



**BELGISCH INSTITUUT VOOR POSTDIENSTEN
EN TELECOMMUNICATIE**

**ADVIES VAN DE RAAD VAN HET BIPT
VAN 15 MEI 2019
BETREFFENDE
HET ONTWERP VAN KONINKLIJK BESLUIT TOT UITVOERING VAN DE NIS-
WET, ALSOOK VAN SOMMIGE BEPALINGEN VAN DE WET “KRITIEKE
INFRASTRUCTUREN”**

INHOUDSOPGAVE

1. Voorwerp	3
2. Samenvatting van het ontwerp van koninklijk besluit	3
3. Opmerkingen van het BIPT over de inhoud van het ontwerp van koninklijk besluit.....	4
3.1. Woord vooraf.....	4
3.2. Titels van de hoofdstukken 3 en 4	4
3.3. Artikel 5. Beveiligd meldingsplatform.....	4
3.4. De artikelen 6 en 7. Melding van de incidenten.....	5
3.5. Artikel 9. Protocolakkoord.....	5
3.6. Artikel 10. Vrijwillige meldingen.....	5
3.7. Artikel 11. Accreditatie van de instellingen voor de conformiteitsbeoordeling.....	6
4. Bijlage	8

1. Voorwerp

1. In een brief van 2 mei 2019 heeft het Centrum voor Cybersecurity België (hierna het CCB) aan het BIPT, als sectoroverheid voor de digitale infrastructuur, gevraagd om tegen uiterlijk 17 mei 2019 een advies te verstrekken over artikel 11 van het ontwerp van koninklijk besluit (hierna het ontwerp van koninklijk besluit) tot uitvoering van de NIS-wet alsook sommige bepalingen van de wet “kritieke infrastructuren” (zie bijlage)¹.
2. Conform artikel 14, § 1, 1^o, van de BIPT-statuutwet² verstrekt het BIPT een advies aan de minister³ of aan de Kamer van volksvertegenwoordigers. Aangezien de NIS-wet⁴ niet bepaalt dat het advies van het BIPT over het ontwerp van koninklijk besluit aan het CCB moet worden verstrekt, wordt dit advies gericht aan minister Philippe De Backer, minister van Digitale Agenda en Telecommunicatie. Er wordt een kopie van dit advies bezorgd aan het CCB. Het BIPT herinnert er aan dat dit advies zal worden gepubliceerd op zijn website.
3. In zijn brief vraagt het CCB uitsluitend over artikel 11 van het ontwerp van koninklijk besluit advies aan het BIPT, aangezien krachtens de NIS-wet de sectoroverheden advies moeten uitbrengen over dit artikel 11 maar niet over de andere bepalingen van het ontwerp van koninklijk besluit. Toch formuleert het BIPT enkele opmerkingen over de andere artikelen van het ontwerp van koninklijk besluit op basis van de mogelijkheid die het krijgt krachtens artikel 14, § 1, 1^o, van de BIPT-statuutwet om op eigen initiatief een advies te verstrekken aan de minister⁵.
4. Het BIPT is van oordeel dat een openbare raadpleging over het ontwerp van koninklijk besluit en het formulier voor melding van veiligheidsincidenten erg nuttig had geweest maar begrijpt ook de noodzaak om het koninklijk besluit snel aan te nemen zodat de omzetting van de NIS-richtlijn kan worden voltooid⁶.

2. Samenvatting van het ontwerp van koninklijk besluit

5. Het ontwerp van koninklijk besluit legt de volgende regels vast:
 - 5.1. Hoofdstuk 1 omvat definities;

¹ De volledige titel van het ontwerp van koninklijk besluit luidt: “ontwerp van koninklijk besluit tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, alsook van sommige bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren”.

² Zie artikel 14, § 1, 1^o, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector: § 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:

1^o het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers;”.

³ Volgens artikel 2, 4^o, van de BIPT-statuutwet dient onder “minister” te worden verstaan “de minister of staatssecretaris die bevoegd is voor de aangelegenheden die de postdiensten of telecommunicatie betreffen.”

⁴ Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

⁵ Zie voetnoot nr. 2.

⁶ Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

- 5.2. Hoofdstuk 2 en bijlagen 1 en 2 bepalen wie de bevoegde overheden zijn, met name het CCB, de Algemene Directie Crisiscentrum (ADCC), de sectoroverheden en de inspectiediensten⁷;
- 5.3. Hoofdstuk 3 bevat regels inzake de melding en de behandeling van de incidenten;
- 5.4. Hoofdstuk 4 bevat regels inzake de vrijwillige meldingen;
- 5.5. Hoofdstuk 5 bevat regels inzake de accreditatie van de instellingen voor de conformiteitsbeoordeling.

3. Opmerkingen van het BIPT over de inhoud van het ontwerp van koninklijk besluit

3.1. Woord vooraf

6. De inleiding van het ontwerp van koninklijk besluit geeft aan dat het genomen wordt “gelet op het advies van de sectorale overheden over artikel 11 van de wet van 7 april 2019”. Het BIPT veronderstelt dat deze considerans in werkelijkheid doelt op artikel 11 van het ontwerp van koninklijk besluit en niet op artikel 11 van de NIS-wet. Zoals hierboven vermeld, geeft het BIPT zijn advies over het hele ontwerp van koninklijk besluit en niet enkel over artikel 11 ervan.

3.2. Titels van de hoofdstukken 3 en 4

7. De titels van de hoofdstukken 3 en 4 zouden moeten worden herzien omdat de vrijwillige meldingen (van incidenten) bedoeld in hoofdstuk 4 een vorm van incidentmelding zijn in de zin van hoofdstuk 3.

3.3. Artikel 5. Beveiligd meldingsplatform

8. Artikel 5 van het ontwerp van koninklijk besluit bepaalt het volgende:

“Art. 5. Een beveiligd meldingsplatform wordt opgericht met het oog op:

1°) het melden van beveiligingsincidenten door aanbieders van essentiële diensten en digitaalgedienstverleners aan het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de ADCC, krachtens de wet van 7 april 2019;

2°) het eventueel melden van inbreuken in verband met persoonsgegevens door aanbieders van essentiële diensten en digitaalgedienstverleners aan een toezichthoudende autoriteit persoonsgegevens, zoals bepaald in artikel 31, § 1, tweede lid van de wet. ”

9. Er dient te worden gepreciseerd dat het om minimumtaken van het meldingsplatform gaat aangezien het de bedoeling is dat dit platform ook de melding van de veiligheidsincidenten van de telecomoperatoren aan het BIPT mogelijk maakt. Er zou ook kunnen worden beoogd dat dit platform wordt gebruikt voor bepaalde vrijwillige meldingen van veiligheidsincidenten, indien in de praktijk blijkt dat dat het versturen of behandelen van deze meldingen vergemakkelijkt.

⁷ Het BIPT wordt niet vermeld in het koninklijk besluit, wat te verklaren valt doordat het de wet zelf is die de hoedanigheid van sectorale overheid en van inspectiedienst van het BIPT toewijst voor de sector van de digitale infrastructuren.

3.4. De artikelen 6 en 7. Melding van de incidenten

10. De artikelen 6 en 7 van het ontwerp van koninklijk besluit bepalen het volgende:

“Art. 6. § 1. De melding gebeurt via het meldingsplatform met behulp van het formulier voor het melden van incidenten dat is opgesteld door het nationale CSIRT. [...]

Art. 7. Het nationale CSIRT bepaalt de modaliteiten voor de melding door aanbieders van essentiële diensten en digitaalgedienstverleners indien het meldingsplatform bedoeld in artikel 6 niet beschikbaar is.”

11. De melding van veiligheidsincidenten vormt een essentiële bron van informatie voor de uitoefening van de bevoegdheid van het BIPT. Deze laatste meent dan ook dat het in overleg is met de sectorale overheid, waaronder het BIPT, dat het nationale CSIRT de inhoud van het incidentmeldingsformulier zou moeten vastleggen alsook de nadere regels voor de melding die de aanbieders van essentiële diensten en digitaalgedienstverleners moeten hanteren in geval van onbeschikbaarheid van het meldingsplatform.

3.5. Artikel 9. Protocolakkoord

12. Artikel 9 van het ontwerp van koninklijk besluit bepaalt het volgende:

“Het nationale CSIRT, de sectorale overheden en de ADCC sluiten een protocolakkoord onder meer voor het vastleggen van:

1° de modaliteiten voor het beheer van het meldingsplatform;

2° de modaliteiten voor de verwerking van meldingen, bedoeld in artikel 8, § 3;

3° de modaliteiten betreffende de verzoeken om bijkomende informatie gericht aan de aanbieder van essentiële diensten of digitaalgedienstverlener bedoeld in artikel 6, § 4.”

13. Het BIPT meent dat dit protocol niet enkel “de modaliteiten betreffende de verzoeken om bijkomende informatie gericht aan de aanbieder van essentiële diensten of digitaalgedienstverlener bedoeld in artikel 6, § 4.” (3°) zou moeten vastleggen maar ook de nadere regels voor artikel 8, § 1, dat het volgende bepaalt:

“Art. 8. § 1. Het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT of de ADCC kunnen de aanbieder van essentiële diensten of digitaalgedienstverlener bijkomende informatie vragen over diens meldingen.”

14. Net zoals voor artikel 6, § 4, bestaat het risico dat de tenuitvoerbrenging van artikel 8, § 1, leidt tot parallelle verzoeken om bijkomende informatie van de overheden ten aanzien van een aanbieder van essentiële diensten.

3.6. Artikel 10. Vrijwillige meldingen

15. Artikel 10, § 3, van het ontwerp van koninklijk besluit bepaalt het volgende: “Het nationale CSIRT bezorgt de informatie over deze meldingen aan de ADCC en aan de sectorale overheden of sectorale CSIRT’s die mogelijk geïnteresseerd zijn.”
16. Aangezien de melding van veiligheidsincidenten essentieel is voor het BIPT zou deze laatste de vrijwillige melding willen ontvangen en niet enkel de informatie met betrekking tot deze melding.

3.7. Artikel 11. Accreditatie van de instellingen voor de conformiteitsbeoordeling

17. De NIS-wet beoogt een accreditatie van de instellingen voor de conformiteitsbeoordeling in de twee volgende artikelen:

17.1. Artikel 22, § 2: “De naleving van de eisen bedoeld in paragraaf 1 [met name het feit dat het databeveiligingsbeleid van de aanbieder van essentiële diensten beantwoordt aan de vereisten van de norm ISO/IEC 27001 of een andere nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend] wordt aangetoond aan de hand van een certificaat uitgereikt door een instelling voor de conformiteitsbeoordeling die volgens de norm ISO/IEC 17021 of ISO/IEC 17065 geaccrediteerd is door de accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de “European Cooperation for Accreditation” medeondertekend heeft. (wij onderlijnen)

17.2. Artikel 38, § 2: “De aanbieder van essentiële diensten laat, minstens om de drie jaar en op zijn kosten, een externe audit uitvoeren door een instelling voor de conformiteitsbeoordeling die geaccrediteerd is door de accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de “European Cooperation for Accreditation” medeondertekend heeft. [...]” (wij onderlijnen)

18. In de praktijk is een “instelling voor de conformiteitsbeoordeling” bedoeld in die twee artikelen, een “instantie die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer ijken, testen, certificeren en inspecteren”⁸ en is de “accreditatieoverheid” bedoeld in artikel 38, § 2⁹, BELAC, dat is opgericht binnen de FOD Economie, K.M.O., Middenstand en Energie¹⁰.

⁸ Artikel 6, 5°, van de NIS-wet definieert een instelling voor conformiteitsbeoordeling als volgt: “instelling bedoeld in artikel I.9 van het Wetboek van economisch recht”. Artikel I. 9 bevat de volgende definities:

4° Accreditatie: formele verklaring van de nationale accreditatie-instelling dat een conformiteitsbeoordelingsinstantie voldoet aan de eisen die zijn bepaald door geharmoniseerde normen en, indien van toepassing, aan aanvullende eisen, zoals die welke zijn opgenomen in de relevante sectorale regelingen, vereist om een specifieke conformiteitsbeoordelingsactiviteit te verrichten;

5° "Accreditatiesysteem": systeem met eigen beheersregels bedoeld om de uitvoering van de accreditatieprocedure toe te laten;

6° "Conformiteitsbeoordeling": het proces waarin wordt aangetoond of voldaan is aan vastgestelde eisen voor een product, proces, dienst, systeem, persoon of instantie;

7° "Instelling voor de conformiteitsbeoordeling": instelling die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer kalibratie, proeven, certificatie en keuring;”

⁹ Artikel 22, § 2, beoogt de “accreditatieoverheid” maar het BIPT veronderstelt dat het in werkelijkheid gaat om de nationale accreditatieoverheid.

¹⁰ Artikel 6, 7°, van de NIS-wet definieert een “nationale accreditatieoverheid” als een “instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het wetboek van economisch recht”. Dit artikel [VIII.30](#) bepaalt het volgende: “§ 1. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, alle nuttige maatregelen treffen om een accreditatiesysteem op te richten. Hij zal daartoe inzonderheid één nationale accreditatie-instelling en een nationale Raad voor Accreditatie oprichten.

§ 2. De nationale accreditatie-instelling is verantwoordelijk voor het beheer van de accreditatieprocedure, met inbegrip van de toekenning en de intrekking van de accreditaties. [...]”

§ 4. De Koning stelt, na raadpleging van de Nationale Raad voor Accreditatie, bij een besluit, vastgesteld na overleg in de Ministerraad, de accreditatiecriteria vast van de instellingen voor de conformiteitsbeoordeling.

§ 5. De certificaten en verslagen van de conformiteitsbeoordeling afgeleverd door instellingen die op grond van deze Titel zijn geaccrediteerd, worden door de Belgische Staat erkend. ”

19. Artikel 39, § 1, van de NIS-wet bepaalt het volgende: “De Koning moet, na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1 [in de praktijk het CCB], de accreditatievoorwaarden bepalen. 1° Deze moeten gebaseerd zijn op de normen ISO/IEC 17021 of ISO/IEC 17065.”

20. Deze bepaling wordt als volgt ten uitvoer gebracht in artikel 11 van het ontwerp van koninklijk besluit:

“De instellingen voor de conformiteitsbeoordeling die geaccrediteerd wensen te worden voor de externe audit van aanbieders van essentiële diensten, bedoeld in artikel 38, § 2, van de wet, of van digitaalendienst-verleners, moeten een aanvraag indienen bij de nationale accreditatie-autoriteit of bij een officiële accreditatie-instelling van een ander land.

Om daarvoor te worden geaccrediteerd, moet de instelling voor de conformiteitsbeoordeling de volgende voorwaarden vervullen:

1° op ieder ogenblik voldoen aan de accreditatiecriteria, zowel wat de operationaliteit van het toegepaste managementsysteem als wat de specifieke technische aspecten vermeld in de betrokken norm ISO/IEC 17021 of ISO/IEC 17065 betreft;

2° voldoen aan de werkingsprocedures van het accreditatiesysteem die van toepassing zijn op de geaccrediteerde instellingen.”

21. In de eerste plaats zou artikel 11 van het ontwerp van koninklijk besluit niet enkel moeten verwijzen naar de externe audits bedoeld in artikel 38, § 2, van de NIS-wet maar ook naar de conformiteit van het informatiebeveiligingsbeleid (I.B.B.) waarvan sprake in artikel 22, § 2, van diezelfde wet, aangezien de regels die artikel 11 oplegt, relevant zijn voor beide artikelen.

22. Om vervolgens te zorgen voor conformiteit tussen de artikelen 22, § 2 en 38, § 2, van de NIS-wet enerzijds en artikel 11 van het ontwerp van koninklijk besluit anderzijds, dient in dit artikel “een instelling die de erkenningsakkoorden van de “European Cooperation for Accreditation” medeondertekend heeft” te worden beoogd, zoals vastgelegd in de artikelen 22, § 2 en 38, § 2, en geen “officiële accreditatie-instelling van een ander land”¹¹.

23. Ten slotte zijn de volgende elementen uit artikel 11 niet duidelijk voor het BIPT:

- Wat moet worden verstaan onder “de accreditatiecriteria, zowel wat de operationaliteit van het toegepaste managementsysteem als wat de specifieke technische aspecten vermeld in de betrokken norm ISO/IEC 17021 of ISO/IEC 17065 betreft”? Over welk “toegepast managementsysteem” gaat het en wat wordt bedoeld met “specifieke technische aspecten”? Bestaan er technische aspecten die niet specifiek zijn?
- Wat zijn de “werkingsprocedures van het accreditatiesysteem die van toepassing zijn op de geaccrediteerde instellingen”? Op basis waarvan zijn ze van toepassing?

24. Het BIPT stelt vast dat het verslag aan de Koning geen antwoord biedt op deze verschillende vragen.

25. Het BIPT raadt aan om BELAC erbij te betrekken voor de duidelijkheid van de tekst.

¹¹ Artikel 11 van het ontwerp van koninklijk besluit beoogt “de nationale accreditatie-autoriteit” (l’*autorité d’accréditation nationale*) maar volgens artikel 6, 7° van de NIS-wet gaat het om de nationale accreditatieautoriteit (l’*autorité nationale d’accréditation*).

4. Bijlage

26. Als bijlage is het ontwerp van koninklijk besluit opgenomen waarvoor het advies wordt verstrekt.

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