Besluit
Openbaar

Ons kenmerk: ACM/DJZ/2014/201921_OV
Zaaknummer: 13.0503.32.1.01
Datum: 13 juni 2014

Beslissing op bezwaar van de Autoriteit Consument en Markt inzake het bezwaarschrift van KPN B.V. gericht tegen het besluit van 16 december 2013 waarbij aan KPN B.V. een boete is opgelegd van EUR 364.000 voor overtredingen van artikel 11.3, eerste lid, jo. artikel 11.2 en artikel 18.7, derde en vijfde lid, van de Telecommunicatiewet, alsmede tegen het besluit van 14 februari 2014 waarbij op grond van artikel 8 van de Wet openbaarheid van bestuur is bepaald dat het eerstgenoemde besluit openbaar zal worden gemaakt

Muzenstraat 41 | 2511 WB Den Haag
Postbus 16326 | 2500 BH Den Haag
T 070 722 20 00 | F 070 722 23 55
info@acm.nl | www.acm.nl | www.consuwijzer.nl

1. Samenvatting

1. Eerdergenoemde boete is opgelegd omdat de Autoriteit Consument en Markt (hierna: ACM) heeft vastgesteld dat KPN B.V. (hierna: KPN) in de periode van september 2010 tot en met 15 januari 2012[1] (onderzoeksperiode I) onvoldoende passende, hoofdzakelijk organisatorische, maar ook technische maatregelen heeft getroffen in het belang van bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. De opgelegde boete is verhoogd met 30% omdat KPN het bestaan van een relevant intern onderzoek niet heeft gemeld.

2. In deze beslissing op bezwaar verklaart ACM de bezwaren van KPN tegen het besluit van 16 december 2013[2] (hierna: het sanctiebesluit) ongegrond. Dit betekent dat het besluit tot oplegging van een boete van EURO 364.000 geheel in stand blijft.

3. ACM verklaart het bezwaar tegen het besluit van 14 februari 2014[3] tot openbaarmaking van het sanctiebesluit (hierna: het publicatiebesluit) deels gegrond, zodat dit besluit grotendeels in stand blijft.

4. Het is voor consumenten van belang dat hun persoonsgegevens door aanbieders van openbare elektronische communicatiediensten en -netwerken op een adequate wijze worden beveiligd. Om gebruik te kunnen maken van de diensten van die aanbieders moeten consumenten persoonsgegevens aan hen verstrekken. Met de beperking van het risico dat die persoonsgegevens in handen vallen van onbevoegden is een zwaarwegend belang gemoeid, omdat dit schadelijke gevolgen kan hebben voor de betrokken consumenten. Het is daarom zaak dat aanbieders van dergelijke diensten en netwerken maatregelen treffen om de

[1] Onderzoeksrapport, randnummer 90.
[2] Kenmerk ACM/DJZ/2013/206321.
[3] Kenmerk ACM/DJZ/2014/200868.

beveiliging van persoonsgegevens voldoende te waarborgen. Om die reden heeft de wetgever er voor gekozen om in dat kader een zorgplicht in de Tw op te nemen waaraan de aanbieders van die diensten en netwerken moeten voldoen.

5. Het onderzoek dat in dit geval heeft geleid tot het opleggen van een boete aan KPN, vloeit voort uit het feit dat in januari 2012 bekend werd dat een hacker had ingebroken in het netwerk van KPN. ACM heeft vervolgens een onderzoek ingesteld naar de wijze waarop KPN invulling geeft aan de op haar rustende wettelijke zorgplicht ten aanzien van de beveiliging van de persoonsgegevens die in haar systemen zijn opgeslagen. Uit dit onderzoek kwam naar voren dat KPN voor een aantal essentiële beveiligingsmaatregelen geen (centraal) beleid had opgesteld, dan wel dat het onderhoud en/of de uitvoering van het opgestelde beleid onvoldoende heeft plaatsgevonden. Ook had KPN onder meer haar netwerkbeheer niet op orde en had zij op het gebied van netwerk- en systeembewaking onvoldoende passende maatregelen getroffen.

6. Na de hack heeft KPN het oplossen van de problemen de hoogste prioriteit te geven. Ook heeft zij haar procedures geëvalueerd om de kans op mogelijke hacks in de toekomst te verkleinen. De wijze van handelen van KPN in de onderzochte periode na de hack (onderzoeksperiode II: van 16 januari tot 15 maart 2012)[4], was zodanig dat ACM heeft geoordeeld dat destijds de zorgplicht door KPN wel werd nageleefd.

7. Dit besluit heeft de volgende opbouw: allereerst beschrijft ACM het verloop van de procedure (hoofdstuk 2). Vervolgens vat zij het bestreden besluit samen (hoofdstuk 3). Daarna volgen een weergave van de bezwaren van KPN (hoofdstuk 4), het toepasselijke juridische kader (hoofdstuk 5) en de overwegingen van ACM ten aanzien van die bezwaren (hoofdstuk 6).

2. Verloop van de procedure

8. Bij besluit van 16 december 2013[5] heeft ACM aan KPN een boete opgelegd voor het overtreden van de in artikel 11.3, eerste lid, jo. artikel 11.2 Tw neergelegde zorgplicht en artikel 18.7, derde en vijfde lid, Tw.

9. KPN heeft op 27 januari 2014 pro forma bezwaar gemaakt tegen het sanctiebesluit.

[4] Onderzoeksrapport, randnummer 91.
[5] Kenmerk ACM/DJZ/2013/206321.

10. Bij besluit van 14 februari 2014[6] heeft ACM besloten het boetebesluit te publiceren.

11. KPN heeft bij brief van 28 februari 2014 de gronden van haar bezwaar tegen het boetebesluit kenbaar gemaakt en tevens bezwaar gemaakt tegen het publicatiebesluit.

12. Verder heeft KPN op dezelfde datum een verzoek ingediend bij de rechtbank Rotterdam om een voorlopige voorziening te treffen ter voorkoming van de publicatie van het boetebesluit.

13. Op 27 maart 2014 heeft ten kantore van ACM een hoorzitting plaatsgevonden waarin KPN haar bezwaren tegen het sanctie- en het publicatiebesluit mondeling heeft toegelicht. Van de hoorzitting is een verslag gemaakt. Het verslag is gelijktijdig met het deze beslissing naar KPN gestuurd.

14. De zitting van de voorzieningenrechter van de rechtbank Rotterdam (hierna: de voorzieningenrechter) ter mondelinge behandeling van het verzoek van KPN heeft plaatsgevonden op 6 mei 2014.

15. Bij brief van 9 mei 2014[7] heeft ACM de voorzieningenrechter – onder strikte voorwaarden – toegezegd de openbaarmaking van het sanctiebesluit feitelijk aan te houden totdat de rechtbank Rotterdam in de bodemzaak uitspraak heeft gedaan op het nog door KPN tegen deze beslissing op bezwaar in te stellen beroep.

3. De bestreden besluiten

16. ACM heeft KPN beboet, omdat KPN in de periode van september 2010 tot en met 15 januari 2012 onvoldoende passende, hoofdzakelijk organisatorische, maar ook technische maatregelen heeft getroffen in het belang van bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers.

17. Bij besluit van 16 december 2013 heeft ACM hiervoor aan KPN een boete opgelegd van EUR 280.000 vanwege overtreding van de zorgplicht en deze boete met 30% verhoogd omdat KPN niet volledig heeft meegewerkt aan het onderzoek. In totaal is dus een boete opgelegd van EUR 364.000.

[6] Kenmerk ACM/DJZ/2014/200868.
[7] Kenmerk ACM/DJZ/2014/202701.

3.1 Sanctiebesluit zorgplicht

18. In het sanctiebesluit heeft ACM vastgesteld dat KPN de op haar rustende zorgplicht neergelegd in artikel 11.3, eerste lid, jo. artikel 11.2 Tw niet heeft nageleefd, omdat zij in onvoldoende mate passende, hoofdzakelijk organisatorische, maar ook technische maatregelen heeft genomen betreffende:

    - het opzetten en het handhaven van beveiligingsbeleid
    - netwerkinrichting
    - afscherming
    - netwerk- en systeembewaking, en
    - patchmanagement

19. Verder is door ACM vastgesteld dat KPN artikel 18.7, derde en vijfde lid, Tw heeft overtreden, omdat zij het bestaan van een relevant intern onderzoek, het Intern onderzoek Victor, in reactie op de informatievordering van 29 februari 2012 van ACM niet heeft gemeld.

3.2 Publicatiebesluit

20. Bij besluit van 14 februari 2014 (hierna: het publicatiebesluit) heeft ACM besloten dat het sanctiebesluit in de zaak KPN Zorgplicht van 16 december 2013 openbaar te maken.

21. Het door KPN bij brief van 13 januari 2014 ingediende verzoek bepaalde in het sanctiebesluit opgenomen informatie als (bedrijfs)vertrouwelijk aan te merken, is gedeeltelijk ingewilligd. De reden hiervoor is dat ACM van oordeel is dat een gedeelte van die informatie niet kwalificeert als (bedrijfs)vertrouwelijke informatie in de zin van artikel 10 Wet openbaarheid van bestuur (hierna: Wob). Voor het overige is het verzoek van KPN bepaalde in het sanctiebesluit opgenomen informatie als (bedrijfs)vertrouwelijk aan te merken gedeeltelijk niet ingewilligd, omdat niet in alle gevallen de gehele passage aangemerkt kan worden als informatie die na openbaarmaking mogelijk tot onevenredige benadeling van KPN kan leiden.

22. Meerdere in het publicatiebesluit genoemde algemene belangen dienden naar het oordeel van ACM zwaarder te wegen dan het belang van KPN bij het voorkomen van publicatie. Van de aanwezigheid van bijzondere belangen of omstandigheden op grond waarvan in dit geval moet worden afgezien van publicatie is ACM niet overtuigd geraakt.

4. Bezwaargronden

4.1 Sanctiebesluit zorgplicht

Interpretatie wettelijke norm

23. KPN stelt ten eerste dat opvallend is dat ACM slechts summier ingaat op de meer principiële, inhoudelijke aspecten met betrekking tot inhoud en reikwijdte van de zorgplicht die KPN heeft aangevoerd in haar zienswijze. Met name ten aanzien van de juridische analyse van de zorgplicht neergelegd in de artikelen 11.2 en 11.3 Tw acht KPN het sanctiebesluit over de hele gehele linie dan ook onvoldoende gemotiveerd.

24. De manier waarop ACM de norm zoals neergelegd in de artikelen 11.2 en 11.3 Tw heeft uitgelegd, komt er volgens KPN feitelijk op neer dat zij de wettelijke zorgplicht heeft geschonden omdat een incident heeft plaatsgevonden. KPN meent dat een incident aanleiding kan vormen voor een onderzoek, maar dat de vraag of de zorgplicht is geschonden niet beantwoord mag worden door een incident in isolement te beoordelen. KPN vindt dat ACM het ten onrechte heeft nagelaten naar objectieve maatstaven, en onderbouwd met gedegen literatuur- en praktijkonderzoek, zelf de stand der techniek vast te stellen. ACM had volgens KPN aldus een norm moeten stellen voor de zorgplicht. Vervolgens had ACM de maatregelen die KPN heeft getroffen daaraan moeten toetsen. Daarbij acht KPN het ook relevant om te kijken naar wat vergelijkbare dienstaanbieders al dan niet doen ter bescherming van persoonsgegevens.

25. KPN wijst er verder op dat zij heeft toegelicht dat de artikelen 11.2, 11.3 en 11.3a Tw in onderlinge samenhang moeten worden beschouwd. De verschillende artikelen werken volgens KPN als communicerende vaten.

26. De Wet bescherming persoonsgegevens (hierna: Wbp) vormt het algemene kader waarbinnen de verwerking van persoonsgegevens moet plaatsvinden en blijft dus onverminderd gelden. KPN stelt zich dan ook op het standpunt dat bij de interpretatie van artikel 11.3 Tw moet worden aangesloten bij het vrijwel gelijkluidende artikel 13 Wbp.

27. KPN meent bovendien dat, indien ACM daadwerkelijk de “business as usual” had willen onderzoeken, zij daarbij juist alle door KPN getroffen beveiligingsmaatregelen en -onderwerpen had moeten betrekken en niet slechts een select aantal zeer concrete beveiligingsonderwerpen dat verband houdt met het onderhavige incident. Volgens KPN blijkt uit het juridisch kader echter duidelijk dat herstelmaatregelen na incidenten een belangrijk onderdeel zijn van de beveiligingsplicht en dus moeten worden meegewogen bij de vraag of

aan de zorgplicht is voldaan. ACM oordeelt ook niet dat KPN niet adequaat heeft gereageerd op het incident, aldus KPN.

28. KPN stelt dat wanneer ACM rekening had gehouden met het verband tussen de beveiligingsplicht, de informatieplicht en de meldplicht, zij niet had kunnen komen tot het sanctiebesluit. Ook deze verplichtingen beschouwt KPN als communicerende vaten.

Vaststellen overtreding

29. ACM heeft volgens KPN geen objectieve beoordeling verricht. Het onderzoek is beperkt gebleven tot een vijftal – door het incident ingegeven – beveiligingsonderwerpen, namelijk het opstellen en handhaven van een beveiligingsbeleid, netwerkinrichting, afscherming, netwerk- en systeembewaking, en patchmanagement. Voor KPN was niet te voorspellen dat een dergelijk beperkte toets zou worden aangelegd, ook omdat beleidsregels ter zake ontbreken.

30. KPN vindt dat ACM te zwaar leunt op het Intern onderzoek Victor en Fox-IT-rapport vastgestelde tekortkomingen. In ieder geval is de toets die in het onderzoeksrapport is gehanteerd volgens KPN veel te beperkt. KPN stelt dat er, op het aanhalen van één literatuurbron na (de CISSP All-in-One – Exam Guide), geen verder onderzoek is gedaan naar de stand van de techniek en wat een “passend beveiligingsniveau” is. Verder zou er ten onrechte geen vergelijking met andere dienstaanbieders zijn gemaakt en mocht ACM de onderzoeksbevindingen niet zo maar overnemen.

31. KPN stelt dat ACM ten aanzien van de vijf gekozen beveiligingsonderwerpen bovendien lijkt te suggereren dat de beveiliging 100% ‘waterdicht’ had moeten zijn. Door deze strenge en concrete normen te formuleren, heeft ACM miskend dat de wetgever de door aanbieders te nemen maatregelen bewust niet nader heeft uitgewerkt.

32. Verder wijst KPN er op dat ACM zich in het sanctiebesluit niet heeft beperkt tot de vraag of KPN het vereiste resultaat heeft bereikt, maar dat de handelwijze van KPN ten onrechte is getoetst aan de door ACM geformuleerde, zeer concrete, normen. Daarmee zou ACM KPN en andere aanbieders de mogelijkheid ontnemen om zelf de vereiste (beleids)afwegingen te maken.

33. De (strenge) normen die ACM hanteert, zijn volgens KPN ook overigens niet in overeenstemming met de stand van de techniek. KPN betoogt dat de in het onderzoeksrapport geformuleerde normen strenger zijn dan algemeen geaccepteerde beveiligingsstandaarden en de richtsnoeren van het College bescherming persoonsgegevens (hierna: Cbp).

Opleggen sanctie

34. Als KPN al (op onderdelen) de zorgplicht zou hebben overtreden, is het opleggen van een punitieve sanctie in een situatie als deze volgens haar niet op zijn plaats. KPN wijst er in dit verband op dat de gevolgen van het incident beperkt zijn gebleven omdat de hack geen gevolgen zou hebben gehad voor de persoonsgegevens van abonnees en gebruikers.

35. Verder voert KPN aan dat dit de eerste keer is dat ACM de zorgplicht van artikel 11.2 en 11.3 Tw 'toepast' en dat deze norm door ACM ook niet is uitgewerkt in (geldende) beleidsregels. KPN stelt dat het voor haar en andere aanbieders daarom niet duidelijk is hoe ACM de zorgplicht zal invullen. Omdat de daaraan in casu door ACM gegeven invulling door KPN vooralsnog ook als onjuist wordt gezien, is het volgens KPN niet juist om nu een boete op te leggen.

36. ACM vermeldt in het sanctiebesluit dat het feit dat geen persoonsgegevens zijn verwerkt "niet maakt dat bedoeld beveiligingsniveau toch als toereikend kan worden beschouwd''. ACM miskent hiermee volgens KPN dat dit argument door KPN is aangedragen in het kader van haar (meer subsidiaire) argument dat de boetebeleidsregels verkeerd worden toegepast, en niet om te betogen dat geen overtreding heeft plaatsgevonden. KPN stelt dat het in het kader van het vaststellen van de hoogte van de boete wel degelijk relevant is in hoeverre er daadwerkelijk schade is opgetreden. KPN betoogt dat het onjuist is dat de ernst van de overtreding niet wordt beïnvloed door de vraag of er al dan niet daadwerkelijk persoonsgegevens zijn verwerkt, omdat de toelichting bij artikel 3.5 van bedoelde boetebeleidsregels nu juist in dit kader aangeeft dat dit wel relevant is.

37. Verder meent KPN dat ACM bij het vaststellen van de ernst van de boete rekening dient te houden met alle omstandigheden van het geval. In het sanctiebesluit is ACM volgens KPN in het geheel niet meer ingegaan op de door KPN in dit verband aangedragen omstandigheden, namelijk de beveiligingsmaatregelen die wel door KPN zijn getroffen, de (adequate) handelwijze van KPN na constatering van het incident of met de medewerking die KPN heeft verleend aan het onderzoek.

38. KPN stelt dat het vaststellen van de basisboete op EUR 280.000 overigens betrekkelijk willekeurig overkomt en ook niet goed is onderbouwd. ACM zou niet motiveren waarom de boete EUR 20.000 lager is dan het maximum, zodat KPN niet goed kan inschatten of de reden hiervoor wellicht meer gewicht zou moeten toekomen.

4.2 Publicatiebesluit

39. Bij brief van 13 januari 2014 heeft KPN gemotiveerd aangegeven welke onderdelen van het sanctiebesluit als vertrouwelijk dienen te worden aangemerkt en om die reden uit het te publiceren besluit zouden moeten worden geschrapt. Ten aanzien van een aantal onderdelen heeft ACM naar de mening van KPN echter ten onrechte besloten deze niet als vertrouwelijk aan te merken. KPN maakt dan ook bezwaar tegen het publicatiebesluit voor zover daarin de volgende onderdelen niet als vertrouwelijk zijn aangemerkt:

- ACM vermeldt in randnummer 61, tweede bulletpoint, van het sanctiebesluit dat de beveiligingsmaatregel “patchmanagement” niet is ingevoerd. Deze opmerking dient volgens KPN te worden geschrapt omdat zij stelt dat dit onjuist is.
- KPN had verzocht om het schrappen van een gehele alinea in randnummer 75. Indien dat ook na heroverweging door ACM niet gebeurt, vindt KPN in elk geval dat de eerste, derde en vierde volzin moeten worden geschrapt. ACM heeft tekst met dezelfde materiële inhoud wel geschrapt in randnummer 61, tweede bulletpoint en deze dient ook in randnummer 75 te worden verwijderd. KPN stelt dat de opmerking kwaadwillenden uitnodigt in te breken op de systemen van KPN.
- Meerdere randnummers van het besluit dienen volgens KPN alsnog geheel als vertrouwelijk te worden aangemerkt (alsmede alle overige tekst waaruit afgeleid kan worden dat de hack heeft plaatsgevonden ten gevolge van een kwetsbaarheid in de [vertrouwelijk]) omdat daaruit alleen de naam “[vertrouwelijk]” is geschrapt. KPN betoogt dat uit de overige tekst, zeker door geïnformeerde kwaadwillenden, gemakkelijk kan worden afgeleid dat het om deze software gaat. Volgens KPN heeft dit in hoge mate een uitnodigend effect op kwaadwillenden om te trachten deze kwetsbaarheid te vinden en te misbruiken.

5. Juridisch kader

5.1 Handhavingsbevoegdheid

40. Tot 1 april 2013 was OPTA op grond van artikel 15.1, derde lid, Tw belast met het toezicht op de naleving van artikelen 11.2, 11.3, 18.7 en 18.13 Tw. Per 1 april 2013 is ACM, als rechtsopvolger van, onder meer, OPTA, belast met dit toezicht.

41. Tot 1 april 2013 was OPTA op grond van artikel 18.7 Tw bevoegd voor een juiste uitvoering van het bepaalde bij of krachtens de Tw van een ieder te allen tijde inlichtingen te vorderen voor zover dit redelijkerwijs voor de vervulling van haar taak nodig is. Per 1 april 2013 komt deze bevoegdheid toe aan ACM.

42. Artikel 15.4, vierde lid, Tw, bepaalt dat ACM in geval van overtreding van de bij of krachtens de in artikel 15.1, derde lid, Tw bedoelde voorschriften de overtreder een boete kan opleggen van ten hoogste € 450.000 per overtreding.

43. Gezien de maximumboete ex artikel 15.4, vierde lid, Tw dient ACM op grond van artikel 5:48 juncto artikel 5:53 Awb bij overtreding van artikelen 11.2, 11.3, en 18.7 Tw een rapport op te maken.

44. De Minister van Economische Zaken heeft op 19 april 2013 beleidsregels vastgesteld voor het opleggen van bestuurlijke boetes door ACM[8] (hierna: Boetebeleidsregels ACM). De Boetebeleidsregels ACM zijn in werking getreden op 25 april 2013. Zij bevatten de criteria die worden meegewogen bij het bepalen van de ernst van de overtreding, bij het bepalen van de hoogte van de basisboete en bij het bepalen van eventuele boeteverhogende of -verlagende omstandigheden.

5.2 Zorgplicht

45. Artikel 11.2 Tw luidt:

> *Onverminderd de Wet bescherming persoonsgegevens en het overigens bij of krachtens deze wet bepaalde dragen de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk, onderscheidenlijk zijn dienst.*

46. Artikel 11.3, eerste lid, Tw luidt:[9]

> *1. De in artikel 11.2 bedoelde aanbieders treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.*

[8] Beleidsregels van de Minister van Economische Zaken voor het opleggen van bestuurlijke boetes door de ACM (*Stcrt.* 2013, nr. 11214, 24 april 2013).
[9] De nummering is gebaseerd op de versie van de Tw zoals die gold ten tijde van onderzoeksperiode I en onderzoeksperiode II (zie randnummer 90 van het onderzoeksrapport en verder). Met ingang van 5 juni 2013 is artikel 11.3 gewijzigd. Het (voormalige) tweede lid is vernummerd tot derde lid, maar is inhoudelijk niet aangepast.

47. Artikel 11.2 Tw is een vangnetbepaling en artikel 11.3, eerste lid, Tw is een nadere uitwerking van artikel 11.2 Tw ten aanzien van de veiligheid en beveiliging van aangeboden netwerken en diensten. Om deze reden is in het onderzoeksrapport primair onderzocht of artikel 11.3, eerste lid, Tw is overtreden, en fungeert artikel 11.2 Tw als vangnet.[10]

5.3 Medewerkingsplicht

48. Relevante delen van artikel 18.7 Tw[11]:

> *1. Onze Minister, onderscheidenlijk het college, is bevoegd voor een juiste uitvoering van het bepaalde bij of krachtens deze wet of bij de roamingverordening van een ieder te allen tijde inlichtingen te vorderen voor zover dit redelijkerwijs voor de vervulling van zijn taak nodig is.*
>
> *2. (…)*
>
> *3. Degene van wie krachtens het eerste lid inlichtingen zijn gevorderd, is verplicht deze onverwijld te geven, maar in elk geval binnen de daartoe door Onze Minister, onderscheidenlijk het college, te stellen termijn.*
>
> *4. In een vordering op grond van het eerste lid kan wat betreft de te geven inlichtingen worden volstaan met:*
>
> *a. het omschrijven van het onderwerp waarover inlichtingen moeten worden gegeven en*
>
> *b. de bij het verstrekken van de inlichtingen aan te houden mate van detail.*
>
> *5. Degene van wie de verstrekking van inlichtingen is gevorderd, is verplicht binnen de door Onze Minister, onderscheidenlijk het college, te bepalen redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij het uitoefenen van zijn bevoegdheden. Artikel 5:20, tweede lid, van de Algemene wet bestuursrecht is van toepassing.*
>
> (…)

[10] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 39 en p. 118-119 en *Kamerstukken II* 1997/98, 25 533, nr. 5, p. 12.
[11] Op 1 april 2013 is artikel 18.7 Tw aangepast. Met deze wijziging komt de bevoegdheid toe aan ACM.

5.4 Openbaarmaking sanctiebesluit

49. Artikel 8, eerste lid, Wob luidt:

> *1. Het bestuursorgaan dat het rechtstreeks aangaat, verschaft uit eigen beweging informatie over het beleid, de voorbereiding en de uitvoering daaronder begrepen, zodra dat in het belang is van een goede en democratische bestuursvoering.*

6. Overwegingen

50. In dit hoofdstuk zal ACM beginnen met het bespreken van de door KPN opgeworpen bezwaargronden die het vaststellen van de overtreding betreffen. Die gronden zijn in te delen in drie (hoofd)categorieën (interpretatie wettelijke norm, inrichting onderzoek en overige bezwaren), en zullen ook in die volgorde worden behandeld. In paragraaf 6.2 worden de bezwaargronden betreffende de aan KPN opgelegde sanctie behandeld. In paragraaf 6.3 worden de bezwaren tegen het publicatiebesluit behandeld. Tot slot sluit ACM het hoofdstuk af met een conclusie.

6.1 Bezwaren m.b.t. vaststellen overtreding

6.1.1 Interpretatie wettelijke norm

Parlementaire geschiedenis

51. Uit de parlementaire geschiedenis volgt dat artikel 11.3, eerste lid, Tw kan worden beschouwd als een nadere uitwerking van de algemene zorgplichtbepaling die is neergelegd in artikel 11.2 Tw.

52. Over de verhouding tussen artikel 11.2 en artikel 11.3, eerste lid, Tw en over de aanbieders waaraan de zorgplicht wordt opgelegd wordt in de betreffende Memorie van Toelichting het volgende opgemerkt:

> "*6.3.1* (…) *Teneinde te bewerkstelligen dat abonnees en gebruikers van telecommunicatienetwerken en –diensten in ieder geval steeds op een zekere bescherming van de persoonlijke levenssfeer en van persoonsgegevens aanspraak kunnen maken, wordt een algemene zorgplicht in de wet opgenomen. Die zorgplicht wordt gelegd op de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. Die zorgplicht geldt onverminderd de verantwoordelijkheden die aanbieders uit anderen hoofde reeds hebben. Waar het gaat om de bescherming van de persoonlijke levenssfeer moet daarbij worden gedacht aan de Wet persoonsregistraties, en in de nabije toekomst de Wet bescherming persoonsgegevens*. (…) *De zorgplicht wordt*

nader ingevuld met regels die rechtstreeks voortvloeien uit de bepalingen van de bijzondere privacyrichtlijn. (…)"[12]

53. Verder wordt in de artikelsgewijze toelichting van genoemde Memorie van Toelichting het volgende overwogen:

6.1.2 "Artikel 11.2

Zoals reeds in het algemeen deel van de toelichting is uiteengezet wordt voorgesteld een algemene zorgplichtbepaling in het leven te roepen ten behoeve van abonnees en gebruikers van telecommunicatienetwerken en -diensten. Hiermee is in ieder geval verzekerd dat abonnees en gebruikers over ten minste een algemene waarborg beschikken met behulp waarvan de rechten op bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer die uit de nationale en internationale privacyregelgeving voortvloeien, kunnen worden gegarandeerd. (…) *Deze zorgplicht werkt uiteraard subsidiair ten opzichte van de andere bepalingen van Hoofdstuk 11 en de Wet persoonsregistraties.* (…)

6.1.3 Artikel 11.3

Dit artikel dient ter uitvoering van artikel 4 van de bijzondere privacyrichtlijn. Er is voor gekozen de zorg voor de veiligheid en de beveiliging zowel op aanbieders van netwerken als op de aanbieders van telecommunicatiediensten te leggen. De verwevenheid van netwerken en diensten op fysiek en technisch niveau is zodanig nauw dat het weinig zinvol lijkt uitsluitend de dienstaanbieders deze verplichting op te leggen. Bij de naleving van die verplichting zal de dienstaanbieder hoe dan ook afhankelijk zijn van de netwerkbeheerder. Het lijkt daarom niet onredelijk ook de netwerkbeheerder met een verplichting terzake te belasten.

De tweede volzin belast de desbetreffende aanbieder met een afweging tussen het veiligheidsrisico enerzijds en beveiligingsniveau anderzijds. Daarbij moet de aanbieder rekening houden met de stand van de techniek en de kosten van uitvoering. Mag deze afweging enerzijds een last voor het bedrijfsleven betekenen, bedacht moet worden dat deze bepaling anderzijds ook de nodige vrijheid geeft. Het stelt de aanbieders in staat diverse netwerken en diensten met elkaar te laten concurreren op het punt van de beveiliging. Dat is niet afwijkend van de reeds bestaande situatie. (…)"[13]

[12] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 39 (MvT).
[13] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 118-119 (MvT).

Blijkens de geschiedenis van artikel 11.2 Tw heeft deze bepaling het karakter van een vangnet:

> "*Artikel 11.2 is geformuleerd als een zorgplichtbepaling. Een dergelijke bepaling heeft door zijn formulering het karakter van een vangnet. De telecommunicatiesector is gebaat bij een adequate bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. Het onvoldoende erkennen van dit belang zou een efficiënte bedrijfsvoering schaden. Door het betrekkelijk gedetailleerde karakter van de bepalingen van hoofdstuk 11 is overigens niet te verwachten dat op artikel 11.2 veel zal moeten worden teruggegrepen.* (…)"[14]

54. In het sanctiebesluit is, gelet op het bovenstaande, artikel 11.2 Tw beschouwd als een vangnetbepaling en artikel 11.3, eerste lid, Tw als een nadere uitwerking van eerstgenoemd artikel ten aanzien van de veiligheid en beveiliging van aangeboden netwerken en diensten. Omdat artikel 11.2 Tw een vangnetbepaling is heeft ACM primair beoordeeld of artikel 11.3, eerste lid, Tw is overtreden.

55. Uit de parlementaire geschiedenis kan verder worden gedestilleerd hoe de wetgever vorm heeft willen geven aan de wijze waarop de in de artikelen 11.2 tot en met 11.3a Tw neergelegde verplichtingen zich onderling tot elkaar verhouden. Deze verplichtingen vertonen een zekere samenhang, maar uit niets blijkt concreet dat de wetgever de betreffende normen beschouwt als communicerende vaten in de door KPN bedoelde zin. Twee voorbeelden van passages die in dit verband relevant zijn luiden als volgt:

> "*Naast genoemde maatregelen* [bedoeld wordt de introductie van de maatregelen zoals neergelegd in het huidige artikel 11.3, tweede lid, Tw, ACM] *blijft op grond van artikel 11.3, derde lid, van de wet (het oude tweede lid van artikel 11.3) voor aanbieders de verplichting bestaan hun abonnees te informeren over bijzondere risico's voor doorbreking van de veiligheid of beveiliging van het aangeboden netwerk of de aangeboden dienst. Daarbij dienen ze tevens aan te geven welke middelen kunnen worden aangewend door de abonnee om die risico's tegen te gaan.* (…)
>
> *Van deze mogelijkheid* [bedoeld wordt de in het huidige artikel 11.3, tweede lid, Tw neergelegde mogelijkheid om aan aanbieders van openbare elektronische communicatiediensten verplichtingen en beperkingen op te leggen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten, ACM] *wordt gebruik gemaakt door in aanvulling op artikel 11.3, eerste en tweede lid, in artikel 11.3,*

[14] *Kamerstukken II* 1997/98, 25 533, nr. 5, p. 120.

vierde lid, een grondslag op te nemen voor het kunnen opleggen van nadere verplichtingen en beperkingen."[15] [onderstreping ACM]

56. Uit het volgende citaat blijkt verder dat de wetgever niet heeft beoogd dat de op aanbieders van openbare elektronische communicatiediensten en/of dito netwerken rustende meldingsplicht (ex artikel 11.3a Tw) iets afdoet aan de reeds eerder van kracht geworden zorgplicht (ex artikel 11.3, eerste lid, jo. artikel 11.2 Tw):

> "*Het doel van de melding bij de toezichthouder is dat deze kan nagaan of de inbreuk gevolgen kan hebben voor de persoonlijke levenssfeer van degene wiens persoonsgegevens het betreft, of de door de aanbieder genomen maatregelen ter bescherming van de persoonsgegevens redelijkerwijs als afdoende konden worden beschouwd en of er aanleiding is de abonnee wiens gegevens het betreft te informeren over de inbreuk.*" [onderstreping ACM]

De meldplicht heeft mede als doel dat de toezichthouder in kennis wordt gesteld van een inbreuk, zodat deze vervolgens kan nagaan of de door de aanbieder getroffen maatregelen ter bescherming van de persoonsgegevens redelijkerwijs als afdoende konden worden beschouwd. Uit niets blijkt dat het naar behoren naleven van de ene verplichting maakt dat de andere verplichting minder snel zal worden overtreden door dezelfde overtreder.

Communicerende vaten

57. KPN betoogt dat de artikelen 11.2, 11.3, 11.3a Tw en 13 Wbp in onderlinge samenhang moeten worden beschouwd, en aldus werken als communicerende vaten. ACM volgt KPN niet in haar stelling dat het feit dat ACM in het sanctiebesluit niet uitvoerig is ingegaan op dit betoog van KPN, een aan het sanctiebesluit klevend motiveringsgebrek oplevert. Het betoog van KPN komt er op neer dat de (herstel)maatregelen die na de hack door haar zijn genomen een mitigerend effect hebben op de geconstateerde gebreken in beveiligingsmaatregelen die KPN voordien heeft getroffen.

58. ACM wijst er nogmaals op dat zij het niet logisch acht dat bedoelde verplichtingen – zonder dat daarvoor een expliciete wettelijke grondslag in het leven is geroepen – werken als communicerende vaten in de door KPN bedoelde zin. De lezing van de onderhavige bepalingen door KPN, door haar aangemerkt als communicerende vaten, zou ook een eigenaardige en ongewenste uitwerking hebben. Feitelijk zou het er op neerkomen dat het

[15] *Kamerstukken II* 2010/11, 32 549, nr. 3, p. 73 (MvT).

betrachten van onvoldoende preventieve zorg (door de aanbieder) voor de veiligheid van persoonsgegevens, minder ernstig is indien de aanbieder achteraf, bij een inbreuk op die beveiliging alsnog passende maatregelen treft.[16] ACM constateert dat voor deze verstrekkende stelling eenvoudigweg ook geen concrete aanknopingspunten zijn te vinden in het positief recht en/of de wetsgeschiedenis.

59. Verder heeft KPN betoogd dat ACM alle door KPN getroffen beveiligingsmaatregelen en onderwerpen had moeten betrekken bij het in haar sanctiebesluit neergelegde oordeel en niet slechts een select aantal zeer concrete beveiligingsonderwerpen dat verband houdt met het onderhavige incident. Hoewel het toepassingsbereik van de in artikel 11.3, eerste lid, jo. artikel 11.2 Tw vastgelegde zorgplicht zich in beginsel ook kan uitstrekken tot bijvoorbeeld herstel- en fysieke maatregelen, betekent dit niet dat een onderzoek naar de mogelijke overtreding van de zorgplicht niet mag zijn toegespitst op bepaalde beveiligingsaspecten, zoals bijvoorbeeld netwerkinrichting. Het onderzoeken van fysieke maatregelen (zoals het hang- en sluitwerk van gebouwen) is in die context eenvoudigweg niet relevant.

60. De herstelmaatregelen die KPN heeft genomen zijn wel onderzocht, hetgeen ACM heeft gebracht tot de conclusie dat die maatregelen op een zodanig wijze zijn getroffen dat in zoverre geen sprake was van een overtreding van de zorgplicht. Als dit niet het geval zou zijn geweest, had dit kunnen leiden tot het oordeel dat nog een separate overtreding zou zijn begaan door KPN, of dat de geconstateerde overtreding ernstiger, omvangrijker en/of langduriger zou zijn geweest.

61. Het geven van richting aan een onderzoek in vorenbedoelde zin geeft op zichzelf geen blijk van willekeur of onzorgvuldigheid. Dit zou slechts anders kunnen zijn als bijvoorbeeld duidelijk ontlastende bewijzen zouden zijn veronachtzaamd of als algemene beginselen van behoorlijk bestuur zouden zijn geschonden, waarvan in het onderhavige geval geen sprake is.

62. KPN stelt verder dat ACM geen onderscheid heeft mogen maken tussen de periode tot de hack (onderzoeksperiode I) en de periode daarna, vanaf de hack (onderzoeksperiode II). Volgens KPN heeft ACM hiermee miskend dat KPN herstelmaatregelen heeft genomen in reactie op de hack. ACM heeft hiermee inbreuk gemaakt op de onderlinge samenhang van de artikelen 11.2, 11.3 en 11.3a, Tw, aldus KPN.[17]

---

[17] Verzoekschrift voorlopige voorziening, randnummer 30.

63. ACM meent dat dit argument evenmin een ander licht op de zaak werpt. De artikelen 11.2 en 11.3 Tw leggen aan aanbieders van openbare elektronische communicatienetwerken en -diensten kortweg een rechtsplicht op om veiligheidsmaatregelen te treffen ter bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de abonnees. En daarnaast legt artikel 11.3a Tw[18] aan die aanbieders de rechtsplicht op om in geval van een inbreuk op die beveiliging, ACM daarvan in kennis te stellen en herstelmaatregelen te nemen.

64. Beide rechtsplichten strekken ter bescherming van de persoonsgegevens en de persoonlijke levenssfeer, maar regelen wel degelijk verschillende onderwerpen. De ene norm ziet op het voorkomen van veiligheidsinbreuken, preventie dus, en de andere norm ziet op de te nemen maatregelen - en de rol van ACM daarbij - indien de preventie niet heeft geholpen en herstelmaatregelen nodig zijn.

Invloed Wet bescherming persoonsgegevens

65. KPN merkt verder in haar bezwaarschrift nog op, dat ACM bij het nemen van het sanctiebesluit zich onvoldoende rekenschap zou hebben gegeven van artikel 13 Wbp.[19] ACM volgt KPN niet in dit betoog.

66. Artikel 11.3 Tw valt aan te merken als lex specialis ten opzichte van de lex generalis, in artikel 13 Wbp. Het Cbp en ACM hebben onderling afgestemd dat ACM het onderhavige onderzoek ter hand zou nemen. Anders dan KPN met haar argument kennelijk veronderstelt, is ACM niet bevoegd bij de uitvoering van de Tw toepassing te geven aan de Wbp (of aan daarop gebaseerde beleidsregels die door een ander bestuursorgaan zijn vastgesteld).

67. Voor de goede orde wijst ACM er nog op dat het sanctiebesluit ook niet in strijd is met die wet, noch met de door het Cbp vastgestelde richtsnoeren. Het is voor ACM overigens onduidelijk in welk opzicht het KPN zou baten als ACM de feiten en omstandigheden van de onderhavige zaak wel concreet zou toetsen aan de door het Cbp vastgestelde richtsnoeren, waarnaar KPN meermaals heeft verwezen.[20] Gelet op de interpretatie van de wettelijke zorgplicht die door ACM wordt gehanteerd en de wijze waarop daaraan in dit geval invulling is gegeven, ziet ACM niet in waarom toetsing aan de minimumnormen van bedoelde richtsnoeren/beleidsregels zou moeten leiden tot de conclusie dat KPN in casu de zorgplicht niet zou hebben overtreden.

[18] De bepaling is in de Tw ingevoegd bij "Wet van 10 mei 2012 tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen", *Stb.* 2012, 235, te raadplegen sinds 4 juni 2012.
[19] Aanvullend bezwaarschrift, randnummers 48 en verder.
[20] Ibidem en zienswijze KPN d.d. 29 augustus 2013, randnummers 92 en verder.

Tussenconclusie

68. Gelet op het voorgaande treffen de door KPN aangevoerde bezwaren tegen de wijze waarop ACM in dit geval artikel 11.3, eerste lid, jo. artikel 11.2 Tw heeft geïnterpreteerd geen doel.

6.1.4 Inrichting onderzoek

Het onderzoek en de gemaakte keuzes

69. Het centrale betoog van KPN is dat ACM bij het nemen van het boetebesluit een doelredenering zou hebben gevolgd.[21] Volgens KPN heeft ACM de vaststelling van de overtreding ten onrechte (uitsluitend) gebaseerd op de hack. ACM zou de door de hack blootgelegde kwetsbaarheden in het systeem van KPN hebben verheven tot de stand van de techniek, waaraan KPN vervolgens had moeten voldoen. KPN stelt eveneens dat ACM haar eigen onderzoek grotendeels heeft gebaseerd op interne onderzoeken van KPN. Volgens KPN zijn alle overtredingen die ACM vaststelt in het bestreden besluit, terug te voeren op het Intern onderzoek Victor en het rapport van Fox-IT.

70. ACM volgt het betoog van KPN niet. Daartoe overweegt ACM als volgt.

71. Op 28 januari 2012 heeft KPN OPTA telefonisch op de hoogte gebracht van de door haar geconstateerde inbreuk op haar netwerk. Op 30 januari 2012 heeft KPN OPTA vervolgens uitgenodigd voor een presentatie over dit beveiligingsincident. Op 10 februari 2012 heeft KPN een update gegeven over de gebeurtenis en de situatie. De aanleiding voor het instellen van het onderzoek voor OPTA was dat er op 16 januari 2012 een inbraak (hack) heeft plaatsgevonden in het [vertrouwelijk] van KPN, waardoor mogelijk de bescherming van persoonsgegevens en de persoonlijke levenssfeer in het geding was geweest. OPTA wilde nagaan in hoeverre KPN aan de zorgplicht heeft voldaan. Op 14 februari 2012 is aan KPN meegedeeld dat het onderzoek naar de naleving van artikel 11.3 Tw was gestart.

72. De hack is aanleiding geweest voor het starten van het onderzoek naar de naleving van artikel 11.3 Tw. Anders dan KPN steeds stelt, is de hack geen onderwerp van het onderzoek geweest. De in het onderzoeksrapport genoemde Onderzoeksperiode I, waarop de boete betrekking heeft (de zogenoemde pleegperiode), omvat zelfs niet eens het moment van de hack. Deze onderzoeksperiode liep immers van september 2010 tot en met 15 januari 2012. De hack vond plaats op 16 januari 2012 en viel daar dus buiten.

[21] Verzoekschrift voorlopige voorziening, randnummers 24 en verder.

73. Het gedeelte van het netwerk van KPN ([vertrouwelijk]) waar de hack heeft plaatsgevonden en de aanwezigheid van persoonsgegevens in het [vertrouwelijk] zijn wel richtinggevend geweest voor de keuzes die in het onderzoek zijn gemaakt. OPTA heeft in het onderzoek 'ingezoomd' op de technische en organisatorische beveiligingsmaatregelen in of met betrekking tot het [vertrouwelijk] in het kader van de bescherming van de daarin opgeslagen elektronische persoonsgegevens en de daarmee gemoeide persoonlijke levenssfeer.

74. In het onderzoek is gekozen voor twee onderzoeksperiodes: 1) een periode voor de hack en 2) een periode na de hack. Het onderzoek richt zich op de maatregelen die KPN heeft getroffen voorafgaand aan het moment van de hack en de maatregelen die KPN nadien heeft getroffen.

75. Beveiliging van elektronische opgeslagen persoonsgegevens valt onder het begrip 'informatiebeveiliging'. Het onderzoek richt zich daarom op de informatiebeveiliging bij KPN en dan (in dat kader) alleen op de aspecten integriteit en vertrouwelijkheid van persoonsgegevens.

76. Artikel 11.3, eerste lid, Tw verplicht aanbieders passende technische en organisatorische maatregelen te treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. In dit artikel zijn geen specifieke maatregelen vermeld waaraan een aanbieder zou moeten voldoen. In het onderzoek is gekozen voor beveiligingsonderwerpen[22] die in vakliteratuur als algemeen geldend worden aanvaard. Ook is gekeken naar op dat moment geldende ISO-normen.

77. De gekozen beveiligingsonderwerpen raken ook direct aan de hack. Dit blijkt ook uit de gesprekken die gevoerd zijn met de medewerkers van KPN gedurende het onderzoek.[23] Ten aanzien van de andere beveiligingsonderwerpen die volgens KPN door ACM onterecht niet zijn onderzocht, is ACM van oordeel dat deze (mogelijk) wel aan de 'zorgplicht' raken, maar niet relevant zijn voor de beoordeling van de beveiliging en bescherming van inbreuken vanaf het internet. OPTA heeft haar onderzoek zo ingericht dat het (mogelijke) achterliggende probleem – dat ten grondslag ligt aan de hack – wordt geadresseerd. Onderwerpen die daar evident geen weerslag op hebben gehad, zijn daarom bewust niet onderzocht.

78. Zoals in het bovenstaande is omschreven, zijn er keuzes gemaakt bij de aanvang van het onderzoek. Op basis van de gemaakte keuzes heeft OPTA informatie gevorderd bij KPN. Zo

[22] De gekozen beveiligingsonderwerpen: 1) het opstellen en handhaven van beveiligingsbeleid, 2) netwerkinrichting, 3) afscherming, 4) netwerk- en systeembewaking, en 5) patchmanagement.
[23] O.a. bijlagen ACM 5 en 7 t/m 10 bij het onderzoeksrapport.

heeft OPTA op 18 februari 2013 informatie gevorderd bij KPN over de vijf beveiligingsonderwerpen.[24] KPN had toen het Intern onderzoek Victor nog niet overgelegd. Naast de informatievorderingen heeft OPTA tijdens het onderzoek ook gesprekken gevoerd met medewerkers van KPN over de vijf beveiligingsonderwerpen. Op grond van de feiten en gegevens die tijdens het onderzoek zijn vergaard, heeft OPTA vervolgens de conclusie gebaseerd dat KPN ten aanzien van vijf beveiligingsonderwerpen geen of onvoldoende passende technische en organisatorische maatregelen heeft getroffen. De bevindingen in het rapport zijn, anders dan KPN stelt, niet uitsluitend gebaseerd op de interne onderzoeken van KPN.[25] De interne onderzoeken hebben eerdere bevindingen bevestigd.

79. Dat de bevindingen in het rapport niet uitsluitend zijn gebaseerd op de interne onderzoeken van KPN blijkt overigens eveneens uit de getalsmatige verhouding van de verschillende verwijzingen naar onderliggende stukken in het onderzoeksrapport. In de voetnoten van het onderzoeksrapport wordt slechts in een klein aantal gevallen verwezen naar het rapport van Fox-IT en het Intern onderzoek Victor; namelijk in minder dan een kwart van de gevallen.[26] Het onderzoeksrapport is grotendeels gebaseerd op informatie die KPN heeft verstrekt naar aanleiding van informatievorderingen van OPTA en interviews die OPTA met medewerkers van KPN heeft gehouden.

Beveiligingsonderwerpen

80. KPN neemt verder ten onrechte aan dat het onderhavige onderzoek is gebaseerd op slechts één literatuurbron (de CISSP All-in-One – Exam Guide), en dat geen verder onderzoek is gedaan naar de stand van de techniek en wat een “passend beveiligingsniveau” is. Voor de algemene beschrijving van organisatorische en technische maatregelen in de hoofdstukken 9 tot en met 13 van het onderzoeksrapport zijn immers standaarden, normen en vakliteratuur op het gebied van informatiebeveiliging binnen informatietechnologie gebruikt. In deze

[24] In de punten 8 tot en met 10 de documentatie gevorderd waarin voor [vertrouwelijk] en haar twee voorgangers het beveiligingsbeleid is vastgelegd, waaronder: (…) *het beleid ten aanzien van netwerk beheer, software beheer, patch management, logging, intrusion detection, firewall en filtering, hardening en beveiliging van digitaal opgeslagen gegevens* (…).
[25] Fox-IT en het Intern onderzoek Victor.
[26] In de voetnoten van het onderzoeksrapport is 200 maal verwezen naar het onderzoeksmateriaal, d.w.z. het door KPN op vordering geleverde materiaal, de gespreksverslagen van ACM, literatuurverwijzingen en overig onderzoeksmateriaal. Daarbij ging het in 29 gevallen om verwijzingen naar het Intern onderzoek Victor en in 18 gevallen naar het rapport van Fox-IT. (Literatuurverwijzingen: 20 en onderzoeksmateriaal [anders dan Victor en Fox-IT]: 133.) Minder dan een kwart van de verwijzingen betrof derhalve de rapporten Victor en Fox-IT.

hoofdstukken wordt in de inleidende paragrafen ter duiding van de stand der techniek[27] en de beschrijving van het onderwerp verwezen naar onderstaande werken.

- NEN–ISO 27001: Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2005,IDT), november 2005.
- NEN-ISO 27002: *Code voor informatiebeveiliging (ISO/IEC 27002:2005,IDT)*, november 2007.
- National Institute of Standards and Technology (NIST) Special Publication 800-92: *Guide to Computer Security Log Management*, 2006.
- National Institute of Standards and Technology (NIST) Special Publication 800-94: *Guide to Intrusion Detection and Prevention Systems (IDPS)*, 2007.
- S. Harris, *CISSP® All-in-One Exam Guide*, Fifth Edition, 2010.[28]
- C.P. Pfleeger & S.L. Pfleeger, *Security in Computing*, Fourth Edition, 2006.[29]

81. In het navolgende zullen de vijf beveiligingsonderwerpen waaraan ACM de door KPN in onderzoekperiode I getroffen beveiligingsmaatregelen heeft getoetst, in samengevatte vorm worden behandeld.[30]

82. De constatering uit het onderzoeksrapport dat adequaat beveiligingsbeleid een algemeen geldend en aanvaard onderdeel van informatiebeveiliging is, is mede gebaseerd op één of meer van de genoemde bronnen.[31] In dat verband wordt er op gewezen dat het opstellen, onderhouden en in de organisatie beleggen van informatiebeveiligingsbeleid een algemeen aanvaarde organisatorische maatregel is. Beveiligingsbeleid is echter pas effectief indien het aan bepaalde vereisten voldoet.

[27] Met betrekking tot de gebruikte vakliteratuur is gekozen voor de op 15 januari 2012 beschikbare uitgaven en geldende normen en standaarden.
[28] Certified Information Systems Security Professional (CISSP) is een internationaal erkende studie en titel op het gebied van informatiebeveiliging.
[29] Dit is academisch materiaal m.b.t. informatiebeveiliging binnen de faculteit Informatica van de Open Universiteit.
[30] In het onderzoeksrapport worden deze onderwerpen uitvoeringer behandeld (zie de paragrafen 9.1, 10.1, 11.1, 12.1 en 13.1).
[31] Onderzoeksrapport, paragraaf 9.1. In die paragraaf wordt ook de stand van de techniek inzake beveiligingsbeleid (onder verwijzing naar technische ISO-standaarden en vakliteratuur) geschetst.

83. Uit vakliteratuur en (NEN-)ISO-normen blijkt dat het informatiebeveiligingsbeleid van een organisatie – wil het succesvol zijn – bekend moet zijn en toegepast moet worden in alle lagen en onderdelen van de organisatie waar dit beleid een rol speelt. Vervolgens is het ook noodzakelijk dat het informatiebeveiligingsbeleid binnen de organisatie wordt gehandhaafd. Hierbij is het van belang dat de organisatie eveneens consequenties verbindt aan het niet of onvoldoende opvolgen van het informatiebeveiligingsbeleid.[32]

84. Er is geen sprake van het hanteren van een onredelijk strenge maatstaf.[33] Indien informatiebeveiligingsbeleid niet naar behoren bekend is gemaakt en in de organisatie is toegepast, kan dit beleid überhaupt niet effectief zijn. Gelet op het voorgaande behoort het opzetten en handhaven van een beveiligingsbeleid naar het oordeel van ACM tot de te treffen passende maatregelen (ter bescherming van persoonsgegevens en ter bescherming van de persoonlijke levenssfeer van abonnees en gebruikers) ten behoeve van de veiligheid en beveiliging van de door een provider aangeboden netwerken en diensten in de zin van artikel 11.3, eerste lid, Tw.

85. ACM constateert tevens dat adequate netwerkinrichting een algemeen geldend en aanvaard onderdeel van informatiebeveiliging is.[34] Met de inrichting van een netwerk in beveiligingszones, het beheer van de netwerkinrichting, en het juiste gebruik van IP-adressen (onderscheid tussen private en publieke IP-adressen; geen dubbel gebruik van IP-adressen) kan mede de toegang tot systemen op een netwerk en binnen een netwerk worden gefaciliteerd of juist worden geblokkeerd. Daarom concludeert ACM dat deze maatregelen ook een beschermende werking hebben ten aanzien van de gegevens die in de systemen van het betreffende netwerk zijn opgeslagen.

86. Verder wijst ACM er op dat onderdeel van die gegevens persoonsgegevens kunnen zijn van abonnees en gebruikers van de diensten die over dat netwerk worden aangeboden. Het risico van het niet (naar behoren) nemen van de in het vorige randnummer genoemde maatregelen is dat de betreffende persoonsgegevens in handen vallen van derden en dat hierdoor de

[32] Onderzoeksrapport, paragraaf 9.1. In randnummer 113 van dat rapport wordt verwezen naar Harris, die hierover onder meer het volgende opmerkt: "*For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization.*(…) *To be useful,* [security policies, standards, procedures, baselines, and guidelines, toevoeging ACM] *must be put into action. No one is going to follow the rules if people don't know the rules exist. Security policies and the items that support them not only must be developed, but must also be implemented and enforced.*" (S. Harris, *CISSP® All-in One – Exam Guide*, fifth edition, McGraw Hill, p. 102 en p. 109-110).
[33] Dit geldt overigens ook voor de in het navolgende te bespreken maatregelen in het kader van informatiebeveiliging (netwerkinrichting, afscherming, netwerk- en systeembewaking en patchmanagement).
[34] Onderzoeksrapport, paragraaf 10.1. In die paragraaf wordt ook de stand van de techniek inzake netwerkinrichting (onder verwijzing naar vakliteratuur) geschetst.

persoonlijke levenssfeer van de betrokken personen wordt geschaad. Daarom behoren het verdelen van een netwerk in verschillende beveiligingszones, het beheer van de netwerkinrichting en het juiste gebruik van IP-adressen naar het oordeel van ACM tot de te treffen passende maatregelen ten behoeve van de veiligheid en beveiliging van de door een provider aangeboden netwerken en diensten in de zin van artikel 11.3, eerste lid, Tw.

87. Ook heeft ACM vastgesteld dat adequate afscherming een algemeen geldend en aanvaard onderdeel van informatiebeveiliging is.[35] Duidelijk is dat een netwerk dat met het (openbare) internet is verbonden een bepaalde mate van afscherming moeten hebben om te voorkomen dat systemen op dat netwerk vanaf het internet te benaderen zijn. Deze netwerkafscherming wordt doorgaans een firewall genoemd (een basale vorm daarvan wordt ook wel aangeduid met de afkorting ACL [Access Control List]). Een firewall kan ook gebruikt worden om binnen een netwerk verschillende sub-netwerken van elkaar af te schermen. Bepaalde verkeersstromen zullen door een firewall worden tegengehouden, andere verkeersstromen zullen worden toegelaten tot het netwerk.

88. Om de beschermingsfunctie van de firewall effectief te laten zijn, zal al het verkeer tussen het interne netwerk en het internet moeten lopen via de firewall. Van het reguleren van de toegang tot systemen op een netwerk en binnen een netwerk door middel van firewalls en ACL's, gaat ook een beschermende werking uit voor de gegevens die op deze systemen zijn opgeslagen, zoals persoonsgegevens. Hetzelfde kan gesteld worden met betrekking tot 'fencing', hetgeen het gebruik van ACL's betreft waarbij niet de verkeersstromen van een heel netwerk worden gecontroleerd, maar per individueel systeem wordt bepaald voor welke dienst met welk ander individueel systeem datapakketten mogen worden uitgewisseld. Daarom behoren het toepassen van firewalls, ACL's en fencing naar het oordeel van ACM tot de te treffen passende maatregelen ten behoeve van de veiligheid en beveiliging van de door een provider aangeboden netwerken en diensten in de zin van artikel 11.3, eerste lid, Tw.

89. Verder constateert ACM dat adequate netwerk- en systeembewaking ook een algemeen geldend en aanvaard onderdeel van informatiebeveiliging is.[36] In dit kader wordt er op gewezen dat bij een aanval van buitenaf op het netwerk door een hacker het hele stelsel van beveiligingsmaatregelen van een netwerk op de proef wordt gesteld. Onder deze beveiligingsmaatregelen vallen ook de beschermingsmaatregelen van persoonsgegevens van

[35] Onderzoeksrapport, paragraaf 11.1. In die paragraaf wordt ook de stand van de techniek inzake afscherming (onder verwijzing naar vakliteratuur) geschetst.
[36] Onderzoeksrapport, paragraaf 12.1. In die paragraaf wordt ook de stand van de techniek inzake netwerk- en systeembewaking (onder verwijzing naar vakliteratuur) geschetst.

abonnees en gebruikers van diensten die over die netwerken worden aangeboden. Verder wordt opgemerkt dat het risico van het achterwege laten van deze maatregelen, is dat beveiligingsinbreuken niet worden opgemerkt. Hierdoor kan een hacker ongezien zijn gang gaan, hetgeen tot gevolg heeft dat de betreffende persoonsgegevens in handen kunnen vallen van derden en dat deze hierdoor de persoonlijke levenssfeer van de betrokken personen schaden.

90. Omdat niet uitgesloten is dat de beveiliging van systemen en/of netwerken doorbroken kan worden (of doorbroken dreigt te worden), is het van belang dat de set van beveiligingsmaatregelen ook netwerk- en systeembewaking omvat om problemen tijdig te detecteren. Daarbij kan gedacht worden aan logmanagement, intrusion detection, intrusion prevention en monitoring. Alleen op die manier kan door de netwerkbeheerder actie ondernomen worden om de doorbreking van de bescherming van persoonsgegevens te voorkomen, dan wel acties te ondernemen om de schadelijke gevolgen van het doorbreken van de beveiliging van persoonsgegevens zo beperkt mogelijk te houden. Gelet op het voorgaande is ACM van oordeel dat logmanagement (waaronder centrale logging), intrusion detection systems, intrusion prevention systems en monitoring behoren tot de te treffen passende maatregelen ten behoeve van de veiligheid en beveiliging van de door een provider aangeboden netwerken en diensten in de zin van artikel 11.3, eerste lid, Tw.

91. Tot slot wijst ACM er nog op dat zij ten aanzien van adequaat patchmanagement ook heeft geconstateerd dat deze maatregel een algemeen geldend en aanvaard onderdeel van informatiebeveiliging is.[37] Bij vrijwel alle programmatuur wordt regelmatig geconstateerd dat er kwetsbaarheden in zitten. Deze kwetsbaarheden bieden de mogelijkheid om programmatuur anders te gebruiken dan de bedoeling is en maken het bijvoorbeeld mogelijk om de afscherming van gevoelige gegevens zoals persoonsgegevens te doorbreken. Dit zorgt voor een altijd aanwezig veiligheidsrisico. Per jaar worden wereldwijd duizenden kwetsbaarheden in software ontdekt. Om kwetsbaarheden in software te verhelpen publiceren leveranciers regelmatig zogenoemde 'security patches'.[38] Een (professionele) gebruiker van software zal een proces moeten hebben om zelf actief op de hoogte te blijven van de patches die verschijnen voor alle software die hij gebruikt (bijvoorbeeld door het gebruik van speciale scan-software). Daarnaast zal er een proces moeten zijn voor het omgaan met de verschenen patches (daarbij hoort het analyseren van de risico's van de kwetsbaarheid, het testen van de

[37] Onderzoeksrapport, paragraaf 13.1. In die paragraaf wordt ook de stand van de techniek inzake patchmanagement (onder verwijzing naar vakliteratuur) geschetst.

[38] Na het uitvoeren van de security patch worden de kwetsbaarheden opgeheven.

patch, het maken van de afweging om de patch te installeren en de tijdsperiode waarbinnen zich dit allemaal moet afspelen). Verder moet worden bijgehouden welke patches er al dan niet geïnstalleerd zijn op welke systemen.

92. Een onderneming met deugdelijk patchmanagement heeft inzicht in de actuele stand van kwetsbaarheden van de gebruikte software en systemen en in de door de onderneming reeds toegepaste patches. Daarbij dient een onderneming te zorgen voor het invoeren van de noodzakelijke patches en bewaakt zij dat dit patchen zo min mogelijk verstoringen of bijvoorbeeld beveiligingsrisico's voor de bescherming van persoonsgegevens met zich brengt. Een onderneming die haar patchmanagement op orde heeft, draagt daarmee bij aan de bescherming van de elektronisch opgeslagen persoonsgegevens op haar systemen. Daarom is ACM van oordeel dat patchmanagement behoort tot de te treffen passende maatregelen ten behoeve van de veiligheid en beveiliging van de door een provider aangeboden netwerken en diensten in de zin van artikel 11.3, eerste lid, Tw.

93. ACM heeft de stand van de techniek dan ook wel degelijk zelf onderzocht door vast te stellen wat algemeen geldende en aanvaarde onderdelen zijn van informatiebeveiliging. ACM heeft vervolgens normen gehanteerd die in de betrokken beroepsgroep, bedrijfssector en onder deskundigen gebruikelijk zijn. Aldus heeft ACM – in tegenstelling tot wat KPN daarover beweert – de maatregelen die KPN heeft getroffen, getoetst aan die concrete en basale normen.

CISSP

94. Volgens KPN is de door ACM gehanteerde literatuurbron CISSP een Amerikaanse certificering gebaseerd op een zelfstudie voor operationele systeembeveiligers. KPN meent dat de CISSP niet één-op-één bruikbaar is voor invulling van de zorgplichtnorm in de Tw, omdat de materie vanwege de Amerikaanse origine vrij stellig en operationeel is ingestoken. Ook bestaat veel kritiek vanwege de inflexibiliteit van de gehanteerde regels.

95. Een eenvoudige zoekopdracht ('KPN CISSP') op internet levert de volgende resultaten op:

'KPN Consulting biedt de cursus aan, die je op weg helpt binnen de omvangrijke lesstof van CISSP. Bij KPN zelf, als toonaangevende leverancier van 'Security Solutions'. Zijn als zo'n 100 CISSP certified securtiy professionals werkzaam.'

en

'De CISSP certificering is wereldwijd erkend als DE standaard om aan te tonen dat u beschikt over de noodzakelijke kennis op het vakgebied informatiebeveiliging.'

96. Uit de boven aangehaalde teksten blijkt duidelijk dat KPN de CISSP beschouwt als een bruikbare standaard voor informatiebeveiliging. De opmerking over de CISSP die KPN heeft gemaakt in haar bezwaarschrift kan ACM derhalve niet plaatsen.

Maatregelen per beveiligingsonderwerp

97. Om vast te stellen of KPN artikel 11.3, eerste lid, Tw heeft voldaan, is onderzocht of de getroffen maatregelen per beveiligingsonderwerp door KPN voldoende zijn geweest om de veiligheid en beveiliging van haar netwerk in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers te kunnen waarborgen. In het onderzoek heeft ACM de getroffen maatregelen per beveiligingsonderwerp getoetst aan de algemeen geldende en aanvaarde normen in de informatiebeveiliging. Anders dan KPN stelt, heeft ACM haar uitkomsten van de toetsing niet verheven tot de stand der techniek. ACM heeft de door KPN getroffen beveiligingsmaatregelen getoetst aan de minimale eisen die volgen uit de beveiligingsonderwerpen, en vastgesteld of daaraan in voldoende mate was voldaan. ACM heeft geen strengere normen gesteld noch beweerd dat de beveiliging van het netwerk waterdicht moet zijn. Het is aan de aanbieders zelf een adequate invulling te geven aan de zorgplicht.

98. De vijf beveiligingsonderwerpen zijn afzonderlijk in het onderzoeksrapport behandeld en per onderwerp heeft ACM informatie gevorderd bij KPN en gesprekken gevoerd met de medewerkers van KPN. Op basis van deze informatie heeft ACM onderzocht hoe de verschillende beveiligingsonderwerpen in de organisatie van KPN waren geïmplementeerd, en vervolgens is beoordeeld in hoeverre KPN uitvoering heeft gegeven aan de maatregelen die zij volgens haar eigen beleid zou moeten treffen.

99. Ten aanzien van het beveiligingsbeleid heeft ACM vastgesteld dat KPN haar beleid ter zake hiërarchisch heeft opgebouwd; van abstract beleid naar uitwerking in gedetailleerde documenten.[39] ACM heeft tijdens het onderzoek informatie gevorderd over de wijze waarop KPN haar beveiligingsbeleid vormgaf en daaraan uitvoering gaf. Uit de informatie van KPN is gebleken dat het beveiligingsbeleid een onderdeel vormt van haar informatiebeveiliging.

100. KPN heeft voor haar beveiligingsbeleid grotendeels de ISO-normen 207001 en 207002 als

[39] Bijlage KPN 5 bij het Onderzoeksrapport.

uitgangspunten gehanteerd. Het meer concrete beveiligingsbeleid (de implementatie daarvan) is bij KPN decentraal belegd. Het beveiligingsbeleid schrijft voor dat wanneer afgeweken wordt van het (centrale) beleid, door het betrokken management toegelicht moet worden waarom daarvan wordt afgeweken. Dit moet ook worden vastgelegd.

101. KPN stelt in dit verband dat ACM het voeren van een centraal beleid als norm heeft gesteld. ACM heeft zich echter nimmer op het standpunt gesteld dat het voeren van een centraal beveiligingsbeleid een vereiste is op grond van artikel 11.3 Tw. KPN heeft juist de vrijheid om zelf een invulling eraan te geven. ACM heeft in het onderzoek informatie gevorderd over de wijze waarop KPN het beveiligingsbeleid heeft opgesteld en hoe zij uitvoering aan het beleid heeft gegeven.

102. Op basis van de verstrekte informatie heeft ACM vastgesteld dat KPN niet of niet conform haar eigen beleid heeft gehandeld. Volgens KPN was de verantwoordelijkheid voor het onderhouden en uitdragen van het informatiebeveiligingsbeleid belegd bij de afdeling [vertrouwelijk]. Dit blijkt echter niet uit de stukken die KPN in dit verband heeft verstrekt. Hoewel volgens KPN voor iedereen volkomen duidelijk was dat de verantwoordelijkheid voor het beveiligingsbeleid en de bijbehorende documentatie tussen augustus 2011 en 15 januari 2012 bij de [vertrouwelijk] lag, blijkt dit niet uit de stukken die KPN desgevraagd heeft overgelegd. ACM constateert dan ook dat KPN de verantwoordelijkheid voor het centrale informatiebeleid in elk geval op papier niet goed had geregeld.

103. Uit het centrale beveiligingsbeleid van KPN blijkt verder dat het beleid jaarlijks geëvalueerd moet worden. Uit het overzicht van beleidsdocumenten heeft ACM vastgesteld dat KPN het beleid niet jaarlijks heeft geëvalueerd. KPN stelt dat het wel gebeurd is, maar dat niet iedere evaluatie leidt tot aanpassing van de documenten en of de versie-gerelateerde datum daarvan. Op basis van de informatie die KPN heeft verstrekt kan ACM geen andere conclusie trekken dan dat niet uit de overgelegde informatie blijkt dat jaarlijks een evaluatie heeft plaatsgevonden.

104. Verder heeft ACM vastgesteld dat KPN voor patchmanagement geen beleid had vastgesteld. Dit heeft een medewerker van KPN ook bevestigd.[40] Dit blijkt ook uit een van de aanbevelingen van Fox-IT aan KPN. KPN heeft als bijlage bij het bezwaarschrift een overzicht overgelegd met data waarop KPN patches heeft uitgevoerd. Hieruit blijkt echter niet welk beleid KPN hanteert voor het patchmanagement. Bedoeld overzicht toont enkel aan dat KPN

[40] Bijlage ACM 9 bij het onderzoeksrapport.

op bepaalde data gepatcht heeft. Behalve dat er op centraal niveau geen beleid was voor het uitvoeren van patches, heeft KPN op decentraal niveau ook geen aantoonbaar beleid gevoerd.

105. Anders dan KPN stelt, heeft ACM niet de verplichting aan KPN opgelegd dat zij een centraal patchbeleid moet hebben. Wel heeft KPN deze verplichting aan zichzelf opgelegd.[41] ACM heeft op basis van de verstrekte informatie van KPN geconstateerd dat KPN de keuzes voor het wel of niet doorvoeren van patches en wel of niet nemen van andere maatregelen niet heeft vastgelegd. De vastlegging van de gemaakte keuzes is een wezenlijk onderdeel van de informatiebeveiliging.

IP-adressen

106. In het onderzoek heeft ACM op basis van de verstrekte informatie door KPN geconstateerd dat KPN aan meer systemen in haar netwerk ([vertrouwelijk] en de [vertrouwelijk]) een publiek IP-adres had gekoppeld, waardoor deze in beginsel in directe verbinding kunnen staan met het internet.[42] KPN stelt naar aanleiding van deze constatering dat het gebruik van publieke IP-adressen in haar interne netwerken helemaal niet hoeft te leiden tot een 'security risico'.

107. KPN miskent hiermee dat het voorgaande in het licht moet worden gezien van hetgeen door ACM is geconstateerd ten aanzien van de door KPN gehanteerde afschermingsmaatregelen ten tijde van Onderzoeksperiode I.[43] De geconstateerde onvoldoende, of niet genomen maatregelen in de netwerkinrichting en afscherming verhogen het risico van het gebruik van publieke IP-adressen in het private deel van het netwerk. Hierdoor kan de situatie ontstaan dat de desbetreffende machine(s) ongewild en onbewust in direct contact staat/staan met het internet. Het ontbreken van voldoende monitoring en logging, maakt dit bovendien een onzichtbaar risico. Ook KPN onderschrijft in haar bezwaarschift het verband tussen maatregelen onder de verschillende beveiligingsonderwerpen.[44] KPN stelt hier terecht dat het gebruik van publieke IP-adressen in haar private netwerk geen risico hoeft te zijn wanneer (de juiste) maatregelen zijn genomen in de netwerkinrichting (routering) en afscherming (firewall, ACL).

---

[41] Bijlage KPN 15 bij het onderzoeksrapport, regel 155 in de spreadsheet. De maatregelen met een '1' in de kolom 'Baseline KPN Group' maken onderdeel uit van het centrale beleid (vandaar het gebruik van de term 'baseline: minimum'). Het woord patchmanagement komt hierin letterlijk voor, maar de tekst dekt (ook) deze dit beveiligingsonderwerp: "*Er moet tijdig informatie worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten geschikte maatregelen worden genomen voor behandeling van daarmee samenhangende risico's.*"
[42] Onderzoeksrapport, randnummers 195 en 196.
[43] Onderzoeksrapport, randnummers 229-233.
[44] Bezwaarschrift KPN, randnummer 81.

108. Het gebruik van publieke IP-adressen voor interne netwerken is weliswaar niet zonder meer ontoelaatbaar, maar het gebruik van publieke IP-adressen in interne netwerken in samenhang bezien met het niet of onvoldoende nemen van maatregelen op het gebied van andere beveiligingsonderwerpen – zoals afschermingsmaatregelen – levert wel een verhoogd risico op met betrekking tot het toegankelijk worden van de betrokken systemen via het (openbare) internet. Als afschermingsmaatregelen geen of onvoldoende beveiliging bieden, zoals in dit geval is geconstateerd, kan een onbevoegde derde zichzelf direct toegang verschaffen tot het interne netwerk van KPN met gebruikmaking van een publiek IP-adres. Dat publieke adres kan ten volle door kwaadwillende derden worden benut als het niet voldoende van het openbare internet is afgeschermd, en biedt aldus een (extra) ingang in de systemen op de netwerken van bedrijven als KPN. ACM volgt KPN dan ook niet in haar betoog dat het gebruik van publieke IP-adressen in haar netwerkonderdelen geen (extra) beveiligingsrisico's met zich heeft kunnen brengen.

Cyberaanvallen

109. Tot slot wijst ACM er in dit verband nog op dat KPN stelt dat haar netwerk dagelijks met 26.000 zogenoemde cyberaanvallen wordt geconfronteerd. Volgens ACM kan ook die stelling echter evenmin leiden tot het herroepen van de bestreden besluiten.

110. ACM verwijst hiertoe om te beginnen naar de overgelegde verklaringen van KPN-medewerker [vertrouwelijk] van 28 augustus 2013. Uit die verklaring blijkt duidelijk dat het genoemde aantal uiterst onzeker is en tot stand is gekomen onder een reeks van rekenkundige aannamen. Verder is van de zijde van KPN verklaard dat met 26.000 aanvallen feitelijk (ook) scans worden bedoeld, zodat in dat totaal ook het volautomatisch via internet 'aftasten' van de systemen en netwerken van KPN is begrepen.[45]

111. Indien KPN met haar stelling van de 26.000 aanvallen bedoelt te betogen dat haar netwerk wel degelijk naar behoren was beveiligd, kan dat betoog niet slagen. ACM heeft aan de hand van de bewijsmiddelen in het dossier immers op goede gronden vastgesteld dat die beveiliging te wensen overliet.[46]

[45] Zie: Verslag hoorzitting bezwaarfase, p. 8.
[46] Pagina 1, vierde, alinea: "…*programs to exploit this weakness are freely available on the internet*." Pagina 2, laatste alinea: "*We currently do not believe that this was an advanced, directed attack against KPN* (…)" Pagina 3, eerste alinea onder punt 3: "*The download and installation of a fairly recognizable malicious program on a very large number of systems is also not something an intruder would do who is perpetrating a directed attack against KPN and is trying to stay undetected for as long as possible*." Pagina 3, tweede alinea: "*He has claimed in the press that he sought help from friends* (…) *to gain more access*."

Tussenconclusie

112. Op grond van het vorenstaande blijft ACM bij haar standpunt dat KPN per beveiligingsonderwerp, en zeker ook als deze in onderlinge samenhang worden bezien, niet of onvoldoende maatregelen heeft getroffen om haar netwerk te beschermen tegen inbreuken. Daarmee heeft KPN niet voldaan aan de op haar rustende zorgplicht op grond van artikel 11.3, eerste lid, jo. artikel 11.2 Tw.

6.2 Opleggen sanctie

Opleggen bestraffende sanctie opportuun

113. ACM volgt KPN niet in haar betoog dat in dit geval geen boete had kunnen worden opgelegd voor het overtreden van de zorgplicht (zoals neergelegd in artikel 11.3, eerste lid, jo. artikel 11.2 Tw) omdat hiervoor voor het eerst een boete wordt opgelegd en deze norm niet is uitgewerkt door ACM in beleidsregels.[47]

114. Volgens vaste jurisprudentie vereist het systeem van open normen niet dat alle normen tot in detail vooraf in een algemeen verbindend voorschrift of beleidsregels hoeven te worden vastgelegd.[48] Er hoeft niet steeds sprake te zijn van een door de overheid vooraf gegeven norm. Door het bestuursorgaan kan bij de invulling van een open norm ook worden aangehaakt bij normen die in de betrokken beroepsgroep, of bedrijfssector, dan wel bij normen die onder deskundigen gebruikelijk zijn.[49] Dit heeft ACM in dit geval ook gedaan.

115. Bij het voorgaande moet ook niet uit het oog worden verloren dat de wetgever soms met een zekere vaagheid, bestaande in het bezigen van algemene termen, delicten omschrijft om te voorkomen dat gedragingen die strafwaardig zijn, buiten het bereik van de delictsomschrijving vallen. Die vaagheid kan onvermijdelijk zijn, omdat niet altijd te voorzien is op welke wijze de te beschermen belangen in de toekomst zullen worden geschonden en omdat – indien dit wel is te voorzien – delictsomschrijvingen anders te verfijnd worden met als gevolg dat de overzichtelijkheid wegvalt en daarmee het belang van de algemene duidelijkheid van de wetgeving schade lijdt. Indien het om professionele marktdeelnemers gaat, mag worden verlangd dat deze zich terdege laten informeren over de beperkingen waaraan hun

[47] Aanvullend bezwaarschrift, randnummers 4 en 84.
[48] Zie onder meer CBb 24 augustus 2006, AB 2007, 321 en CBB 1 april 2008, LJN PC8268. In laatstgenoemde zaak overwoog het CBb dat van een marktpartij als het ABP mocht worden verwacht dat zij zich op de hoogte zou stellen van het doel en de reikwijdte van de betrokken bepaling en dat zij bij onduidelijkheid daarover zich zou informeren bij de toezichthouder, in die zaak DNB.
[49] Vgl. bijv. ABRvS 7 augustus 2002, *AB* 2003, 176, ABRvS 15 november 2006, *AB* 2007, 266 en CBb 3 december 2003, *AB* 2004, 189.

gedragingen zijn onderworpen.[50]

116. ACM is van oordeel dat KPN kan worden beschouwd als professionele marktdeelnemer in vorenbedoelde zin, die een voldoende begrip heeft – althans behoort te hebben – van veiligheidsnormering van netwerken. De zorgplicht in de Tw is in dat verband voldoende concreet en kenbaar geformuleerd zodat KPN daaruit af heeft kunnen leiden wat haar in het kader van die verplichting te doen stond.

117. Ook volgt ACM de opvatting van KPN niet, dat in dit geval een waarschuwing of herstelmaatregel, zoals een last onder dwangsom, meer voor de hand zou hebben gelegen dan het opleggen van een boete.[51] Een door KPN bedoelde alternatieve sanctie, zoals het bij last onder dwangsom opleggen van een herstelplicht, zou in dit geval geen logische optie zijn, omdat KPN in de weken na de hack voortvarende herstelmaatregelen heeft getroffen, en ACM niet over concrete aanwijzingen beschikte dat sprake was van een voortdurende overtreding van de zorgplicht of een dreigende herhaling daarvan.

118. Verder wijst ACM er in dit verband nog op dat OPTA in 2007 – na een openbare consultatie – op verzoek van marktpartijen, waaronder KPN,[52] heeft besloten (voorlopig) af te zien van het opstellen van beleidsregels inzake artikel 11.3 Tw. KPN stelde zich toentertijd op het standpunt dat dergelijke beleidsregels zouden leiden tot een onwenselijke fixatie en juridisering van de praktijk. Ook in dat opzicht valt aan ACM de afwezigheid van zulke beleidsregels niet tegen te werpen.

119. Gelet op het voorgaande komt ACM tot de conclusie dat de bezwaren van KPN gericht tegen het opleggen van de boete geen doel treffen.

Hoogte boete passend

120. Het argument van KPN dat de boete onredelijk hoog zou zijn, slaagt evenmin. Op grond van de Boetebeleidsregels ACM hadden aan KPN voor overtreding van de zorgplicht en de medewerkingsplicht afzonderlijke boetes van EUR 300.000, in totaal dus EUR 600.000, kunnen worden opgelegd.[53] De haar door ACM uiteindelijk opgelegde totale boete van EUR 364.000 is in dat opzicht niet onredelijk.

---

[50] Zie overweging 4 van de noot van O.J.D.M.L. Jansen bij CBb 24 augustus 2006, *AB* 2007, 321.
[51] Aanvullend bezwaarschrift, randnummer 83.
[52] Brief van KPN van 13 september 2007, kenmerk R/07/U/120.
[53] Artikel 3.10 van de Boetebeleidsregels ACM.

121. Zoals eerder in deze beslissing aan de orde is gesteld, is de basisboete voor de overtreding van de zorgplicht in dit geval vastgesteld op EUR 280.000, gelet op de duur van de overtreding (anderhalf jaar), en de mate waarin de overtredingen aan KPN kunnen worden verweten. KPN heeft immers meer waarschuwingssignalen over kwetsbaarheden in de beveiliging van het netwerk, voorafgaand aan de hack, genegeerd.[54] ACM is daarom van oordeel dat oplegging van een boete passend en geboden is, die het maximum benadert van de ingevolge artikel 3.10 van de Boetebeleidsregels ACM toepasselijke bandbreedte van EUR 0 - 300.000. ACM merkt op dat KPN geen bezwaar heeft gemaakt tegen de toegepaste boeteverhogende omstandigheid.

122. Aldus heeft ACM – gelet op eerdergenoemde omstandigheden – vastgesteld dat oplegging van een boete van EUR 280.000 passend is. Dit betekent niet dat ACM, terug redenerend van het maximum van EUR 300.000, heeft besloten dat het toepassen van een korting van EURO 20.000 passend is. Daarom kan aan die door KPN voorgestane (onjuiste) interpretatie van de vaststelling van de onderhavige boete niet de betekenis worden toegekend die KPN daaraan verbonden wenst te zien.

123. KPN kan evenmin worden gevolgd in haar stelling, dat ACM uitsluitend met de daadwerkelijke (anders dan potentiële) schade bij abonnees rekening had mogen houden. De Toelichting bij de Boetebeleidsregels ACM noemt weliswaar de “daadwerkelijke schade” als rekenfactor bij het bepalen van de boetehoogte, maar uit de bewoordingen van die beleidsregels blijkt duidelijk dat dit een voorbeeld is en dat andere rekenfactoren – zoals potentiële schade – wel degelijk ook relevant zijn.[55]

124. Het bij de boeteberekening meewegen van de potentiële schade bij (in dit geval 2 miljoen) abonnees, ligt hier te meer voor de hand, nu de geschonden artikelen 11.3, eerste lid, juncto artikel 11.2 Tw juist beogen te voorkomen dat persoonsgegevens risico lopen. De rechtbank oordeelde in de zaak van Liander versus ACM - weliswaar ten aanzien van de

[54] In het sanctiebesluit (randnummers 158-160) wordt uiteengezet dat hierbij de volgende omstandigheden in ogenschouw zijn genomen:
- Voor wat betreft de gebrekkige maatregelen voor patchmanagement is van belang dat KPN vóór 15 januari 2012 al expliciet wist dat de [vertrouwelijk] niet up-to-date was. Op 13 december 2011 werd ontdekt dat de website van KPN-dochter Gemnet was gehackt. KPN heeft vervolgens nagelaten om maatregelen te treffen om de kwetsbaarheden in de [vertrouwelijk] te verhelpen.
- KPN was er in 2009 al op gewezen dat het houden van penetratietesten was aan te bevelen (zie p. 124 van het Onderzoeksrapport). KPN heeft vervolgens nagelaten penetratietesten uit te voeren.
- KPN had de beschikking over scansoftware, maar heeft besloten deze niet meer te gebruiken.

[55] Zie de woorden “*onder meer* de omstandigheden, die een rol *kunnen* spelen bij” (artikelgewijze toelichting bij artikel 3.5) en de woorden “*kan onder meer* in aanmerking nemen” (artikelsgewijze toelichting bij artikel 3.13) in de Toelichting bij de Boetebeleidsregels ACM (cursieven toegevoegd door ACM).

bewezenverklaring - in overeenkomstige zin.[56] In zowel deze zaak als de onderhavige zijn wettelijke normen aan de orde met een vergelijkbare strekking: normen die primair tot doel hebben een zeker beveiligingsniveau te waarborgen.

125. Als geen schade ontstaat ten gevolge van een schending van die normen, doet dit – gelet op de waarborgende aard van de onderhavige normcategorie – geen afbreuk aan de ernst van de overtreding. Als het uitgangspunt van de wettelijke norm – zoals in casu – is dat ook het gevaar op het ontstaan van schade zoveel mogelijk moet worden weggenomen, ligt dit niet in de rede. Wel acht ACM het denkbaar dat in het feitelijk ontstaan van schade ten gevolge van de schending van een dergelijke norm, aanleiding wordt gezien de betreffende overtreding als ernstig(er) te beschouwen.

126. ACM deelt evenmin de kritiek van KPN ten aanzien van de verwijzing in het boetebesluit naar de eerdere hack (13 december 2011) op de website van KPN-dochter Gemnet.[57] Die eerdere hack had eveneens te maken met kwetsbaarheden in [vertrouwelijk]. ACM verwees bij onderhavig boetebesluit naar die hack, omdat nu ook KPN zelf heeft nagelaten om naar aanleiding van die hack, waarvan zij volledig op de hoogte was, kwetsbaarheden in haar eigen netwerk ten aanzien van [vertrouwelijk] te verhelpen. Zij heeft daarmee welbewust extra veiligheidsrisico's genomen.

127. KPN stelt verder dat zij op grond van artikel 3.15 van de Boetebeleidsregels ACM aanspraak maakt op boeteverlaging, nu KPN (in haar woorden) de overtreding zelf heeft gesignaleerd, deze heeft gemeld bij ACM, en deze vervolgens uit eigen beweging heeft beëindigd. Ook die stelling van KPN gaat om verschillende redenen niet op.

128. ACM verwijst hiertoe om te beginnen naar haar eerdere betoog, kortweg dat de zorgplicht en de herstelplicht niet zijn aan te merken als communicerende vaten. KPN heeft het beveiligingsincident op basis van het Compliance Handvest aan OPTA gemeld. Bovendien heeft KPN ook niet met zoveel woorden melding gedaan van een overtreding van de zorgplicht, maar van het plaatsvinden van een hack (welke inbreuk op haar beveiliging KPN sinds de inwerkingtreding van artikel 11.3a, eerste lid, Tw op 5 juni 2012 in beginsel ook wettelijk verplicht is te melden aan OPTA/ACM), zodat het in het geheel niet in de rede ligt te

[56] Rb. Rotterdam 13 juni 2013, zaaknrs. Rot 12/4156 en Rot 12/4157. Rechtsoverweging 5.4: "*De rechtbank merkt in dit verband nog op dat blijkens de tekst en strekking van deze bepalingen sprake is van een resultaatsverplichting. Voor overtreding van deze verplichting is het voorts niet noodzakelijk dat daadwerkelijk gebruikt wordt gemaakt van de vertrouwelijke gegevens*."
[57] Verzoekschrift voorlopige voorziening, randnummer 36.

concluderen dat KPN de onderhavige overtreding (van de zorgplicht) meteen uit eigen beweging aan OPTA/ACM heeft gemeld.

129. Er is ook een andere bijzondere omstandigheid, die aanleiding geeft om in dit geval artikel 3.15 van de Boetebeleidsregels ACM niet toe te passen. KPN is namelijk met (destijds) OPTA een Handvest overeengekomen, waarbij KPN in ruil voor een verlicht toezichtregiem zich eraan heeft verbonden eigen overtredingen van de Tw meteen aan OPTA (thans ACM) te melden. Bovendien is de stelling van KPN, dat zij de overtreding bij ACM zou hebben gemeld, niet juist. Zij heeft slechts aan ACM gemeld dat er een hack heeft plaatsgevonden en niet dat zij de zorgplicht heeft geschonden.

130. Anders dan KPN stelt, kan ten slotte ook de reputatieschade die KPN door de hack zou zijn opgelopen, niet leiden tot boeteverlaging. Voor zover dergelijke schade al is ontstaan, is deze direct gelieerd aan overtreding (door KPN zelf) van haar beveiligingsplicht. Niet valt in te zien, waarom die (mogelijke) schade zou moeten leiden tot vermindering van de boete.

Tussenconclusie

131. Op grond van bovenstaande overwegingen treffen de bezwaren van KPN gericht tegen de hoogte van de opgelegde boete geen doel.

6.3 Publicatiebesluit

Algemeen

132. Gelet op hetgeen in het voorgaande al is opgemerkt over de de beweerde (door KPN te lijden) reputatieschade, valt evenmin in te zien waarom die mogelijke omstandigheid de openbaarmaking van het boetebesluit zou moeten verhinderen. KPN haalt hier oorzaak en gevolg door elkaar. Eventuele reputatieschade is een gevolg van de gebrekkige beveiligingsmaatregelen (en de hack die daardoor waarschijnlijk is gefaciliteerd), niet van het sanctiebesluit van ACM. Daarbij komt dat, zoals gezegd, uit de tekst van het sanctiebesluit ook blijkt dat de hack plaatsvond in het verleden en dat KPN inmiddels herstelmaatregelen heeft genomen. De door KPN aangevoerde omstandigheid, dat het boetebesluit mede steunt op twee rapportages van KPN zelf, [58] maakt dat niet anders.

133. Ook de enkele, door KPN aangevoerde omstandigheid dat de bodemrechter zich niet eerder

[58] Verzoekschrift voorlopige voorziening, randnummer 43.

heeft gebogen over de handhaving, door ACM, van de artikelen 11.2 en 11.3 ,eerste lid, Tw kan er niet toe leiden dat openbaarmaking van het boetebesluit niet kan plaatsvinden. ACM is bevoegd ook open normen als die waar het in dit besluit om gaat bestuursrechtelijk te handhaven. Voor dit betoog van KPN valt in de wet, noch in jurisprudentie, enig aanknopingspunt te vinden.

134. ACM volgt KPN evenmin in haar betoog dat veiligheidsrisico's voor haar netwerk in de weg zouden staan aan het openbaar maken van het sanctiebesluit. De veiligheid van het netwerk van KPN heeft reeds ten tijde van de hack in 2012 publieke aandacht gehad en KPN heeft bovendien herstelmaatregelen genomen. Verder zijn de vertrouwelijkheidclaims van KPN grotendeels gehonoreerd.

Vertrouwelijkheidsclaims KPN

135. Ten aanzien van de (op het sanctiebesluit betrekking hebbende) niet-gehonoreerde vertrouwelijkheidsclaims waartegen KPN bezwaar heeft gemaakt,[59] overweegt ACM als volgt. Allereerst wijst ACM er nogmaals op dat zij het grootste gedeelte van die claims heeft ingewilligd omdat zij van oordeel is dat het niet uitgesloten is dat openbaarmaking van die passages hackers (of soortgelijke kwaadwillenden) zouden kunnen helpen in hun pogingen de beveiligingsmaatregelen van KPN te omzeilen of te doorbreken. Dat is ook niet wat ACM met publicatie van het sanctiebesluit beoogt te bereiken. ACM heeft zelfs ambtshalve passages als vertrouwelijk aangemerkt die mogelijk kwaadwillenden zouden helpen in hun pogingen de beveiligingsmaatregelen van KPN te omzeilen of te doorbreken.

136. Anderzijds geldt dat elke publicatie die aandacht richt op deze zaak kan leiden tot een verhoogde aandacht van hackers voor de netwerken en systemen van KPN. Publieke uitingen van de zijde van KPN zelf over deze kwestie (en aanverwante gevallen) hebben dit effect naar alle waarschijnlijkheid ook gehad. Zelfs als in het openbare sanctiebesluit slechts de vijf beveiligingsonderwerpen zouden worden genoemd zonder enige verdere inhoudelijke behandeling, zou dit al de interesse van hackers kunnen opwekken. Het onderwerp en de (internationale) naamsbekendheid van KPN zullen dit mogelijk ook in de hand werken. Toekomstige incidenten die openbaar bekend worden en betrekking hebben op de beveiliging van de systemen en netwerken van KPN, zullen dit effect waarschijnlijk ook weer hebben. ACM meent dat dit inherent is aan de huidige maatschappelijke ontwikkelingen en niet mag leiden tot de slotsom dat besluiten over beveiliging door KPN niet openbaar mogen worden gemaakt.

[59] Aanvullend bezwaarschrift, randnummer 91.

137. Het enkele feit dat deze verhoogde aandacht van hackers mogelijk het tijdelijke gevolg is van de openbaarmaking van het sanctiebesluit, acht ACM op zichzelf dan ook onvoldoende om tot het oordeel te komen dat de niet door haar gehonoreerde vertrouwelijkheidsclaims waartegen KPN bezwaar heeft gemaakt, toch als vertrouwelijk moeten worden behandeld. Dit zou naar het oordeel van ACM slechts anders kunnen zijn als redelijkerwijs is te verwachten dat openbaarmaking van die passages hackers (of soortgelijke kwaadwillenden) daadwerkelijk kunnen helpen in hun pogingen de beveiligingsmaatregelen van KPN te omzeilen of te doorbreken, zodat het aldus ontstaan van schade niet is uitgesloten.

138. In dat geval acht ACM het denkbaar dat sprake is van gegevens waaruit wetenswaardigheden kunnen worden afgelezen of afgeleid met betrekking tot de technische bedrijfsvoering van KPN. Dergelijke gegevens kwalificeren als bedrijfs- en fabricagegegevens in de zin van artikel 10, eerste lid, aanhef en onderdeel c, van de Wob, zodat het verstrekken van die informatie ingevolge die bepaling van de Wob achterwege dient te blijven. Ook acht ACM het niet geheel uitgesloten dat in dat geval eventueel sprake is van een situatie waarin het publieke belang van informatieverstrekking (dat gemoeid is met openbaarmaking van de bedoelde passages) niet opweegt tegen het voorkomen van de onevenredige benadeling van KPN in de zin van artikel 10, tweede lid, aanhef en onderdeel g, van de Wob.

139. ACM is echter van oordeel dat KPN niet concreet inzichtelijk heeft kunnen maken in welk opzicht de gewraakte woorden/passages kwaadwillenden daadwerkelijk kunnen helpen in hun pogingen de beveiligingsmaatregelen van KPN te omzeilen of te doorbreken. Hierop zal ACM hieronder nog kort ingaan:

- KPN maakt er bezwaar tegen dat ACM in randnummer 61, tweede bulletpoint, van het sanctiebesluit vermeldt dat de beveiligingsmaatregel “patchmanagement” niet is ingevoerd. Deze opmerking dient volgens KPN te worden geschrapt omdat zij stelt dat dit onjuist is. Volledigheidshalve wijst ACM er op dat zij allereerst niet inziet in welk opzicht openbaarmaking van deze passage kwaadwillenden daadwerkelijk kan helpen in hun pogingen de beveiligingsmaatregelen van KPN te omzeilen of te doorbreken. Verder wijst ACM er nog op dat in randnummer 61, tweede bulletpoint, van het sanctiebesluit wordt overwogen dat het door KPN opgestelde centrale beveiligingsbeleid (CSP) een aantal verplichte beveiligingsmaatregelen kende waarvan moet worden vastgesteld dat in ieder geval één maatregel, namelijk patchmanagement, niet is ingevoerd en hier geen (centraal) beleid voor aanwezig was. Het feit dat er – zoals KPN aanvoert – wel software door KPN werd en wordt

gepatched, doet niet af aan de conclusie dat er geen aantoonbaar centraal en/of decentraal management (waaronder sturing, afstemming, evaluatie, etc.) van deze activiteit plaatsvond. Daarom ziet ACM in deze stelling van KPN evenmin aanleiding om openbaarmaking van de betreffende passage achterwege te laten.

- Verder heeft KPN verzocht om het schrappen van een gehele alinea in randnummer 75. Indien dat ook na heroverweging door ACM niet gebeurt, vindt KPN in elk geval dat de eerste, derde en vierde volzin moeten worden geschrapt. ACM heeft tekst met dezelfde materiële inhoud wel geschrapt in randnummer 69 tweede bulletpoint en deze dient ook in randnummer 75 te worden verwijderd. KPN stelt dat de opmerking kwaadwillenden uitnodigt in te breken op de systemen van KPN. Op dit aspect van de vertrouwelijkheidsclaim van KPN zal in het volgende randnummer worden ingegaan.
- Meerdere randnummers van het besluit dienen volgens KPN alsnog geheel als vertrouwelijk te worden aangemerkt (alsmede alle overige tekst waaruit duidelijk afgeleid kan worden dat het Incident heeft plaatsgevonden ten gevolge van een kwetsbaarheid in de [vertrouwelijk]) omdat daaruit alleen de naam “[vertrouwelijk]” is geschrapt. KPN betoogt dat uit de overige tekst, zeker door geïnformeerde kwaadwillenden, gemakkelijk kan worden afgeleid dat het om deze software gaat. ACM volgt KPN niet in deze redenering. KPN laat ook in deze context na inzichtelijk te maken in welk opzicht openbaarmaking van deze randnummers kwaadwillenden daadwerkelijk kan helpen in hun pogingen de beveiligingsmaatregelen van KPN te omzeilen of te doorbreken. De woorden “[vertrouwelijk]” zijn consequent uit de openbare versie van het sanctiebesluit verwijderd, aangezien wetenschap over interne namen en gebruikte software van belang zijn bij de voorbereiding en uitvoering van hack-aanvallen. ACM ziet, nu die woorden uit het sanctiebesluit zijn verwijderd, niet in hoe buitenstaanders daaruit alsnog zouden kunnen afleiden dat de onderhavige kwetsbaarheid zich bevond in de [vertrouwelijk]. Van de zijde van KPN is hieromtrent tijdens de hoorzitting die op 25 maart 2014 heeft plaatsgevonden ook niet meer aangevoerd dan dat uit de overige tekst van het sanctiebesluit (toch) kan worden afgeleid dat het gaat om [vertrouwelijk]. Aangezien het geen geheim is dat er een incident heeft plaatsgevonden, kan volgens KPN ook aan de hand daarvan terug worden geredeneerd door middel van indirecte herleiding. ACM acht dit betoog onvoldoende concreet om alsnog te oordelen dat openbaarmaking van de betreffende randnummers achterwege dient te blijven.

140. ACM volgt KPN na heroverweging wel in haar stelling dat de volgende passages uit het besluit

van 16 december 2013 niet openbaar dienen te maken, hetgeen betekent dat deze in de eerste, derde en vierde volzin van randnummer 75 van voornoemd besluit voorkomende passages – conform de wensen van KPN – alsnog als vertrouwelijk zullen worden aangemerkt:

"[vertrouwelijk]"

141. ACM ziet bij nader inzien onvoldoende aanleiding deze passages anders te behandelen dan eerdergenoemde tekst (met vergelijkbare materiële inhoud), zoals opgenomen in randnummer 69, tweede bulletpoint, van het sanctiebesluit. Daarom zal ACM bedoelde passages evenmin openbaar maken, hetgeen betekent dat die ook als vertrouwelijk zullen worden aangemerkt en als zodanig uit randnummer 75 van de openbare versie van het sanctiebesluit zullen worden verwijderd. In zoverre treffen de bezwaren van KPN doel.

142. Ten aanzien van de overige bezwaren van KPN gericht tegen het publicatiebesluit, overweegt ACM als volgt. Omdat ACM in het voorgaande reeds heeft geconcludeerd dat de bezwaren van KPN tegen het sanctiebesluit ongegrond zijn, zodat er geen reden is dit besluit na heroverweging geheel of gedeeltelijk te herroepen, komt ACM – gelet op het in deze paragraaf overwogene – ten aanzien van het publicatiebesluit tot dezelfde conclusie.

Tussenconclusie

143. De bezwaren van KPN die zich richten tegen de openbaarmaking van de in het voorgaande omschreven (in randnummer 75 van het sanctiebesluit opgenomen) passages treffen dan ook doel. Voor het overige is ACM van oordeel dat de door KPN tegen het publicatiebesluit aangevoerde bezwaren geen doel treffen.

6.4 Conclusie

144. Na heroverweging van de bestreden besluiten op grondslag van de door KPN aangevoerde bezwaren, is ACM van oordeel dat de bezwaren die zich richten tegen de openbaarmaking van de in randnummer 140 van dit besluit omschreven passages gegrond zijn. Dit betekent dat het besluit van 14 februari 2014[60] tot openbaarmaking van het sanctiebesluit in zoverre niet in stand blijft. Gelet op alle voorgaande overwegingen acht ACM de door KPN aangevoerde bezwaren voor het overige ongegrond. Dit betekent dat het besluit van 14 februari 2014 tot openbaarmaking van het sanctiebesluit voor het overige in stand blijft. Bij deze beslissing op bezwaar is volledigheidshalve een overeenkomstig herziene openbare versie van het besluit van 16 december 2013[61] gevoegd. Het besluit van 16 december 2013 tot oplegging van een boete aan KPN blijft gelet op het voorgaande wel geheel in stand.

7. Dictum

145. De Autoriteit Consument en Markt:

I. verklaart de bezwaren van KPN B.V. voor zover gericht tegen het sanctiebesluit (met kenmerk ACM/DJZ/2013/206321) ongegrond;

II. verklaart de bezwaren van KPN B.V., gericht tegen het publicatiebesluit van 14

[60] Kenmerk ACM/DJZ/2014/200868.
[61] Kenmerk ACM/DJZ/2013/206321.

Besluit
Openbaar

februari 2014 (met kenmerk ACM/DJZ/2014/200868) gegrond, voor zover deze het openbaar maken betreffen van de in randnummer 140 van dit besluit omschreven passages, zoals opgenomen in het besluit van 16 december 2013 (met kenmerk ACM/DJZ/2013/206321);

III. verklaart de bezwaren van KPN B.V. voor het overige ongegrond.

De Autoriteit Consument en Markt,
namens deze,

w.g.
mr. C.A. Fonteijn
Bestuursvoorzitter

Tegen dit besluit kan degene, wiens belang rechtstreeks is betrokken, binnen zes weken na bekendmaking van dit besluit een gemotiveerd beroepschrift indienen bij de rechtbank Rotterdam, sector bestuursrecht, Postbus 50951, 3007 BM Rotterdam. Nadere informatie over de beroepsprocedure is te vinden op www.rechtspraak.nl.