Belgisch Instituut voor
postdiensten en telecommunicatie

Besluit van de Raad van het BIPT van 23/08/2022 betreffende het niet nemen door Telenet van de gepaste veiligheidsmaatregelen voor zijn site in [vertrouwelijk]

Publieke versie

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipsgebouw C | Koning Albert II-laan 35 bus 1 | 1030 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

1. Doel

1. Aan Telenet wordt verweten dat het niet de gepaste veiligheidsmaatregelen heeft genomen zoals ervan vereist wordt door artikel 107/2 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna: "telecomwet") voor zijn site in [vertrouwelijk] (hierna: "site in [vertrouwelijk]"). Zo is Telenet er in het bijzonder niet in geslaagd om:

   1.1. Deze site te beschermen tegen storm Eunice op 18 februari 2022;

   1.2. De fysieke toegang tot deze site te beveiligen, zoals werd vastgesteld tijdens een bezoek van twee personeelsleden van het BIPT aan deze site op 21 februari 2022.

2. Het BIPT gelast Telenet:

   2.1. de fysieke beveiliging van de toegang tot deze site te versterken, voor zover dit nog niet is gebeurd;

   2.2. het BIPT binnen 15 dagen na dit besluit te informeren over de planning van de reconstructiewerkzaamheden van de site van [vertrouwelijk], met details over de geplande werkzaamheden en termijnen.

3. Het BIPT legt een boete op aan Telenet van € 190.000€.

2. Wettelijk kader

2.1. De telecomwet

4. Artikel 2, 62/2°, van de telecomwet definieert "beveiliging van netwerken en diensten" als volgt :

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

5. Artikel 6 van de telecomwet luidt als volgt :

   "*Art. 6. Bij de uitvoering van de taken die aan het Instituut krachtens deze wet zijn opgelegd: […] 4° bevordert het Instituut de belangen van de burgers, […] door de beveiliging van netwerken en diensten te handhaven*;".

6. De verplichtingen van operatoren betreffende de beveiliging van netwerken en diensten bevinden zich in artikel 107/2 (veiligheidsmaatregelen) en 107/3 (notificatie van incidenten en dreigingen) van de telecomwet. Artikel 107/2, § 1, bepaalt het volgende :

"§ 1. De operatoren analyseren de risico's voor de veiligheid van hun netwerken en diensten. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.
De operatoren nemen de passende en evenredige technische en organisatorische maatregelen, waaronder in voorkomend geval versleuteling, om deze risico's goed te beheersen, alsook om de impact van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden.
Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen.
De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan de in het tweede lid bedoelde maatregelen preciseren, wanneer het in dat lid bedoelde risico voortvloeit uit de organisatie van de operatoren.
Onder voorbehoud van het vierde lid en na advies van het Instituut kan de Koning de maatregelen verduidelijken waarvan sprake in het tweede lid."

7. Artikel 107/4 van de telecomwet bevat bevoegdheden van het BIPT om de beveiliging van netwerken en diensten te handhaven en onder andere de volgende bepalingen:

"*Art. 107/4. § 1. Met het oog op de uitvoering van de artikelen 107/2, 107/3 en van dit artikel kan het Instituut een operator bindende instructies geven, onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies. […]*

§ 2. De operator verschaft het Instituut, op zijn verzoek, alle informatie die nodig is om de veiligheid van zijn netwerken en diensten te beoordelen, met inbegrip van gedocumenteerde beveiligingsmaatregelen. Het Instituut kan de in acht te nemen nadere bepalingen voor de verstrekking van deze informatie vastleggen.

Op verzoek van het Instituut onderwerpt een operator zich aan een veiligheidscontrole uitgevoerd door het Instituut zelf, door een instantie of deels door het Instituut en deels door die instantie. Het Instituut stelt het voorwerp en de nadere regels van de controle vast, alsook de termijn waarbinnen die controle moet worden uitgevoerd, wanneer deze door een instantie wordt verricht. Wanneer de controle wordt uitgevoerd door het Instituut, kan deze controle inspecties ter plaatse omvatten. […]" (we onderlijnen)

2.2. De BIPT-statuutwet

8. Artikel 14, § 1, 3°, a), van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (hierna: "BIPT-statuutwet") geeft het BIPT de taak op de naleving van de telecomwet toe te zien.

9. Dit besluit wordt genomen op grond van artikel 21 van de BIPT-statuutwet, dat als volgt luidt:

"Art. 21. § 1. Indien de Raad over een reeks aanwijzingen beschikt die zouden kunnen wijzen op een inbreuk van de wetgeving of reglementering waarvan de naleving door het Instituut wordt gecontroleerd of van de besluiten van het Instituut genomen ter uitvoering van die wetgeving of reglementering, deelt hij in voorkomend geval zijn grieven mee aan de betrokkene, alsook de beoogde maatregelen bedoeld in paragraaf 5 die toegepast zullen worden, indien de inbreuk bevestigd wordt. De aldus vastgestelde sancties zijn passend,

doeltreffend, evenredig en ontmoedigend.

§ 2. De Raad stelt de termijn vast waarover de betrokkene beschikt om het dossier te raadplegen en zijn schriftelijke opmerkingen voor te leggen. Deze termijn mag niet korter zijn dan tien werkdagen.

§ 3. De betrokkene wordt uitgenodigd om te verschijnen op de datum die door de Raad wordt vastgesteld en per aangetekende brief wordt meegedeeld. Hij mag zich laten vertegenwoordigen door de raadsman van zijn keuze.

§ 4. De Raad kan elke persoon horen die een nuttige bijdrage kan leveren tot zijn informatie, hetzij ambtshalve, hetzij op verzoek van de betrokkene.

§ 5. Indien de Raad een inbreuk constateert, kan hij in een of meer besluiten, een of meer van de volgende maatregelen aannemen :

1° het bevel om een einde te maken aan de inbreuk, ofwel onmiddellijk, ofwel binnen een redelijke termijn die hij bepaalt, voor zover nog geen einde werd gemaakt aan deze inbreuk; het Instituut neemt daartoe gepaste en evenredige maatregelen om te garanderen dat deze voorwaarden in acht worden genomen;

1°/1 voorschriften in verband met de manier waarop de inbreuk ongedaan moet worden gemaakt;

2° de betaling binnen de termijn bepaald door de Raad van een administratieve boete die aan de Schatkist toekomt ten bedrage van maximaal 5 000 euro voor natuurlijke personen en van maximaal 5 % van de geconsolideerde omzet van de overtreder, vóór belastingen en exclusief btw, gedurende het jongste volledige boekjaar in de sector voor elektronische communicatie of voor postdiensten in België of, indien de overtreder geen activiteiten ontwikkelt waarmee een omzet wordt behaald, ten bedrage van maximaal 1 000 000 euro voor rechtspersonen. Voor de inbreuken op hoofdstuk 2 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedraagt de administratieve boete maximaal 5 % van de geconsolideerde omzet die de overtreder, vóór belastingen en exclusief btw, gedurende het jongste volledige boekjaar in de sector in kwestie heeft behaald, beperkt tot 125 000 euro;

2° /1 teneinde een of meer van zijn besluiten te doen naleven, de betaling binnen de termijn bepaald door de Raad van een dwangsom die aan de Schatkist toekomt ten bedrage van maximaal 500 euro per dag vertraging voor natuurlijke personen en van 5 % van de dagomzet per dag vertraging euro voor rechtspersonen. De dwangsom is verschuldigd vanaf de datum vastgesteld door de Raad in zijn besluit;

3° het bevel om de levering van een dienst of dienstenpakket die bij voortzetting zou leiden tot een aanzienlijke verstoring van de mededinging, te staken of op te schorten zolang de toegangsverplichtingen die na een marktanalyse uitgevoerd overeenkomstig de wet van 13 juni 2005 betreffende de elektronische communicatie zijn opgelegd, niet worden nageleefd op de wijze bepaald door de Raad of in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad.

De dagomzet bedoeld in het eerste lid, 2° /1, is de totale geconsolideerde jaaromzet vóór belastingen en exclusief btw, behaald in België, in de sector voor elektronische communicatie of voor postdiensten gedurende het jongste volledige boekjaar gedeeld door 365.

Bij gebrek aan gegevens over de in het eerste lid, 2° en 2° /1, bedoelde omzet, kan het Instituut een omzet bepalen op basis van gegevens verkregen van derden of op basis van de omzet van een vergelijkbare persoon.

§ 5/1. De in paragraaf 5, eerste lid, 2° en 2/1°, bedoelde boetes en dwangsommen zijn niet fiscaal aftrekbaar.

§ 6. Indien de overeenkomstig paragraaf 5 genomen maatregelen niet hebben geleid tot de stopzetting van de inbreuk, kan de Raad, na het volgen van de procedure bepaald in de paragrafen 1 tot 5, een administratieve boete of een dwangsom opleggen waarvan het bedrag of het percentage maximaal het dubbele is van het bedrag of het percentage vermeld in paragraaf 5, eerste lid, 2° en 2° /1.

§ 7. Indien de maatregelen die overeenkomstig paragraaf 5 worden genomen, de

inbreuk niet hebben kunnen verhelpen en als het gaat om een ernstige of herhaalde inbreuk] kan de Raad bovendien :

1° de toegekende gebruiksrechten, waarvan de voorwaarden niet nageleefd werden, opschorten of intrekken of

2° de volledige of gedeeltelijke opschorting bevelen van de exploitatie van het netwerk of van de levering van de betrokken dienst, alsook van het te koop aanbieden of het gebruik van alle betreffende diensten of producten.

§ 7/1. Het Instituut voorziet enkel in sancties in het kader van de in artikel 49/2 van de wet van 13 juni 2005 betreffende de elektronische communicatie beoogde procedure wanneer een onderneming of een overheid, welbewust of door een ernstige nalatigheid, misleidende, foutieve of onvolledige informatie verstrekt.

Bij de bepaling van het bedrag van de boetes of dwangsommen opgelegd aan een onderneming of aan een overheid met toepassing van het eerste lid houdt het Instituut onder andere rekening met de negatieve impact van het gedrag van de onderneming of overheid op de concurrentie en in het bijzonder of, in tegenstelling tot de oorspronkelijk meegedeelde informatie of bij elke update van deze informatie, de onderneming of overheid ofwel een netwerk heeft uitgerold of een netwerk heeft uitgebreid of geüpgraded, ofwel geen netwerk heeft uitgerold en geen objectieve rechtvaardiging heeft verstrekt voor deze planwijziging.

§ 8. Ieder besluit dat overeenkomstig dit artikel wordt genomen wordt onverwijld aan de betrokkene en aan de minister meegedeeld en bekendgemaakt op de website van het Instituut. De kennisgeving aan de betrokkene gebeurt via aangetekende brief.

Het besluit vermeldt de redelijke termijn waarbinnen de betrokkene aan de opgelegde maatregel of maatregelen dient te voldoen."

2.3. Het belang van de beveiliging van de netwerken en diensten

10. De voormelde bepalingen van de telecomwet en de BIPT-statuutwet tonen aan dat een juridisch kader ingevoerd is om ervoor te zorgen dat de operatoren de gepaste maatregelen treffen om de veiligheid van hun elektronische-communicatienetwerken en -diensten te garanderen. Het is immers essentieel voor de maatschappij in haar geheel om elke verstoring van de werking van die netwerken en van die diensten te vermijden en om te kunnen steunen op betrouwbare netwerken en diensten. Uit de voormelde bepalingen blijkt ook dat het BIPT een specifieke rol moet spelen om deze veiligheid van netwerken en diensten te verzekeren (onderzoek van de incidentmeldingen, bindende instructies, controle, sanctie, enz.).

11. De actie van het BIPT wordt benadrukt in het strategisch plan 2020-2022 van het BIPT:

"4.5 Netwerkveiligheid

Context

De nieuwste technologische ontwikkelingen, bijvoorbeeld 5G, brengen enorme opportuniteiten met zich mee om alles overal en altijd met elkaar in verbinding te brengen. Deze ontwikkelingen hebben enerzijds als gevolg dat de afhankelijkheid van onze samenleving van elektronische communicatie enorm zal toenemen. Anderzijds verhogen ze de complexiteit van de elektronische-communicatienetwerken enorm. De noodzaak om over goed beheerde en veilige elektronische-communicatienetwerken te beschikken neemt dus toe.

Werkzaamheden BIPT

Via zijn dienst Netwerkveiligheid waakt het BIPT over de veiligheid van de openbare elektronische-communicatienetwerken en van de openbare elektronische-communicatiediensten.

Zo werkt het BIPT continu samen met de operatoren om de gepaste veiligheidsmaatregelen te nemen om de beschikbaarheid, vertrouwelijkheid en integriteit van hun netwerken te garanderen. De focus ligt hierbij op de kritieke infrastructuren, de grootste netwerkknooppunten in België. Indien er zich ondanks de aanwezige maatregelen een incident voordoet, dan volgt het BIPT dit op en controleert het of de nodige bijkomende maatregelen genomen werden.

Het BIPT bevordert de samenwerking tussen de operatoren en overheidsdiensten zoals de politiediensten, de veiligheids- en inlichtingendiensten en het Centrum voor Cybersecurity België.

Het BIPT ziet daarnaast ook toe op de bereikbaarheid van nooddiensten en ziet erop toe dat de operatoren de nodige maatregelen nemen om de toegang tot deze diensten te garanderen."

3. Procedure

12. De procedure die gevolgd werd is als volgt:

12.1. Op 4 mei 2022 heeft het BIPT aan Telenet het ontwerp van dit besluit toegestuurd (hierna: "het ontwerpbesluit ");

12.2. In een e-mail van 20 mei 2022 heeft Telenet daarop gereageerd (hierna: "de schriftelijke opmerkingen van Telenet van 20 mei 2022");

12.3. Op 23 mei 2022 is Telenet gehoord door de Raad van het BIPT;

12.4. Op 7 juli 2022 is het ontwerpbesluit voorgelegd aan de mediaregulatoren. Die laatsten hebben het BIPT laten weten dat ze geen opmerkingen hadden op het ontwerpbesluit.

4. Grieven

4.1. Inleiding: belang van de Telenet-site in [vertrouwelijk] voor de werking van zijn netwerk

13. Uit de e-mail van 4 februari 2022 van Telenet aan het BIPT blijkt dat zijn site te [vertrouwelijk] de volgende twee onderdelen omvat:

- de "headend" (HE) [vertrouwelijk]. Headends zijn aggregatiepunten van de coaxnetwerken en glasvezels op lokaal niveau. Volgens de voormelde e-mail van Telenet maar zonder hierbij rekening te houden met een eventuele redundantie, zouden er in geval van onderbreking van de werking van deze headend [vertrouwelijk], en;

- een van de [vertrouwelijk] "switching offices" (SO) van Telenet. Deze "switching offices" aggregeren het vaste en mobiele verkeer van de lokale toegangen (headends) en zorgen voor de connectiviteit naar de datacenters. Volgens de voormelde e-mail van Telenet maar zonder hierbij rekening te houden met een eventuele redundantie, zou er in geval van een slecht functioneren van de switching office in [vertrouwelijk] een impact zijn [vertrouwelijk]. De getroffen zone zou dus [vertrouwelijk].

14. In de onderstaande figuur illustreert de plaats van de switching office van [vertrouwelijk] in de backbone het belang ervan voor de connectiviteit [vertrouwelijk]:

[vertrouwelijk]

15. Op de volgende figuur zijn de secundaire aggregatieringen te zien:

[vertrouwelijk]

16. Deze figuur illustreert ook het belang van de site van [vertrouwelijk]voor [vertrouwelijk]. De site van [vertrouwelijk] zorgt voor de connectiviteit van de ringen die in het schema in het oranje en in het groen aangeduid zijn, met de datacenters.

17. Volgens een e-mail van Telenet van 1 april 2021 zijn er onder de kritieke zakelijke klanten die door de switching office van [vertrouwelijk] worden bediend [vertrouwelijk]. In zijn e-mail van 27 april 2022 heeft Telenet bevestigd dat ook [vertrouwelijk] op de site zijn aangesloten.

18. Naar aanleiding van de brief van het BIPT van 7 april 2022 heeft Telenet in zijn e-mail van 27 april 2022 een schatting gegeven van de klanten die aangesloten zijn op de site van [vertrouwelijk]:

Diensten	**Switching office (SO)**	**Headend (HE) [vertrouwelijk]**
Mobiel	+/- [vertrouwelijk] klanten. Telenet merkt op dat deze klanten niet getroffen zouden zijn bij het uitvallen van de switching office [vertrouwelijk].	+/- [vertrouwelijk] klanten.
Vast	[vertrouwelijk] klanten. Telenet merkt op dat deze klanten niet getroffen zouden zijn bij het uitvallen van de switching office [vertrouwelijk].	[vertrouwelijk] klanten, waarvan [vertrouwelijk] particuliere klanten. De andere klanten zijn wholesale- en B2B-klanten via coax.

19. Het BIPT houdt geen rekening met de veiligheidsmaatregelen, met name de eventuele redundantiemaatregelen, om het belang te bepalen van de site van [vertrouwelijk] voor de verstrekking van de elektronische-communicatiediensten van Telenet. Die veiligheidsmaatregelen zijn immers geen maatstaf voor het belang van die site (maar kunnen het belang ervan weerspiegelen), maar stellen in staat de veiligheidsrisico's van de site te verminderen, wanneer ze correct ingevoerd worden en regelmatig getest worden.

20. Wat de mobiele diensten van Telenet betreft, zijn +/- **[vertrouwelijk]** klanten in 2022 aangesloten op de site van [vertrouwelijk], op een totaal van **[vertrouwelijk]** mobiele klanten van Telenet op 31 December 2021. [Vertrouwelijk] klanten is iets meer is dan [vertrouwelijk] van de klanten van de mobiele diensten van Telenet in 2021 (een [vertrouwelijk] is [vertrouwelijk]).

21. Wat de vaste diensten van Telenet betreft, zijn in 2022 **[vertrouwelijk]** klanten aangesloten op de site van [vertrouwelijk], op een totaal van **[vertrouwelijk]** breedband klanten van Telenet op 31 December 2021. **[Vertrouwelijk]** klanten is iets minder dan een [vertrouwelijk] van de klanten van de breedband diensten van Telenet in 2021 (een [vertrouwelijk] is [vertrouwelijk]; dit getal is afgerond).

22. [Vertrouwelijk]. De elektronische-communicatiediensten die via deze site door Telenet worden aangeboden, werden niet getroffen maar de risico's van onbeschikbaarheid van de diensten waren hoog en Telenet diende in te grijpen om de functionaliteiten te migreren of te zorgen voor redundantie.

23. Na dat incident is de site in [vertrouwelijk] met een grote tent overdekt ter bescherming tegen weer en wind. De kwetsbaarheid van de site is daardoor enorm toegenomen, want een tent houdt meer veiligheidsrisico's in dan een gebouw of een container.

24. In haar schriftelijke opmerkingen van 20 mei 2022 legt Telenet uit "*dat voorafgaand aan de storm* [Eunice van 18 februari 2022]*, alle actieve apparatuur reeds afgeschakeld was in het beschadigde gedeelte van het [vertrouwelijk] gebouw, er zijn dus geen actieve diensten meer in het beschadigde gedeelte.*"

25. Uit de hoorzitting van Telenet en uit de work breakdown van Telenet (bijlage bij stuk 1) begrijpt het BIPT dat er actieve apparatuur was verplaatst naar het niet beschadigde deel van het gebouw en dat bepaalde diensten werden gemigreerd naar containers op de site.

26. In haar schriftelijke opmerkingen van 20 mei 2022 legt Telenet het volgende uit : "*Telenet heeft de massieve inspanningen (in totaal ongeveer 3000 externe en interne manuren) geleverd om te zorgen voor redundantie van de [vertrouwelijk]site [vertrouwelijk] . Telenet heeft onmiddellijk na [vertrouwelijk – het incident] ingegrepen. [Vertrouwelijk] waren alle kritische diensten dermate ontdubbelt dat bij verder [vertrouwelijk – incident] deze essentiële diensten zouden blijven functioneren. [Vertrouwelijk] was dat reeds het geval voor meer dan 80% van de kritische diensten.*"

27. Uit de hoorzitting blijkt dat redundantie voor de switching office altijd is voorzien: voorheen site-redundant (van alles twee exemplaren op eenzelfde site), maar sinds het incident in [vertrouwelijk] is georedundantie uitgevoerd (van alles nog een tweede exemplaar op een andere site, in casu op de site van de switching office van [vertrouwelijk]).

28. Volgens het BIPT moet het argument van Telenet, dat het "massieve inspanningen" zou geleverd hebben, gerelativeerd worden. De redundantie op de site (site-rendundant) die op de site van [vertrouwelijk] voor het incident [vertrouwelijk] ingevoerd was, was immers ontoereikend in vergelijking met de goede praktijken inzake de netwerkarchitectuur voor de backbone van het netwerk. Een incident zou een impact gehad kunnen hebben op de volledige site van [vertrouwelijk], zodat de redundantie op de site niet zou functioneren.

De inspanningen die door Telenet geleverd zijn om een georedundantie in te voeren, waren dus in elk geval noodzakelijk.

4.2. Eerste grief: risico dat de tent over de site van [vertrouwelijk] wegvliegt tijdens de storm Eunice op 18 februari 2022

29. Op 17 februari 2022 heeft het BIPT naar Telenet een e-mail gestuurd met de vraag om rekening te houden met de bijzondere situatie van de site van [vertrouwelijk], aangezien er voor 18 februari 2022 slechte weersomstandigheden (storm Eunice) waren aangekondigd.

30. De ochtend van 18 februari 2022 (om 9.25 uur) heeft Telenet per e-mail het volgende antwoord naar het BIPT gestuurd:

"We hebben gisteren nog een externe firma laten komen om de tent te onderwerpen aan een extra controle en deze controle was in orde.

Voor het overige voert de bewaking een permanente controle uit om de toestand van dichtbij te monitoren.

Alles is wat ons betreft onder controle."

31. Dezelfde dag, 18 februari 2022, maar in de namiddag (om 15.28 uur), in volle storm, neemt Telenet contact op met het BIPT, zonder via de wachtdienst voor netwerkveiligheid van het BIPT te gaan (24/7 bereikbaar), met de uitleg dat er dreigend gevaar is dat de tent zal wegvliegen en dat de hulp van de brandweer vereist is.

32. Het BIPT heeft dat verzoek doorgegeven aan het Crisiscentrum van de regering en de brandweer werd prioritair ter plaatse gestuurd binnen 45 minuten. Bij de interventie van de brandweer zijn de dekzeilen aan de voor- en achterkant van de tent weggenomen, om de winddruk te verminderen. De neerslag binnen de site is gelukkig beperkt geweest.

33. Aan Telenet wordt verweten dat het geen correcte analyse heeft gemaakt van het risico dat de tent zou wegvliegen (Telenet heeft zich gebaseerd op één enkele onderaannemer die een verkeerde schatting heeft gemaakt) en dat het niet de nodige voorzorgsmaatregelen heeft getroffen om dat risico te voorkomen, zoals geëist wordt door de paragrafen 1 en 3 van artikel 107/2 van de telecomwet:

"§1. De operatoren analyseren de risico's voor de veiligheid van hun netwerken en diensten. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.
De operatoren nemen de passende en evenredige technische en organisatorische maatregelen, waaronder in voorkomend geval versleuteling, om deze risico's goed te beheersen, alsook om de impact van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden.
Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen.
De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan de in het tweede lid bedoelde maatregelen preciseren, wanneer het in dat lid bedoelde risico voortvloeit uit de organisatie van de operatoren.

Onder voorbehoud van het vierde lid en na advies van het Instituut kan de Koning de maatregelen verduidelijken waarvan sprake in het tweede lid." (eigen onderlijning)

"§ 3. De operatoren nemen alle noodzakelijke maatregelen, inclusief preventieve, om de beschikbaarheid van de spraakcommunicatiediensten en van de internettoegangsdiensten zo volledig mogelijk te waarborgen in geval van uitzonderlijke netwerkuitval of in geval van overmacht.

De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan deze maatregelen preciseren wanneer het risico voor uitval of van overmacht voortvloeit uit de organisatie van de operatoren.

Onverminderd het tweede lid kan de Koning na advies van het Instituut deze maatregelen verduidelijken." (eigen onderlijning)

34. In haar schriftelijke opmerkingen van 20 mei 2022 heeft Telenet het volgende uitgelegd : "*Telenet heeft op 16 februari 2022 preventief en proactief een professionele tentenfirma (vertrouwelijk) on site laten komen om de tent te controleren en waar nodig extra te beveiligen, gelet op het aangekondigde stormweer.*"

35. Die bewering (tussenkomst van [vertrouwelijk] op 16 februari 2022) is echter niet in lijn met de voormelde e-mail van Telenet aan het BIPT op 18 februari 2022, waarin stond dat die tussenkomst op 17 februari 2022 had plaatsgevonden.

36. Volgens Telenet was er op geen enkel ogenblik een risico op het vlak van de dienstverlening naar de eindgebruikers. Alle actieve apparatuur in het beschadigde gedeelte van het gebouw was al afgeschakeld voorafgaand aan de stormen in februari. Er waren geen actieve noch passieve diensten meer in het beschadigde gedeelte. Door deze maatregelen zou er zelfs bij het volledig wegvliegen van de tent geen enkele impact kunnen geweest zijn op de veiligheid van de netwerken en de dienstverlening. De tussenkomst van de brandweer was enkel nodig omdat er een mogelijk risico bestond dat de tent schade had kunnen veroorzaken aan passanten en omwonenden.

37. In tegenstelling tot wat Telenet beweert, is het niet zeker dat de tent, mocht die door de storm weggevlogen zijn, de werking van de netwerken en de elektronische-communicatiediensten van Telenet niet beïnvloed zou hebben.

38. Gezien het gewicht en de afmetingen van de tent en het feit dat ze het volledige gebouw bedekt (en dus ook de delen van het gebouw die niet beschadigd zijn en die actieve elementen beschutten), zou ze immers, bij het wegvliegen, het gebouw, de schoorsteenkanalen of de airconditioning kunnen beschadigen, wat de verstrekking van netwerken of elektronische-communicatiediensten van Telenet zou kunnen beïnvloed hebben. Het is moeilijk denkbaar dat de tent "verticaal" wegvliegt zonder het gebouw, de schoorsteenkanalen of de airconditioning te raken om dan buiten de site van Telenet neer te vallen. Daarentegen kan redelijkerwijs ingeschat worden, dat de tent bij het wegvliegen, het gebouw, zijn schoorsteenkanalen of airconditioning zou geraakt hebben en schade op de site zelf zou hebben aangericht.

39. Krachtens artikel 107/2, § 1, van de telecom wet moeten de operatoren de passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de veiligheid van hun netwerken en diensten goed te beheersen. Artikel 107/2 beoogt dus de risico's voor de veiligheid van de netwerken en diensten. Welnu, het risico bestond dat het

wegvliegen van de tent de verstrekking van netwerken of elektronische-communicatiediensten van Telenet zou beïnvloeden.

40. Als voor de vaststelling van de grief een incident (het daadwerkelijke wegvliegen van de tent) vereist is dat een reële impact heeft gehad op de werking van het netwerk of de dienst, zou dat betekenen dat het BIPT zijn controletaak krachtens voormeld artikel 107/2 niet ten volle zou kunnen uitoefenen.

41. Samengevat is het BIPT van mening dat de eerste grief (het feit dat er niet op tijd maatregelen zijn genomen om het wegvliegen van de tent te voorkomen) is vastgesteld, en dat Telenet artikel 107/2, § 1, van de telecomwet niet heeft nageleefd:

"§1. De operatoren analyseren de risico's voor de veiligheid van hun netwerken en diensten. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.
De operatoren nemen de passende en evenredige technische en organisatorische maatregelen, waaronder in voorkomend geval versleuteling, om deze risico's goed te beheersen, alsook om de impact van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden.
Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen.
De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan de in het tweede lid bedoelde maatregelen preciseren, wanneer het in dat lid bedoelde risico voortvloeit uit de organisatie van de operatoren.
Onder voorbehoud van het vierde lid en na advies van het Instituut kan de Koning de maatregelen verduidelijken waarvan sprake in het tweede lid."

4.3. Tweede grief: onvoldoende maatregelen voor fysieke beveiliging van de toegang tot de site van [vertrouwelijk]

4.3.1. Inleiding

42. Na een verzoek van het Crisiscentrum van de regering om verslag uit te brengen en gelet op het belang van de site van [vertrouwelijk] voor de werking van het netwerk van Telenet, heeft het BIPT het volgende aan Telenet gevraagd:

Voorwerp van de aanvraag	Uitwisselingen tussen het BIPT en Telenet
- Een beschrijving van de rampenmaatregelen die Telenet genomen heeft [vertrouwelijk];	Het BIPT heeft zijn verschillende vragen via verschillende e-mails [vertrouwelijk] gesteld en Telenet heeft daarop dezelfde maand geantwoord.
- Een analyse van de potentiële impact van het totale verlies van het gebouw ([vertrouwelijk] en op datum van 1	Het BIPT heeft die vraag gesteld in een mail van 1 februari 2022 en Telenet heeft daarop geantwoord in zijn e-mail van 4 februari 2022.

februari 2022, met de ingestelde redundantie);	
- De site van [vertrouwelijk] mogen bezoeken;	Het BIPT heeft die vraag aan Telenet gericht via een mail van 16 februari 2022 en latere mails. Telenet heeft voorgesteld om dat bezoek op 20 april 2022 te laten plaatsvinden, waarbij uit te voeren werkzaamheden werden geopperd.
- Een overzicht te geven van de fysieke beveiligingsmaatregelen bij de site van [vertrouwelijk] en aan het BIPT enkele foto's hiervan te bezorgen.	Het BIPT heeft deze vraag gesteld in een e-mail van 17 februari 2022. Telenet heeft daarop geantwoord met zijn mail van 21 februari 2022, om 15.51 uur (zonder foto's te verstrekken).

43. Wegens het uitblijven van een antwoord van Telenet voor 21 februari 2022 met betrekking tot de maatregelen inzake fysieke beveiliging van de site van [vertrouwelijk], het risico dat de tent op 18 februari 2022 weg had kunnen vliegen en de interventie van de brandweer (zie sectie 4.2) zijn twee leden van de dienst Netwerkveiligheid van het BIPT op 21 februari 2022 's morgens ter plaatse gegaan, op de site van [vertrouwelijk], om de toestand te evalueren.

44. In haar schriftelijke opmerkingen van 20 mei 2022 beweert Telenet dat het niet redelijk is "*dat het BIPT eerst de indruk geeft te willen wachten tot midden april met een plaatsbezoek, vervolgens op 21 februari 2022 een overzicht krijgt van Telenet van de fysieke beveiligingsmaatregelen om daarna in paragraaf [433] te concluderen dat een onmiddellijk plaatsbezoek vereist was "wegens het uitblijven van een antwoord van Telenet"*".

45. Het is waar dat Telenet een bezoek op 20 april 2022 heeft voorgesteld, maar het BIPT heeft het bezoek vervroegd gezien de in paragraaf 433 voormelde feiten en omdat Telenet een datum heeft voorgesteld die meer dan anderhalve maand later is dan de data die werden voorgesteld door het BIPT. Op het moment van het bezoek had het BIPT nog steeds geen antwoord van Telenet gekregen met betrekking tot de maatregelen inzake fysieke beveiliging van de site van [vertrouwelijk].

46. Bovendien verhindert niets het BIPT om onaangekondigde controles uit te voeren bij de operatoren. Het onaangekondigde bezoek in [vertrouwelijk] heeft ook zijn nut bewezen daar het aan het licht heeft gebracht dat de fysieke toegang tot de site niet in orde was.

47. Die controle berust op de volgende twee wettelijke grondslagen:

    47.1. Zoals al uitgelegd geeft artikel 14, §1, 3°, a), van de BIPT-statuutwet het BIPT de taak op de naleving van de telecom wet toe te zien;

47.2. Artikel 107/4, § 2, lid 2, van de telecomwet luidt als volgt :

"*Op verzoek van het Instituut onderwerpt een operator zich aan een veiligheidscontrole uitgevoerd door het Instituut zelf, door een instantie of deels door het Instituut en deels door die instantie. Het Instituut stelt het voorwerp en de nadere regels van de controle vast, alsook de termijn waarbinnen die controle moet worden uitgevoerd, wanneer deze door een instantie wordt verricht. Wanneer de controle wordt uitgevoerd door het Instituut, kan deze controle inspecties ter plaatse omvatten.*"

4.3.2. De rol van [vertrouwelijk]

48. Ter plaatse hebben de twee leden van de dienst Netwerkveiligheid van het BIPT vastgesteld dat de site beveiligd werd door [vertrouwelijk](24/7), maar :

48.1. [vertrouwelijk]

48.2. [vertrouwelijk]

48.3. [vertrouwelijk]

49. In haar schriftelijke opmerkingen van 20 mei 2022 schrijft Telenet het volgende :

> "*- De bewakingsagent ter plaatse heeft de afgesproken procedure (zie bijlage 1: toegangscontrole [vertrouwelijk]) niet toegepast door de identiteit van de BIPT-inspecteurs niet te controleren. Dit valt o.a. te verklaren doordat de [vertrouwelijk] site vlak voor het bezoek van het BIPT nog frequent bezocht werd door externe bezoekers in het kader van de gerechtelijke expertise [vertrouwelijk] waarbij heel wat advocaten en verzekeringsexperts de site hebben bezochten. De bewakingsagent ter plaatse heeft wellicht verkeerdelijk uitgegaan dat de BIPT-inspecteurs de site bezochten in het kader van de gerechtelijke expertise. In ieder geval, had de bewakingsagent ter plaatse de identiteit van de BIPT-inspecteurs moeten controleren. Telenet heeft haar onderaannemer [vertrouwelijk] ter verantwoording geroepen en heeft recent herhaald dat de identiteit van externe bezoekers steeds moet gecontroleerd worden (zie bijlage 2: mail van 11 mei 2022 van Telenet aan [vertrouwelijk]).*
>
> *- Gelet op de ruime wettelijke bevoegdheden van het BIPT, vraagt Telenet de nodige richtlijnen te krijgen van het BIPT en te verduidelijken of de BIPT-inspecteurs de sites van Telenet mogen betreden zonder begeleiding door Telenet. De ingebrekestelling insinueert dat het BIPT verwacht dat een bezoek van de site enkel mogelijk is met begeleiding door Telenet.*"

50. Het BIPT betwist niet dat Telenet met [vertrouwelijk] een procedure heeft afgesproken. Die procedure werd echter niet toegepast bij het bezoek van de personeelsleden van het BIPT (en potentieel ook niet voor de advocaten, verzekeringsexperts en firma's die zich bij de bewakingsagent hebben aangemeld). Aan Telenet wordt verweten dat ze zich niet heeft vergewist dat die procedure effectief werd toegepast. Dat was des te belangrijker gezien het grote aantal bezoekers aan de site ten gevolge van de gerechtelijke expertises en de afbraakwerken die er plaatsvonden.

51. Het BIPT verwacht niet dat zijn bezoek van de site enkel mogelijk is met begeleiding door Telenet of door een bewakingsagent van [vertrouwelijk], maar de potentiële negatieve gevolgen van een gebrekkige identificatie van een bezoeker zijn nog groter indien die bezoeker niet wordt begeleid tijdens zijn bezoek.

52. Tijdens hun bezoek waren de personeelsleden van het BIPT in staat om het niet-beschadigde gedeelte van het gebouw te betreden (via een openstaande deur onder de tentstructuur).

4.3.3. De toegang tot de site, de camera's en de alarmen

53. Tijdens hun bezoek hebben de personeelsleden van het BIPT het volgende vastgesteld :

53.1. [vertrouwelijk];

53.2. [vertrouwelijk].

54. In haar schriftelijk opmerkingen van 20 mei 2022 heeft Telenet het volgende beantwoord:

- "*Telenet heeft de ingebrekestelling van het BIPT niet afgewacht om bijkomende maatregelen te nemen om de fysieke veiligheid van de [vertrouwelijk]site te verbeteren. Zo was Telenet al bezig met de installatie van bijkomende camera's (voorziene installatie in de loop van mei 2022) om het zicht op de site opnieuw te vervolledigen, met inbegrip van een zicht op de achterkant van de site. Een deel van de camera's bevonden zich voor [vertrouwelijk – het incident] immers in het beschadigde gedeelte van de site alsook aan de [vertrouwelijk] buitenmuur*";
- "*Om de veiligheid van de site nog te optimaliseren, had Telenet ook voor de ingebrekestelling van het BIPT al opdracht gegeven om een nieuwe inbraakcentrale en inbraakalarmsysteem te installeren (voorzien in mei 2022). Door deze bijkomende beveiligingsmaatregelen [vertrouwelijk]. Vanaf dit moment, zal de toegang tot de [vertrouwelijk] site, net zoals de meeste andere kritieke infrastructuur van Telenet, enkel nog volgens de algemeen toegepaste protocollen gevalideerd worden.* "

55. Tijdens de hoorzitting heeft Telenet het volgende toegevoegd: camera's kunnen uiteraard alleen worden opgehangen na afbraak van de site en dus moest Telenet wachten op het concretiseren van de planning voor de heropbouw en de effectieve heropbouw zelf vooraleer nieuwe camera's en een alarm te laten installeren.

56. Het BIPT noteert dat Telenet de volgende ontwerpplanning van de reconstructiemaatregelen heeft meegedeeld in haar schriftelijke opmerkingen van 20 mei 2022 (onder voorbehoud van o.a. de beschikbaarheid van de nodige resources en het verkrijgen van de noodzakelijke vergunningen):

56.1. [vertrouwelijk]

56.2. [vertrouwelijk]

56.3. [vertrouwelijk]

56.4. [vertrouwelijk]

56.5. [vertrouwelijk]

56.6. [vertrouwelijk]

57. Het BIPT vindt het niet onaanvaardbaar dat er nog geen camera werd geïnstalleerd, gezien het zo'n lange periode betreft [vertrouwelijk].

4.3.4. De airconditioninginfrastructuur

58. Ter plaatse hebben de twee leden van de dienst Netwerkveiligheid van het BIPT vastgesteld dat de airconditioninginfrastructuur zich aan de buitenkant in een naburige weide bevond en vrij toegankelijk was.

59. Het antwoord van Telenet in haar schriftelijke opmerkingen van 20 mei 2022 is als volgt : "*Op het moment van de inspectie bevond de airconditioninginfrastructuur zich inderdaad buiten de perimeter van de site om plaats vrij te maken voor de afbraak in het beschadigde gedeelte van de site. Ondertussen heeft Telenet al de nodige maatregelen getroffen om de airco's terug te verplaatsen en die bevinden zich nu binnen de perimeter van de site (zie onderstaande foto).*"

60. Tijdens de hoorzitting heeft Telenet aangegeven dat de airconditioning niet nodig was voor de koeling van het onder de tent geplaatste gedeelte maar dat die airconditioning kon ingezet worden voor extra koelingscapaciteit in de switching office van [vertrouwelijk] indien nodig (indien de switching office in de zomer te hoge temperaturen bereikt).

61. Het BIPT meent dat als een airconditioning in het begin nodig was voor de goede werking van de site, dat die ook nodig is na de verplaatsing van de actieve elementen van het beschadigde gedeelte van het gebouw naar andere delen van de site en met des te meer reden aangezien de verplaatsing van die actieve elementen meer materiaal in eenzelfde ruimte impliceert. In elk geval kan niet worden uitgesloten dat die airconditioning op een gegeven moment noodzakelijk had kunnen zijn voor de goede werking van de site (bijvoorbeeld ten gevolge van een hoge buitentemperatuur of ten gevolge van de concentratie van apparatuur in een lokaal na de verplaatsing van actieve elementen).

62. De uitleg van Telenet neemt niet weg dat de airconditioning in de periode dat deze koeling zich buiten de beveiligde perimeter bevond vrij toegankelijk was en dus vatbaar voor schadelijke manipulatie door een voorbijganger. Deze schadelijke manipulatie had een weerslag kunnen hebben op de veiligheid van de netwerken en de dienstverlening.

4.3.5. Conclusie

63. De tweede grief wordt aangenomen. Telenet heeft niet voldoende veiligheidsmaatregelen getroffen aangaande de fysieke toegang tot de site, zoals geëist werd door artikel 107/2, paragraaf 1, van de telecomwet:

"§1. De operatoren analyseren de risico's voor de veiligheid van hun netwerken en diensten. Het Instituut kan de nadere regels van deze risicoanalyse vaststellen.
De operatoren nemen de passende en evenredige technische en organisatorische maatregelen, waaronder in voorkomend geval versleuteling, om deze risico's goed te beheersen, alsook om de impact van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden.
Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen.
De Koning, op voorstel van het Instituut of op eigen initiatief, na advies van het Instituut, kan de in het tweede lid bedoelde maatregelen preciseren, wanneer het in dat lid bedoelde risico voortvloeit uit de organisatie van de operatoren.
Onder voorbehoud van het vierde lid en na advies van het Instituut kan de Koning de maatregelen verduidelijken waarvan sprake in het tweede lid."

5. Door Telenet te nemen maatregelen om de fysieke toegang tot de site van [vertrouwelijk] te beveiligen

64. Gelet op de tweede grief die gericht is aan Telenet (punt 4.3. Onvoldoende maatregelen voor fysieke beveiliging van de toegang tot de site van [vertrouwelijk]) en voor zover dat ondertussen nog niet is gedaan, gelast het BIPT Telenet om onmiddellijk de adequate en evenredige maatregelen van technische en organisatorische aard bedoeld in artikel 107/2, § 1, van de telecomwet, te treffen teneinde de fysieke toegang tot zijn site in [vertrouwelijk] te beveiligen, met name: [vertrouwelijk].

65. Deze instructies berusten op het volgende:

65.1. Art. 21, § 5, van de BIPT-statuutwet: *"Indien de Raad een inbreuk constateert, kan hij in een of meer besluiten, een of meer van de volgende maatregelen aannemen :*
1° het bevel om een einde te maken aan de inbreuk, ofwel onmiddellijk, ofwel binnen een redelijke termijn die hij bepaalt, voor zover nog geen einde werd gemaakt aan deze inbreuk; het Instituut neemt daartoe gepaste en evenredige maatregelen om te garanderen dat deze voorwaarden in acht worden genomen;
1°/1 voorschriften in verband met de manier waarop de inbreuk ongedaan moet worden gemaakt;"

65.2. Art.107/4 van de telecomwet : "*§ 1. Met het oog op de uitvoering van de artikelen 107/2, 107/3 en van dit artikel kan het Instituut een operator bindende instructies geven, onder meer de maatregelen die nodig zijn om een beveiligingsincident op te lossen of te voorkomen wanneer een significante dreiging is vastgesteld, alsook het tijdschema voor de uitvoering van die instructies.*";

66. Het BIPT zal nieuwe controles verrichten op deze site om na te gaan of deze maatregelen genomen zijn.

67. Bovendien gelast het BIPT Telenet om binnen 15 dagen na dit besluit de planning van de reconstructiewerkzaamheden van de site van [vertrouwelijk] aan het BIPT mee te delen, met details over de geplande werkzaamheden en termijnen.

68. Het feit dat de site van [vertrouwelijk] ondergebracht is in een tent schept immers meer veiligheidsrisico's dan als die site zich in een gebouw zou bevinden. Dat risico moet zoveel mogelijk worden beperkt.

69. Dit verzoek om inlichtingen is gebaseerd op de volgende bepalingen:

69.1. artikel 107/4, § 2, van de telecomwet: « *§ 2. De operator verschaft het Instituut, op zijn verzoek, alle informatie die nodig is om de veiligheid van zijn netwerken en diensten te beoordelen, met inbegrip van gedocumenteerde beveiligingsmaatregelen. Het Instituut kan de in acht te nemen nadere bepalingen voor de verstrekking van deze informatie vastleggen.*";

69.2. artikel 14, § 2, 2°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector dat voorschrijft: *"In het kader van zijn bevoegdheden : (…) 2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld.*"

6. Opleggen van een administratieve boete

6.1. Noodzaak om een boete op te leggen

70. Het BIPT is van oordeel dat het opleggen van een administratieve boete aan Telenet gerechtvaardigd is, gelet op zowel de grieven als de (mogelijke) impact van een incident op de site van [vertrouwelijk] op de goede werking van zijn netwerk en bijgevolg op de belangen van de eindgebruikers (zie afdeling 4.1).

71. De afwezigheid van een boete zou het signaal geven dat de telecomwet zomaar overtreden kan worden zonder dat de operator hiervoor gestraft wordt. Het is onaanvaardbaar, dat een operator de telecomwet overtreedt en vervolgens aan elke sanctie ontsnapt, zodra hij de nodige maatregelen neemt nadat het BIPT hem heeft gewezen op die overtreding.

6.2. Principes voor de berekening van het bedrag van de boete

72. Artikel 21, § 1, van de BIPT-statuutwet stelt het volgende : "*De aldus vastgestelde sancties zijn passend, doeltreffend, evenredig en ontmoedigend.*"

73. Daarnaast legt de BIPT-statuutwet enkel de plafonds vast voor het bedrag van de boetes, maar verduidelijkt niet de werkwijze die het BIPT moet hanteren om die boetes te berekenen. Onder die plafonds, hangt de bepaling van het bedrag van de boete dan ook af van de discretionaire bevoegdheid van het BIPT.

74. De hoogte van de boete wordt bepaald aan de hand van de richtsnoeren die het BIPT hiervoor heeft opgesteld in zijn mededeling van 31 maart 2020 betreffende richtsnoeren voor de berekening van het bedrag van de administratieve boetes die door het BIPT worden opgelegd (hierna: "Boete Richtsnoeren").

75. De boetes zijn enerzijds bedoeld om een gepaste reactie te geven op het niet-naleven van reglementering en anderzijds om een ontradend effect te hebben. Het gaat hier niet om de vergoeding van slachtoffer voor het onregelmatige gedrag. Het afschrikkingseffect is tweeledig: het is zaak om de overtreder aan te moedigen om de overtreding niet meer te plegen (specifiek afschrikkingseffect) en om derden aan te zetten om de overtreding (of een gelijkaardige overtreding) niet te plegen (algemeen afschrikkingseffect).

76. Krachtens het evenredigheidsbeginsel moet het bedrag van de boete voldoende hoog zijn om de nagestreefde doelstellingen te verwezenlijken zonder verder te gaan dan wat nodig is om deze doelstellingen te halen.

77. Het maximumbedrag van de boete is "maximaal 5 % van de omzet van de overtreder gedurende het jongste volledige boekjaar in de sector voor elektronische communicatie of voor postdiensten in België" (krachtens artikel 21, § 5, 2°, van de BIPT-statuutwet). Het meest recente volledige boekjaar dat voor het BIPT bekend is, is boekjaar 2021.

78. Het bedrag van de boete dat in het onderhavige geval in aanmerking wordt genomen, ligt ver onder dat maximumbedrag.

79. Het BIPT detailleert in de volgende paragrafen de elementen waarmee het rekening heeft gehouden voor de berekening van het bedrag van de boete.

6.3. Berekening van het basisbedrag

6.3.1. Relevante omzet

80. De eerste fase bij de berekening van het basisboetebedrag bestaat er in het omzetcijfer van de overtreder te bepalen. Het BIPT acht het gepast om rekening te houden met de jaarlijkse omzet die de overtreder verwezenlijkt op de markt waarop de overtreding werd begaan en, desgevallend, op de markt(en) waarop de gevolgen van de overtreding zich laten voelen ("relevante omzet").

81. Telenet biedt via de site [vertrouwelijk] "alle" diensten aan:

- mobiele en vaste data; en
- mobiele en vaste telefonie.

82. Daarom houdt het BIPT rekening met de omzet die Telenet in 2021 heeft behaald voor zijn verschillende diensten, namelijk € [vertrouwelijk]:

Voorwerp	
Total net retail revenues of which revenues related to telecommunication	[vertrouwelijk]
Total wholesale revenues	[vertrouwelijk]
Total	[vertrouwelijk]

83. De "switching office" in [vertrouwelijk] is een van de maar [vertrouwelijk] "switching offices" die Telenet heeft. Daarom houdt het BIPT rekening met een [vertrouwelijk] van de voormelde omzet, namelijk € [vertrouwelijk] (afgerond naar [vertrouwelijk]).

84. Het BIPT houdt rekening met de omzet van Telenet gedurende een jaar om de volgende redenen. De tent is op de site van [vertrouwelijk] geïnstalleerd nadat een deel van de infrastructuur op die site [vertrouwelijk]. De inspectie door de twee personeelsleden van het BIPT op deze site had plaats op 21 februari 2022, wat iets minder dan [vertrouwelijk].

85. Telenet heeft in de maand mei 2022 ([vertrouwelijk]) bepaalde acties ondernomen om het niveau van beveiliging van de fysieke toegang tot de site te verhogen:

85.1. E-mail van 11 mei 2022 naar [vertrouwelijk] waarbij opnieuw herinnerd wordt aan het overeengekomen protocol inzake toegangscontrole tot de site van [vertrouwelijk];

85.2. concrete planning van het installeren van bijkomende camera's, van een nieuwe inbraakcentrale en van een inbraakalarmsysteem;

85.3. het terug binnen de perimeter van de site plaatsen van de airconditioning.

86. Bij de berekening van de relevante omzet, vraagt Telenet dat het BIPT rekening houdt met de georedundantie met de Switch Office [vertrouwelijk]. Bij het volledig uitvallen van zowel de switching office en headend site te [vertrouwelijk], konden volgens Telenet immers maximaal [vertrouwelijk] mobiele klanten getroffen zijn en [vertrouwelijk] vaste klanten, i.e. de klanten die aangesloten zijn op de headend site te [vertrouwelijk].

87. Het BIPT volgt die redenering niet om de volgende redenen :

87.1. Het is steeds mogelijk dat een incident in de switching office van [vertrouwelijk] vandie aard is dat de georedundantie ook faalt (bijvoorbeeld omdat de switching office in [vertrouwelijk] al verzadigd is). Bovendien blijkt uit de praktijk dat redundantie niet altijd werkt.

87.2. Tijdens de hoorzitting van 23 mei 2022 heeft Telenet aangegeven dat de switching office van [vertrouwelijk] (samen met die van [vertrouwelijk]) de georedundantie verzekert voor de switching office in [vertrouwelijk]. In geval van een onderbreking van de switching office in [vertrouwelijk] zou er bijgevolg geen volledige redundantie meer zijn voor de switching office in [vertrouwelijk], wat belangrijke gevolgen zou hebben in geval van problemen bij de switching office in [vertrouwelijk].

6.3.2. De ernst van de inbreuk

88. De tweede stap van de berekening van het basisbedrag bestaat erin de relevante omzet te vermenigvuldigen met een percentage dat de ernst van de overtreding weergeeft, die licht, gemiddeld, ernstig of zeer ernstig kan zijn.

89. Het BIPT beoordeelt de graad van ernst van de overtreding geval per geval voor elk type van overtreding, rekening houdend met de aard van de overtreding en de werkelijke en/of mogelijke impact ervan op de regelgevende doelstellingen[1].

90. In geval van een beperkte schending van één van de doelstellingen in kwestie of een schending van een louter administratieve verplichting, kunnen we spreken van een lichte overtreding. In geval van schending van verscheidene doelstellingen, kan deze schending als een gemiddelde tot ernstige overtreding worden beschouwd. Een beduidende schending van een doelstelling kan daarentegen een zeer ernstige overtreding vormen. De overtreding is des te meer ernstig indien ze een beduidende schending vormt van verscheidene doelstellingen. Bij het onderzoek van de werkelijke en/of mogelijke impact van de overtreding op deze doelstellingen, houdt het BIPT rekening met de relevante omstandigheden van het beschouwde geval. De graad van ernst varieert in principe tussen 0% en 5% van de relevante omzet.

91. Het betreft in dit geval een mogelijke schending van de belangen van de eindgebruikers (particulieren, bedrijven en overheden, die klanten bij Telenet zijn). Een onderbreking van de dienst wegens een defect van de site van [vertrouwelijk] zou hun belangen rechtstreeks aantasten.

92. Het BIPT kwalificeert de overtreding als gemiddeld:

92.1. gezien de mogelijks ernstige impact van een onderbreking van de werking van de site van [vertrouwelijk];

92.2. wegens het feit dat er zich uiteindelijk geen veiligheidsincident heeft voorgedaan en dat er in de praktijk geen impact is geweest.

93. Het BIPT neemt dus een percentage van 0,5% in aanmerking op de in aanmerking genomen omzet van € [vertrouwelijk] zodat het basisbedrag neerkomt op € [vertrouwelijk] (afgerond bedrag).

6.4. Verzwarende en verzachtende omstandigheden

6.4.1. Inleiding

94. Verder acht het BIPT het gepast en evenredig om het basisbedrag aan te passen naargelang van het concrete gedrag van de overtreder, rekening houdend met de verzwarende en/of verzachtende omstandigheden die het basisbedrag van de boete respectievelijk kunnen verhogen en/of verlagen.

95. Het BIPT weerhoudt de volgende drie verzwarende omstandigheden.

[1] Deze regelgevende doelstellingen zijn onder andere de bevordering of het behoud van de concurrentie, de bevordering van de belangen van de consument, het stimuleren van de economie, de bescherming van het openbare belang, de bevordering van het doeltreffend beheer van schaarse middelen (spectrum), etc.

6.4.2. Verzuim van Telenet ondanks de oproep van het BIPT

96. Telenet heeft de toegang tot de site van [vertrouwelijk] onvoldoende beveiligd, terwijl het BIPT haar herhaaldelijk gevraagd had (zie onder andere de e-mails van 16 en 17 februari 2022) om deze site te mogen bezoeken om de fysieke beveiliging van de toegang tot de site te verifiëren.

97. Telenet wist dan ook dat dit punt bijzondere aandacht moest krijgen en heeft toch verzuimd om het nodige toe doen, zoals is vastgesteld.

6.4.3. Onvoldoende medewerking met het BIPT tijdens storm Eunice

98. Als voorbereiding van storm Eunice heeft het BIPT op vrijdag 18 februari 2022 om 9.30 uur een vergadering belegd met de voornaamste operatoren die actief zijn in België.

99. Tijdens die vergadering heeft het BIPT aan de operatoren gevraagd om tijdens de storm de volgende informatie te verstrekken, zodat het aan het Crisiscentrum van de regering regelmatig verslag kon uitbrengen over de staat van de netwerken:

    99.1. Verslag volgens een template geleverd door het BIPT om de twee uur (herzienbare periode naargelang van de situatie);

    99.2. De geografische coördinaten van de verstoorde antennes in een tabel met twee kolommen (X en Y).

100. Dat is een vereenvoudigde vorm van rapportering om het werk van de operator te vergemakkelijken.

101. Telenet is de enige operator die deze informatie niet heeft verstrekt of niet te gepasten tijde of niet in het gewenste formaat, zoals weergegeven in de tabel hieronder:

Datum en uur van de gevraagde rapportering	Ontvangst van het rapport van Telenet
18 februari 2022 – 13.00 u	13.59 u
18 februari 2022 – 15.00 u	-
18 februari 2022 – 17.00 u	17.26 u
18 februari 2022 – 19.00 u	20.23 u
18 februari 2022 – 21.00 u	-
19 februari 2022 – 9.00 u	-

102. Er dient te worden opgemerkt dat Telenet reeds tijdens de voormelde vergadering van 18 februari 2022 had gemeld dat het geen regelmatige rapportering van de staat van het netwerk kon garanderen. Het BIPT had toen de nadruk gelegd op het belang en de noodzaak van deze rapportering. In een mail die op 23 februari 2022 naar het BIPT is verzonden, kaartte Telenet opnieuw aan dat het niet had kunnen voldoen aan de verzoeken

van het BIPT om verslag uit te brengen. Het BIPT herinnert evenwel eraan dat Telenet de enige operator is die deze rapportering niet heeft volbracht zoals gevraagd was.

103. In haar schriftelijk opmerkingen van 20 mei 2022 legt Telenet het volgende uit : het "*heeft op de dag van de storm het BIPT op de hoogte gehouden van de status van het netwerk via regelmatige status updates (om 13u59, 15u43, 16u02, 16u18, 17u26 en 20u23), weliswaar niet in het specifieke formaat gevraagd door het BIPT. Het BIPT was op die manier volledig op de hoogte van de toestand van het netwerk van Telenet.*"

104. Het BIPT erkent dat Telenet hem een e-mail heeft gestuurd op 18 februari 2022 om 15u43, 16u02 en om 16u18. Maar die e-mails geven geen "statusbericht" van het Telenet-netwerk (een momentopname van de toestand van het netwerk, meer specifiek de lijst met antennes die niet meer correct functioneerden ten gevolge van de storm), maar vragen om de medewerking van het BIPT in het kader van het risico op het wegvliegen van de tent op de site van [vertrouwelijk].

105. Bovendien, zoals uitgelegd in sectie 4.2, heeft Telenet toen het op 18 februari 2022 contact opnam met het BIPT gezien het risico dat de tent over de site van [vertrouwelijk] zou wegvliegen door storm Eunice, de escalatiematrix genegeerd door naar een lid van de dienst Netwerkveiligheid van het BIPT te bellen in plaats van te bellen naar de wachtdienst voor netwerkveiligheid van het BIPT (de permanentie). Welnu, het BIPT heeft in het verleden en herhaaldelijk Telenet, net als de andere operatoren, wel degelijk op de hoogte gebracht van deze escalatiematrix en van de communicatieprocedure (e-mails van 15 maart 2018 en 17 september 2021). Het is belangrijk dat Telenet deze in acht neemt:

105.1. om te garanderen dat de personeelsleden van Telenet die een beveiligingsincident behandelen deze kennen en het automatisme hebben om contact op te nemen met de permanentie;

105.2. om een correcte verspreiding van de informatie en een daadwerkelijk antwoord op de vragen te waarborgen. Alleen de permanentie is 24/7 beschikbaar en door contact op te nemen met de permanentie kan men garanderen dat de informatie gecentraliseerd is bij het personeelslid van het BIPT dat verantwoordelijk is voor de permanentie op het moment van de melding van het incident. De verwerking van de informatie is cruciaal bij incidentenbeheer. Door de procedures niet na te leven kunnen situaties die al kritiek zijn, erger worden en leiden tot economisch verlies of het verlies van mensenlevens die vermeden zouden kunnen worden als de procedures waren gevolgd, met name ingeval de toegang tot de nooddiensten gestoord is.

106. Telenet erkent dat het eerste telefonische contact met het BIPT niet via de permanentie is verlopen. Volgens Telenet heeft het BIPT echter op geen enkel moment – niet tijdens de storm en ook niet tijdens een post-mortem bespreking - aangegeven dat Telenet een ander nummer bij het BIPT had moeten bellen. Bovendien heeft Telenet vrijwel onmiddellijk na het initiële telefonische gesprek een e-mail gestuurd naar de permanentie van het BIPT, zoals voorzien in de BIPT-escalatie matrix, met de vraag aan het BIPT om tussenbeide te komen.

107. Volgens het BIPT verschoont het niet-naleven van de procedure niet ineens omdat het BIPT dit verwijt vroeger aan Telenet had kunnen meedelen.

108. Het BIPT is daarentegen van mening dat het feit dat Telenet zijn e-mails gericht heeft aan het e-mailadres van de permanentie, zoals hierboven is uitgelegd, de omvang van de verzwarende omstandigheden vermindert.

6.4.4. Het regelmatig niet-naleven door Telenet van de procedures tijdens incidenten onderstreept het gebrek aan wil om gepaste interne processen en expertise inzake crisisbeheer toe te passen.

109. In de follow-up van het beheer van dat incident (risico op het wegvliegen van de tent tijdens de storm) werd het BIPT naar verscheidene aanspreekpunten van Telenet doorverwezen die niet over alle informatie beschikten en kreeg het geen toestemming om contact op te nemen met de persoon verantwoordelijk voor het beheer van het incident. Telenet heeft dus geen gevolg gegeven aan het verzoek van het BIPT om een uniek aanspreekpunt aan te duiden, aangezien hierbij verscheidene personen betrokken waren met ieder hun eigen contactgegevens en geen van hen was overigens in staat om de nodige informatie te verschaffen.

110. In haar schriftelijke opmerking van 20 mei 2022 schijft Telenet het volgende: "*Het BIPT onderbouwt de vaststellingen in deze paragraaf niet met concrete voorbeelden. Telenet is niet op de hoogte dat zij "regelmatig" de procedures bij incidenten niet zou hebben nageleefd. Voor zover er tekortkomingen zouden zijn aan de interne processen, zouden we graag concrete voorbeelden hiervan ontvangen zodat we de nodige maatregelen kunnen treffen. Bij aantoonbare tekortkomingen is Telenet uiteraard bereid om aanpassingen aan haar processen te bekijken en de processen in samenspraak met het BIPT te optimaliseren*."

111. Tijdens de hoorzitting heeft Telenet toegegeven dat er soms een issue is bij echt kritische incidenten wegens onderverdeling tussen enerzijds de SOC en anderzijds de SPOC binnen regulatory.

112. Tijdens de storm Eunice was het aanspreekpunt bij Telenet voor het BIPT niet in staat een algemeen overzicht van het netwerk te verschaffen, ofwel bij gebrek aan beschikbare informatie, ofwel bij gebrek aan tijd. Tijdens de storm heeft een medewerker van Telenet de leden van de dienst Netwerkveiligheid van het BIPT doorverwezen naar zijn collega, die de leden dan weer doorverwees naar de eerste medewerker.

113. Tijdens de incidenten in 2021 (10/03/2021 en 23/03/2021) functioneerden de nummers die Telenet aan de permanentie van het BIPT had verstrekt, niet of niemand beantwoordde de oproepen. Die situaties die nadelig zijn voor het incidentenbeheer, worden veroorzaakt doordat Telenet de monitoring aan een onderaannemer uitbesteedt. Telenet lijkt problemen te hebben om vereenvoudigde verslagen uit te brengen door het grote aantal actoren. Het BIPT heeft altijd op die problemen gereageerd door Telenet of andere operatoren te herinneren aan de telefoonnummers die moeten worden gebruikt of de regels die moeten worden gevolgd.

114. Er wordt echter bij de berekening van het percentage van de verzwarende omstandigheden geen rekening gehouden met de opmerkingen uit de twee voorgaande paragrafen, aangezien er hiervan geen schriftelijk bewijs is.

6.4.5. Conclusies inzake de verzwarende omstandigheden

115. Gezien de argumenten van Telenet beperkt het BIPT de verhoging van het basisbedrag tot 5% in plaats van 10% in het ontwerpbesluit, zodat het basisbedrag van de boete neerkomt op [vertrouwelijk] € (afgerond bedrag).

6.5. Uiteindelijke berekening van het bedrag van de boete

116. Het BIPT verlaagt uiteindelijk het bedrag van de boete naar € 190.000 (afgerond bedrag) om tot een evenredig bedrag te komen. Deze vermindering (min [vertrouwelijk] %) is aanzienlijk. Deze vermindering wordt gerechtvaardigd door het evenredigheidsbeginsel dat het BIPT hanteert conform zijn "Boeterichtsnoeren" :

"24. Tijdens de verschillende voormelde fasen houdt het BIPT rekening met de evenredigheid en de noodzaak om de boete een ontradend effect te geven wat, in voorkomend geval, tot een bijstelling van het boetebedrag naar omhoog of naar omlaag kan leiden. […]

27. Tot slot moet het voorgestelde bedrag van de boete voldoende hoog zijn om de nagestreefde doelstellingen te verwezenlijken maar, conform het evenredigheidsbeginsel, zou dat bedrag niet mogen overstijgen wat nodig is om deze doelstellingen te halen. Om de evenredigheid van het boetebedrag te beoordelen zal het BIPT rekening houden met de omvang van de overtreder en zijn financieel vermogen."

117. De omvang van de vermindering is gerechtvaardigd gezien het de eerste keer is dat een inbreukprocedure wordt ingeleid voor dergelijk voorval. Hiermee wenst het BIPT een duidelijk signaal geven aan operatoren zoals Telenet voor dergelijke overtredingen die in de toekomst eveneens het voorwerp kunnen uitmaken van een inbreukprocedure. Anderzijds is het BIPT van oordeel dat de boete in deze sterk verlaagd kan worden aangezien er van uit wordt gegaan dat dit in principe tot een gepaste reactie zal leiden op het niet-naleven van deze verplichting en tevens een voldoende ontradend effect zal hebben op verdere overtredingen. Het BIPT houdt zich het recht voor om deze boetebepaling strenger te maken ingeval dat nodig zou zijn.

118. De uiteindelijk opgelegde boete is dus heel ver van het wettelijke maximum dat toegestaan is door artikel 21 van de BIPT-statuutwet. Bovenstaande overwegingen dragen ertoe bij dat de boete die opgelegd wordt in de onderhavige omstandigheden echter evenredig geacht wordt ten opzichte van de vooropgestelde doelstelling van de boete, met name een gepaste reactie stimuleren op de inbreuk en een ontradend effect hebben naar de toekomst toe.

7. Besluit

119. Het BIPT:

119.1. stelt dat Telenet artikel 107/2, § 1 , van de wet van 13 juni 2005 betreffende de elektronische communicatie heeft geschonden;

119.2. gelast Telenet om de adequate en evenredige maatregelen van technische en organisatorische aard bedoeld in artikel 107/2, § 1, van de telecomwet, te treffen teneinde de fysieke toegang tot zijn site in [vertrouwelijk] te beveiligen, met name de maatregelen bedoeld in punt 64;

119.3. gelast Telenet om binnen 15 dagen na dit besluit de planning eraan mee te delen van de reconstructiewerkzaamheden van de site van [vertrouwelijk], met details over de geplande werkzaamheden en termijnen;

119.4. legt Telenet hiervoor een administratieve boete van 190.000 euro op. Deze boete komt aan de Schatkist toe.

Beroepsmogelijkheden

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 onontvankelijkheid die ambtshalve wordt uitgesproken, ingesteld door middel van een ondertekend verzoekschrift, waarbij het aangevochten besluit is bijgevoegd en 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.

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

Bernardo Herman
lid van de Raad

Luc Vanfleteren
lid van de Raad

Michel Van Bellinghen
voorzitter van de Raad