BELGISCH INSTITUUT VOOR POSTDIENSTEN EN TELECOMMUNICATIE

ONTWERPBESLUIT VAN DE RAAD VAN HET BIPT VAN XX/XX/XXXX BETREFFENDE DE DREMPELS EN MODALITEITEN VOOR KENNISGEVING VAN VEILIGHEIDSINCIDENTEN BINNEN DE SECTOR ELECTRONISCHE COMMUNICATIE

WERKWIJZE OM OP DIT DOCUMENT TE ANTWOORDEN

Antwoordtermijn:	tot 15/09/2017
Werkwijze om te antwoorden:	Aan: consultation.sg@bipt.be Onderwerp: « CONSULT-2017-C2 »
Aanspreekpunt:	Tim Masy, Ingenieur-adviseur (+32 (0)2 226 89 74)

Antwoorden dienen elektronisch te worden verzonden naar het opgegeven adres.

Er wordt gevraagd om het "Formulier dat als voorpagina dient te worden gebruikt bij het antwoord op een door het BIPT georganiseerde openbare raadpleging" te gebruiken.

Het BIPT wenst ook dat de commentaren verwijzen naar de paragrafen en/of onderdelen waarover ze handelen. Op het document moet duidelijk worden aangegeven wat vertrouwelijk is.

INHOUDSOPGAVE

1 Context

1.1 Voorwerp

1 Dit besluit vervangt het besluit van de Raad van het BIPT van 1 april 2014 tot vaststelling van de hypothesen waarin de operatoren aan het BIPT een veiligheidsincident moeten melden en van de nadere bepalingen van deze kennisgeving.

1.2 Doel

2 Na evaluatie van de kennisgevingen van veiligheidsincidenten (hierna "*kennisgevingen*") ontvangen sinds het besluit van 1 april 2014, blijkt een verlaging en vereenvoudiging van de drempels nodig voor een betere kennis van het BIPT over veiligheidsincidenten (hierna "*incidenten*") met een belangrijke impact. Daarnaast is het wijzigen van de modaliteiten voor kennisgevingen nodig voor een geautomatiseerde verzameling en gestructureerde opslag van de kennisgevingen.

3 De voorgestelde wijzigingen zullen bijdragen tot een efficiëntere monitoring van de veiligheid van netwerken en diensten. Op basis hiervan kan een fijnere risicoanalyse voor de sector uitgevoerd worden om de minimale veiligheidsmaatregelen voor de sector hieraan te kunnen aanpassen.

4 Dit besluit is gebaseerd op de recentste technische richtsnoeren van ENISA in de materie[1] en heeft o.a. tot doel de coherentie te verzekeren tussen de kennisgevingen van de operatoren aan het BIPT en het beknopte verslag van het BIPT aan ENISA en de Europese Commissie. Zoals geadviseerd in de richtsnoeren[2] worden voor nationale kennisgevingen strengere drempels en een ruimer toepassingsgebied gehanteerd.

1.3 Juridische basis

5 Artikel 114/1, § 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna 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. 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.".*

6 Voor de aspecten uit de huidige discussie die geen betrekking hebben op de hypothetische gevallen waarin de inbreuk op de veiligheid of het verlies van integriteit een belangrijke impact heeft, beroept het huidig besluit zich op Artikel 114/2, § 1 van de WEC, dat het volgende bepaalt:

> *"§ 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.*".

---

[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] Quote uit hoofdstuk 6 Annual summary reporting: *"In dit deel definiëren we de scope en de drempels voor de jaarlijkse beknopte rapportering door de NRI's aan ENISA en de EC. We benadrukken dat dit deel niet mag worden opgevat als een aanbeveling over de incidenten die (nationaal) significant zijn, noch over welke incidenten nationaal gerapporteerd zouden moeten worden. De NRI's moeten, wanneer dat relevant is, een ruimere scope en striktere drempels toepassen, rekening houdende met de nationale omstandigheden en eisen."* (vrije vertaling).

1.4 Procedure

1.4.1 Openbare raadpleging

7 Van XX/XX/2017 tot XX/XX/2017 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.

1.4.2 Raadpleging van de mediaregulatoren

8 Krachtens artikel 3 van het samenwerkingsakkoord van 17 november 2006[3] heeft het BIPT op XX/XX/2017 dit ontwerpbesluit overgezonden naar de mediaregulatoren van de gemeenschappen, namelijk de CSA, de Medienrat en de VRM.

1.4.3 Machtiging van de minister

9 Met zijn brief van XX/XX/2017 heeft de heer Alexander De Croo, vice-premier en minister van Ontwikkelingssamenwerking, Digitale Agenda, Telecom en Post, de voorafgaande machtiging gegeven, waarvan sprake in artikel 114/1, § 2, van de WEC.

2 Hypotheses voor het melden van incidenten

2.1 Toepassingsgebied

10 De meldingsplicht voorzien in dit besluit, uit hoofde van artikel 114/1, § 2 van de WEC, is van toepassing op zowel ondernemingen die openbare elektronische communicatienetwerken[4] (hierna "*netwerken*") aanbieden als ondernemingen die openbare elektronische-communicatiediensten[5] (hierna "*diensten*") aanbieden. Deze ondernemening worden hierna “operatoren” genoemd.

11 Dit besluit is van toepassing op alle netwerken en diensten[6].

12 Voor de toepassing van dit besluit wordt onder “*incident*” verstaan een inbreuk op de veiligheid of een verlies van integriteit die een impact kan hebben op de goede werking of beveiliging van netwerken en diensten[7].

13 De "*beveiliging van netwerken en diensten*" wordt gedefinieerd[8] als het vermogen van elektronische-communicatienetwerken en -diensten om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerken of diensten worden aangeboden of toegankelijk zijn, in gevaar brengen.

---

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 De term "*elektronische-communicatienetwerk*" wordt gedefinieerd in artikel 2, 3°, van de WEC.

5 De term "*elektronische-communicatiedienst*" wordt gedefinieerd in artikel 2, 5°, van de WEC.

6 Hieronder vallen o.a. de volgende diensten: vaste telefonie, vast internet, mobiele telefonie, mobiel internet, huurlijnen, SMS, MMS, internationale roaming, publieke wifi, web gebaseerde spraakdiensten, web gebaseerde berichtendiensten, publieke email.

7 Gebaseerd op definitie uit ENISA technische richtsnoer hoofdstuk 3.3.

8 Definitie uit voorstel 2016/0288(COD) van de Europese Commissie voor een RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD tot vaststelling van het Europees wetboek voor elektronische communicatie.

2.2 Drempels

14 De meldingsplicht geldt voor elk incident dat een belangrijke impact heeft op de exploitatie en veiligheid van netwerken en diensten. De impact van een incident wordt belangrijk beschouwd, indien minstens één van de volgende drempels wordt bereikt of overschreden:

1) het incident duurt minstens 1 uur en treft minstens 25.000 eindgebruikers[9];
2) het incident heeft een impact op het netwerk waardoor de toegang tot de nooddiensten[10] via dit netwerk getroffen wordt.
3) het incident heeft een impact op interconnecties[11] waardoor andere operatoren in binnen- of buitenland getroffen worden;
4) het incident heeft een impact op een netwerkelement dat de operator als kritiek beschouwd voor de exploitatie van zijn netwerken of diensten.

15 Indien een operator het nuttig acht kan hij elk incident melden, zelfs indien het incident niet beantwoordt aan de voormelde drempels.

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

17 Wanneer het aantal getroffen eindgebruikers niet exact bepaald kan worden[12], maakt de aanbieder naar best vermogen een schatting van het aantal getroffen eindgebruikers rekening houdende met het normale gebruik van de getroffen inrichtingen.

18 In vele incidenten worden gelijktijdig meerdere diensten getroffen. Het aantal getroffen gebruikers kan verschillen per getroffen dienst. In deze gevallen meldt de operator aparte aantallen per getroffen dienst in dezelfde melding.

19 Deze sectie doet geen afbreuk aan de mogelijkheid van het BIPT om aan één of meer operatoren, op basis van artikel 114/2, §2 van de WEC, te vragen om kennisgevingen voor een specifiek type incidenten. Deze kennisgevingen gebeuren ook volgens de modaliteiten in sectie 3 hieronder.

3 Modaliteiten voor het melden van incidenten

20 Onverwijld na vaststelling van het incident wordt een beknopte schriftelijke kennisgeving verzonden naar het elektronisch adres "incident@bipt.be", dat enkel basisinformatie omvat over het incident en de impact[13]. Wanneer er belangrijke ontwikkelingen plaatsvinden, wordt een nieuwe kennisgeving verzonden.

21 Binnen de 3 dagen na vaststelling van het incident wordt een volledige kennisgeving naar het BIPT verzonden via het formulier op het elektronisch kennisgevingsplatform dat ter beschikking gesteld wordt door het BIPT[14]. Dit formulier omvat minstens de essentiële elementen van informatie zoals hernomen in onderdeel 7 "Incident Report Template" van de voormelde technische richtsnoeren van ENISA.

---

9 Deze drempel is gebaseerd op de ondergrenzen uit de voormelde technische richtsnoer van ENISA voor drempels betreffende het aantal getroffen eindgebruikers en de duur van het incident: "*Uitgesloten zijn heel kleine incidenten, die minder dan 25.000 aansluitingen van gebruikers treffen, alsook zeer kortdurende incidenten, die minder dan 1 uur duren.*" (vrije vertaling).

10 De term "*nooddienst*" wordt gedefinieerd in artikel 2, 58°, van de WEC.

11 De term "*interconnectie*" wordt gedefinieerd in artikel 2, 19°, van de WEC.

12 Bijvoorbeeld voor mobiele elektronische communicatiegebruikers of omdat er diensten worden geleverd aan andere operatoren (MVNO's, …) of derden en dus niet rechtstreeks aan de eindgebruiker.

13 Onder andere de reeds beschikbare informatie over de diensten, netwerken, aantal eindgebruikers en geografische zone die getroffen werden.

14 www.incident.bipt.be

4 Inwerkingtreding en beroepsmogelijkheden

4.1 Inwerkingtreding

22 Dit besluit treedt in werking op 1 januari 2018 en vervangt op die dag het Besluit van de Raad van het BIPT van 1 april 2014 tot vaststelling van de hypothesen waarin de operatoren aan het BIPT een veiligheidsincident moeten melden en van de nadere bepalingen van deze kennisgeving.

4.2 Beroepsmogelijkheden

23 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 Marktenhof, 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.

24 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 het gerecht genotificeerd is. Elke belanghebbende partij kan in de zaak tussenkomen binnen dertig dagen na deze publicatie.

Axel Desmedt
Lid van de Raad

Jack Hamande
Lid van de Raad

Luc Vanfleteren
Lid van de Raad

Michel Van Bellinghen
Voorzitter van de Raad