ECLI:NL:RBROT:2013:CA1010

Instantie	Rechtbank Rotterdam
Datum uitspraak	16-05-2013
Datum publicatie	27-05-2013
Zaaknummer	AWB ROT 12/1229
Rechtsgebieden	Bestuursrecht
Bijzondere kenmerken	Eerste aanleg - meervoudig
Inhoudsindicatie	Besluit van de Autoriteit Consument en Markt (voorheen: Opta) van 13 september 2011 waarbij de registratie van Diginotar als certificatiedienstverlener (CSP) per 14 september 2011 om 12.00 uur is beëindigd. Verweerder heeft zich gebaseerd op onderzoek verricht door Fox-IT. Eiser heeft niet betwist dat Fox-IT over een bijzondere deskundigheid op het vlak van IT veiligheid beschikt om een onderzoek uit te voeren naar aanleiding van het beveiligingsincident bij Diginotar. Voorts bestaat er voor de rechtbank geen aanleiding om te veronderstellen dat Fox-IT in haar onderzoek of rapportage niet onafhankelijk zou hebben gehandeld. Gelet op de situatie ten tijde van het primaire en het betreden besluit was het interim-rapport van Fox-IT in dit kader goed bruikbaar. Uit het door verweerder verrichte onderzoek is genoegzaam gebleken dat het netwerk dat door Diginotar werd gebruikt voor de uitgifte van gekwalificeerde certificaten door een hack van het systeem ernstig was gecompromitteerd. Bijgevolg was, mede doordat achteraf niet te achterhalen is wat de hacker precies heeft gedaan, de betrouwbaarheid van de gekwalificeerde certificaten die via deze servers werden gegenereerd, niet langer te garanderen. Een nader onderzoek of daadwerkelijk misbruik van gekwalificeerde certificaten heeft plaatsgevonden is niet relevant. Bij Diginotar bestond geen adequate beveiliging (meer) tegen het vervalsen van gekwalificeerde certificaten. Diginotar voldeed niet (meer) aan de belangrijke verplichtingen als bedoeld in artikel 2, eerste lid, aanhef en onder c en d, van het Besluit electronische handtekeningen. Uit de wetsgeschiedenis bij artikel 2.2, vierde lid, aanhef en onder c, van de Telecommunicatiewet blijkt dat de bevoegdheid van verweerder om een herstelmogelijkheid te bieden uitsluitend bedoeld is voor gevallen waarin geen sprake is van twijfels over de betrouwbaarheid van de gekwalificeerde certificaten. De rechtbank is van oordeel dat verweerder in het onderhavige geval terecht op grond van artikel 2.2, vierde lid, aanhef en onder b, van de Tw, zonder hersteltermijn, tot beëindiging van de registratie van Diginotar als CSP is overgegaan. Het beroep dient daarom ongegrond te worden verklaard.
Vindplaatsen	Rechtspraak.nl

Uitspraak

RECHTBANK ROTTERDAM

Team Bestuursrecht 1

zaaknummer: ROT 12/1229

uitspraak van de meervoudige kamer van 16 mei 2013 in de zaak tussen

[naam], in zijn hoedanigheid van curator in het faillissement van Diginotar B.V. (hierna: Diginotar), eiser,

gemachtigde: mr. M.F.A. Dankbaar,

en

de Autoriteit Consument en Markt (voorheen: het college van de Onafhankelijke Post en Telecommunicatie Autoriteit), verweerder,

gemachtigden: mr. R. Klein en mr. dr. drs. W.A.M. Steenbruggen.

Procesverloop

Bij besluit van 13 september 2011 (het primaire besluit) heeft verweerder de registratie van Diginotar als certificatiedienstverlener per 14 september 2011, om 12.00 uur, beëindigd.

Bij besluit van 6 februari 2012 (het bestreden besluit) heeft verweerder het bezwaar van eiser, voor zover gericht tegen een onvoldoende belangenafweging niet-ontvankelijk verklaard, en voor het overige ongegrond verklaard.

Eiser heeft tegen het bestreden besluit beroep ingesteld.

Verweerder heeft op 24 juli 2012 een verweerschrift ingediend. Op 28 februari 2013 heeft verweerder een aanvullend verweerschrift ingediend.

Eiser heeft op 28 februari 2013 een aanvullend gedingstuk ingediend.

Op 7 maart 2013 heeft verweerder een nadere reactie ingezonden.

Het onderzoek ter zitting heeft plaatsgevonden op 18 maart 2013. Eiser is verschenen, bijgestaan door zijn gemachtigde en [namen]. Verweerder heeft zich laten vertegenwoordigen door zijn gemachtigden, bijgestaan door [naam].

Overwegingen

Juridisch kader ten tijde van het bestreden besluit

1.1 Artikel 2.2, vierde lid van de Telecommunicatiewet (Tw) luidt, voor zover relevant als volgt:

Het college beëindigt of wijzigt de registratie:

a. indien de grond voor registratie is vervallen;

b. indien een certificatiedienstverlener activiteiten of diensten verricht in strijd met het bepaalde bij of krachtens deze wet,

c. indien het college heeft vastgesteld dat de certificatiedienstverlener niet of niet geheel voldoet aan de eisen bedoeld in artikel 18.15, eerste en tweede lid, en de certificatiedienstverlener niet binnen de door het college gestelde termijn heeft aangetoond aan deze eisen te voldoen. Indien de certificatiedienstverlener aantoont redelijkerwijs niet binnen de gestelde termijn aan de eisen te kunnen voldoen, kan het college de termijn verlengen; of

d. indien het college heeft vastgesteld dat de certificatiedienstverlener de gegevens, bedoeld in artikel 2.1, vijfde lid, onder b, of wijzigingen daarin niet, onvolledig of niet juist heeft verstrekt, en de certificatiedienstverlener niet binnen de door het college gestelde termijn de volledige of juiste gegevens alsnog verstrekt.

Artikel 18.15 van de Tw luidt, voor zover relevant:

1. Een certificatiedienstverlener die certificaten als gekwalificeerde certificaten aanbiedt of afgeeft aan het publiek en in Nederland een vestiging heeft, voldoet aan de eisen, gesteld bij of krachtens algemene maatregel van bestuur.

2. Certificaten die als gekwalificeerd certificaat aan het publiek worden aangeboden of afgegeven, voldoen aan de eisen gesteld bij of krachtens algemene maatregel van bestuur.

3. ()

Artikel 18.16 van de Tw luidt, voor zover relevant:

1. Onze Minister kan een of meer organisaties aanwijzen die bevoegd zijn

certificatiedienstverleners te toetsen op overeenstemming met de bij en krachtens deze wet

gestelde eisen en daartoe een bewijs van toetsing af te geven.

()

Artikel 18.16a van de Tw luidt:

1. Een certificatiedienstverlener die in het bezit is van een geldig bewijs van toetsing van een op grond van artikel 18.16, eerste lid, aangewezen organisatie, wordt vermoed te voldoen aan artikel 18.15, eerste lid.

2. De certificaten die als gekwalificeerd aan het publiek worden aangeboden of afgegeven door een certificatiedienstverlener als bedoeld in het eerste lid, worden vermoed te voldoen aan artikel 18.15, tweede lid.

1.2 Artikel 2 van het Besluit elektronische handtekeningen (Beh) luidt, voor zover relevant, als volgt:

1.Een certificatiedienstverlener als bedoeld in artikel 18.15, eerste lid, van de wet voldoet aan de volgende eisen:

a. hij beschikt over betrouwbare middelen en hanteert betrouwbare procedures voor het aanbieden van certificatiediensten aan het publiek;

b. hij past procedures en processen op het gebied van administratie en beheer toe overeenkomstig een beschreven kwaliteitssysteem dat in overeenstemming is met de laatste ontwikkelingen op het gebied van kwaliteitssystemen;

c. hij maakt uitsluitend gebruik van betrouwbare systemen en producten die procedureel of

overeenkomstig de stand der techniek beveiligd zijn en die de technische en crypto-grafische veiligheid van de processen die zij ondersteunen garanderen;

d. hij neemt adequate maatregelen tegen het vervalsen van de gekwalificeerde certificaten die hij heeft uitgegeven en tegen het uitgeven van illegale gekwalificeerde certificaten en, indien hij gegevens voor het aanmaken van handtekeningen genereert, garandeert hij de vertrouwelijkheid van het proces waarmee dit gebeurt;

()

m. hij slaat de gegevens voor het aanmaken van elektronische handtekeningen van de personen aan wie hij sleutelbeheerdiensten heeft verleend niet op, en hij kopieert deze gegevens evenmin;

().

1.3 Artikel 2 van de Regeling elektronische handtekeningen (Reh) luidt, voor zover relevant, als volgt:

1. Een certificatiedienstverlener wordt vermoed te voldoen aan de eisen, gesteld in artikel 2, eerste lid, onderdelen a tot en met m, o en r van het besluit, indien hij voldoet aan de technische specificatie ETSI TS 101 456.

2. De tijdsduur tussen het ontvangen van een verzoek tot intrekking van een gekwalificeerd

certificaat en publicatie van die intrekking, als bedoeld in artikel 2, eerste lid, onderdeel k, van het besluit, bedraagt ten hoogste 24 uur.

3. Een certificatiedienstverlener zorgt ervoor dat belanghebbenden gedurende de periode dat de verplichting, bedoeld in artikel 2, eerste lid, onderdeel l, van het besluit, om statusgegevens te publiceren aanwezig is, deze gegevens van afgegeven gekwalificeerde certificaten op elk tijdstip kunnen raadplegen.

Feiten en achtergronden

2.1 Diginotar was een zogenoemde certificatiedienstverlener (CSP) die certificaten afgaf en andere diensten in verband met elektronische handtekeningen verleende. Een certificaat is in wezen niets anders dan een computerbestand dat een crypto-grafische sleutel koppelt aan een bepaalde entiteit en deze daarmee identificeerbaar maakt. Deze certificaten vormen de basis voor elektronische handtekeningen. De belangrijkste functies van een CSP zijn het controleren van de identiteit van de aanvrager van het certificaat en het koppelen van deze identiteit aan een uniek en betrouwbaar certificaat. In dit geschil staat centraal de naleving door Diginotar als CSP van de eisen met betrekking tot het aanbieden of afgeven van gekwalificeerde certificaten.

2.2 Voor het aanbieden of afgeven van gekwalificeerde certificaten gelden op grond van de Tw strikte eisen. Deze eisen zijn nodig, omdat het gebruik van dergelijke handtekeningen op grond van artikel 3:15a, eerste lid, van het BW, in het rechtsverkeer gelijk wordt gesteld met een schriftelijke handtekening, mits de methode die daarbij wordt gebruikt voldoende betrouwbaar is. Die betrouwbaarheid wordt, blijkens artikel 3:15a, tweede lid, van het BW, aangenomen, indien gebruik wordt gemaakt van een geavanceerde elektronische handtekening die gebaseerd is op een gekwalificeerd certificaat als bedoeld in artikel 1.1, aanhef en onder tt, van de Tw en is gegenereerd door een veilig middel voor het aanmaken van handtekeningen als bedoeld in artikel 1.1, aanhef en onder ww, van de Tw.

2.3 De eisen waar CSPs en gekwalificeerde certificaten aan moeten voldoen zijn neergelegd in de Tw - waarbij de Richtlijn elektronische handtekeningen (Richtlijn 99/93/EG) in nationaal recht is omgezet - en nader uitgewerkt in het Beh. De eisen van Bijlage I en II van de Richtlijn 99/93/EG zijn door middel van artikel 18.15 van de Tw en het daarop gebaseerde Beh in nationaal recht omgezet en nader uitgewerkt.

2.4 Op grond van artikel 15.1 van de Tw wordt de naleving van de regels door certificatiedienstverleners zowel preventief gewaarborgd als repressief gehandhaafd.

Het preventieve toezicht is zo ingevuld dat CSPs die gekwalificeerde certificaten aan het publiek aanbieden of afgeven en die een vestiging in Nederland hebben, op grond van artikel 2.1, vijfde lid, van de Tw, bij verweerder geregistreerd moeten zijn. In de praktijk hebben alle CSPs, die bij verweerder zijn geregistreerd, zich laten toetsen door een op grond van artikel 18.16 van de Tw door het ministerie van Economische Zaken aangewezen certificatie-instelling. Deze instellingen toetsen daarbij aan de technische normen die ter uitwerking van de eisen in de bijlagen van de Richtlijn 99/93/EG zijn ontwikkeld en vastgesteld in de standaard ETSI 101 456 van het European Telecommunications Standards Institute (ETSI). Diginotar heeft zich laten toetsen door PriceWaterhouseCoopers (PWC).

Repressieve handhaving komt aan de orde als door de CSP in strijd met de regels is gehandeld. Verweerder is bevoegd om de registratie van een CSP te beëindigen. Hij zal direct van de bevoegdheid gebruik moeten maken, indien hij vaststelt dat de CSP niet voldoet aan de in de bij of krachtens de wet

gestelde eisen (artikel 2.2, vierde lid, aanhef en onder b, van de Tw). Indien evenwel de betrouwbaarheid van afgegeven gekwalificeerde certificaten als zodanig niet ter discussie staat, kan verweerder de CSP nog op grond van artikel 2.2, vierde lid, aanhef en onder c, van de Tw een termijn gunnen om alsnog aan te tonen aan de eisen te voldoen, voordat hij tot beëindiging overgaat. Bij de beoordeling van de vraag of de betrouwbaarheid van de afgegeven gekwalificeerde certificaten ter discussie staat, komt verweerder enige beoordelingsvrijheid toe. Komt verweerder evenwel tot de conclusie dat deze betrouwbaarheid niet langer kan worden gewaarborgd, dan dient hij de registratie te beëindigen. Van enige discretionaire ruimte is dan niet langer sprake.

De door Diginotar uitgegeven gekwalificeerde certificaten werden voor een belangrijk deel gebruikt door notarissen en gerechtsdeurwaarders voor het inschrijven van aktes in het Kadaster. Daarnaast verzorgde Diginotar ook de PKI-overheid-certificaten voor grote delen van de Nederlandse overheid waaronder die van DigiD en de Rijksdienst voor het Wegverkeer (RDW). PKI staat voor Public Key Infrastructure, wat neer komt op een betrouwbare elektronische wijze van communiceren met de Nederlandse overheid.

Op maandag 29 augustus 2011 verschenen in diverse media de eerste berichten over door Diginotar ten onrechte uitgegeven (valse) Secure Sockets Layer (SSL)-certificaten. Bijna direct werd duidelijk dat Diginotar deze certificaten niet zelf had uitgegeven, maar dat de systemen van Diginotar moesten zijn misbruikt door een onbevoegde derde: een hacker. Omdat verweerder geen toezicht houdt op SSL-certificaten, maar wel op gekwalificeerde certificaten, heeft verweerder onderzoek gedaan naar de beveiliging bij Diginotar met betrekking tot de uitgifte van gekwalificeerde certificaten.

Daarnaast heeft Diginotar op 30 augustus 2011 zelf het bedrijf Fox-IT verzocht om een onderzoek in te stellen naar het beveiligingsincident dat bij Diginotar had plaatsgevonden en daarover een rapport op te stellen. Bij e-mail van 31 augustus 2011 heeft verweerder Diginotar verzocht om het laatste auditrapport van PWC te verstrekken. Tevens heeft verweerder Diginotar verzocht het onderzoeksrapport van Fox-IT dat in opdracht van Diginotar onderzoek deed naar het beveiligingsincident, vóór 1 september 2011 17:00 uur aan verweerder te doen toekomen. Omdat Diginotar het onderzoeksrapport niet binnen de gestelde termijn aan verweerder heeft verstrekt, heeft verweerder dit (interim)rapport bij brief van 5 september 2011 direct bij Fox-IT gevorderd. Fox-IT heeft het interim-rapport op 5 september 2011 in persoon aan verweerder overhandigd en toegelicht.

Bij brief van 7 september 2011 heeft verweerder Diginotar meegedeeld dat hij heeft geconstateerd dat Diginotar op een aantal belangrijke punten niet voldoet aan de eisen van artikel 18.15, eerste en tweede lid, van de Tw, zoals nader uitgewerkt in het Beh en de Reh. Daarnaast is aan Diginotar gemeld dat verweerder het voornemen heeft de registratie van Diginotar als certificatiedienstverlener te beëindigen en haar uitgenodigd om binnen twee dagen hierop te reageren. Diginotar heeft bij brief van 9 september 2011 gereageerd.

Bij het primaire besluit heeft verweerder het besluit genomen om de registratie van Diginotar als certificatiedienstverlener per 14 september 2011, om 12.00 uur, te beëindigen.

Bij brief van 15 september 2011 heeft Diginotar meegedeeld dat zij geen nieuwe gekwalificeerde certificaten zal verstrekken. Tevens heeft zij verweerder bericht dat zij alle reeds uitgegeven certificaten op 27 september 2011 zal intrekken.

Bij brief van 22 september 2011 heeft PWC verweerder meegedeeld dat zij op 21 september 2011 aan Diginotar heeft bericht, dat het recht om het op 1 november 2010 aan Diginotar verstrekte TTP.NL certificaat met nummer ETSI 10-0020 te gebruiken, per 21 september 2011 is ingetrokken, omdat de rechtbank Haarlem Diginotar bij uitspraak van 20 september 2011 in staat van faillissement heeft verklaard.

Op 24 september 2011 hebben de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders, de Koninklijke Notariële Beroepsorganisatie en de Stichting Netwerk Gerechtsdeurwaarders (hierna: betrokkenen) verweerder gedagvaard om op 26 september 2011 voor de voorzieningenrechter van de sector civielrecht van de rechtbank Den Haag ter zitting te verschijnen. Betrokkenen hebben gevorderd verweerder te gebieden dat het Diginotar toestaat de gekwalificeerde certificaten niet in te trekken voor zover deze zijn uitgegeven aan notarissen en gerechtsdeurwaarders, tot het moment waarop betrokkenen beschikken over nieuwe gekwalificeerde certificaten. Bij uitspraak van 27 september 2011, LJN: BT6781, heeft de voorzieningenrechter de vordering van betrokkenen afgewezen.

Bij brief van 26 september 2011 heeft eiser bezwaar ingediend tegen het primaire besluit. Tevens heeft eiser bij deze rechtbank een verzoek om een voorlopige voorziening ingediend. Bij uitspraak van 27 september 2011, LJN: BT6349, heeft de voorzieningenrechter van deze rechtbank geoordeeld dat er geen sprake was van een spoedeisend belang en het verzoek om een voorlopige voorziening afgewezen.

Het bestreden besluit

3. Bij het bestreden besluit heeft verweerder aangegeven dat hij zich bij het nemen van het primaire besluit heeft gebaseerd op de feiten die Fox-IT als vaststaand in het interim-rapport heeft opgenomen. Op basis hiervan heeft verweerder geconcludeerd dat de CA-servers (CA=certificaatautoriteit) van Diginotar ernstig gecompromitteerd waren en dat de maatregelen die Diginotar heeft genomen tegen het uitgeven van vervalste certificaten en tegen het vervalsen van uitgegeven gekwalificeerde certificaten niet adequaat waren, zodat Diginotar niet voldeed aan artikel 2, eerste lid, aanhef en onder d, van het Beh.

3.1 Op basis van het Fox-IT rapport heeft verweerder verder geconcludeerd dat de beveiliging van de systemen en producten die door Diginotar werden gebruikt bij de uitgifte van gekwalificeerde certificaten niet overeenkomstig de stand der techniek waren beveiligd. Verweerder is van mening dat hij ook zonder de inbraak tot het oordeel zou zijn gekomen dat Diginotar niet voldeed aan de eisen gesteld in artikel 2, eerste lid, aanhef en onder c, van het Beh.

3.2 Gezien het feit dat de gevolgen van de compromittering van de servers niet meer ongedaan kunnen worden gemaakt en er activiteiten dan wel diensten zijn verricht die in strijd zijn met het bepaalde bij of krachtens de Tw, heeft verweerder geconcludeerd dat hij niet anders kon dan de registratie van Diginotar als CSP-er bij het primaire besluit zonder hersteltermijn te beëindigen op grond van artikel 2.2, lid 4, aanhef en onder b, van de Tw. Verweerder voelt zich daarbij gesterkt door de uitspraak van de voorzieningenrechter van de rechtbank Den Haag. Deze heeft als volgt geoordeeld: Uitgaande van de juistheid van hetgeen OPTA heeft geconstateerd aan de hand van het onderzoek van Fox-IT B.V., valt overigens niet in te zien dat OPTA anders had kunnen beslissen dan het deed op 13 september 2011, gelet op het dwingende karakter van het bepaalde in artikel 2.2, lid 4, aanhef en onder b van de Tw.

Standpunt eiser

4. Eiser heeft zich, kort samengevat, op het standpunt gesteld dat Fox-IT niet onafhankelijk is en dat het interim-rapport van Fox-IT de conclusies van verweerder niet kan dragen. Verweerder had nader onderzoek moeten doen omdat het interim-rapport flinke slagen om de arm houdt en daarnaast kennelijke onjuistheden en veel subjectieve elementen bevat. Bovendien was het interim-rapport niet bedoeld om definitieve conclusies te trekken over de conformiteit van Diginotar aan de normen voor CSP-ers. Voorts heeft verweerder op verkeerde gronden geconcludeerd dat Diginotar in strijd handelde met de eisen die zijn verwoord in artikel 2, eerste lid, aanhef en onder c en d, van het Beh. Naar de mening van eiser kon verweerder op basis van de beschikbare informatie ten tijde van het primaire besluit bovendien niet het besluit nemen om de registratie van Diginotar onmiddellijk te beëindigen, op grond van artikel 2.2, vierde lid, aanhef en onder b, van de Tw. Als er al strijd was met de genoemde eisen als bedoeld in artikel 2, eerste lid, aanhef en onder c en d, van het Beh, dan had verweerder niet eerder tot beëindiging van de registratie over kunnen gaan, dan nadat een herstelterm

Diginotar en dat verweerder in strijd heeft gehandeld met het beginsel van een zorgvuldige voorbereiding, het motiveringsbeginsel en het evenredigheidsbeginsel.

Beoordeling

5. De rechtbank stelt in de eerste plaats vast dat eiser niet heeft betwist dat Fox-IT over een bijzondere deskundigheid op het vlak van IT veiligheid beschikt om een onderzoek uit te voeren naar aanleiding van het beveiligingsincident bij Diginotar. Daarnaast merkt de rechtbank op dat het Diginotar zelf is geweest die Fox-IT op basis van diens deskundigheid heeft ingeschakeld en daarbij volledige medewerking heeft verleend aan het door Fox-IT te verrichten onderzoek. Voorts bestaat er voor de rechtbank geen aanleiding om te veronderstellen dat Fox-IT in haar onderzoek of rapportage niet onafhankelijk zou hebben gehandeld. Diginotar heeft Fox-IT in eerste instantie zelf ingeschakeld als onafhankelijke expert en Diginotar heeft er ook mee ingestemd dat met de overdracht van het operationele beheer ook het onderzoek door Fox-IT zou worden voortgezet in opdracht van het ministerie van Binnenlandse Zaken. De stelling dat Fox-IT als rapporterende partij een zeker belang bij ingrijpen door verweerder zou hebben omdat het rapport dan meer publiek zou worden, is op geen enkele wijze door eiser nader onderbouwd en zou - als algemene stelling - op iedere onderzoeker van toepassing zijn geweest.

5.1 Het betoog van eiser dat verweerder, alvorens het primaire besluit te nemen, eerst een nader onderzoek had moeten verrichten omdat het interim-rapport flinke slagen om de arm houdt, slaagt niet. Naar het oordeel van de rechtbank stelt verweerder zich terecht op het standpunt dat er een duidelijk onderscheid kan worden gemaakt tussen de definitieve conclusies die door Fox-IT konden worden getrokken uit de feiten die reeds waren vastgesteld enerzijds en de (voorlopige) conclusies die door Fox-IT zijn getrokken met betrekking tot zaken waarnaar nog verder onderzoek moest plaatsvinden anderzijds. Gelet op de situatie ten tijde van het primaire en het bestreden besluit was het interim-rapport in dit kader goed bruikbaar.

5.2 Ter zake van de stelling van eiser dat het interim-rapport kennelijke onjuistheden bevat, benoemt hij er slechts één. Eiser stelt dat de servers die rechtstreeks in verbinding stonden met het internet wel degelijk waren voorzien van antivirus software. Uit het interim-rapport blijkt dat het onderzoek van Fox-IT zich richtte op de vraag welke CA-omgevingen van Diginotar door de hack waren gecompromitteerd. Fox-IT heeft daartoe alle CA-servers in het beveiligde netwerksegment van Diginotar onderzocht waaronder de Qualified CA-server. Op geen van deze door Fox-IT onderzochte CA-servers is door Fox-IT antivirus software aangetroffen. Dat deze vaststelling onjuist zou zijn, wordt niet door eiser gesteld noch onderbouwd. Dat op de servers buiten het beveiligde netwerksegment wel antivirussoftware stond is niet strijdig met de conclusies van Fox-IT, nu deze servers niet (uitvoerig) door Fox-IT zijn onderzocht.

5.3 De stelling van Fox-IT, dat binnen het beveiligde netwerksegment van Diginotar zich kwaadaardige software bevond die door de meeste gratis antivirussoftware wordt herkend, wordt wellicht (door eiser) als een subjectief element aangemerkt, doch maakt niet dat de aanwezigheid van deze kwaadaardige software op de servers binnen het beveiligde netwerksegment van Diginotar niet afdoende aantoont dat het netwerk van Diginotar als geheel in ieder geval niet afdoende tegen virussen was beschermd. Om de CA-servers afdoende te beschermen volstaat het niet om alleen antivirus software te installeren op servers die direct met het internet zijn verbonden. Virussen, malware en andere ongeautoriseerde software kunnen immers ook op andere wijzen in een netwerk terecht komen, zoals via een geïnfecteerde CD, DVD, USB-apparaat of laptop.

5.4 Met zijn stelling dat het interim-rapport ten onrechte een negatieve indruk wekt over de beveiliging van Diginotar, nu in het interim-rapport ten onrechte achterwege is gelaten dat Diginotar gebruik maakte van Hardware Security Modules (HSM), geschikt voor gebruik in een netwerkomgeving, welke tot taak hadden om de uitgifte op hoog niveau te beveiligen, miskent eiser dat als gevolg van een onjuist gebruik van deze HSMs, de geboden beveiliging kon worden omzeild.

5.5 Ook het feit dat volgens eiser het netwerk van Diginotar in 24 verschillende interne netwerksegmenten was opgedeeld en dat er zowel een interne als een externe demilitarized zone (DMZ) en vele firewalls in werking waren die het verkeer tussen verschillende segmenten beperkten en een belangrijke beveiligingswal vormden voor met name Secure-net, doet er naar het oordeel van de rechtbank niet aan af dat de getroffen beveiligings¬maatregelen van Diginotar, inclusief de netwerksegmentering door het gebruik van firewalls, onvoldoende zijn gebleken om te voorkomen dat de hacker de administratieve rechten kon bemachtigen van de domeinserver. Daarmee had de hacker toegang tot de CA- servers die zich allen binnen één domein bevonden. Dat Fox-IT geen uitgebreid onderzoek heeft gedaan naar de door eiser genoemde last line of defence van de CA-omgevingen, laat onverlet dat al vast stond dat de hacker deze verdedigingslinie had weten te omzeilen.

5.6 Het betoog van eiser dat verweerder, nu er slechts bij één wachtwoord, voor een server buiten Secure-net, onmiskenbaar is gebleken dat deze relatief zwak en voor kundige hackers vrij eenvoudig te kraken was, niet tot de conclusie heeft kunnen komen dat de systemen van Diginotar als geheel niet voldoende veilig waren, faalt.

De hacker had niet zomaar een wachtwoord verkregen, maar het wachtwoord van de domein administrator. Door gebruikmaking van dit wachtwoord kon met de domein administrator rechten toegang tot alle CA-servers binnen het beveiligde segment van het Diginotar netwerk worden verkregen. Dat het wachtwoord door middel van brute-force te kraken was, toont aan dat het inderdaad ging om een relatief zwak wachtwoord. Brute force is namelijk slechts een simpele hackmethode die bestaat uit het botweg uitproberen van alle mogelijke opties net zo lang tot het juiste wachtwoord is gevonden. Dat de hacker het wachtwoord heeft kunnen kraken, bevestigt dat het wachtwoord niet sterk genoeg was voor het doel dat zij diende: het voorkomen van ongeautoriseerde toegang tot de systemen van Diginotar.

5.7 Eisers standpunt, dat verweerder ten onrechte stelt dat het onderbrengen van alle CA-servers in één domein een schending van 7.4.6.d van ETSI norm 101 456 oplevert, mist doel.

De rechtbank merkt in dit verband op dat op basis van de vaststaande feiten van het interim-rapport is gebleken dat de CA-servers van Diginotar onderdeel uitmaakten van hetzelfde Windows-domein waarvan een onbevoegde derde er in juni 2011 is in geslaagd om de administratieve rechten te verkrijgen. De administratieve rechten zijn de hoogste rechten die een gebruiker kan hebben. Een gebruiker met administratieve rechten kan alles binnen het betreffende domein inzien en wijzigen. Omdat alle CA-servers onderdeel uitmaakten van hetzelfde Windows domein, kon met de administratieve rechten op de domeinserver de controle worden verkregen over de verschillende CA-servers van Diginotar. Door Fox-IT is verder vastgesteld dat op 1 en 2 juli 2011 in de nachtelijke uren met de administratieve rechten ook daadwerkelijk is ingelogd op de CA-server die werd gebruikt voor uitgifte van gekwalificeerde certificaten. De hacker had zich zodoende toegang verschaft tot het beveiligde segment (secure-net) van het netwerk van Diginotar. Dat betekent dat een hacker gegevens via het internet van en naar het beveiligd netwerksegment van Diginotar kon versturen. Met deze administratieve rechten had de hacker toegang tot de gehele productieomgeving van Diginotar. Er bestond voor de hacker geen enkele beperking van de autorisatie. Verweerder heeft dan ook terecht vastgesteld dat artikel 7.4.6.d van ETSI-norm 101 456 is geschonden. Als gevolg hiervan was immers niet langer gewaarborgd dat de toegang tot systemen beperkt is tot de personen die de betreffende systemen moeten gebruiken om hun functie uit te kunnen oefenen.

5.8 Eiser betoogt verder dat Fox-IT in het interim-rapport niet meer dan speculaties verschaft over de betekenis en relevantie van de serienummers die Fox-IT niet meer heeft kunnen koppelen aan daadwerkelijk uitgegeven certificaten. Aangezien de logfiles van de QC en PKI-overheid CA nog intact waren, in tegenstelling tot de CAs die zeker frauduleuze certificaten hebben uitgegeven, had verweerder moeten inzien dat het veel waarschijnlijker was dat de twee niet door Fox-IT thuisgebrachte serienummers van de QC en PKI-overheid CA door andere oorzaken waren ontstaan dan de hack en niet zuiver mogen uitgaan van de speculatie van Fox-IT dat deze serienummers mogelijk zouden kunnen relateren aan frauduleuze gekwalificeerde certificaten. Anderzijds wordt wel in het interim-rapport gemeld dat er geen

aparte centrale logging aanwezig is, maar niet wat voor logs er allemaal wel door Diginotar werden bewaard en gemonitord. Deze selectieve wijze van rapportage leidt er toe dat verweerder dit opvat alsof Diginotar geheel geen netwerklogging op orde had, hetgeen onjuist is.

5.8.1 De rechtbank overweegt in dit verband dat verweerder niet gesteld heeft dat er op de systemen van Diginotar überhaupt geen logging plaatsvond. Verweerder heeft slechts vastgesteld dat bij Diginotar geen beveiligd centraal systeem aanwezig was dat de netwerkactiviteit registreert en opslaat. Bij beveiligde centrale netwerk logging gaat het om infrastructuur waarbij de relevante loggegevens die hun oorsprong vinden op diverse systemen op een centrale plaats veilig worden opgeslagen. Het belang van beveiligde centrale netwerk logging is onder andere dat er na een incident onderzoek kan plaatsvinden op basis van gegevens waarvan de juistheid kan worden gegarandeerd, maar uiteraard ook dat door het monitoren van deze gegevens een incident direct kan worden gedetecteerd. Als gevolg van het ontbreken bij Diginotar van een dergelijke veilige gecentraliseerde logserver moest het onderzoek plaatsvinden op basis van loggegevens die hun oorsprong vinden op systemen die waren gecompromitteerd. Bovendien is door Fox-IT op een aantal gecompromitteerde systemen bewijs aangetroffen waaruit blijkt dat de hacker loggegevens heeft verwijderd of gemanipuleerd. Hierdoor valt niet uit te sluiten dat de hacker certificaten heeft aangemaakt die niet tot loggegevens zouden leiden. Omdat de hacker zelf de inhoud van zijn certificaten kon bepalen, en daarmee ook de uitgiftedatum van de certificaten, konden de eerder uitgegeven certificaten niet langer met zekerheid binnen systeem worden geverifieerd en kon dus niet langer van de integriteit en authenticiteit van deze certificaten worden uitgegaan. Als gevolg daarvan kon de onzekerheid met betrekking tot de betrouwbaarheid van de gekwalificeerde certificaten van Diginotar niet worden weggenomen. Dit had voorkomen kunnen worden door gebruik te maken van veilige centrale netwerk logging. Daarmee wordt een scheiding aangebracht tussen de beveiligingsomgeving en de normale productie omgeving, hetgeen ook een vereiste is uit de ETSI 101 456-norm.

5.8.2 Voorts is door Fox-IT vastgesteld dat er sporen van hackeractiviteit aanwezig waren op een aantal CA-servers. Deze sporen tonen aan dat de aanvaller met domain administrator rechten was ingelogd op het betreffende systeem. Dat de betreffende servers geen sporen vertonen van verwijderde logfiles, bewijst niet dat de logfiles ook daadwerkelijk intact zijn gebleven. De hacker had immers ook de logfiles kunnen vervangen door de oude logfiles van voor de hack of anderszins zijn sporen kunnen wissen.

5.8.3 Door Fox-IT zijn daarnaast serienummers van certificaten gevonden die niet overeenkwamen met enig certificaat dat ooit door Diginotar is uitgegeven. Dit betekent dat van de CA-servers waarop onbekende serienummers zijn aangetroffen, niet mag worden uitgesloten dat met deze servers frauduleuze certificaten zijn uitgegeven. Aangezien ook op de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten twee serienummers zijn aangetroffen van certificaten die niet in de administratie van Diginotar zijn terug te vinden, kon dus geenszins worden uitgesloten dat ook daadwerkelijk frauduleuze gekwalificeerde certificaten zijn aangemaakt, zoals in het bestreden besluit is vastgesteld. Daarbij komt dat ook de CA-servers, waarvan is vastgesteld dat deze werden gebruikt bij de uitgifte van frauduleuze certificaten, gebruik maakten van dezelfde beveiligingsmaatregelen waarvan dus al vaststond dat deze door de hacker konden worden omzeild. Deze twijfel heeft eiser niet kunnen wegnemen.

6. Op grond van het voorgaande is de rechtbank van oordeel dat het netwerk dat door Diginotar werd gebruikt voor de uitgifte van gekwalificeerde certificaten in dit geval ernstig is gecompromitteerd. Bijgevolg was, mede doordat achteraf niet te achterhalen is wat de hacker precies heeft gedaan, de betrouwbaarheid van de gekwalificeerde certificaten die via deze servers werden gegenereerd, niet langer te garanderen. Een nader onderzoek of daadwerkelijk misbruik van gekwalificeerde certificaten heeft plaatsgevonden is niet relevant omdat, zelfs als aangetoond had kunnen worden dat op dat moment nog geen misbruik van de bij de inbraak toegankelijke gegevens en programmatuur op de CA-server voor gekwalificeerde certificaten had plaatsgevonden, door de compromittering van de CA-servers niet uitgesloten kan worden dat dit nog op elk moment zou kunnen gebeuren.

6.1 Eveneens is vast komen te staan dat de integriteit van de gegevens op de CA-servers die werden gebruikt voor de aanmaak en uitgifte van gekwalificeerde certificaten niet meer was te garanderen. Bij Diginotar bestond dus geen adequate beveiliging (meer) tegen het vervalsen van gekwalificeerde certificaten. Hierdoor voldeed zij niet (meer) aan artikel 2, eerste lid, aanhef en onder d, van het Beh.

6.2 Voorts is komen vast te staan dat er niet meer vermoed kon worden dat Diginotar aan de eisen van de ETSI norm, als bedoeld in artikel 2, eerste lid, van de Reh voldeed. Het gebruik van een DMZ doet er niet aan af dat de CA-servers in één Windows-domein waren ondergebracht en dat het mogelijk was om toegang te verkrijgen tot alle CA-servers met één inlognaam-wachtwoordcombinatie. Daarnaast vereist artikel 2, eerste lid, aanhef en onder c, van het Beh dat een CSP die gekwalificeerde certificaten aanbiedt uitsluitend gebruik maakt van betrouwbare systemen en producten die procedureel of overeenkomstig de stand van de techniek beveiligd zijn en die de technische en crypto-grafische veiligheid van de processen die zij ondersteunen garanderen. Hiervoor is onder randnummer 5.7 en 5.8 vastgesteld dat de systemen en producten die door Diginotar werden gebruikt bij de uitgifte van gekwalificeerde certificaten niet overeenkomstig de stand der techniek waren beveiligd en niet meer voldeed aan de resultaatsverplichting uit artikel 2, eerste lid, aanhef en onder c, van het Beh.

6.3 Diginotar voldeed, zoals blijkt uit het interim-rapport, ten tijde van het primaire besluit dus niet (meer) aan de twee belangrijke verplichtingen als bedoeld in artikel 2, eerste lid, onder c en d, van het Beh.

7. De rechtbank stelt vervolgens vast dat zowel het definitieve eindrapport van Fox-IT van 13 augustus 2012 als de (ten dele) door eiser overgelegde contra-expertise van Hoffmann Bedrijfsrecherche van 16 november 2012 de belangrijkste conclusies van het interim-rapport ondersteunen.

7.1 De conclusies dat alle CA-servers bij Diginotar door de aanvaller gecompromitteerd waren en dat de hacker zich daadwerkelijk toegang heeft verschaft tot de Qualified CA server zijn niet weersproken. Ook maakt het eindrapport duidelijk dat de mogelijkheid voor de hacker bestond om frauduleuze gekwalificeerde certificaten aan te maken en dat niet kan worden uitgesloten dat hij deze heeft aangemaakt, of dat hij deze later wellicht alsnog had kunnen aanmaken. In het eindrapport wordt ook vastgesteld dat de hacker erin is geslaagd om tunnels te creëren tussen de verschillende netwerksegmenten. Met deze tunnels konden de firewalls, die werden gebruikt om het Secure-net te scheiden van de overige netwerksegmenten, worden omzeild. Hoewel de verschillende netwerksegmenten op papier van elkaar gescheiden werden door middel van firewalls, was er van een scheiding in de praktijk onvoldoende sprake.

7.2 Ook op basis van het onderzoek van Hoffmann kan niet worden uitgesloten dat frauduleuze gekwalificeerde certificaten zijn uitgegeven. Hoffmann stelt voorts in haar contra-expertise dat de hacker bestaande certificaten en certificaatdiensten (CRLs) heeft gemanipuleerd, hetgeen is aan te merken als een overtreding van artikel 2, eerste lid, aanhef en onder m, van het Beh. Als gevolg daarvan was het voor de hacker niet alleen mogelijk om nieuwe gekwalificeerde certificaten aan te maken met een inhoud die door hem zelf kon worden vastgesteld, maar was het voor de hacker ook mogelijk om certificaten die de rechtmatige gebruiker heeft laten intrekken opnieuw uit te geven en te misbruiken.

Met deze na het bestreden besluit vastgestelde rapportages wordt naar het oordeel van de rechtbank de juistheid van de door verweerder in aanmerking genomen bevindingen in het interim-rapport van Fox-IT niet ontkracht.

8. Volgens eiser is het uiterst onwaarschijnlijk dat de gekwalificeerde certificaten werkelijk gecompromitteerd waren. Eiser stelt zich dan ook op het standpunt dat, als er al sprake was van een beëindigingsgrond, het in de rede zou hebben gelegen dat verweerder artikel 2.2, vierde lid, aanhef en onder c, van de Tw zou hebben toegepast en Diginotar in de gelegenheid zou hebben gesteld om eventuele geconstateerde gebreken te herstellen.

Eiser betwist in dit verband de stelling van verweerder dat, indien de betrouwbaarheid van (het uitgifteproces) van de gekwalificeerde certificaten niet langer kan worden gewaarborgd, de Tw geen

andere mogelijkheid biedt dan (onmiddellijk) de registratie te beëindigen omdat van enige discretionaire ruimte geen sprake zou zijn. Volgens eiser staat dat niet in de wet en gaat de Tw en de wetsgeschiedenis uit van een te stellen termijn, indien na onderzoek geconstateerd wordt dat niet aan bepaalde eisen is voldaan. Ter zitting heeft eiser er nadrukkelijk op gewezen dat het bestreden besluit enkel op het Beh is gebaseerd. Met name in het geval hieraan (en met de eisen bedoeld in artikel 18.15, eerste en tweede lid, van de Tw) niet wordt voldaan, is de c-grond destijds in 2003 aan artikel 2.2, vierde lid, van de Tw toegevoegd, teneinde de CSP-er de mogelijkheid te bieden om gebreken te herstellen. De zogenoemde b-grond dateert al uit 1998 en ziet meer op registraties in het algemeen.

8.1 Naar het oordeel van de rechtbank kan dit betoog van eiser niet slagen. Uit hetgeen hiervoor is overwogen volgt dat niet is uit te sluiten dat de gekwalificeerde certificaten zijn gecompromitteerd. Voorts bepaalt het vierde lid van artikel 2.2, aanhef en onder b, van de Tw, dat verweerder de registratie beëindigt indien een certificatiedienstverlener activiteiten of diensten verricht in strijd met het bepaalde bij of krachtens deze wet. Deze b-grond ziet dus op zowel artikel 18.15 van deze wet als op het Beh en is eveneens bedoeld voor certificatiedienstverleners. De c-grond is destijds met name aan het vierde lid van artikel 2.2 van de Tw toegevoegd in verband met een vrijwillige accreditatieregeling voor de CSP-er ter verbetering van certificatiedienstverlening. Op het moment dat een aangewezen certificatie-instelling twijfelt of een CSP-er aan de eisen van het Beh voldoet en verweerder hiervan in kennis stelt, kan verweerder aan de CSP-er een termijn stellen om een en ander te laten herstellen.

8.2 De rechtbank wijst in dit verband op de wetsgeschiedenis bij artikel 2.2, vierde lid, aanhef en onder c, van de Tw (Kamerstukken II 2000/2001, 27 743, nr. 3, p. 21), waaruit blijkt dat de bevoegdheid van verweerder om een herstelmogelijkheid te bieden uitsluitend bedoeld is voor gevallen waarin geen sprake is van twijfels over de betrouwbaarheid van de gekwalificeerde certificaten:

Het stellen van een termijn wordt noodzakelijk geacht in verband met de mogelijke niet naleving van bepaalde vereisten die de betrouwbaarheid van een gekwalificeerd certificaat niet direct in twijfel trekken.

Die twijfels waren er in het onderhavige geval wel. Er is vastgesteld dat bij Diginotar sprake is geweest van een ernstige inbraak en compromittering van de systemen die werden gebruik voor de aanmaak van gekwalificeerde certificaten, waardoor de betrouwbaarheid van de door Diginotar uitgegeven certificaten ter discussie stond. Gezien het feit dat de gevolgen van de compromittering van de servers niet meer ongedaan konden worden gemaakt en er activiteiten dan wel diensten zijn verricht die in strijd zijn met het bepaalde bij of krachtens de Tw, had verweerder naar het oordeel van de rechtbank geen andere keus dan op grond van artikel 2.2, vierde lid, aanhef en onder b, van de Tw, zonder hersteltermijn, tot beëindiging van de registratie van Diginotar als CSP over te gaan. Dat verweerder, aldus eiser, bij een incident met een hacker bij KPN niet tot prompte beëindiging heeft besloten, ziet op het feit dat er bij verweerder in dat geval geen sprake was van enige twijfel over de betrouwbaarheid van gekwalificeerde certificaten. Die twijfels waren er in dit geval wel.

9. Het betoog van eiser dat verweerder ten onrechte geen belangen heeft afgewogen, kan evenmin slagen. Hoewel artikel 2.2, vierde lid, aanhef en onder b, van de Tw geen ruimte biedt voor een belangenafweging, heeft verweerder zich bij het besluit tot beëindiging van de registratie van Diginotar wel degelijk rekenschap gegeven van de gevolgen die deze beëindiging voor Diginotar zou kunnen hebben. Dit blijkt uit het feit dat verweerder Diginotar niet heeft gedwongen om direct de reeds uitgegeven gekwalificeerde certificaten in te trekken, maar haar daarvoor een termijn van twee weken heeft gegeven.

De niet-ontvankelijkverklaring bij het bestreden besluit dient, zo heeft verweerder ter zitting nader uiteen gezet, in het licht te worden gezien van de discussie die is ontstaan over de begeleidende brief bij het primaire besluit. Naar het oordeel van de rechtbank heeft verweerder toereikend gemotiveerd dat hij daarmee alleen heeft bedoeld aan te geven dat Diginotar bij de begeleidende brief slechts is gewezen op de wettelijke verplichtingen die volgen uit artikel 2 van het Beh, terwijl er voor verweerder in beginsel geen ruimte is voor enige belangenafweging.

10. Gelet op hetgeen hiervoor is overwogen is de rechtbank van oordeel dat verweerder terecht op grond van artikel 2.2, vierde lid, aanhef en onder b, van de Tw, zonder herstelltermijn, tot beëindiging van de registratie van Diginotar als CSP is overgegaan. Het beroep dient daarom ongegrond te worden verklaard.

11. Voor een veroordeling in de proceskosten ziet de rechtbank geen aanleiding.

Beslissing

De rechtbank verklaart het beroep ongegrond.

Deze uitspraak is gedaan door mr. A.I. van Strien, voorzitter, en mr. J.H. de Wildt en mr. M.J.S. Korteweg-Wiers, leden, in aanwezigheid van mr. A. Vermaat, griffier. De beslissing is in het openbaar uitgesproken op 16 mei 2013.

griffier voorzitter

Afschrift verzonden aan partijen op:

Rechtsmiddel

Tegen deze uitspraak kan binnen zes weken na de dag van verzending daarvan hoger beroep worden ingesteld bij het College van Beroep voor het bedrijfsleven.