Besluit
Openbaar

Ons kenmerk: ACM/DJZ/2013/206321_OV
Zaaknummer: 13.0503.32
Datum: 16 december 2013

Besluit van de Autoriteit Consument en Markt tot het opleggen van een boete aan KPN B.V. voor overtredingen van de zorgplichtbepalingen zoals neergelegd in artikel 11.3, eerste lid, juncto artikel 11.2 van de Telecommunicatiewet

1 Samenvatting

1. Het is voor consumenten van belang dat hun persoonsgegevens door aanbieders van openbare elektronische communicatiediensten en –netwerken op een adequate wijze beveiligd worden. Om gebruik te kunnen maken van de diensten moeten consumenten persoonsgegevens aan hen verstrekken. Wanneer persoonsgegevens in handen vallen van onbevoegden kan dit schadelijke gevolgen hebben voor de betrokken consumenten. In algemene zin wordt bij een onvoldoende bescherming van persoonsgegevens het vertrouwen van consumenten in het veilig gebruik van elektronische communicatiediensten en –netwerken ondergraven. Het is van groot belang dat aanbieders van dergelijke diensten en netwerken maatregelen treffen om de beveiliging van persoonsgegevens voldoende te waarborgen. Om die reden heeft de wetgever er voor gekozen om in dat kader een zorgplicht in de Telecommunicatiewet op te nemen waaraan de aanbieders van die diensten en netwerken moeten voldoen. De Autoriteit Consument en Markt (hierna: ACM) houdt toezicht op de naleving van die wet. Dit besluit is een uitvloeisel van het toezicht dat ACM houdt op de naleving van bedoelde zorgplicht.

2. In januari 2012 werd bekend dat een hacker had ingebroken in het netwerk van KPN B.V. (hierna: KPN). Deze hack was aanleiding om een onderzoek in te stellen 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 gedurende de onderzoeksperiode onvoldoende passende, hoofdzakelijk organisatorische, maar ook technische maatregelen heeft getroffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van haar abonnees en gebruikers. Zo was voor een aantal essentiële beveiligingsmaatregelen geen centraal beleid opgesteld en heeft het onderhoud van het opgestelde beleid onvoldoende plaatsgevonden. Ook had KPN haar netwerkbeheer niet op orde en had zij op het gebied van netwerk- en systeembewaking onvoldoende passende maatregelen getroffen. KPN heeft daarmee niet voldaan aan de op haar rustende zorgplicht van artikel 11.3, eerste lid, juncto artikel 11.2 van de Telecommunicatiewet (hierna: Tw). Voor deze overtreding legt ACM KPN een boete op van in totaal EUR 364.000.

3. 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.

2 Achtergronden en verloop van de procedure

4. KPN is een aanbieder van openbare elektronische communicatiediensten en van een openbaar elektronisch communicatienetwerk. Op grond van artikel 11.2 Tw is KPN verplicht om zorg te dragen voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van haar diensten. Artikel 11.3, eerste lid, Tw is een nadere invulling van artikel 11.2 Tw. Op grond van artikel 11.3, eerste lid, Tw is KPN verplicht passende technische en organisatorische maatregelen te treffen voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van haar diensten. Beide wetsartikelen worden ook wel aangeduid als “de zorgplicht”.

5. In januari 2012 werd bekend dat er in het netwerk van KPN was ingebroken, waardoor mogelijk de bescherming van persoonsgegevens en de persoonlijke levenssfeer in het geding was geweest. Deze gebeurtenis (hierna aangeduid als “de hack”) was voor het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: OPTA) aanleiding om een onderzoek in te stellen naar de naleving van voormelde zorgplicht door KPN. ACM heeft, vanaf 1 april 2013, als rechtsopvolger van OPTA, dit onderzoek voortgezet. Dit onderzoek heeft geresulteerd in het onderzoeksrapport van 22 juli 2013, dat aan het onderhavige besluit ten grondslag ligt.

6. In het kader van het onderzoek heeft OPTA bij brief van 29 februari 2012 met kenmerk OPTA/ACNB/2012/200646 op grond van artikel 18.7 Tw inlichtingen gevorderd van KPN.

7. KPN diende binnen tien werkdagen – dus uiterlijk op 14 maart 2012 – aan die informatievordering te voldoen.

8. Op 14 maart 2012 heeft KPN een deel van de gevorderde informatie op een USB-stick aangeleverd.[1]

9. Bij brief van 8 maart 2013 heeft KPN – in reactie op een latere informatievordering van OPTA – Intern onderzoek Victor aan OPTA verstrekt.

[1] Zie: Onderzoeksrapport, bijlage 3 KPN, reactie op informatievordering zonder kenmerk.

10. Bij brief van 29 augustus 2013 heeft KPN ACM een schriftelijke zienswijze ten aanzien van het onderzoeksrapport toegezonden. Tijdens een hoorzitting ten kantore van ACM op 25 september 2013 heeft KPN haar zienswijze nog nader mondeling toegelicht. Van deze hoorzitting is een verslag gemaakt, dat aan het dossier is toegevoegd.

3 Het onderzoeksrapport

11. In het onderzoeksrapport constateert de Directeur van de Directie Consumenten van ACM dat de rechtspersonen Koninklijke KPN N.V. en KPN B.V. niet hebben voldaan aan de zorgplicht, die op grond van artikel 11.3, eerste lid, juncto artikel 11.2 Tw op hen rust, omdat zij in de periode september 2010 tot en met 15 januari 2012 onvoldoende passende, hoofdzakelijk organisatorische, maatregelen hebben getroffen betreffende:

- het *opzetten en het handhaven van beveiligingsbeleid* in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers;
- *netwerkinrichting* in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en;
- *afscherming* in het belang van de bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers;
- *netwerk- en systeembewaking* in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers;
- *patchmanagement* in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers .

12. Ten aanzien van de periode kort na de hack, te weten de periode van 16 januari 2012 tot en met tot 15 maart 2012 constateert de Directeur Consumenten in het onderzoeksrapport dat KPN B.V. en Koninklijke KPN N.V.:

- vrijwel onmiddellijk na ontdekking van de hack code Oranje hebben afgekondigd en toen de ernst van de hack groter bleek op twee momenten zijn overgeschakeld op code Rood;
- bij de eerste herstelacties een onderzoek hebben ingesteld naar een mogelijke inbreuk op de bescherming van persoonsgegevens;
- het oplossen van de problemen de hoogste prioriteit hebben gegeven;
- [vertrouwelijk] in het belang van de bescherming van persoonsgegevens haar e-maildienst buiten werking hebben gesteld;

- na afloop van de code Rood-periodes hun procedures hebben geëvalueerd.

13. Koninklijke KPN N.V. en KPN B.V. hebben hiermee in lijn gehandeld met hun eigen procedures. In het rapport wordt ten aanzien van deze periode dan ook geen overtreding van artikel 11.3, eerste lid, Tw geconstateerd.

14. Daarnaast constateert de Directeur Consumenten in het onderzoeksrapport dat Koninklijke KPN N.V. en KPN B.V. artikel 18.7, derde en vijfde lid, Tw hebben overtreden, omdat zij naar aanleiding van de informatievordering van OPTA van 29 februari 2012[2] om een volledig overzicht te geven van de geplande, nog door haar vanaf die datum op te stellen, rapporten, documentatie, tussenrapportages, bevindingen, presentaties, terugkoppelingen en gespreksverslagen, het zogenoemde Intern onderzoek Victor van 15 maart 2012[3] niet onverwijld, dan wel binnen de door OPTA gestelde termijn, hebben verstrekt en evenmin het bestaan ervan hebben gemeld in hun reactie op die informatievordering.[4]

4 Zienswijze KPN

15. In zijn algemeenheid geldt dat KPN zich niet herkent in het beeld dat in het rapport van haar onderneming en haar beveiligingsbeleid wordt geschetst. KPN stelt zich in haar schriftelijke zienswijze op het standpunt dat geen sprake is van schending van de zorgplicht door KPN en in ieder geval niet van vijf verschillende overtredingen van de zorgplicht, zoals in het rapport wordt geconcludeerd. Evenmin is sprake geweest van overtreding van artikel 18.7 Tw. Zij voert daartoe – samengevat weergegeven – het volgende aan.

Onterechte en onjuiste toepassing van artikel 11.2 en 11.3 Tw

16. In het rapport wordt een onjuiste toepassing gegeven aan artikel 11.2 en 11.3 Tw. Ten eerste wordt ten onrechte uitgegaan van twee (willekeurige) onderzoeksperiodes – één voor en één na de hack. Beide onderzoeksperiodes hadden tezamen moeten worden beoordeeld en bezien had moeten worden of KPN over het geheel genomen voldoende maatregelen had genomen. Zo heeft KPN voldoende herstelmaatregelen getroffen door de calamiteitenprocedure in werking te stellen en door toezichthouders, overheidsinstanties en betrokkenen te informeren.

17. Ten tweede heeft ACM alleen onderzoek gedaan naar de beveiligingsplicht, zoals neergelegd in artikel 11.3, eerste lid, Tw. De informatieplicht, zoals neergelegd in artikel 11.3, tweede lid,

---

[2] Zie: Onderzoeksrapport, bijlage 4 ACM, informatievordering met kenmerk OPTA/ACNB/2012/2000646.

[3] Zie: Onderzoeksrapport, bijlage 8 KPN, reactie op de informatievordering.

[4] Zie: Onderzoeksrapport, randnummers 319 en 320.

Tw heeft ACM ten onrechte buiten de reikwijdte van het onderzoek gelaten. De juridische toets is dan ook te beperkt geweest. De beveiligingsplicht en de informatieplicht zijn twee communicerende vaten die niet los van elkaar kunnen worden gezien. Bovendien heeft ACM zich beperkt tot de technische en organisatorische beveiligingsmaatregelen in of met betrekking tot het deel van het netwerk van KPN dat door de hacker is benaderd en heeft zij andere beveiligingsmaatregelen, waaronder fysieke beveiligingsmaatregelen en bijvoorbeeld integriteitsbeleid, gezien. Deze beperking wordt bevestigd in de door OPTA vastgestelde beleidsregels ten aanzien van de informatieplicht, waarin is vermeld dat de beveiligingsplicht en de informatieplicht tezamen vaak worden aangeduid als de zorgplicht.

18. Ten derde is de zorgplicht zoals vervat in de artikelen 11.2 en 11.3 Tw erop gericht persoonsgegevens te beschermen tegen onrechtmatige verwerking ervan. Bij de hack in het netwerk van KPN zijn geen persoonsgegevens verwerkt. Er is door de hacker slechts toegang verkregen tot de systemen, maar hij heeft geen verwerkingshandelingen in de zin van de Wet bescherming persoonsgegevens verricht.

19. Ten vierde worden in het rapport vijf beveiligingsonderwerpen besproken, waarna ten aanzien van elk daarvan wordt geconcludeerd dat KPN geen passend beveiligingsniveau kon garanderen. Hiermee is door ACM een verkeerde toets gehanteerd. Het gaat bij artikel 11.3 Tw niet om allemaal afzonderlijke zorgplichten, die op zichzelf beschouwd tot schending van artikel 11.3 Tw kunnen leiden. Het gaat om de vraag of KPN over het geheel genomen heeft voldaan aan de zorgplicht. Bovendien volgen de vijf onderwerpen niet uit de wet. Het lijkt erop alsof bewust een “vijftrapsraket” is geformuleerd om vijf boetes te kunnen opleggen.

Geen schending van de zorgplicht

20. Het belang van de zorgplicht is de bescherming van de persoonlijke levenssfeer, in het bijzonder de bescherming van persoonsgegevens. Vooropgesteld zij dat de zorgplicht geen absolute beveiliging vereist. De mate van beveiliging is afhankelijk van verschillende factoren. Gelet hierop moet in de eerste plaats rekening worden gehouden met de aard van de betreffende persoonsgegevens: hoe gevoeliger de gegevens, hoe verstrekkender in beginsel de te nemen beveiligingsmaatregelen. Ook moet rekening worden gehouden met de context waarbinnen de gegevens worden gebruikt. In dit geval heeft de hacker geen toegang gekregen tot persoonsgegevens. Er zijn ten tijde van de hack geen persoonsgegevens verwerkt in de zin van de Wbp. Dat betekent dat het object van de bescherming niet in het geding is geweest. Ook als tijdens de hack wel persoonsgegevens zouden zijn verzameld, is het de vraag welke schade dit tot gevolg zou hebben gehad voor de betrokken abonnees. Op de servers stonden alleen de volgende persoonsgegevens: naam, adres, woonplaats, telefoonnummer, e-mailadres, bankrekeningnummer, transacties en facturen. Dit zijn geen gevoelige persoonsgegevens als bedoeld in artikel 16 Wbp. Het risico dat met deze persoonsgegevens identiteitsfraude wordt gepleegd is volgens KPN nihil. ACM heeft bij haar beoordeling van de

vraag of sprake is geweest van een overtreding van de zorgplicht ten onrechte geen aandacht besteed aan de aard van de persoonsgegevens en de context waarbinnen deze worden gebruikt. De geringe gevolgen van de hack zijn ten onrechte buiten beschouwing gelaten. KPN meent dat gezien de aard van de persoonsgegevens in deze zaak en de context waarin deze gebruikt werden, zij niet hoefde te voldoen aan hogere eisen dan de ondergrens die het College bescherming persoonsgegevens (hierna: CBP) stelt in haar richtsnoeren van 2001. KPN voldoet aan deze door het CBP gestelde ondergrens.

21. In de tweede plaats moet bij de beantwoording van de vraag of maatregelen passend zijn, rekening worden gehouden met de specifieke organisatie van de betreffende aanbieder. In het rapport is met de specifieke kenmerken van KPN ten onrechte geen rekening gehouden. Zo is KPN een grote onderneming met een lange historie die is opgedeeld in meerdere, voor een groot deel autonome eenheden. Een gevolg daarvan is dat bovenaf opgelegd beleid binnen de onderneming weinig effect sorteert. De belegging van het veiligheidsbeleid is dan ook op lagere niveaus decentraal 'risk based' georganiseerd. Bovendien is een organisatie als KPN continu aan veranderingen onderhevig, waardoor het beleid en de verdeling van de onderlinge verantwoordelijkheden complex is en het beheer ervan tijds- en arbeidsintensief. Door de grootte van de organisatie van KPN heeft nieuw beleid vaak een implementatietraject nodig van enkele maanden en soms van jaren.

22. In de derde plaats dat bij de beoordeling van de vraag of is voldaan aan de zorgplicht ook rekening dient te worden gehouden met de aard van de aangeboden diensten. In dit geval zijn systemen gecompromitteerd binnen het [vertrouwelijk].Op dit domein worden niet-kritieke diensten geleverd.

23. In het rapport is niet of onvoldoende rekening gehouden met de stand van de techniek. Zo is de afbakening van onderzoeksperiode I willekeurig gekozen en is onduidelijk of ACM meent dat KPN de zorgplicht heeft overtreden van het begin tot en met het eind van onderzoeksperiode I of slechts op bepaalde momenten in die onderzoeksperioden. Daar komt bij dat ACM geen onderzoek heeft gedaan naar de stand van de techniek specifiek ten aanzien van KPN. Om televisiediensten aan te kunnen bieden [vertrouwelijk] is KPN genoodzaakt om een bepaalde technische inrichting te kiezen waardoor de performance van haar diensten op peil blijft. Ten slotte is geen rekening gehouden met de identiteit en intentie van de hacker. Bij de keuze van het beveiligingsniveau is de kans dat een hack wordt gepleegd een relevant gegeven. Van belang is dat het in dit geval een ervaren hacker betrof, die zijn gespecialiseerde kennis heeft ingezet om gericht in te breken in de systemen van KPN, met het waarschijnlijke doel hier informatie te zoeken waarmee hij voor zichzelf financieel voordeel kon behalen. De betreffende hack moet dan ook worden gezien als een uitzonderlijk beveiligingsincident. ACM heeft ten onrechte geen onderzoek gedaan naar het risico dat een hack als deze zich zou voordoen. KPN wijst er op dat per dag meer dan 26.000 pogingen worden gedaan om in te

breken in het netwerk van KPN en dat er op 16 januari 2012 één is geslaagd. De beveiligingsmaatregelen die ACM voor staat, zouden voor KPN disproportionele kosten met zich brengen.

Beginselen van behoorlijk bestuur

24. KPN voert aan dat ACM bij de handhaving van haar bevoegdheden onzorgvuldig en willekeurig te werk is gegaan. Ten eerste wordt in het rapport vrijwel alleen uitgegaan van de gegevens die door KPN zelf zijn aangeleverd, zoals het Fox-IT-rapport en Intern onderzoek Victor en de interviews met medewerkers van KPN. Hierbij wordt onvoldoende rekening gehouden met het feit dat zowel het Fox-IT-rapport als Intern onderzoek Victor zijn opgesteld naar aanleiding van de hack. Fox-IT en KPN zijn in voormelde rapporten vanzelfsprekend zeer kritisch geweest op de maatregelen van KPN. De bevindingen en conclusies uit de onderzoeken (in opdracht van KPN) kunnen niet zonder meer worden toegepast in het onderhavige onderzoek, laat staan dat deze onderzoeken de enige onderbouwing daarvan vormen.

25. Ten tweede wekt het rapport de schijn dat het enkele feit dat de hack heeft kunnen gebeuren, aanleiding heeft gegeven tot de conclusie dat de zorgplicht is geschonden. Dat de hack wordt aangegrepen om onderzoek te doen is gerechtvaardigd. De hack kan echter nooit afdoende bewijs zijn dat de zorgplicht is geschonden. Er lijkt sprake van een doelredenering, aldus KPN.

26. Ten derde is ACM op onzorgvuldige wijze tewerk gegaan bij het interviewen van medewerkers van KPN. De geïnterviewde personen waren weliswaar kundig op het gebied van beveiliging van informatie, maar hadden geen zicht op het decentraal geregelde beleid. Ten slotte worden in het rapport alleen passages uit de interviews weergegeven die in de kraam te pas komen. Dit geeft een verkeerd beeld.

Intern onderzoek Victor

27. KPN is van mening dat zij op het moment van de informatievordering niet gehouden was tot het verstrekken van Intern onderzoek Victor, vanwege de datum, het karakter en de inhoud ervan. Intern onderzoek Victor was op het moment van de informatievordering nog niet afgerond en moest nog worden voorgelegd aan de verantwoordelijke afdelingen en managers. Bovendien betreft het een uitsluitend intern rapport van KPN met als doel – kort na de hack – vast te stellen wat er was gebeurd, wat de mogelijke dreigingen waren en om zo snel mogelijk tot adequate acties te komen.

28. KPN beroep zich ten aanzien van Intern onderzoek Victor dan ook op haar zwijgrecht. KPN wijst er op dat dit rapport niet onafhankelijk van haar wil tot stand is gekomen. Aangezien voor KPN geen verplichting bestond om het betreffende rapport af te geven, kan haar daarvoor evenmin een overtreding van artikel 18.7 Tw worden verweten.

Geen plaats voor het opleggen van een boete

29. Volgens KPN is voor het opleggen van een boete in deze situatie geen plaats, onder meer omdat de gevolgen van de hack beperkt zijn gebleven. Een door ACM op te leggen sanctie zou niet gericht moeten zijn op leedtoevoeging, maar op het voorkomen van herhaling van de overtreding. Een herstelmaatregel als een last onder dwangsom ligt daarom meer in de rede. KPN verwijst naar de beleidsregels die OPTA destijds heeft opgesteld ten aanzien van de informatieplicht (artikel 11.3, tweede lid, Tw). Uitgangspunt in die beleidsregels is bovendien dat de toezichthouder eerst een waarschuwing geeft, alvorens over te gaan tot het opleggen van bestuursrechtelijke sancties. Volgens KPN geldt een en ander eveneens ten aanzien van de beveiligingsplicht (artikel 11.3, eerste lid, Tw). Het snel beëindigen van de overtreding kan een reden zijn om niet over te gaan tot het opleggen van een boete. Bovendien is er volgens KPN geen sprake van een ernstige overtreding, nu geen persoonsgegevens aan haar netwerk zijn onttrokken. Daar komt nog bij dat het gaat om een open norm, die noch door de wetgever, noch door de toezichthouder nader is ingevuld. Voor dienstaanbieders is het dan ook onduidelijk wat van hen wordt verwacht op het gebied van beveiliging.

Onjuiste toepassing boetebeleidsregels

30. In het geval ACM toch tot de conclusie komt dat sprake is van een overtreding die het opleggen van een boete rechtvaardigt, wijst KPN er op dat in het rapport de boetebeleidsregels onjuist worden toegepast. Zo meent KPN dat de vermeende overtreding niet in de categorie “zware overtredingen” valt, maar dat de kwalificatie “minder zwaar” in dit geval opgaat. Er zijn immers geen persoonsgegevens aan het netwerk van KPN onttrokken, waardoor de belangen van eindgebruikers niet, of in zeer beperkte mate zijn geschaad. De vaststelling van de ernst van de overtreding is volgens de boetebeleidsregels afhankelijk van de omstandigheden in concreto. Gelet op het feit dat geen persoonsgegevens zijn verwerkt en gelet op de beveiligingsmaatregelen die KPN wél heeft getroffen, haar adequate handelwijze na de constatering van de hack, de medewerking die zij heeft verleend aan OPTA en de omstandigheid dat hacks vaker voorkomen, zou de overtreding die KPN verweten wordt, moeten vallen in de categorie “minder ernstige overtreding”. Dit betekent dat de aan KPN op te leggen boete maximaal EUR 100.000 kan bedragen. KPN is van mening dat haar echter geen verwijt treft, omdat zij wel degelijk afdoende beveiligingsmaatregelen heeft getroffen. Daar komt bij dat de in het rapport gehanteerde onderzoeksperiodes niets zeggen over de vermeende lange duur van de overtreding. Ook boeteverhogende omstandigheden ontbreken. Boeteverlagende omstandigheden zijn wél aanwezig. Zo heeft KPN de overtreding zelf gesignaleerd, deze uit eigen beweging beëindigd en bij ACM gemeld.

Toerekening

31. KPN N.V. kan niet als overtreder worden aangemerkt. KPN N.V. is louter een holdingmaatschappij en voert geen activiteiten uit. Dat KPN N.V. verantwoordelijk is voor de

Corporate Security Policy en als zodanig verantwoordelijk is voor het beveiligingsbeleid, is dan ook onjuist en kan niet worden afgeleid uit de documenten waarnaar in het rapport wordt verwezen.

5 Juridisch kader

5.1 Bevoegdheid van ACM/OPTA

32. 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. Vanaf 1 april 2013 is ACM, als rechtsopvolger van, onder meer, OPTA, belast met dit toezicht.

33. 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. Vanaf 1 april 2013 komt deze bevoegdheid toe aan ACM.

34. 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.

35. 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.

36. De Minister van Economische Zaken heeft op 19 april 2013 beleidsregels vastgesteld voor het opleggen van bestuurlijke boetes door ACM[5] (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 bescherming persoonsgegevens en persoonlijke levenssfeer

37. Artikel 11.2 Tw luidt:

Onverminderd de Wet bescherming persoonsgegevens en het overigens bij of

[5] Beleidsregels van de Minister van Economische Zaken voor het opleggen van bestuurlijke boetes door de ACM (Stcrt. 2013, nr. 11214, 24 april 2013).

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.

38. Artikel 11.3, eerste lid, Tw luidt:[6]

> 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.*

39. 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.[7]

5.3 Medewerkingsplicht

40. Relevante delen van artikel 18.7 Tw[8]:

> 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. *(…)*

---

[6] 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 (voorheen) tweede lid is vernummerd tot derde lid, maar is inhoudelijk niet aangepast.

[7] *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.

[8] Op 1 april 2013 is artikel 18.7 Tw aangepast. Met deze wijziging komt de bevoegdheid toe aan ACM.

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.*

(…)

6 Overwegingen ACM

41. Op grond van artikel 11.3, eerste lid, Tw dienen netwerk- en dienstaanbieders, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De aanbieders worden geacht de veiligheidsrisico's af te wegen tegen het beveiligingsniveau en hebben daarmee de nodige ruimte om ook te concurreren op beveiligingsniveau.[9]

42. De omstandigheid dat een hacker wist in te breken in het netwerk van KPN vormde voor OPTA – en later ACM - de aanleiding een onderzoek in te stellen naar de wijze waarop KPN de op haar rustende zorgplicht ex artikel 11.3 Tw naleefde. De hack vormde op zichzelf niet het onderwerp van het onderzoek.

43. ACM houdt toezicht op de naleving van de zorgplicht ex artikel 11.3, eerste lid, juncto artikel 11.2 Tw. Het is voor consumenten van belang dat bedrijven deze zorgplicht serieus nemen.

---

[9] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 119.

Consumenten moeten er op kunnen vertrouwen dat hun persoonsgegevens voldoende worden beveiligd. Als dit niet gebeurt, is de bescherming van de persoonlijke levenssfeer van de consumenten in het geding.

44. Hoewel de hack niet het op zichzelf staande onderwerp is geweest van het onderhavige onderzoek, is dat incident wel richtinggevend geweest voor de inrichting van dat onderzoek, zo blijkt uit het onderzoeksrapport. Er is bijvoorbeeld voor gekozen het onderzoek te beperken tot het deel van het netwerk van KPN dat door de hacker is benaderd (het "[vertrouwelijk]"). Ook is niet onderzocht of KPN mogelijk ook het tweede lid van artikel 11.3 Tw heeft overtreden en heeft het onderzoek zich beperkt tot de technische en organisatorische beveiligingsmaatregelen in of met betrekking tot het [vertrouwelijk] in het kader van de bescherming van de daarin elektronisch opgeslagen persoonsgegevens en de daarmee gemoeide persoonlijke levenssfeer. Ten slotte heeft het onderzoek zich beperkt tot de informatiebeveiliging bij KPN. In het onderzoeksrapport is daarbij aangesloten bij praktijk en literatuur, waarbij bij informatiebeveiliging de aspecten beschikbaarheid, integriteit en vertrouwelijkheid van informatie van belang zijn. Beschikbaarheid van persoonsgegevens komt in het geding bij het optreden van storingen en uitval. Aangezien daarvan bij KPN in dit geval geen sprake was, is dit aspect bij het onderzoek buiten beschouwing gelaten.

45. ACM volgt KPN niet in haar stelling dat zij de informatieplicht, zoals bedoeld in het tweede lid van artikel 11.3 Tw ten onrechte buiten de reikwijdte van het onderzoeksrapport gelaten. In de optiek van ACM is van 'communicerende vaten' – zoals KPN meent[10] – geen sprake, en zijn het eerste en tweede lid bepalingen die afzonderlijk kunnen worden overtreden. De stelling dat het zou gaan om bepalingen die niet los van elkaar kunnen worden bezien, vindt geen steun in de onderhavige wetgeving, noch in de daarbij behorende wetsgeschiedenis. ACM volgt KPN niet in haar betoog dat ACM, voor een juiste beoordeling van de vraag of KPN in dit geval heeft voldaan aan de onderhavige zorgplicht, rekening had moeten houden met de wijzigingen die hoofdstuk 11 van de Tw heeft ondergaan of met richtsnoeren (met de titel 'Beveiliging van persoonsgegevens') die het CBP heeft uitgevaardigd.[11] De aanpassingen van hoofdstuk 11 van de Tw, waarop KPN doelt, waren niet van invloed op de in casu aan de orde zijnde (zelfstandige) normen die zijn neergelegd in artikel 11.2 en 11.3, eerste lid, Tw. Verder zijn de genoemde richtsnoeren van het CBP niet bedoeld om een nadere invulling te geven op artikel 11.3 Tw. Deze zijn daarom niet toegepast in het onderzoek en in dit besluit.

---

[10] Zo is het volgens KPN blijkbaar denkbaar dat het treffen van adequate maatregelen na een beveiligingsincident, eventuele voorafgaande gebreken in het (informatie)beveiligingsniveau van een aanbieder (van elektronische communicatiediensten) geheel kan compenseren, in die zin dat per saldo wordt geoordeeld dat aldus toch is voldaan aan de zorgplicht. Zie: Schriftelijke zienswijze 29 augustus 2013, p. 28.

[11] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 26-28.

46. Aangezien het onderzoek zich richtte op informatiebeveiliging van persoonsgegevens zijn andere beveiligingsmaatregelen, waaronder fysieke beveiligingsmaatregelen en integriteitsbeleid, terecht buiten de reikwijdte van het onderzoek gehouden. De vraag of voldoende fysieke beveiligingsmaatregelen zijn getroffen is immers slechts relevant indien fysieke inbreuken op de beveiliging aan de orde zijn. Daarvan is in casu geen sprake geweest. Voor zover bekend heeft de hack immers slechts langs digitale weg plaatsgevonden. Ook de vraag of het integriteitsbeleid afdoende was, acht ACM in dit geval niet relevant omdat er geen aanwijzingen zijn dat de integriteit van medewerkers een rol heeft gespeeld bij de hack in het netwerk van KPN. Dat KPN op die aandachtsgebieden mogelijk voldoende maatregelen heeft getroffen doet ook niet af aan het feit dat zij tekort is geschoten ten aanzien van de aandachtsgebieden die hieronder aan de orde zullen komen.

47. In aanvulling op het voorgaande wijst ACM er ook nog op dat als uitgangspunt geldt dat de wijze waarop een onderzoek wordt ingericht, behoort tot de discretionaire bevoegdheid van een toezichthouder zolang een en ander geschiedt binnen de grenzen die het recht stelt. Hetzelfde geldt voor de keuze van de onderzoeksperiode(s). Bij het maken van die keuze heeft ACM er voor gekozen het moment dat de hack in het netwerk van KPN plaatsvond, het einde van onderzoeksperiode I en het begin van onderzoeksperiode II te laten bepalen.

48. Het is gepast om de situatie inzake informatiebeveiliging voorafgaand aan een incident – in dit geval een hack – en de situatie die daarna ontstaat, op zichzelf te beoordelen (hetgeen tot uiting komt in de keuze voor twee verschillende onderzoeksperiodes, namelijk onderzoeksperiode I en II).[12] De eerste periode geeft immers een beeld van het niveau van de maatregelen die zijn getroffen ter bescherming van persoonsgegevens zonder dat er voor KPN een bijzondere aanleiding was – in dit geval de hack – een en ander zelf nog eens kritisch te beoordelen, en daar waar nodig additionele maatregelen te treffen. De stand van zaken na de hack is daarom niet te vergelijken met de situatie die voordien werd aangetroffen. ACM is daarom van oordeel dat het niet aangaat om onderzoeksperiode I en II als één onderzoeksperiode te beschouwen en vervolgens het 'gemiddelde' beveiligingsniveau gedurende die periode tot uitgangspunt te nemen, zoals KPN suggereert. Uit niets blijkt concreet dat de onderhavige wettelijke regeling een dergelijke benadering voorschrijft.

49. Blijkens het voorgaande zijn de keuzes die zijn gemaakt bij de inrichting van het onderzoek gebaseerd op redelijke en logische overwegingen, zodat van willekeur duidelijk geen sprake is. Overigens ziet ACM ook geen aanleiding te veronderstellen dat de in het voorgaande beschreven benadering zou afdoen aan de constatering dat KPN gedurende onderzoeksperiode I niet heeft voldaan aan de zorgplicht, hetgeen op zichzelf reeds een overtreding oplevert van 11.3, eerste lid, juncto artikel 11.2 Tw.

---

[12] Zie: Onderzoeksrapport, paragraaf 7.2.

50. Het onderzoek heeft geresulteerd in een onderzoeksrapport dat aan dit besluit ten grondslag ligt. In dit onderzoeksrapport wordt geconstateerd dat KPN de op haar rustende zorgplicht niet heeft nageleefd, omdat zij onvoldoende passende maatregelen heeft genomen betreffende:

    het opstellen en het handhaven van beveiligingsbeleid;
    netwerkinrichting;
    afscherming;
    netwerk- en systeembewaking; en
    patchmanagement.

51. Aan het onderzoeksrapport ligt onder meer Intern onderzoek Victor ten grondslag. Aangezien KPN zich ten aanzien van Intern onderzoek Victor beroept op haar zwijgrecht en meent dat zij in beginsel niet gehouden was om dit stuk aan OPTA te verstrekken, zal ACM hieronder eerst ingaan op dit verweer van KPN.

6.1 Intern onderzoek Victor

52. Naar het oordeel van ACM beroept KPN zich ten onrechte op het door artikel 6 EVRM gewaarborgde zwijgrecht ten aanzien van Intern onderzoek Victor. Dit zwijgrecht gaat immers niet zover dat iedere vorm van medewerking aan het verzamelen van belastend materiaal kan worden geweigerd. ACM overweegt daartoe het volgende.

53. Voor de vraag of KPN zich met succes kan beroepen op haar zwijgrecht is van belang of er op het moment van de (eerste) informatievordering van OPTA d.d. 29 februari 2012 sprake was van een ‘criminal charge’. Er is sprake van een criminal charge vanaf het moment waarop van overheidswege jegens een (rechts)persoon een handeling is verricht waaruit deze persoon in redelijkheid moet vrezen voor vervolging, dan wel, in bestuursrechtelijke zin, redelijkerwijs uit die handeling heeft kunnen afleiden dat aan hem een punitieve sanctie zal worden opgelegd.

54. ACM meent dat op het moment van de informatievordering van 29 februari 2012 van een criminal charge (nog) geen sprake was. Zij merkt daartoe op dat OPTA, gelet op de haar wettelijk toegekende onderzoeksbevoegdheden, van KPN medewerking aan het door haar ingestelde onderzoek naar mogelijke overtreding van de zorgplicht van artikel 11.3 juncto artikel 11.2 Tw mocht verlangen. Aan het enkele gebruik van die toezichtshandelingen, zeker in dit stadium van het onderzoek, kon KPN niet redelijkerwijs de conclusie verbinden dat aan haar een boete opgelegd zou worden. De omstandigheid dat OPTA bij brief van 14 februari 2012 aan KPN heeft medegedeeld dat zij een onderzoek was gestart naar mogelijke overtreding van voormelde zorgplicht maakt dit niet

anders, daar uit het enkele instellen van een onderzoek in zijn algemeenheid en ook in deze zaak niet volgt dat een punitieve sanctie zal worden opgelegd. KPN was op basis van artikel 18.7 Tw verplicht aan voormelde informatievordering medewerking te verlenen en kon zich niet beroepen op haar zwijgrecht.

55. Intern onderzoek Victor is pas op 8 maart 2013 – dus bijna een jaar later – tezamen met de informatie die zag op een latere informatievordering toegezonden. Daarom kan niet gezegd worden dat ACM Intern onderzoek Victor onder dwang heeft verkregen. ACM meent dan ook dat zij Intern onderzoek Victor als bewijs mag gebruiken en dat dit gebruik niet in strijd is met artikel 6 EVRM.

56. Hieronder zal ACM aan de hand van de in randnummer 50 vermelde punten bezien of KPN op die punten aan de op haar rustende zorgplicht heeft voldaan. ACM wijst er op dat voormelde punten niet, zoals KPN meent, een zogenaamde 'vijftrapsraket' vormen, maar dat het treffen van onvoldoende maatregelen met betrekking tot een enkel op zichzelf staand aandachtspunt, of ten aanzien van een andere combinatie van meer of minder (andere) aandachtspunten, kan leiden tot de conclusie dat niet is voldaan aan de zorgplicht. ACM benadrukt daarbij tevens dat de omgekeerde situatie, dat wil zeggen de situatie waarin wordt voldaan aan voormelde punten, niet per definitie betekent dat is voldaan aan de zorgplicht. Per geval zal steeds moeten worden beoordeeld of aan de zorgplicht van artikel 11.3, eerste lid, juncto artikel 11.2 Tw is voldaan. Gelet op de samenhang in het onderhavige feitencomplex heeft ACM het in dit specifieke geval niettemin gepast geacht de geconstateerde tekortkomingen in hun onderlinge verband in ogenschouw te nemen. ACM komt vervolgens tot een daarop gebaseerd integraal oordeel over de vraag of in casu artikel 11.3, eerste lid, juncto artikel 11.2 Tw door KPN is overtreden.

57. ACM wijst er nog op dat om te kunnen vaststellen of het samenstel van de bevindingen in het onderzoeksrapport ten aanzien van de onderscheidenlijke aandachtsgebieden als een overtreding van artikel 11.3, eerste lid, Tw kan worden aangemerkt, de te beoordelen maatregelen moeten voldoen aan het gestelde in de tweede zin van artikel 11.3, eerste lid, Tw, namelijk:

    - dat de maatregelen een passend beveiligingsniveau dienen te garanderen dat in verhouding staat tot het desbetreffende risico;
    - waarbij rekening wordt gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging.

58. Of het beveiligingsniveau passend is in verhouding tot het desbetreffende risico, zal in de volgende paragrafen per aandachtsgebied worden besproken. Daarbij zal ook telkens kort aandacht worden besteed aan de ter zake relevante stand van de techniek. Het aspect van de

kosten van de tenuitvoerlegging zal separaat worden behandeld in paragraaf 6.7.

6.2 Opstellen en handhaven beveiligingsbeleid

59. Het opstellen en handhaven van een beveiligingsbeleid is een algemeen geldend en aanvaard onderdeel van informatiebeveiliging. Dit vormt ook een onderdeel van de informatiebeveiliging bij KPN. Ten aanzien van dit onderdeel merkt ACM het volgende op.

60. KPN heeft haar beveiligingsbeleid hiërarchisch opgezet, met als uitgangspunt onder andere de ISO-normen 27001 en 27002.[13]

61. In het onderzoeksrapport worden de volgende tekortkomingen geconstateerd ten aanzien van het opzetten en handhaven van beveiligingsbeleid door KPN in onderzoeksperiode I:

- Voor een aantal essentiële beveiligingsmaatregelen[14] was geen centraal beleid opgesteld, en werd de beslissing om hiervoor beleid op te stellen overgelaten aan de afdelingen. Voor de afdeling [vertrouwelijk] en haar voorgangers [vertrouwelijk] en [vertrouwelijk] is gebleken dat KPN voor deze beveiligingsmaatregelen geen beleid heeft opgesteld.[15]
- Het door KPN opgestelde centrale beveiligingsbeleid (CSP) kende een aantal verplichte beveiligingsmaatregelen waarvan moet worden vastgesteld dat in ieder geval één maatregel, namelijk patchmanagement, niet is ingevoerd en hier geen (centraal) beleid voor aanwezig was.[16]
- De verantwoordelijkheid voor het centrale beveiligingsbeleid (CSP) is tussen augustus 2011 en 15 januari 2012 meerdere malen verschoven binnen KPN. Gedurende circa vijf maanden is de positie van CISO[17] formeel niet ingevuld geweest. Dat heeft onder andere tot gevolg gehad dat de documentatie van het beveiligingsbeleid tussen augustus 2011 en 15 januari 2012 niet geactualiseerd werd.[18]
- Het onderhoud van het opgestelde beleid, zowel centraal als decentraal, heeft niet, of onvoldoende, plaatsgevonden. Het merendeel van de onderzochte beleidsdocumenten was op 15 januari 2012 meer dan één jaar niet bijgewerkt,

---

[13] Zie: Onderzoeksrapport, randnummer 119.

[14] Zie: Onderzoeksrapport, randnummers 121-143.

[15] Zie: Onderzoeksrapport, randnummers 123-131.

[16] Zie: Onderzoeksrapport, randnummers 120 en 144-156.

[17] De Corporate Security Policy van KPN is vastgelegd in documentatie. De verantwoordelijkheid voor dit beveiligingsbeleid en de bijbehorende documentatie ligt bij de Chief Information Security Officer (CISO)..

[18] Zie: Onderzoeksrapport, randnummers 159-161.

terwijl gedurende deze periode er wel veranderingen in omstandigheden plaats hebben gevonden.[19]

- ACM stelt op basis van het vorenstaande vast dat het KPN beveiligingsbeleid in onderzoeksperiode I niet volledig belegd was in de organisatie vanwege onbekendheid bij werknemers en/ of problemen bij de toepassing van het beleid door werknemers.

62. Gelet op het hierboven vermelde samenstel van tekortkomingen in het opstellen en handhaven van beveiligingsbeleid, komt ACM tot de conclusie dat KPN geen passend beveiligingsniveau kon garanderen voor het risico van doorbreking van de bescherming van de elektronisch opgeslagen persoonsgegevens.

63. ACM is van oordeel dat KPN ten aanzien van het opstellen en handhaven van beveiligingsbeleid onvoldoende rekening heeft gehouden met de eisen aan beveiligingsbeleid, zoals beschreven in paragraaf 9.1 van het onderzoeksrapport. In deze paragraaf wordt uiteengezet dat het opstellen, onderhouden en in de organisatie beleggen van informatiebeveiligingsbeleid een algemeen aanvaarde organisatorische maatregel is, en dat dergelijk beleid – wil het succesvol zijn belegd in de organisatie – bekend moet zijn en moet worden toegepast in alle relevante lagen en onderdelen van de betreffende organisatie.

64. Op basis van randnummer 114 van het onderzoeksrapport in samenhang met voorgaande randnummers, komt ACM tot de conclusie dat KPN op het gebied van het opstellen en handhaven van beleid onvoldoende passende maatregelen ten behoeve van de veiligheid en beveiliging van haar netwerken en diensten als bedoeld in artikel 11.3, eerste lid, Tw heeft genomen en dat KPN daarmee artikel 11.3, eerste lid, juncto artikel 11.2 Tw heeft overtreden.[20]

65. ACM stelt zich op het standpunt dat de fouten in hoofdstuk 9 van het onderzoeksrapport, waarop KPN in haar schriftelijke zienswijze wijst,[21] geen werkelijke fouten betreffen en in elk geval niet afdoen aan voorgaande conclusie.

66. Weliswaar was bij KPN sprake van een beveiligingsbeleid op centraal niveau, maar dit omvatte niet alle beveiligingsonderwerpen. Zo maakte patchmanagement bijvoorbeeld geen onderdeel uit van het centraal belegde beveiligingsbeleid. Het centrale beleid had bovendien een hoog

---

[19] Zie: Onderzoeksrapport, randnummers 157-158.

[20] Welke rechtspersoon binnen KPN aangemerkt wordt als overtreder en of deze rechtspersoon aan te merken is als een aanbieder van een openbare elektronische communicatiedienst en/of -netwerk wordt vastgesteld in paragraaf 6.9 van dit besluit (zie ook: hoofdstuk 16 van het onderzoeksrapport).

[21] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 10-11.

abstractieniveau. Daarbij is niet gebleken dat het decentrale beleid, dat op het centrale beveiligingsbeleid is gebaseerd, compleet was. KPN heeft niet weersproken dat met betrekking tot de meeste beveiligingsonderwerpen geen documenten voorhanden waren waarin op decentraal niveau per beveiligingsonderwerp (zoals ten aanzien van het onderwerp patchbeleid[22]) de te hanteren procedures en de verantwoordelijkheden per functie of personeelslid zijn vastgelegd.[23] ACM onderschrijft dan ook de conclusie in het onderzoeksrapport dat binnen KPN een informatiebeveiligingsbeleid wordt toegepast, gehandhaafd en onderhouden dat niet voldoet aan de in artikel 11.3, eerste lid, juncto artikel 11.2 Tw neergelegde zorgplicht. Hetzelfde geldt voor de constatering dat aan het onvoldoende opvolgen van dat beleid concrete consequenties blijken te zijn verbonden, waarmee onvoldoende invulling is gegeven aan de handhaving daarvan.

67. De stelling dat de rol van de Chief Information Security Officer (CISO) enige tijd is waargenomen door het Group Compliance Office van KPN, doet niet af aan de conclusie dat de verantwoordelijkheid voor het centrale beveiligingsbeleid (CSP) in de periode van augustus 2011 tot 15 januari 2012 meerdere malen is verschoven en dat het beveiligingsbeleid in diezelfde periode niet is geactualiseerd.

68. Het argument van KPN dat in het onderzoeksrapport ten onrechte wordt geconcludeerd dat zij haar beveiligingsbeleid niet of onvoldoende heeft onderhouden, werpt geen ander licht op de zaak. Nog daargelaten dat KPN dit argument niet nader heeft onderbouwd, doet het niet af aan de constatering in het onderzoeksrapport dat het merendeel van de onderzochte beleidsdocumenten vlak voor de hack in haar netwerk meer dan één jaar niet was bijgewerkt, terwijl er gedurende deze periode wel veranderingen in relevante omstandigheden hebben plaatsgevonden.[24]

6.3 Netwerkinrichting

69. ACM constateert dat de volgende tekortkomingen zijn vastgesteld ten aanzien van de

---

[22] ACM meent dat het door KPN overgelegde change- en patchoverzicht geen (sluitend) bewijs vormt van het voeren van adequaat beveiligingsbeleid met betrekking tot patchmanagement. Hieruit blijkt hoogstens dat er patches werden uitgevoerd. In tegenstelling tot hetgeen KPN daaromtrent beweert (zie: Schriftelijke zienswijze 29 augustus 2013, p. 10), blijkt ook nergens duidelijk uit dat patchmanagement in concreto onderdeel uitmaakt van het centrale beveiligingsbeleid (CSP) KPN.

[23] De inhoud van de bijlagen van het onderzoeksrapport (bijlagen 12 t/m 18, 20, 21, 23 en 25 KPN), waarnaar KPN verwijst (zie: Schriftelijke zienswijze 29 augustus 2013, p. 8) ter onderbouwing van het tegendeel, is onvoldoende concreet en toegesneden op de aan de orde zijnde beveiligingsonderwerpen, om een andersluidende conclusie te kunnen dragen

[24] Zie: Onderzoeksrapport, randnummers 157-158.

daadwerkelijke netwerkinrichting door KPN in onderzoeksperiode I:

- KPN had het eigen ontwerp van indeling in beveiligingszones niet nageleefd.[25]
- KPN had sommige IP-adressen in het [vertrouwelijk] aan meerdere systemen gekoppeld, wat fouten kan opleveren bij beheer. Daarbij waren zelfs gevallen waarbij [vertrouwelijk] wat de gevolgen van eventuele beheerfouten voor de bescherming van persoonsgegevens in beveiligingszones groter maakt.[26]
- KPN had aan meerdere systemen in de [vertrouwelijk] en in de [vertrouwelijk] een publiek IP-adres gekoppeld, waardoor deze in beginsel in directe verbinding kunnen staan met het openbare internet.[27]
- KPN had het netwerkbeheer (configuratiemanagement) niet op orde, wat bijvoorbeeld blijkt uit het feit dat KPN van [vertrouwelijk] systemen niet wist in welke beveiligingszone deze zich bevonden.[28]

70. Uit het hierboven vermelde samenstel van tekortkomingen in de netwerkinrichting blijkt dat KPN geen passend beveiligingsniveau kon garanderen voor het risico van doorbreking van de bescherming van de elektronisch opgeslagen persoonsgegevens.

71. ACM stelt vast dat KPN ten aanzien van de netwerkinrichting onvoldoende rekening heeft gehouden met de stand van de techniek,[29] zoals beschreven in paragraaf 10.1 van het onderzoeksrapport.

72. Op basis van randnummer 188 van het onderzoeksrapport in samenhang met voorgaande randnummers, is ACM van oordeel dat KPN op het gebied van netwerkinrichting onvoldoende passende maatregelen ten behoeve van de veiligheid en beveiliging van haar netwerken en diensten als bedoeld in artikel 11.3, eerste lid, Tw heeft genomen en dat KPN daarmee artikel 11.3, eerste lid, juncto artikel 11.2 Tw heeft overtreden.[30]

---

[25] Zie: Onderzoeksrapport, paragraaf 10.2.1.

[26] Zie: Onderzoeksrapport, randnummer 194.

[27] Zie: Onderzoeksrapport, randnummer 195.

[28] Zie: Onderzoeksrapport, paragraaf 10.2.3.

[29] Ook KPN zelf constateert in dit kader: *"De aanwezige principes [uit de netwerk- en security architectuur, toevoeging door ACM] zijn ook in een later stadium onvoldoende toegepast op bestaande omgevingen. De 'legacy' systemen van KPN voldoen hierdoor niet aan de huidige basisprincipes en stand van de techniek*", zie: Onderzoeksrapport, bijlage 8 KPN, Definitief rapport Intern onderzoek Victor, p. 15.

[30] Welke rechtspersoon binnen KPN aangemerkt wordt als overtreder en of deze rechtspersoon aan te merken is als een aanbieder van een openbare elektronische communicatiedienst en/of –netwerk wordt vastgesteld in paragraaf 6.9 van dit besluit (zie ook: hoofdstuk 16 van het onderzoeksrapport).

73. ACM stelt zich op het standpunt dat de fouten in hoofdstuk 10 van het onderzoeksrapport, waarop KPN in haar schriftelijke zienswijze wijst,[31] geen werkelijke fouten betreffen en in elk geval niet afdoen aan voorgaande conclusie.

74. KPN wijst er op dat zij meent toch te hebben voldaan aan het ontwerp van indeling in beveiligingszones, maar erkent tegelijkertijd dat er wel paden bestonden tussen netwerksegmenten. Deze enkele erkenning toont aan dat de in het onderzoeksrapport getrokken conclusie over het niet naleven van het ontwerp van indeling in beveiligingszones door KPN, wel degelijk valide is.

75. Verder wijst KPN er op dat de conclusie dat de kans op beheerfouten groter wordt [vertrouwelijk], niet mag worden getrokken. ACM volgt KPN niet in haar betoog. Hoewel het klopt dat [vertrouwelijk], kan dit wel problemen opleveren tijdens werkzaamheden in het kader van beheer. In dat geval is het immers mogelijk dat bij dergelijke werkzaamheden er een [vertrouwelijk], zodat het beheer mogelijk ongemerkt wordt uitgevoerd op het verkeerde systeem. In het onderzoeksrapport wordt dan ook terecht geconcludeerd dat deze omstandigheid beheerfouten kan opleveren die gevolgen kunnen hebben voor de bescherming van persoonsgegevens.[32]

76. KPN meent dat de conclusie dat het gebruik van publieke IP-adressen in de [vertrouwelijk] en de [vertrouwelijk] kan leiden tot direct contact tussen [vertrouwelijk] en het openbare internet, onjuist is. KPN meent dat dit geheel voorkomen kan worden door maatregelen in het kader van routering en filtering. Hoewel met dergelijke maatregelen direct contact in vorenbedoelde zin grotendeels kan worden voorkomen, is het vrijwel onmogelijk een volledig betrouwbare afsluiting te realiseren. Door zekerheidshalve geen publieke IP-adressen te gebruiken in [vertrouwelijk], wordt in elk geval wel voorkomen dat er vanuit het openbare internet direct verbinding kan worden gemaakt met de betreffende systemen. Dit komt de beveiliging van het gehele netwerk met daarin de opgeslagen persoonsgegevens ten goede. ACM gaat dan ook uit van de juistheid van de conclusies in het onderzoeksrapport.

77. Ook de conclusie uit het onderzoeksrapport dat KPN haar netwerkbeheer (configuratiebeheer) niet op orde had, wordt door KPN betwist. Hiertoe voert KPN aan dat het feit dat de van de zijde van KPN bij het onderzoek betrokken personen niet van het netwerkbeheer op de hoogte waren, niet betekent dat KPN als geheel in dat opzicht onwetend was. Het onderzoeksrapport[33] bevat meerdere op concreet onderzoek steunende aanknopingspunten[34]

---

[31] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 11-12.

[32] Zie: Onderzoeksrapport, randnummer 201.

[33] Zie: Onderzoeksrapport, randnummers 197-199.

die de conclusie ondersteunen dat KPN haar netwerkbeheer (configuratiebeheer) niet op orde had. Zo heeft KPN niet betwist dat gedurende de periode na de hack een lijst werd bijgehouden – de zogenoemde '[vertrouwelijk] list' – met mogelijk door de hack getroffen systemen. Op [vertrouwelijk] list stond vermeld welk systeem zich in welke zone bevond. Uit de lijst blijkt dat van 146 systemen onbekend was in welke beveiligingszone deze systemen zich bevonden.[35] Gelet op het vorenstaande komt ACM dan ook tot de conclusie dat KPN haar netwerkbeheer niet op orde had.

6.4 Afscherming

78. ACM constateert dat de volgende tekortkomingen zijn vastgesteld ten aanzien van de afscherming door KPN in onderzoeksperiode I:

- De firewall tussen [vertrouwelijk] en [vertrouwelijk] stond voor een aantal servers open voor alle verkeer via de poorten boven poortnummer [vertrouwelijk].[36] Daardoor was het eenvoudiger deze poorten te misbruiken voor andere toepassingen dan de toepassingen waarvoor KPN enkele van deze poorten nodig had.
- Er was geen firewall tussen [vertrouwelijk] en [vertrouwelijk] ,[37] wat de afscherming tussen de twee beveiligingszones relatief zwak maakt.
- De ACL's[38] die de scheidingen tussen de verschillende diensten bepaalden, waren te generiek ingesteld.[vertrouwelijk] Door deze te generieke instelling kunnen de scheidingen makkelijk overbrugd worden en worden de systemen kwetsbaar. Daardoor vermindert de bescherming van persoonsgegevens op die systemen.
- Zodoende was er voor het misbruiken van de kwetsbaarheid in de afscherming geen geavanceerde kennis of programmatuur nodig.[39]
- De documentatie die door KPN is verstrekt omtrent het afschermbeleid met ACL's

---

[34] Bij gebreke van een nadere onderbouwing van dit betoog, ziet ACM ziet op voorhand geen aanleiding te twijfelen aan het kennisniveau van de aangehaalde bronnen met betrekking tot de wijze waarop KPN haar netwerkbeheer ten tijde van het onderhavige onderzoek had vormgegeven.

[35] Zie: Bijlage ACM 9, Verslag interview dhr. [X] op 5 december 2012, p. 45-46.

[36] Zie: Onderzoeksrapport, randnummer 229.

[37] Zie: Onderzoeksrapport, bijlage 3 KPN, Reactie op informatievordering, geen kenmerk, afzender de heer [Y], antwoord op vraag 14.

[38] Deze afkorting staat voor Access Control List (ACL), hetgeen een (primitieve) firewall is in een netwerk, welke firewall feitelijk functioneert als filter, Bedoeld filter bestaat uit een lijst met regels, die wordt toegepast op elk datapakket dat bij de firewall aankomt. De firewall loopt vervolgens de lijst met regels af en bepaalt op basis daarvan of een datapakket de firewall mag passeren of dat deze erdoor tegengehouden wordt.

[39] Zie: Onderzoeksrapport, randnummer 74.

voor het [vertrouwelijk], bevat onvoldoende beleid voor de manier waarop ACL's moeten zijn opgezet.[40] Daardoor kunnen makkelijker onregelmatigheden of fouten in de opzet van ACL's ontstaan, wat een risico vormt voor de bescherming van de opgeslagen persoonsgegevens in het netwerk.

- Uit de documentatie die door KPN is verstrekt omtrent het afschermbeleid met ACL's voor het [vertrouwelijk] valt niet op te maken in hoeverre deze geldt voor het gehele [vertrouwelijk].[41]

79. Uit het hierboven vermelde samenstel van tekortkomingen in de afscherming blijkt dat KPN geen passend beveiligingsniveau kon garanderen voor het risico van doorbreking van de bescherming van de elektronisch opgeslagen persoonsgegevens.

80. ACM stelt vast dat KPN ten aanzien van de afscherming onvoldoende rekening heeft gehouden met de stand van de techniek, zoals beschreven in paragraaf 11.1 van het onderzoeksrapport.

81. Op basis van randnummer 221 van het onderzoeksrapport in samenhang met voorgaande randnummers, is ACM van oordeel dat KPN op het gebied van afscherming onvoldoende passende maatregelen ten behoeve van de veiligheid en beveiliging van haar netwerken en diensten als bedoeld in artikel 11.3, eerste lid, Tw heeft genomen en dat KPN daarmee artikel 11.3, eerste lid, juncto artikel 11.2 Tw heeft overtreden.[42]

82. ACM stelt zich op het standpunt dat de fouten in hoofdstuk 11 van het onderzoeksrapport, waarop KPN in haar schriftelijke zienswijze wijst,[43] geen werkelijke fouten betreffen en in elk geval niet afdoen aan voorgaande conclusie.

83. KPN wijst er in dit verband op dat de betreffende poort tussen de systemen in de verschillende zones wel open moest staan om mogelijk te maken dat er [vertrouwelijk] kunnen worden gemaakt, omdat de [vertrouwelijk] applicatie anders in het geheel niet zou kunnen functioneren. Daarom is KPN van mening dat een firewall de hack niet had kunnen voorkomen. Volgens ACM gaat KPN daarmee voorbij aan het feit dat niet alleen de poort voor dataverkeer open stond die nodig was voor het functioneren van de [vertrouwelijk] (te weten, poort [vertrouwelijk]), maar ook alle poorten [vertrouwelijk]. Deze – niet door KPN betwiste –

---

[40] Zie: Onderzoeksrapport, randnummers 222-224.

[41] Zie: Onderzoeksrapport, randnummer 136.

[42] Welke rechtspersoon binnen KPN aangemerkt wordt als overtreder en of deze rechtspersoon aan te merken is als een aanbieder van een openbare elektronische communicatiedienst en/of -netwerk, wordt vastgesteld in paragraaf 6.9 van dit besluit (zie ook: hoofdstuk 16 van het onderzoeksrapport).

[43] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 12-13.

omstandigheid heeft in belangrijke mate bijgedragen aan de in het onderzoeksrapport opgenomen conclusie dat het eenvoudig was de betreffende poort(en) te misbruiken om toegang te verkrijgen tot het netwerk van KPN. Verder is tijdens de hoorzitting die op 25 september 2013 heeft plaatsgevonden door KPN erkend dat – in tegenstelling tot wat KPN daaromtrent beweert in haar schriftelijke zienswijze – er weliswaar een fysieke netwerkconnectie bestond tussen de [vertrouwelijk] en [vertrouwelijk], maar dat die verbinding wel een zekere mate van afscherming kent. KPN wil hiermee blijkbaar bepleiten dat het weinig kwaad kon dat de poorten openstonden omdat die afscherming bestond tussen de [vertrouwelijk] en [vertrouwelijk]. In meer algemene zin is in het voorgaande echter al toegelicht dat de afschermingsmaatregelen die KPN had getroffen niet naar behoren waren. ACM is dan ook van oordeel dat aan het enkele verweer dat er sprake was van enige vorm van afscheiding tussen de [vertrouwelijk] en [vertrouwelijk] in dit verband geen doorslaggevend gewicht kan worden toegekend.

84. [Vertrouwelijk].

85. [Vertrouwelijk]. Dit heeft tot gevolg dat zij, om te zorgen dat haar performance op peil blijft, keuzes moet maken ten aanzien van firewallbescherming en netwerksegmentatie. In het onderzoek is daar ten onrechte aan voorbij gegaan en is geen onderzoek gedaan naar de stand van de techniek specifiek ten aanzien van KPN. De complexiteit van haar organisatie is eveneens ten onrechte buiten beschouwing gelaten, aldus KPN.

86. ACM wijst er op dat ten tijde van de onderzoeksperiodes in het rapport geen specifieke beveiligingsmaatregelen in artikel 11.3, eerste lid, Tw stonden vermeld. OPTA en later ACM hebben er daarom voor gekozen het onderzoek te beperken tot de beveiligingsonderwerpen die in de vakliteratuur als algemeen geldend en aanvaard gesteld worden en direct raken aan de hack, die de aanleiding tot het onderzoek vormde. ACM ziet niet in waarom deze algemeen geldende en aanvaarde beveiligingsonderwerpen anders zouden zijn voor KPN, noch waarom de stand van de techniek ten opzichte van KPN zou verschillen van andere bedrijven. ACM gaat dus uit van de beveiligingsonderwerpen die destijds in de vakliteratuur als algemeen geldend en aanvaard gesteld werden en die ook in het rapport van Fox-IT en Intern onderzoek Victor aan bod komen.

87. Een van die beveiligingsonderwerpen betreft afscherming. Een netwerk dat met het openbare internet is verbonden, zoals het [vertrouwelijk] van KPN, zal een bepaalde mate van afscherming moeten hebben om te voorkomen dat systemen op dat netwerk vanaf het internet te benaderen zijn. In het onderzoeksrapport worden de verschillende vormen van afscherming in het algemeen besproken en vervolgens is de afscherming van het netwerk van KPN tegen het licht gehouden. Het is dus niet zo dat ACM daaraan, zoals gesteld, is voorbij gegaan.

88. Tijdens het onderzoek is vastgesteld – en dit wordt door KPN ook erkend – dat om performance redenen de firewall tussen [vertrouwelijk] en [vertrouwelijk] open stond voor alle verkeer via de poorten boven poortnummer [vertrouwelijk]. Evenmin was om die reden een firewall geplaatst tussen [vertrouwelijk] en [vertrouwelijk] van het [vertrouwelijk], waardoor de hacker toegang kon krijgen tot systemen waarop [vertrouwelijk] geïnstalleerd was en die zich in de [vertrouwelijk] bevonden [vertrouwelijk]. De afscherming tussen deze twee zones was dus relatief zwak.

89. Naar het oordeel van ACM ontslaan overwegingen met betrekking tot performance KPN niet van haar verplichting om persoonsgegevens die zijn opgeslagen in de systemen die onderdeel uitmaken van haar netwerk, afdoende te beveiligen, hetgeen naar de stand van de techniek ten tijde van de onderzoeksperiodes ook mogelijk was. Dat KPN daarbij wellicht verkeerde keuzes of afwegingen heeft gemaakt is een omstandigheid die voor haar eigen risico komt.

90. Hetzelfde geldt voor de complexiteit van haar organisatie. Dat KPN, zoals zij stelt, een conglomeraat van organisaties en bedrijven is en dat haar legacy maakt dat systeembeheer eindeloos meer complex is dan in jonge, kleine organisaties, die 'from scratch' opnieuw kunnen beginnen,[44] moge zo zijn. Deze omstandigheid ontslaat een professionele marktpartij als KPN echter evenmin van haar verplichting om persoonsgegevens die op haar netwerk zijn opgeslagen afdoende te beveiligen. Daarnaast blijkt uit Intern onderzoek Victor dat de basisprincipes waarmee bij netwerk- en security architectuur rekening moet worden gehouden[45] onvoldoende zijn toegepast op bestaande systemen. De legacy-systemen van KPN voldeden hierdoor niet aan die basisprincipes en stand van de techniek.

6.5 Netwerk- en systeembewaking

91. ACM constateert dat de volgende tekortkomingen zijn vastgesteld ten aanzien van de netwerk- en systeembewaking door KPN in onderzoeksperiode I:

> Het [vertrouwelijk] had geen systemen voor intrusion detection en voor intrusion prevention (IDS en IPS).[46]
> Er was geen centrale logging.[47]
> De logging die er wel was, registreerde geen gebeurtenissen met betrekking tot uitgaand verkeer.[48]

---

[44] Zie verslag van de hoorzitting van 25 september 2013, p. 4.

[45] Security by design, Defence in depth, Least privilege, Default deny en Fail secure.

[46] Zie: Onderzoeksrapport, paragraaf 12.2.2.

[47] Zie: Onderzoeksrapport, randnummer 260.

[48] Zie: Onderzoeksrapport, randnummer 260.

> Logbestanden waren niet altijd te achterhalen.[49]
> De monitoring die er was in het [vertrouwelijk] heeft de onregelmatigheid in het netwerkverkeer, dat door de hack is veroorzaakt) niet gesignaleerd.[50] De monitoring was niet effectief.

92. Uit het hierboven vermelde samenstel van tekortkomingen in de netwerk- en systeembewaking blijkt dat KPN geen passend beveiligingsniveau kon garanderen voor het risico van doorbreking van de bescherming van de elektronisch opgeslagen persoonsgegevens.

93. ACM stelt vast dat KPN ten aanzien van de netwerk- en systeembewaking onvoldoende rekening heeft gehouden met de stand van de techniek, zoals beschreven in paragraaf 12.1 van het onderzoeksrapport.

94. Op basis van randnummer 258 van het onderzoeksrapport in samenhang met voorgaande randnummers, is ACM van oordeel dat KPN op het gebied van netwerk- en systeembewaking onvoldoende passende maatregelen ten behoeve van de veiligheid en beveiliging van haar netwerken en diensten als bedoeld in artikel 11.3, eerste lid, Tw heeft genomen en dat KPN daarmee artikel 11.3, eerste lid, juncto artikel 11.2 Tw heeft overtreden.[51]

95. ACM stelt zich op het standpunt dat de fouten in hoofdstuk 12 van het onderzoeksrapport, waarop KPN in haar schriftelijke zienswijze wijst,[52] geen werkelijke fouten betreffen en in elk geval niet afdoen aan voorgaande conclusie.

96. KPN is het niet eens met de in het onderzoeksrapport getrokken conclusie dat er geen IDS en IPS werd toegepast in het [vertrouwelijk] en dat onvoldoende centrale en achterhaalbare logging plaatsvond. Er is volgens KPN ten onrechte geen rekening gehouden met de omstandigheid dat zij inmiddels een project heeft opgestart om een verbeterde monitoring en bewaking in te voeren bij de 'IT-datacenters', waaronder het instellen van een Security Operations Center (SOC). Verder wijst KPN er op dat zij ten tijde van de hack al wel over een zogenoemde '[vertrouwelijk]' beschikte die virussen en spam signaleert en waarvan de werking volgens haar vergelijkbaar is met IDS en het inrichten van een goede systeembewaking nu eenmaal complex en tijdrovend is. Verder meent KPN dat aan het onopgemerkt blijven van één beveiligingsincident niet de conclusie kan worden verbonden dat de wijze waarop

---

[49] Zie: Onderzoeksrapport, randnummer 261.

[50] Zie: Onderzoeksrapport, randnummers 262 en 267.

[51] Welke rechtspersoon binnen KPN aangemerkt wordt als overtreder en of deze rechtspersoon aan te merken is als een aanbieder van een openbare elektronische communicatiedienst en/of -netwerk wordt vastgesteld in paragraaf 6.9 van dit besluit (zie ook: hoofdstuk 16 van het onderzoeksrapport).

[52] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 13.

monitoring van haar netwerk plaatsvond, niet effectief is.

97. In het onderzoeksrapport[53] wordt geconcludeerd dat logmanagement, waaronder centrale logging, intrusion detection systems, intrusion prevention systems en monitoring tot de te treffen passende maatregelen behoren. Deze maatregelen zijn hoofdzakelijk van technische aard, zoals bedoeld in artikel 11.3, eerste lid, Tw. Deze vier maatregelen behoren tot de stand van de techniek ten tijde van onderzoeksperiode I. KPN suggereert dat van haar redelijkerwijs nog niet kon worden verwacht dat zij de genoemde maatregelen inzake netwerkbewaking naar behoren had getroffen ten tijde van onderzoeksperiode I. Zij volstaat in dat verband met het argument dat het complex en tijdrovend is om dergelijke maatregelen te treffen. Wat daar ook van zij, die omstandigheid ontslaat KPN er op zichzelf niet van maatregelen inzake netwerkbewaking tijdig, naar behoren en volledig te treffen.

98. In het onderzoeksrapport wordt overwogen dat KPN ten tijde van onderzoeksperiode I gelet op de geconstateerde tekortkomingen in de netwerk- en systeembewaking, geen passend beveiligingsniveau kon garanderen voor het risico van doorbreking van de bescherming van de elektronisch opgeslagen persoonsgegevens.[54]

99. Hetgeen KPN in dit verband heeft aangevoerd, staat naar oordeel van ACM niet in de weg aan de conclusie dat de geconstateerde tekortkomingen in de netwerk- en systeembewaking haar kan worden verweten. Dat reeds een begin was gemaakt met het treffen van maatregelen doet daaraan niet af. Het betoog dat het onopgemerkt blijven van één incident niet de conclusie rechtvaardigt dat de wijze waarop monitoring van het netwerk van KPN plaatsvond, niet effectief is, leidt niet tot een andere conclusie. Het gaat immers niet om de constatering dat de hack onopgemerkt is gebleven, maar om de vaststelling dat de door KPN getroffen maatregelen met betrekking tot netwerk- en systeembewaking geen passend beveiligingsniveau konden garanderen ten tijde van onderzoeksperiode I.

100. Voor zover KPN in haar schriftelijke zienswijze heeft aangegeven dat ACM ten onrechte geen rekening heeft gehouden met projecten om monitoring te verbeteren, waaronder [vertrouwelijk], wijst ACM er op dat KPN op de hoorzitting desgevraagd heeft verklaard dat dit project geen betrekking had op het door de hacker gehackte [vertrouwelijk], maar op een ander bedrijfsonderdeel. In het kader van het onderzoek naar aanleiding van de hack was [vertrouwelijk] in de optiek van ACM dan ook niet relevant.

101. Het beroep dat KPN doet op de zogenoemde '[vertrouwelijk]' treft evenmin doel. KPN heeft op de hoorzitting de werking van deze [vertrouwelijk] desgevraagd toegelicht. De [vertrouwelijk]

---

[53] Zie: Onderzoeksrapport, randnummer 258.

[54] Zie: Onderzoeksrapport, randnummer 270.

was specifiek bedoeld om oneigenlijk gebruik van het netwerk door onbevoegde personen te ondervangen voor zover het e-mail betrof. KPN heeft op de hoorzitting bevestigd dat deze [vertrouwelijk] niet geschikt was om de onderhavige hack te detecteren.[55]

6.6 Patchmanagement

102. ACM constateert dat de volgende tekortkomingen zijn vastgesteld ten aanzien van patchmanagement door KPN in onderzoeksperiode I:

- Gedurende onderzoeksperiode I bestond er geen (centraal) beleid met betrekking tot patchmanagement en geen centrale coördinatie van kwetsbaarheden in systemen en oplossingen hiervoor.[56]
- De in onderzoeksperiode I uitgevoerde werkzaamheden met betrekking tot het vinden van kwetsbaarheden werd slechts voor een deel van het [vertrouwelijk] uitgevoerd, en er was geen coördinatie en/of communicatie tussen de afdeling die kwetsbaarheden opspoorde en de afdelingen die deze kwetsbaarheden moesten opheffen.[57]
- De software [vertrouwelijk] was binnen het [vertrouwelijk] geïnstalleerd op veel servers. De geïnstalleerde versies van deze software bevatten een kwetsbaarheid die een aanvaller van buiten de mogelijkheid bood root-rechten op de betreffende systemen te krijgen, willekeurige programmatuur op deze systemen te plaatsen en alle bestanden op deze systemen te bereiken.[58]
- Deze kwetsbaarheid is publiek gemaakt door de leverancier en door beveiligingsorganisaties in juni 2011. In december 2011 is KPN door KPMG er op gewezen dat KPN deze kwetsbare softwareversie gebruikte. Op 15 januari 2012 gebruikte KPN nog steeds verschillende softwareversies van [vertrouwelijk] met bovengenoemde kwetsbaarheid.[59] Het feit dat de door de leverancier aangeboden patch niet afdoende de kwetsbaarheid oploste, zoals aangegeven door KPN,[60] doet hierbij niet ter zake. KPN heeft namelijk pas ná[61] de hack actie ondernomen om de desbetreffende patch, die nog niet door KPN was geïnstalleerd, te analyseren en te

[55] Zie: Verslag van de hoorzitting d.d. 25 september 2013, p. 22-23.

[56] Zie: Onderzoeksrapport, randnummer 286.

[57] Zie: Onderzoeksrapport, randnummers 288-290.

[58] Zie: Onderzoeksrapport, randnummers 70-75 en 292.

[59] Zie: Onderzoeksrapport, randnummer 294.

[60] Zie: Onderzoeksrapport, bijlage 3 KPN, Reactie op informatievordering, geen kenmerk, afzender de heer [Y] gedateerd 14 maart 2012, antwoord op vraag 14.

[61] Zie: Onderzoeksrapport, bijlage 5 ACM, Verslag bijeenkomst KPN-OPTA op 4 april 2012, p. 29.

testen (samen met Fox IT).[62] KPN had dit direct na bekendwording moeten doen en had, toen bleek dat de patch onvoldoende effect zou hebben, andere technische maatregelen moeten nemen om de kwetsbaarheid tegen te gaan.

- Voor het misbruiken van de kwetsbaarheid in [vertrouwelijk] was geen geavanceerde kennis of programmatuur nodig.[63]
- KPN had met een eenvoudige penetratietest van het [vertrouwelijk] de kwetsbaarheid in de software van [vertrouwelijk] - en daarmee de noodzaak tot het installeren van een patch - kunnen detecteren.[64]
- KPN hield geen patchhistorie bij. Dit had onder meer tot gevolg dat voor de [vertrouwelijk] software KPN geen patch-historie heeft kunnen overleggen.[65]

103. Uit het hierboven vermelde samenstel van tekortkomingen in het patchmanagement blijkt dat KPN geen passend beveiligingsniveau kon garanderen voor het risico van doorbreking van de bescherming van de elektronisch opgeslagen persoonsgegevens.

104. ACM stelt vast dat KPN ten aanzien van patchmanagement onvoldoende rekening heeft gehouden met de stand van de techniek, zoals beschreven in paragraaf 13.1.

105. Op basis van randnummer 285 van het onderzoeksrapport in samenhang met voorgaande randnummers is ACM van oordeel dat KPN op het gebied van patchmanagement onvoldoende passende maatregelen ten behoeve van de veiligheid en beveiliging van haar netwerken en diensten als bedoeld in artikel 11.3, eerste lid, Tw heeft genomen en dat KPN daarmee artikel 11.3, eerste lid, juncto artikel 11.2 Tw heeft overtreden.[66]

106. ACM stelt zich op het standpunt dat de fouten in hoofdstuk 13 van het onderzoeksrapport, waarop KPN in haar schriftelijke zienswijze wijst,[67] geen werkelijke fouten betreffen en in elk

---

[62] Zie: Onderzoeksrapport, bijlage 3 KPN, Reactie op informatievordering, geen kenmerk, afzender de heer [Y] gedateerd 14 maart 2012, antwoord op vraag 14.

[63] Zie: Onderzoeksrapport, randnummer 74.

[64] Zie: Onderzoeksrapport, bijlage 9 KPN, Rapportage Fox-IT gedateerd 22 februari 2012, p. 3.

[65] Zie: Onderzoeksrapport, bijlage 3 KPN, Reactie op informatievordering, geen kenmerk, afzender de heer [Y] gedateerd 14 maart 2012, antwoord op vraag 14. Door middel van deze vraag 14 vorderde OPTA de patch- en update historie en de door KPN daadwerkelijke uitgevoerde patches en updates van [vertrouwelijk], inclusief datumvermelding, zie: Onderzoeksrapport, bijlage 4 ACM, Informatievordering, kenmerk OPTA/ACNB/2012/200646, gedateerd 29 februari 2012.

[66] Welke rechtspersoon binnen KPN aangemerkt wordt als overtreder en of deze rechtspersoon aan te merken is als een aanbieder van een openbare elektronische communicatiedienst en/of -netwerk wordt vastgesteld in paragraaf 6.9 van dit besluit (zie ook: hoofdstuk 16 van het onderzoeksrapport).

[67] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 13.

geval niet afdoen aan voorgaande conclusie.

107. In reactie op de conclusie in het onderzoeksrapport dat er geen centraal beleid bestond met betrekking tot patchmanagement en er geen centrale coördinatie was van kwetsbaarheden in systemen en oplossingen hiervoor, wijst KPN er nogmaals op dat zij wel degelijk over een decentraal patchbeleid beschikt. Volgens KPN was elke beheerafdeling zelf verantwoordelijk voor de keuzes die met betrekking tot implementatievraagstukken werden gemaakt.

108. Verder voert KPN aan dat de servers van [vertrouwelijk] inderdaad niet werden gescand met de software [vertrouwelijk] van [vertrouwelijk], maar dat [vertrouwelijk] wel degelijk beschikte over een uitgebreid patchbeleid en dat het feit dat de ene afdeling geen zeggenschap had over wat er met de scanresultaten werd gedaan, nog niet betekent dat die scans geen onderdeel vormen van het decentrale beleid.

109. Dat er, zoals KPN stelt, sprake was van gedecentraliseerd patchmanagement, doet niet af aan de conclusie dat deze vorm van management als onvolledig kon/kan worden beschouwd. In elk geval was de verantwoordelijkheid voor patchmanagement binnen KPN niet centraal gecoördineerd. Zoals KPN ook zelf heeft geconcludeerd is centrale coördinatie noodzakelijk om een totaaloverzicht te behouden van aanwezige kwetsbaarheden en risico's en dienen daartoe structureel KPN-breed ervaringen te worden uitgewisseld.[68] Dit gebeurde blijkbaar niet. ACM volgt dan ook de conclusie in het onderzoeksrapport dat gedurende onderzoeksperiode I binnen KPN geen centraal beleid bestond met betrekking tot patchmanagement, en er ook geen sprake was van centrale coördinatie van kwetsbaarheden in systemen en oplossingen hiervoor.

110. Verder ondersteunt het feit dat KPN heeft aangevoerd dat de servers van [vertrouwelijk] inderdaad niet werden gescand met de software [vertrouwelijk] van [vertrouwelijk], de conclusie dat de in onderzoeksperiode I uitgevoerde werkzaamheden met betrekking tot het vinden van kwetsbaarheden slechts voor een deel van het [vertrouwelijk] werd uitgevoerd. ACM erkent dat aan het enkele feit dat aan de praktijk dat er geen coördinatie en/of communicatie was tussen de afdeling die kwetsbaarheden opspoorde en de afdelingen die deze kwetsbaarheden moesten opheffen, niet zonder meer de gevolgtrekking kan worden verbonden dat het uitvoeren van scans überhaupt geen onderdeel uitmaakt van het decentrale patchbeleid van KPN (hetgeen overigens ook niet wordt geconcludeerd in het onderzoeksrapport). Duidelijk is echter dat een gebrek aan coördinatie en/of communicatie in dit geval heeft geleid tot een gebrek aan overzicht met betrekking tot de aanwezige kwetsbaarheden en risico's in de systemen en netwerken van KPN.

---

[68] Zie: Onderzoeksrapport, randnummer 156.

111. Dat het naar behoren patchen van de software van de [vertrouwelijk] mogelijk geen grote verbetering in het niveau van informatiebeveiliging zou opleveren, zoals KPN beweert, rechtvaardigt niet dat die software gedurende een aanzienlijke periode helemaal niet is gepatcht, noch dat geen patchhistorie is bijgehouden. De keuze om van een patch af te zien, had schriftelijk moeten worden verantwoord. Hetzelfde geldt voor eventuele andere maatregelen. In dat geval is het voor de gehele organisatie duidelijk op grond van welke overwegingen keuzes zijn gemaakt. Dat in casu aan deze eis niet is voldaan blijkt, zoals reeds eerder opgemerkt, al uit het feit dat KPN voor de [vertrouwelijk] software überhaupt geen patchhistorie heeft kunnen overleggen.

6.7 Kosten van tenuitvoerlegging

112. De kosten van tenuitvoerlegging van de hierboven genoemde maatregelen worden blijkens het onderzoeksrapport niet disproportioneel geacht. Daarin wordt geoordeeld dat deze maatregelen onderdeel uitmaken van de algemene informatiebeveiliging en ter bescherming dienen van de zakelijke belangen van KPN, zoals beschreven in randnummer 117 van het onderzoeksrapport. De maatregelen worden derhalve niet specifiek genomen in het kader van artikel 11.3, eerste lid, Tw. In het onderzoeksrapport wordt geoordeeld dat de kostenoverweging van de tenuitvoerlegging van deze maatregelen door KPN niet, of in ieder geval niet voor een substantieel deel, gerelateerd kan worden aan de maatregelen die in het kader van artikel 11.3, eerste lid, Tw dienen te worden genomen.

113. ACM ziet geen concrete aanknopingspunten om het in het onderzoeksrapport vervatte oordeel inzake de kosten van tenuitvoerlegging van de hierboven genoemde maatregelen niet te volgen of onzorgvuldig te achten (zoals KPN suggereert). Daarbij neemt ACM in ogenschouw dat uit niets blijkt dat het maken van dergelijke kosten geen onderdeel behoort te zijn van de normale zorgvuldige bedrijfsvoering van een aanbieder van (openbare) elektronische communicatiediensten en/of dit netwerken. Evenmin is concreet gebleken dat in dit geval bij het vaststellen van de maatregelen die volgens het onderzoeksrapport minimaal nodig zijn (om een passend beveiligingsniveau te garanderen), in de zin van artikel 11.3, eerste lid, Tw, onvoldoende rekening is gehouden met kosten van de tenuitvoerlegging (in samenhang bezien met de stand van de techniek).

114. KPN heeft in dit verband betoogd dat het wel degelijk zo is dat het nemen van de maatregelen die blijkens het onderzoeksrapport verplicht worden geacht, zou leiden tot disproportionele kosten. Dat wordt volgens haar al aangetoond door het enkele feit dat zij dagelijks meer dan 26.000 pogingen tot inbraak in haar systemen/netwerken weet af te weren. Het maken van kosten voor een veel hoger beveiligingsniveau naar aanleiding van één geslaagde hack is alleen op basis daarvan al disproportioneel te noemen volgens KPN. Ter illustratie wijst KPN er op dat wanneer zij al haar systemen continu volledig zou patchen, de kosten daarvan

zouden neerkomen op [vertrouwelijk] terwijl er alternatieve beveiligingsmogelijkheden zijn met aanzienlijk lagere kosten.

115. KPN lijkt met het voorgaande te bepleiten dat in het onderzoeksrapport tot uitgangspunt is genomen dat KPN haar systemen en netwerken zodanig dient te patchen/beveiligen dat het volstrekt onmogelijk wordt daarop in te breken. De inhoud van het onderzoeksrapport biedt echter geen concrete aanknopingspunten om te komen tot een dergelijke conclusie. Daarin wordt immers overwogen dat de te treffen maatregelen onderdeel uitmaken van de algemene informatiebeveiliging (en overigens ook zouden dienen ter bescherming van de zakelijke belangen van KPN).[69] Verder wordt over patchmanagement opgemerkt dat er in beginsel ruimte is voor het maken van een afweging om de patch al dan niet te installeren[70] en het voldoende is de *noodzakelijke* patches door te voeren.[71] In elk geval dienen wel minimaal zodanige maatregelen te worden genomen – onder andere met betrekking tot patchmanagement – dat een passend beveiligingsniveau is gegarandeerd dat in verhouding staat tot het desbetreffende risico (rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging).

116. Uit het verweer van KPN blijkt niet concreet waarom het (met passende maatregelen corresponderende) beveiligingsniveau dat in het onderzoeksrapport als uitgangspunt wordt gehanteerd, voor KPN zou leiden tot disproportionele kosten. In elk geval blijkt niet concreet uit het onderzoeksrapport dat KPN kosten moet maken voor het bewerkstelligen van een onredelijk hoog beveiligingsniveau naar aanleiding van één geslaagde hack. KPN heeft te kennen gegeven een dergelijke eis disproportioneel te achten. Als maatstaf is echter 'een passend beveiligingsniveau' in de zin van artikel 11.3, eerste lid, Tw gehanteerd. Uit het onderzoeksrapport volgt dat daarvan in casu geen sprake is. Als criterium is niet gebruikt dat KPN zodanige maatregelen moet treffen dat incidenten nooit meer plaats zullen vinden.

6.8 Bespreking overige bedenkingen KPN

117. Zoals reeds is opgemerkt, voert KPN aan dat ACM bij de handhaving van haar bevoegdheden onzorgvuldig en willekeurig te werk is gegaan. Ten eerste wordt in het rapport vrijwel alleen uitgegaan van de gegevens die door KPN zelf zijn aangeleverd, zoals het Fox-IT-rapport, Intern onderzoek Victor en de interviews met medewerkers van KPN. Er zou moeten worden beoordeeld of KPN, alle genomen maatregelen in aanmerking nemend, over het geheel genomen heeft voldaan aan de zorgplicht in plaats van alle nadruk te leggen op beveiligingsonderwerpen die geheel lijken te zijn gebaseerd op de bevindingen van KPN zelf.

---

[69] Zie: Onderzoeksrapport, (o.a.) randnummer 170.

[70] Zie: Onderzoeksrapport, randnummer 283.

[71] Zie: Onderzoeksrapport, randnummer 284.

Verder wijst KPN er in dit verband op dat het onderzoeksrapport de schijn wekt dat een doelredenering is gebruikt, waarbij het uitgangspunt wordt gehuldigd dat het enkele plaatsvinden van de hack afdoende bewijs is voor de conclusie dat de zorgplicht is geschonden.

118. KPN lijkt daarmee te bepleiten dat de wettelijke zorgplicht zo moet worden verstaan, dat aan de toets of aan de uitgangspunten daarvan is voldaan, een systeem van communicerende vaten ten grondslag ligt. ACM heeft in de inleiding van hoofdstuk 6 van dit besluit reeds uiteengezet waarom zij KPN niet volgt in dit betoog. Evenmin zijn er rechtsregels of fundamentele rechtsbeginselen die zich er zonder meer tegen verzetten dat de in een onderzoeksrapport opgenomen conclusies omtrent het begaan van een overtreding, mede worden gebaseerd op onderzoek dat de betrokkene zelf heeft verricht, waaruit feiten en/of omstandigheden blijken die kunnen bijdragen aan het komen tot die conclusies.

119. Dat ACM haar conclusies vooral baseert op de gebreken die zijn geconstateerd ten aanzien van beveiligingsonderwerpen waarop KPN haar eigen onderzoek heeft geconcentreerd, rechtvaardigt niet de conclusie dat ACM onvoldoende onderzoek heeft verricht. Indien wordt geconstateerd dat slechts ten aanzien van één beveiligingsonderwerp onvoldoende passende maatregelen zijn genomen, kan dit in beginsel reeds leiden tot de conclusie dat de wettelijke zorgplicht niet is nageleefd. De in artikel 11.3, eerste lid, juncto artikel 11.2 Tw neergelegde regeling sluit dit in geen enkel opzicht uit. Ook is het denkbaar dat deze conclusie wordt getrokken naar aanleiding van het feit dat ten aanzien van één of meerdere andere beveiligingsonderwerpen onvoldoende passende maatregelen zijn genomen. Eén lek kan immers voldoende zijn om tot de conclusie te komen dat een passend beveiligingsniveau niet gegarandeerd is geweest. Dat op een ander gebied wel grondige maatregelen zijn genomen, betekent niet noodzakelijkerwijs dat het lek – en daarmee de bedreiging van veiligheid van de persoonsgegevens en de persoonlijke levenssfeer van haar abonnees – is voorkomen. Dit geldt ook voor het voorliggende geval: niet is gebleken dat de geconstateerde gebreken in de maatregelen die KPN had getroffen ten behoeve van de veiligheid en beveiliging van haar netwerken en diensten – voor zover überhaupt van toepassing – , zijn opgeheven ten gevolge van andere maatregelen die later door KPN zijn getroffen, zodat het lek aantoonbaar is voorkomen.

120. Het enkele feit dat onvoldoende maatregelen zijn genomen ter beveiliging van persoonsgegevens en eventuele andere informatie betreffende de persoonlijke levenssfeer van abonnees, hetgeen in dit geval een beveiligingslek heeft opgeleverd, kan al voldoende aanleiding vormen voor de conclusie dat aan de zorgplicht niet is voldaan, zelfs als het lek nadien heel grondig wordt gedicht.

121. De conclusie dat KPN de zorgplicht heeft overtreden is niet gebaseerd op de enkele

constatering dat de hack heeft plaatsgevonden. Het incident is wel aanleiding geweest voor ACM om een onderzoek naar het naleven van de zorgplicht door KPN te beginnen. Deze conclusie is juist gestoeld op de vaststelling dat de door KPN getroffen maatregelen[72] niet naar behoren waren, en er daarom geen passend beveiligingsniveau kon worden gegarandeerd (in de zin van artikel 11.3 eerste lid, Tw) ten tijde van onderzoeksperiode I.

122. KPN wijst er op dat er geen concrete aanwijzingen zijn dat de hacker uiteindelijk toegang heeft verkregen tot de persoonsgegevens van klanten van KPN. Dit doet naar het oordeel van ACM echter niet af aan het feit dat KPN niet heeft voldaan aan de op haar rustende zorgplicht. Die plicht strekt immers tot het treffen van passende technische en organisatorische maatregelen in het belang van de bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers. De vraag of dit naar behoren is gebeurd, is naar het oordeel van ACM zelfs de essentie van de in artikel 11.3, eerste lid, Tw neergelegde zorgplicht. Dat KPN in dit geval onvoldoende maatregelen heeft getroffen om te voldoen aan die zorgplicht, blijkt duidelijk uit het voorgaande en het onderzoeksrapport.

Medewerkingsplicht

123. Zoals in het voorgaande reeds is opgemerkt, heeft OPTA naar aanleiding van voormelde hack in het netwerk van KPN een onderzoek ingesteld naar de naleving van de op KPN rustende zorgplicht ex artikel 11.3 juncto 11.2 Tw. In het kader van dit onderzoek heeft OPTA bij brief van 29 februari 2012 op grond van artikel 18.8 Tw het volgende gevorderd van KPN:

"6. Alle rapporten, documentatie, tussenrapportages, bevindingen, presentaties, terugkoppelingen en gespreksverslagen van alle afdelingen van KPN die zich met onderzoek naar de hack bezig houden, waaronder in ieder geval KPN CERT, die zijn opgesteld naar aanleiding van de geconstateerde hack, tot en met de datum van dagtekening van deze brief. 7. Een volledig overzicht van de geplande, nog door KPN op te stellen, rapporten, documentatie, tussenrapportages, bevindingen, presentaties, terugkoppelingen en gespreksverslagen vanaf de datum van dagtekening van deze brief."

124. Vast staat dat KPN bij brief van 8 maart 2013 – ter gelegenheid van een reactie op een latere informatievordering van OPTA – Intern onderzoek Victor aan OPTA heeft verstrekt. ACM constateert dat Intern onderzoek Victor is gedateerd op 15 maart 2012 en is geschreven door de KPN-afdelingen [vertrouwelijk]. De datering van Intern onderzoek Victor – daags na de reactie van KPN op de informatievordering van 29 februari 2012 – staat haaks op de reactie van KPN op punt 7 van de informatievordering van 29 februari 2012 *"dat er thans geen toekomstige rapporten of andere documentatie is voorzien."*

[72] Gedoeld wordt – voor zover überhaupt van toepassing – op de maatregelen die in het kader van de verschillende beveiligingsonderwerpen zijn getroffen (welke onderwerpen in het voorgaande uitvoerig separaat zijn behandeld).

125. Naar het oordeel van ACM heeft KPN daarmee niet voldaan aan de informatievordering van 29 februari 2012. Uit het onderzoek, noch tijdens de hoorzitting is duidelijk geworden waarom KPN Intern onderzoek Victor niet aan OPTA heeft gemeld, noch waarom KPN Intern onderzoek Victor een jaar later ineens aan OPTA heeft verstrekt. Zoals één van de vertegenwoordigers van KPN tijdens de hoorzitting van 25 september 2013 ook aangaf, had KPN in elk geval moeten melden dat Intern onderzoek Victor er nog aan kwam. Door dit na te laten heeft KPN in strijd gehandeld met artikel 18.7, derde lid, juncto artikel 18.7, vijfde lid, Tw.

126. Gelet op de omstandigheid dat KPN Intern onderzoek Victor uiteindelijk wel aan OPTA heeft verstrekt, zal ACM voor deze overtreding geen afzonderlijke boete opleggen, maar de omstandigheid dat KPN het bestaan van een onderzoek dat voor het onderzoek van OPTA cruciaal was, niet heeft gemeld, betrekken bij de bepaling van de hoogte van de boete voor de schending van de zorgplicht.

6.9 Overtreders

127. Uitgangspunt is dat een bestuurlijke boete of een last onder dwangsom kan worden opgelegd aan degene die een overtreding pleegt of medepleegt.[73]

128. De zorgplicht als bedoeld in artikel 11.3, eerste lid, juncto artikel 11.2 Tw richt zich tot zowel de aanbieder van een openbaar elektronisch communicatienetwerk als de aanbieder van een openbare elektronische communicatiedienst.

129. Vast staat dat de hack bij KPN heeft plaatsgevonden binnen het [vertrouwelijk]. Dit is een onderdeel van een openbaar elektronisch communicatienetwerk dat valt onder de rechtspersoon KPN B.V. De afdelingen [vertrouwelijk], [vertrouwelijk] en [vertrouwelijk] vallen eveneens onder de rechtspersoon KPN B.V.

130. Uit de gegevens op de website www.kpn.com blijkt dat KPN B.V. in de onderzoeksperiode een aantal elektronische communicatiediensten aanbood die gebruik maakten van één of meerdere systemen binnen het [vertrouwelijk]. Het betrof de diensten [vertrouwelijk], [vertrouwelijk], [vertrouwelijk] en [vertrouwelijk]

131. Naar het oordeel van ACM diende KPN B.V. – en dit wordt overigens ook door KPN erkend – het bepaalde in de artikelen 11.3 en 11.2 Tw in acht te nemen. Uit de voorgaande paragrafen blijkt dat zij onvoldoende passende, hoofdzakelijk

[73] Zie: artikel 5:1 Awb juncto artikel 15.4 Tw.

organisatorische, maar ook technische maatregelen heeft getroffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. ACM merkt KPN B.V. gelet op het vorenstaande dan ook aan als overtreder van artikel 11.3, eerste lid, juncto artikel 11.2 Tw.

132. ACM ziet in deze zaak geen aanleiding om Koninklijke KPN N.V. eveneens als overtreder aan te merken.

6.10 Conclusie

133. ACM komt op grond van het vorenstaande tot de conclusie dat KPN gedurende onderzoeksperiode I onvoldoende passende, hoofdzakelijk organisatorische, maar ook technische maatregelen heeft getroffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. KPN heeft daarmee niet voldaan aan de op haar rustende zorgplicht van artikel 11.3, eerste lid, juncto artikel 11.2 Tw.

134. Ten aanzien van onderzoeksperiode II, 16 januari 2012 tot en met 15 maart 2012, waarin het onderzoek zag op de maatregelen die KPN heeft genomen ná de hack, stelt ACM vast dat KPN heeft gehandeld in lijn met haar eigen procedures. ACM ziet geen aanleiding om het handelen van KPN in onderzoeksperiode II aan te merken als een overtreding van artikel 11.3, eerste lid, juncto artikel 11.2 Tw.

135. ACM stelt op grond van het vorenstaande vast dat KPN artikel 18.7, derde lid, juncto artikel 18.7, vijfde lid, Tw heeft overtreden.

7 Ernst van de overtreding

7.1 Boetebeleid ACM

136. Bij de vaststelling van de hoogte van de boete houdt ACM op grond van artikel 5:46, tweede lid, Awb in ieder geval rekening met de ernst van de overtreding alsmede met de verwijtbaarheid van de overtreder. ACM houdt daarbij, indien daartoe aanleiding bestaat, rekening met andere omstandigheden, zoals de duur van de overtreding. Bij ieder boetebesluit moet worden afgewogen hoe hoog de boete in dat concrete geval moet zijn.

137. De hoogte van de boete dient, behalve te worden afgestemd op de bijzondere omstandigheden van het geval (“maatwerk”), ook bij te dragen aan een doeltreffende toepassing van de Telecommunicatiewet. Als algemene maatstaf daarbij geldt dat de hoogte

van de boete in ieder geval zodanig dient te zijn dat deze de overtreder(s) weerhoudt van nieuwe overtredingen (speciale preventie) en ook in algemene termen een afschrikkende werking heeft (generale preventie).

138. Overeenkomstig hoofdstuk 4 van de Beleidsregels van de Minister van Economische Zaken voor het opleggen van bestuurlijke boetes door de ACM[74] (hierna: de Boetebeleidsregels) bepaalt ACM de ernst van de overtreding door eerst de zwaarte van de overtreding in abstracto te bepalen en deze daarna te bezien in het licht van de omgevingsfactoren (de economische context alsmede de bijzondere omstandigheden van het geval). Deze 'optelsom' bepaalt de definitieve kwalificatie van de overtreding: zeer ernstig, ernstig of minder ernstig.

139. ACM wijst er in dit verband op dat zij KPN niet volgt in haar betoog[75] dat de Boetebeleidsregels in het onderzoeksrapport onjuist worden toegepast. De Boetebeleidsregels zijn pas aan de orde indien ACM besluit tot oplegging van een boete en niet al in de onderzoeksfase. In dit besluit zal ACM aan de hand van haar Boetebeleidsregels bepalen welke maatregelen zij vanwege de overtreding van artikel 11.3, eerste lid, juncto artikel 11.2 Tw passend acht.

7.2 Zwaarte van de overtreding

140. Bij het bepalen van de zwaarte van de overtredingen neemt ACM de doelstellingen van de Telecommunicatiewet, te weten het bevorderen van concurrentie, de ontwikkeling van een interne markt en het bevorderen van de belangen van eindgebruikers, als uitgangspunt. Aan de hand van deze doelstellingen deelt ACM in de Boetebeleidsregels de mogelijke overtredingen in abstracto in drie types in: zeer zware, zware en minder zware overtredingen. Overtredingen van de verplichtingen die strekken tot bescherming van persoonsgegevens en de persoonlijke levenssfeer in de zin van artikel 11.2 Tw en 11.3, eerste lid, Tw, worden volgens de toelichting op artikel 3.4 van de Boetebeleidsregels in abstracto als zware overtredingen aangemerkt. Ten aanzien van de ernst van de overtreding van artikel 11.3, eerste lid, juncto artikel 11.2 Tw in concreto, overweegt ACM als volgt.

7.3 Omgevingsfactoren

7.3.1 Schade bij abonnees en gebruikers

141. Indien persoonsgegevens van abonnees of gebruikers zijn opgenomen in een bestand van een aanbieder van een openbare elektronische communicatiedienst of -netwerk en een dergelijk bestand in handen van een onbevoegde valt, dan kunnen als gevolg hiervan de belangen van deze abonnees en gebruikers worden geschaad. Dat kunnen ook op geld

[74] Zie: *Stcrt.* 2013, 11214.
[75] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 48.

waardeerbare belangen zijn. Hoewel uit onderzoek niet is gebleken dat de hacker bij de hack van 16 januari 2012 persoonsgegevens heeft ingezien, gewijzigd, verwijderd, gekopieerd of gestolen, had de hacker in elk geval toegang tot bestanden met persoonsgegevens en had hij die kunnen kopiëren naar een andere locatie en/of kunnen vernietigen. Na het kopiëren van dergelijke bestanden had de hacker vervolgens alle tijd de versleutelde inhoud daarvan te ontcijferen.[76] Uit het Intern onderzoek Victor[77] blijkt ook dat door de tekortkomingen in de beveiligingsmaatregelen in het [vertrouwelijk] van KPN servers (in de netwerklaag die met '[vertrouwelijk]' wordt aangeduid) die klantgegevens bevatten benaderbaar waren door onbevoegden.

142. Dat er geen concrete aanwijzingen zijn dat er persoonsgegevens zijn verwerkt ten gevolge van het incident, doet aan de ernst van de onderhavige overtredingen niet af. De in wettelijke normen die zijn neergelegd in artikel 11.3, eerste lid, en artikel 11.2 Tw strekken immers tot de bescherming van persoonsgegevens door een passend beveiligingsniveau te bewerkstelligen. Het enkele feit dat bij een incident geen concrete aanwijzingen zijn gevonden dat er persoonsgegevens zijn verwerkt ten gevolge daarvan, maakt niet dat bedoeld beveiligingsniveau toch als toereikend kan worden beschouwd. In het onderhavige geval zijn geen concrete aanknopingspunten voorhanden dat het beveiligingsniveau van de door KPN aangeboden netwerken en diensten ten tijde van het incident zodanig was, dat daardoor is voorkomen dat in dit geval persoonsgegevens van klanten van KPN zijn verwerkt. Dat dit in casu waarschijnlijk niet is gebeurd, doet derhalve naar oordeel van ACM niet af aan de ernst van de geconstateerde overtredingen.

143. Naar het oordeel van ACM doet het evenmin aan de ernst van de onderhavige overtredingen af dat het in dit geval, zoals KPN stelt, niet ging om de bescherming van (bijzonder) 'gevoelige' persoonsgegevens, zoals biometrische persoonsgegevens. KPN bagatelliseert hiermee de gevolgen die de hack had kunnen hebben. Er zijn immers geen aanknopingspunten in de wetsgeschiedenis te vinden voor de aanname dat de zorgplicht zoals neergelegd in artikel 11.3, eerste lid, en artikel 11.2 Tw alleen ziet op de bescherming van gevoelige persoonsgegevens.

144. ACM volgt het oordeel uit het onderzoeksrapport dat zowel KPN als de abonnees en gebruikers van haar diensten ernstig zouden kunnen worden geschaad wanneer de hacker wel misbruik zou hebben gemaakt van de in het [vertrouwelijk] elektronisch opgeslagen persoonsgegevens van abonnees en gebruikers.[78]

---

[76] Zie: Onderzoeksrapport, randnummers 75 en 76.
[77] Zie: Onderzoeksrapport, Bijlage 8 KPN, Definitief rapport Intern onderzoek Victor, p. 10.
[78] Zie: Onderzoeksrapport, randnummer 83, waar is vastgesteld dat deze persoonsgegevens in het [vertrouwelijk] waren opgeslagen.

145. Op grond van het bovenstaande stelt ACM vast dat een niet-adequate bescherming van elektronisch opgeslagen persoonsgegevens van abonnees en gebruikers kan leiden tot misbruik daarvan. Hierbij kan worden gedacht aan het onrechtmatig verkrijgen van toegang tot e-mailberichten van de klanten van KPN en mogelijk ook aan het begaan van identiteitsfraude. Een en ander kan leiden tot aanzienlijke schade voor de betrokken abonnees en gebruikers. Kortheidshalve verwijst ACM verder naar hetgeen hieromtrent in het onderzoeksrapport is overwogen.[79]

146. ACM volgt KPN niet in haar stelling dat de economische schade die abonnees en gebruikers ten gevolge van het incident hadden kunnen lijden in dit geval niet mag worden meegewogen ter bepaling van de ernst van de geconstateerde overtredingen.[80] De Boetebeleidsregels bepalen immers dat de mate waarin de overtreding de belangen van abonnees en gebruikers feitelijk heeft geschaad, kan worden meegewogen bij het bepalen van de ernst daarvan.

147. Anderzijds wijst ACM er in dit verband op dat het enkele feit dat de hack niet heeft geleid tot het daadwerkelijk ontstaan van schade, de geconstateerde overtredingen niet minder ernstig maken. Het gaat er immers om dat KPN het beveiligingsniveau van de door haar aangeboden netwerken en diensten niet op orde had, waardoor de bescherming van persoonsgegevens in het geding is geweest. Als dat niveau niet naar behoren is, maar er bij een incident – zoals het onderhavige – niettemin door abonnees en/of gebruikers geen schade wordt geleden, doet dat niet zonder meer af aan de ernst van de overtredingen. Dat kan immers het gevolg zijn van een omstandigheid die buiten de invloedssfeer ligt van KPN.

7.3.2 Geschonden belang

148. Het belang dat is gemoeid met het beschermen van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers, blijkt mede uit de preambule van de Richtlijn betreffende privacy en elektronische communicatie[81] (hierna: e-Privacyrichtlijn). Artikel 4 van die richtlijn is door middel van artikel 11.3, eerste lid, Tw geïmplementeerd. In de preambule van e-Privacyrichtlijn wordt onder meer overwogen dat de ontwikkeling van de informatiemaatschappij wordt gekenmerkt door de invoering van nieuwe elektronische communicatiediensten en dat toegang tot digitale mobiele netwerken voor een breed publiek beschikbaar en betaalbaar is geworden. Deze digitale netwerken beschikken over grote capaciteiten en mogelijkheden voor de verwerking van persoonsgegevens. Gewezen wordt op het feit dat de succesvolle grensoverschrijdende ontwikkeling van deze diensten gedeeltelijk afhangt van het vertrouwen van de gebruikers dat hun persoonlijke levenssfeer zal worden geëerbiedigd. Verder wordt overwogen dat algemeen beschikbare elektronische

[79] Zie: Onderzoeksrapport, randnummers 340-343.
[80] Zie: Schriftelijke zienswijze 29 augustus 2013, p. 50.
[81] Richtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2006/24/EG en Richtlijn/2009/136/EG.

communicatiediensten via het internet de gebruikers nieuwe mogelijkheden bieden, maar ook nieuwe gevaren inhouden voor de bescherming van hun persoonsgegevens en persoonlijke levenssfeer. Daarbij komt dat in dit verband geldt dat die gebruikers in beginsel ook niet zelf in staat zijn maatregelen te treffen ter bescherming van hun persoonsgegevens en persoonlijke levenssfeer. In dat opzicht zijn zij afhankelijk van de maatregelen die de aanbieders van elektronische communicatiediensten en elektronische communicatienetwerken ter zake treffen.

149. Daarom zijn wettelijke waarborgen geïntroduceerd om de fundamentele rechten en vrijheden van natuurlijke personen en de rechtmatige belangen van rechtspersonen te beschermen tegen met name de steeds grotere mogelijkheden in verband met de geautomatiseerde opslag en verwerking van gegevens met betrekking tot de abonnees en de gebruikers. De in artikel 11.3, eerste lid, Tw neergelegde bepaling is geïntroduceerd om op nationaal niveau vorm te geven aan de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen en de rechtmatige belangen van rechtspersonen.

7.3.3 Aantal betrokken abonnees en gebruikers die aan risico waren blootgesteld door overtredingen

150. Het aantal abonnees en gebruikers dat door de overtreding van KPN nadelige gevolgen had kunnen ondervinden wegens gebrek aan bescherming van persoonsgegevens en de persoonlijke levenssfeer, bedroeg blijkens het onderzoeksrapport minimaal 2 miljoen.[82] Dit aantal vertegenwoordigt het aantal abonnees met een e-mailaansluiting van KPN op 10 februari 2012, waaronder de diensten '[vertrouwelijk]', '[vertrouwelijk]' en '[vertrouwelijk]'. Het aantal gebruikers van de e-maildienst lag vermoedelijk nog hoger, omdat bijvoorbeeld een abonnee die een internettoegangsdienst met bijbehorende e-maildienst afneemt, zijn mailaccount kan uitbreiden naar meerdere personen (bijvoorbeeld huisgenoten).

151. ACM gaat er van uit dat op 10 februari 2012 in elk geval 2 miljoen abonnees en gebruikers door de overtreding van KPN nadelige gevolgen hadden kunnen ondervinden (wegens gebrek aan bescherming van persoonsgegevens en de persoonlijke levenssfeer).

7.4 Conclusie ten aanzien van de ernst van de overtreding

152. Naar het oordeel van ACM is er sprake van een zeer groot aantal betrokken abonnees en gebruikers (minstens 2 miljoen). Deze abonnees en gebruikers konden – door de door KPN begane overtredingen van artikel 11.3, eerste lid, juncto artikel 11.2 Tw – worden geconfronteerd met de risico's die samenhangen met het onvoldoende beschermd zijn van

[82] Zie: Onderzoeksrapport, randnummer 344.

hun persoonsgegevens en persoonlijke levenssfeer, zoals identiteitsfraude.[83] ACM neemt in ogenschouw dat misbruik van de in het [vertrouwelijk] elektronisch opgeslagen persoonsgegevens van abonnees en gebruikers had kunnen leiden tot aanzienlijk schade bij leden van die groep. Tevens acht ACM het van belang dat het geschonden belang in dit geval van zwaarwegende aard is. Het betreft immers de bescherming van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers, hetgeen raakt aan de fundamentele rechten en vrijheden van natuurlijke personen en de rechtmatige belangen van rechtspersonen. De in die sfeer aangerichte schade is vaak onomkeerbaar. Op grond van het voorgaande merkt ACM de overtredingen van artikel 11.3, eerste lid, juncto artikel 11.2 Tw, begaan door KPN, aan als ernstig. Dit indiceert een boete van maximaal EUR 300.000 per overtreding.

153. De omstandigheid dat over onderzoeksperiode II in dit besluit geen overtreding wordt vastgesteld, doet geen afbreuk aan de ernst van de in onderzoeksperiode I geconstateerde overtredingen. Als – zoals in casu – het uitgangspunt is dat de veiligheid en het beveiligingsniveau van de door KPN aangeboden netwerken en diensten niet adequaat was, wordt die situatie op zichzelf immers niet minder ernstig, doordat dat beveiligingsniveau nadien wordt verbeterd naar aanleiding van een incident dat de gebrekkigheid van de aanvankelijke beveiligingsmaatregelen heeft blootgelegd.

154. Gelet op het voorgaande kwalificeert ACM de onderhavige overtreding(en) van de zorgplicht als ernstig.

8 Vaststelling van de hoogte van de boete

155. Binnen de bandbreedte van de boetecategorie stelt ACM met inachtneming van de mate waarin de overtreding aan de overtreder kan worden verweten en, indien daartoe aanleiding bestaat, andere omstandigheden, zoals de duur van de overtreding, de hoogte van de basisboete vast.

8.1 Verwijtbaarheid

156. Over de verwijtbaarheid van KPN ten aanzien van het niet naleven van de zorgplicht merkt ACM het volgende op.

157. In zijn algemeenheid stelt ACM vast dat KPN in een bepaalde periode structureel tekort is

[83] De betrokken bestanden met persoonsgegevens kunnen ook wachtwoorden bevatten behorende bij e-mailaccounts van klanten van KPN, zie: Onderzoeksrapport, Bijlage ACM 5, Verslag hoorzitting KPN op 4 april 2012, p. 18.

geschoten met het treffen van passende technische en organisatorische maatregelen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers.

158. In het bijzonder stelt ACM vast dat KPN bewust het risico heeft genomen om de kwetsbaarheid in de beveiliging van het netwerk, die de [vertrouwelijk] heeft veroorzaakt, niet weg te nemen.

159. Op 13 december 2011 werd namelijk ontdekt dat de website van KPN-dochter Gemnet was gehackt. KPN is daarvan op de hoogte gesteld. KPN heeft vervolgens nagelaten om maatregelen te treffen om de kwetsbaarheden in de software van de [vertrouwelijk] te verhelpen. Deze kwetsbaarheden zijn (mede) de oorzaak geweest van de hack die op 15 januari 2012 heeft plaatsgevonden.

160. Daarnaast is KPN er in 2009 al op gewezen dat het houden van penetratietesten was aan te bevelen. KPN heeft deze aanbeveling niet opgevolgd. Bovendien had KPN de beschikking over scansoftware, maar heeft rond 2008/2009 besloten deze software nadien niet meer te gebruiken.[84]

161. Gelet op het voorgaande acht ACM de overtredingen van artikel 11.3, eerste lid, juncto artikel 11.2 Tw volledig verwijtbaar en rekent deze toe aan KPN.

8.2 Duur

162. De periode waarin de overtredingen zijn begaan betreft ruim anderhalf jaar, namelijk van september 2010 tot en met 15 januari 2012. ACM is van oordeel dat KPN gedurende deze periode structureel geen of onvoldoende maatregelen heeft getroffen om te voldoen aan de op haar rustende zorgplicht om persoonsgegevens voldoende te beschermen.

8.3 Basisboete

163. Gelet op het vorenstaande zal ACM de basisboete in dit geval vaststellen op EUR 280.000.

8.4 Boeteverhogende en/of -verlagende omstandigheden

164. Zoals eerder in dit besluit is vastgesteld heeft KPN in strijd gehandeld met artikel 18.7, derde lid, juncto artikel 18.7, vijfde lid, Tw, door het bestaan van een cruciaal intern onderzoek, Intern onderzoek Victor, in reactie op de informatievordering van 29 februari 2012 niet te melden aan OPTA. ACM zal deze overtreding in dit geval aanmerken als een boeteverhogende

[84] Zie: Onderzoeksrapport, randnummer 287.

omstandigheid.

165. De inhoud van Intern onderzoek Victor bevat informatie die bij uitstek van belang was voor het onderzoek van OPTA. Doordat KPN Intern onderzoek Victor niet heeft gemeld bij OPTA heeft zij de toezichthouder belemmerd in de vervulling van haar (kern)taak. Ook heeft KPN daardoor het onderzoek van OPTA bemoeilijkt en vertraagd.

166. ACM meent dat de overtreding van de medewerkingsplicht KPN kan worden verweten.

167. Dit klemt te meer omdat op 24 april 2008 tussen OPTA en KPN een Compliance Handvest[85] is gesloten, dat gedurende de onderzoeksperiode onverkort van kracht was. Op basis van het Compliance Handvest mocht OPTA er op vertrouwen dat KPN zich volledig zou inzetten om openheid en transparantie te betrachten, zodat op grond daarvan mag worden verwacht dat volledig wordt meegewerkt aan onderzoeken van OPTA/ACM.

168. Dat ACM heeft moeten constateren dat KPN zich niet compliant heeft gedragen door in het onderzoek dat naar aanleiding van de hack heeft plaatsgevonden geen melding te maken van een relevant intern onderzoek, doet afbreuk aan het door ACM in KPN gestelde vertrouwen.

169. Gelet op het vorenstaande zal ACM de in paragraaf 8.3 bepaalde basisboete met 30% verhogen.

170. ACM stelt tevens vast dat KPN voor het overige goed heeft medegewerkt. Deze medewerking ging echter niet verder dan waartoe KPN op grond van de wet gehouden was en leidt in de optiek van ACM niet tot boeteverlaging.

8.5 Conclusie ten aanzien van de vaststelling van de hoogte van de boete

171. Ingevolge artikel 3:4, tweede lid, van de Awb neemt ACM bij het bepalen van de hoogte van de boete het evenredigheidsbeginsel in acht. Op grond van deze bepaling mogen de voor één of meer belanghebbenden nadelige gevolgen van een besluit niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen.

172. In aanmerking genomen de ernst van de overtreding alsmede de duur van de overtreding, de mate van verwijtbaarheid van KPN, legt ACM aan KPN B.V. een boete op ten bedrage van:

EUR 280.000 (basisboete)

[85] Het Compliance Handvest tussen OPTA en KPN van 24 april 2008 is te vinden op de website van ACM (www.acm.nl).

Besluit
Openbaar

EUR	84.000	(30% verhoging)
EUR	364.000	(totaal)

Besluit
Openbaar

9 Besluit

De Autoriteit Consument en Markt:

I. stelt vast dat KPN B.V. de volgende artikelen heeft overtreden:
a) artikel 11.3, eerste lid, juncto artikel 11.2 Tw (zorgplicht)
b) artikel 18.7, derde lid, juncto artikel 18.7, vijfde lid, Tw (medewerkingsplicht);

II. rekent de onder I. genoemde overtredingen volledig toe aan KPN B.V.;

III. legt voor de onder I. onder a vermelde overtreding aan KPN B.V. een boete op van in totaal EUR 364.000 (EUR 280.000 + 30% boeteverhoging).

De Autoriteit Consument en Markt,
namens deze,

w.g. mr. J.G. Vegter
bestuurslid

Tegen dit besluit kan degene, wiens belang rechtstreeks bij dit besluit is betrokken, binnen zes weken na de dag van bekendmaking van dit besluit een gemotiveerd bezwaarschrift indienen bij het bestuur van de Autoriteit Consument en Markt, Directie Juridische Zaken, Postbus 16326, 2500 BH Den Haag. In dit bezwaarschrift kan een belanghebbende op basis van artikel 7:1a, eerste lid, van de Algemene wet bestuursrecht, het bestuur van de Autoriteit Consument en Markt verzoeken in te stemmen met rechtstreeks beroep bij de administratieve rechter.

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