details over de grondoorzaak	[*Facultatief*] De te rapporteren incidenten moeten zich toespitsen op de integriteit van het netwerk en de continuïteit van de dienst. Dit kunnen subcategorieën zijn van de grondoorzaken die vermeld zijn in de desbetreffende sectie.
ANDERE INCIDENTINFORMATIE	
Algemene beschrijving	Samenvatting van het incident
Behandeling en respons ten aanzien van incidenten[16]	Alle acties die ondernomen zijn na de vaststelling van het incident en de maatregelen die aangenomen zijn om de dienst in zijn aanvankelijke situatie/niveau te herstellen
Acties na het incident	Beschrijving van eventuele regelingen die getroffen zijn om het risico te verkleinen.
Getroffen nationale interconnectie	Wanneer de getroffen dienst schade/verandering kan veroorzaken aan een activum (of dienst) toebehorend aan een andere operator of aanbieder, dan is dit een getroffen interconnectie.

[15] Document van het ENISA, blz. 13 en 14 Ongeacht of deze oorzaak of oorsprong een inbreuk op de veiligheid of een verlies van integriteit is.

[16] Respons en herstelmaatregelen genomen zowel tijdens als na het incident door de aanbieders.

	Indien van toepassing, details over de betrokken Belgische operatoren
Getroffen internationale interconnectie	In geval van grensoverschrijdende incidenten kan het voorkomen dat een inbreuk op de veiligheid in de ene lidstaat de activa treft van een andere "geïnterconnecteerde" lidstaat. Bepaalde infrastructurele concentraties zijn kwetsbaar en er kan een aanzienlijke verstoring worden veroorzaakt door een plaatselijke fout; geïnterconnecteerde systemen kunnen onderhevig zijn aan aaneengeschakelde technische storingen. Indien van toepassing, details over de betrokken operatoren uit andere lidstaten.
Geografische reikwijdte/getroffen regio	Indien beschikbaar, de regio die door het incident getroffen is.
Geleerde lessen	Beschrijf eventuele acties die na het incident genomen zijn om de veiligheid van het activum te verbeteren en de procedures die van dan af zullen worden gevolgd (of maatregelen die zullen worden genomen). Het verschil tussen dit veld en het veld "Maatregelen na het incident" bestaat erin dat we in dit veld verwijzen naar langetermijnacties.
Andere opmerkingen	Aanvullende inlichtingen over het incident of de kennisgeving van het incident

BIJLAGE 2: RESULTATEN VAN DE OPENBARE RAADPLEGING

[zal later worden aangevuld]