STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 5316
20 februari 2023

Regeling van de Minister van Economische Zaken en Klimaat van 13 februari 2023, nr. WJZ/ 26234325, tot wijziging van de Regeling aanwijzing aanbieders essentiële diensten EZK in verband met de aanvullende aanwijzing van DNS-dienstverleners

De Minister van Economische Zaken en Klimaat,

Gelet op artikel 2 van het Besluit beveiliging netwerk- en informatiesystemen;

Besluit:

ARTIKEL I

De Regeling aanwijzing aanbieders essentiële diensten EZK wordt als volgt gewijzigd:

A

Artikel 2* wordt vernummerd tot artikel 2.

B

In de tabel in artikel 2 (nieuw) wordt in de derde rij betreffende sector digitale infrastructuur 'Een beheerder van een register voor topleveldomeinnamen die bij de IANA is geregistreerd, meer dan 1.000.000 geregistreerde domeinnamen in beheer heeft en ten behoeve van die domeinnamen DNS-diensten verleent als bedoeld in artikel 4, onder 14 en 15, van Richtlijn (EU) 2016/1148' vervangen door

> 'Een aanbieder van DNS-diensten als bedoeld in artikel 4, onder 14 en 15, van Richtlijn (EU) 2016/1148 die ten behoeve van meer dan 400.000 geregistreerde .nl- domeinnamen authoritative DNS-diensten verleent.
> Indien een aanbieder een of meer partnerondernemingen of verbonden ondernemingen als bedoeld in artikel 3, tweede onderscheidenlijk derde lid, van de bijlage bij de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEU 2003, L 124) heeft, wordt uitgegaan van het totale aantal .nl-domeinnamen van de partnerondernemingen of verbonden ondernemingen.'.

C

De artikelen 2 (oud) en 3 worden vernummerd tot respectievelijk de artikelen 3 en 4.

ARTIKEL II

Deze regeling treedt in werking met ingang van 1 juli 2023.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

's-Gravenhage, 13 februari 2023

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

TOELICHTING

1. Algemeen

Deze regeling strekt tot een ruimere aanwijzing van DNS (Domain Name System)-dienstverleners als aanbieder van een essentiële dienst (AED) als bedoeld in de zogenoemde NIB-richtlijn van de Europese Unie[1] en de Wet beveiliging netwerk- en informatiesystemen (Wbni). In de Regeling aanwijzing aanbieders essentiële diensten EZK (hierna: regeling) zijn reeds bepaalde DNS-dienstverleners aangewezen als AED, namelijk beheerders van een register van topleveldomeinnamen – zoals het .nl domein – vanaf 1.000.000 geregistreerde domeinnamen. Naar aanleiding van nadere analyse worden thans meer DNS-dienstverleners als AED aangewezen.

2. Inhoudelijk

Met onderhavige wijzigingsregeling wordt in artikel 2 (nieuw) van de regeling de aanwijzing van AED's in de deelsector digitale infrastructuur gewijzigd. Met deze wijziging wordt de bestaande aanwijzing van DNS-dienstverleners in de regeling uitgebreid en verduidelijkt.

Een DNS is een essentieel onderdeel van de infrastructuur van het internet. Een DNS is 'een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt' (artikel 4, onder 14, van de NIB-richtlijn).

Onderzoek bevestigt dat, wanneer het DNS niet kan worden bevraagd, veel digitale diensten niet meer naar behoren werken.[2] Zo kunnen websites niet meer worden bezocht, omdat het niet mogelijk is om te achterhalen met welk IP-adres er moet worden gecommuniceerd. E-mailbezorging valt stil, omdat een e-mailserver niet meer kan opzoeken welke server de mail in ontvangst kan nemen voor een bepaald domein. Daarnaast zijn er talloze andere diensten voor welke het DNS essentieel is. Naast uitval of verstoring is ook de integriteit van DNS-informatie van belang. Wanneer een kwaadwillende informatie in het DNS kan wijzigen, kan dat nadelige gevolgen hebben, bijvoorbeeld dat verkeer gericht aan een bepaald domein kan worden 'omgeleid' naar een ander adres. Wanneer de DNS-servers van een partij die DNS-diensten aanbiedt worden verstoord, dan kunnen alle klanten van deze partij bovengenoemde problemen ondervinden.

Zogenaamde *authoritative* DNS-servers zijn verantwoordelijk voor het verstrekken van informatie over een of meerdere domeinen (specifieke zones) zoals bijvoorbeeld 'rijksoverheid.nl' of 'janssentransport.nl'.[3] Met deze regeling worden aanbieders van authoritative DNS-servers aangewezen als aanbieders van een essentiële dienst. Uit recent onderzoek blijkt dat een klein aantal partijen de authoritative DNS-dienst realiseert voor een groot deel van de voor Nederland relevante domeinnamen.[4] Het gaat dan vooral om hostingbedrijven die DNS-diensten leveren aan een groot aantal klanten, bijvoorbeeld in het midden- en kleinbedrijf. Een incident bij een aanbieder kan leiden tot verstoring van de DNS-dienst met als gevolg honderdduizenden onbereikbare domeinen en daarmee geleverde diensten. Daarom worden dergelijke aanbieders thans aangewezen als aanbieder van een essentiële dienst in de zin van artikel 1, Wbni. In bijvoorbeeld Duitsland vallen aanbieders van authoritative DNS-diensten ook al onder de regelgeving ter implementatie van de NIB-richtlijn.

In artikel 2 (nieuw) van de regeling wordt daarom als AED aangewezen: een aanbieder van authoritative DNS-diensten ten behoeve van meer dan 400.000 geregistreerde .nl-domeinnamen. Een aanbieder valt onder de aanwijzing wanneer hij meer dan 400.000 .nl-domeinnamen host. Hiermee worden aanbieders vanaf een bepaalde omvang aangewezen. Daarbij is gekozen voor een drempelwaarde op basis van geregistreerde .nl-domeinnamen. Dit is een voor aanbieders duidelijk en hanteerbaar criterium. Alle .nl-domeinnamen worden geregistreerd bij Stichting Internet Domein-registratie Nederland (SIDN). In Nederland gevestigde aanbieders bedienen vooral .nl-domeinnamen. Bovendien maken veel Nederlandse organisaties, publiek en privaat, gebruik van het .nl-topleveldomein. Daarmee is het aantal .nl-domeinnamen een relevante maat voor de invloed die verstoring van de authoritative DNS-dienst heeft op maatschappelijke of economische activiteiten in Nederland.

---

1 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).

2 Zie het rapport 'Inventarisatie aanbieders van DNS-diensten in Nederland' van onderzoeksbureau Dialogic vanaf p.16. Dit rapport is te vinden op https://www.rijksoverheid.nl/documenten/rapporten/2021/02/16/inventarisatie-aanbieders-van-dns-diensten-in-nederland.

3 Zie voor een beschrijving van 'authoritative server' hoofdstuk 6 van RFC 8499, https://datatracker.ietf.org/doc/rfc8499/.

4 Zie het rapport 'Inventarisatie aanbieders van DNS-diensten in Nederland' van Dialogic, https://www.rijksoverheid.nl/documenten/rapporten/2021/02/16/inventarisatie-aanbieders-van-dns-diensten-in-nederland.

Gekozen is voor een drempelwaarde van 400.000 geregistreerde .nl-domeinnamen. Momenteel zijn meer dan 6 miljoen .nl-domeinnamen geregistreerd. Bij een aantal van 400.000 of meer .nl-domeinnamen, circa 7% van het totaal, is het aannemelijk dat verstoring van de authoritative DNS-dienst aanzienlijke gevolgen kan hebben voor maatschappelijke of economische activiteiten. Overigens is gekozen voor een drempelwaarde die hoger ligt dan in andere EU-lidstaten. Dat is passend omdat in Nederland een relatief hoog aantal domeinen geregistreerd is en vanwege de relatief omvangrijke (hosting)sector in Nederland. Naar schatting komen, bij de huidige marktverhoudingen, de vier grootste aanbieders boven de drempelwaarde uit. Bij de keuze voor een drempelwaarde speelt ook consistentie in de wetgeving mee. Met de drempel van 400.000 geregistreerde .nl-domeinnamen wordt aangesloten op de drempelwaarde in het Besluit ongewenste zeggenschap telecommunicatie (Bozt)[5] die geldt voor aanbieders van hostingdiensten. De aanwijzing in deze regeling is niet beperkt tot aanbieders van hostingdiensten, maar veelal gaat het om dergelijke aanbieders, als we kijken naar de in Nederland gevestigde partijen.

De hostingsector typeert zich door overnames en consolidatie. Daardoor maakt een deel van de aanbieders onderdeel uit van een groep ondernemingen. In artikel 2 (nieuw) is verduidelijkt dat in dat geval wordt uitgegaan van het totale aantal .nl-domeinnamen van de partnerondernemingen of verbonden ondernemingen als bedoeld in de bijlage bij de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEU 2003, L 124). Dit geeft duidelijke kaders voor het samentellen van gegevens van ondernemingen waarmee bepaald kan worden of een aanbieder onder deze regeling valt.

Met deze nieuwe, ruimere en verduidelijkte aanwijzing kan de bestaande aanwijzing van DNS-dienstverleners komen te vervallen. De bestaande aanwijzing betreft de DNS-diensten van beheerders van een register voor topleveldomeinnamen vanaf 1.000.000 geregistreerde domeinnamen. Daarbij gaat het al om authoritative DNS-diensten. Zo is de Stichting Internet Domein Registratie (SIDN) authoritative DNS-dienstverlener voor het .nl-domein. Dergelijke diensten vallen onder de nieuwe aanwijzing. De nieuwe aanwijzing betreft wel uitsluitend het .nl-domein, maar in de praktijk zijn er in Nederland geen andere beheerders van topleveldomeinnamen (anders dan SIDN) die boven een drempelwaarde van 400.000 domeinnamen uitkomen. Bij domeinen zoals.amsterdam of.frl (Friesland) gaat het om een aanmerkelijk kleiner aantal geregistreerde domeinnamen. De nieuwe aanwijzing dekt de bestaande aanwijzing dus voldoende af.

3. Regeldruk

De door deze regeling veroorzaakte regeldruk bestaat uit een verantwoorde stijging van de administratieve lasten en inhoudelijke nalevingskosten.

Met deze wijziging wordt een bredere groep AED's aangewezen, waardoor voor hen de verplichtingen uit de Wbni en het Besluit beveiliging netwerk- en informatiesystemen (Bbni) gaan gelden. Het gaat met name om de verplichting om ernstige ICT-incidenten te melden bij het Nationaal Cyber Security Centrum (NCSC) en de Rijksinspectie Digitale Infrastructuur (de bevoegde autoriteit voor de sector digitale infrastructuur, aangewezen in artikel 4, eerste lid, Wbni), zie artikel 10, eerste, tweede en derde lid, Wbni, en om de beveiligingseisen van de artikelen 7 en 8, Wbni, zoals nader uitgewerkt in de bijlage bij artikel 3a, Bbni.

3.1 Meldplicht

Voor het verrichten van een melding zal het veelal gaan om handelingen als het verzamelen van informatie, het schriftelijk en eventueel telefonisch doen van een melding en het eventueel verstrekken van nadere informatie aan het NCSC of de bevoegde autoriteit. De meldplicht geldt alleen voor incidenten met aanzienlijke gevolgen voor de continuïteit van de door de AED verleende dienst. De kosten per AED worden geschat op € 600 per jaar (= 300 minuten gemiddeld per melding x 2 meldingen per jaar x uurtarief van € 60). Hiermee wordt aangesloten op de berekeningen zoals toegelicht in de nota van toelichting bij de Bbni-wijziging van 17 maart 2021.[6]

3.2 Beveiligingseisen

AED's moeten passende technische en organisatorische maatregelen treffen ter beveiliging van hun netwerk- en informatiesystemen. Die zorgplicht is nader uitgewerkt in de bijlage van het Bbni.

[5] Staatsblad 2020, 352.
[6] Staatsblad 2021, 160.

In de eerder genoemde nota van toelichting bij de Bbni-wijziging van 17 maart 2021 is tevens ingegaan op de regeldrukeffecten van de zorgplicht. Van reeds aangewezen AED's is bekend dat er vooral extra kosten zijn ontstaan rondom de beveiligingseisen. AED's hebben extra (interne en externe) capaciteit moeten inzetten om te gaan voldoen aan de beveiligingsmaatregelen die de wet stelde. Echter, voor AED's in de sector digitale infrastructuur bleek dat de additionele kosten als gevolg van de Wbni beperkt waren, met name omdat men voordien al een hoog beveiligingsniveau hanteerde. Voor deze AED's zijn de (beperkte) regeldrukkosten vooral gerelateerd aan het beter inzichtelijk maken van de reeds bestaande praktijk. Dit is naar verwachting ook het geval voor de onder artikel 2 nieuw aangewezen DNS-dienstverleners. Dit betreft vooral grotere aanbieders van hostingdiensten.[7]

Dit beeld is getoetst bij de doelgroep. Uit met aanbieders gevoerde gesprekken blijkt dat ook zonder wetgeving zij al de nodige beveiligingsmaatregelen hebben getroffen, zijnde een combinatie van organisatorische en technische maatregelen. Voor de continuïteit van hun eigen bedrijfsvoering is het immers cruciaal dat maatregelen worden getroffen op het gebied van netwerk- en informatiebeveiliging. Zonder maatregelen zijn deze aanbieders kwetsbaar voor tal van dreigingen, zoals cybercrime en menselijke fouten. Daarbij zouden aanbieders een reëel risico kunnen lopen waarbij een correcte levering van hun eigen diensten in gevaar komt.
Wel is gebleken dat de verwachte regeldruk per aanbieder sterk verschilt. De door aanbieders genoemde jaarlijkse kosten variëren van € 9.600 tot € 137.025. De jaarlijkse kosten per aanbieder worden geraamd op gemiddeld € 70.000. Uitgaande van vier aanbieders, betreft de totale regeldruk € 280.000 per jaar (= 4 x € 70.000).

3.3 Eenmalige kennisnamekosten en toezichtslasten

AED's zullen eenmalig tijd besteden aan het zich verdiepen in en kennisnemen van de Wbni. Organisaties zullen hier naar schatting 16 uur (2 werkdagen) voor nodig hebben. Uitgaande van een uurtarief van € 120 komt dit uit op € 1.920 eenmalige kennisnamekosten per organisatie. Uitgaande van maximaal vier aanbieders, betreft de totale regeldruk € 7.680 (= 4 x € 1.920).
Ook het te woord staan van de bevoegde autoriteit in haar rol als toezichthouder veroorzaakt administratieve lasten voor AED's. Ook deze werkzaamheden kosten een AED naar schatting 16 uur, en daarmee € 1.920, maar dan per jaar. Uitgaande van vier aanbieders, betreft de totale regeldruk € 7.680 per jaar.

3.4 Advies Adviescollege Toetsing Regeldruk

Deze wijzigingsregeling is voorgelegd voor advies aan het Adviescollege Toetsing Regeldruk (ATR). Naar aanleiding van het advies van ATR is de toelichting op enkele punten aangepast. Op hoofdlijnen houden deze aanpassingen verduidelijkingen in en een meer specifieke berekening van de regeldruk.

4. Uitvoerbaarheid en handhaafbaarheid

De Rijksinspectie Digitale Infrastructuur acht deze wijziging van de regeling uitvoerbaar en handhaafbaar. De gevolgen die deze wijziging meebrengt, zijn reeds meegenomen in het Jaarplan Toezicht 2023.

5. Consultatie

Op een eerdere versie van deze wijzigingsregeling zijn reacties ingewonnen door middel van een openbare consultatie op www.internetconsultatie.nl. De reacties zijn afkomstig van een burger, de brancheverenigingDigitale Infrastructuur Nederland en van een aanbieder. Laatstgenoemde reactie is vertrouwelijk. Hieronder wordt gegroepeerd ingegaan op de punten in de reacties.

5.1 Criterium voor aanwijzing

Een respondent stelt dat het gekozen omvangscriterium grotere providers betreft die zich richten op de onderkant van de markt. Deze respondent vindt dat de regulering uit zou moeten gaan van het daadwerkelijk gebruik van domeinen in vitale, essentiële economische ketens. Dit door te kijken naar diensten met een hoog service level. Dat zou ook aansluiten bij de opzet van de aankomende

[7] Een aanbieder van hostingdiensten is een dienstverlener die een klant de mogelijkheid geeft om een website op internet te plaatsen. De aanbieder biedt internetconnectiviteit, IP-adressen, servers, opslag, backup, geografische distributie, caching en meer.

EU-certificeringen onder de Cyberbeveiligingsverordening[8], en de markt wordt niet verstoord. Een andere respondent stelt dat het louter tellen van domeinnamen niet per definitie een juiste indicatie geeft van de maatschappelijke/economische waarde van die domeinnamen. Tenslotte vraagt een respondent waarom niet alle DNS-dienstverleners worden aangewezen, omdat men ook van een kleinere aanbieder afhankelijk kan zijn.

Hierover het volgende. De aanwijzing in deze regeling ziet vooral op de schaal van de gevolgen bij verstoring of uitval van DNS-diensten, namelijk het aantal gebruikers dat geraakt kan worden, in termen van aantallen domeinen, ongeacht of de gebruikers vitaal of niet-vitaal zijn. Dit is een duidelijk en hanteerbaar criterium. Het is een valide punt, dat de maatschappelijke of economische gevolgen bij verstoring of uitval van DNS-diensten ook afhangen van het gebruik van die domeinen. Zo kan een kleinere aanbieder een gebruiker in een vitaal proces of een economisch waardevol domein bedienen. Het identificeren van dergelijke aanbieders zou echter complex zijn, omdat hiervoor gedetailleerde, veelal bedrijfsvertrouwelijke informatie nodig is over een potentieel groot aantal aanbieders en hun klanten. Daarbij is de situatie veranderlijk, omdat gebruikers een domein vrij eenvoudig kunnen verhuizen naar een andere aanbieder. Dit maakt aanwijzing voor de overheid lastig uitvoerbaar. Verder geldt voor gebruikers in vitale processen (zoals betalingsverkeer of de energievoorziening) veelal de zorgplicht van de Wbni. Zij dienen in de risicoanalyse waar relevant rekening te houden met externe afhankelijkheden van netwerk- en informatiesystemen die betrokken worden van toeleveranciers (van bijvoorbeeld DNS-diensten) en daarbij af te wegen welke risico's acceptabel zijn. Om deze redenen is ervoor gekozen de aanwijzing nu te beperken tot (een beperkte groep) aanbieders vanaf een bepaalde omvang. In de toekomst zal de wetgeving van toepassing worden op een grotere groep DNS-dienstverleners ten gevolge van de herziene NIB-richtlijn.

Een respondent zegt niet goed te begrijpen waarom voor een inperking tot alleen het .nl-domein is gekozen, want ook topleveldomeinen zoals .com en .shop spelen in Nederland een belangrijke rol. Hij stelt voor ook naar deze domeinen te kijken, zodat een level playing field in de Nederlandse markt behouden blijft.

Er is een aantal redenen voor deze inperking tot het .nl-domein. In hoofdstuk 2 is gemotiveerd waarom het .nl-domein een relevante maat is voor de invloed die verstoring van de authoritative DNS-dienst heeft op maatschappelijke of economische activiteiten in Nederland. In aanvulling daarop het volgende. Ten eerste is de identificatie of aanwijzing van aanbieders gericht op aanbieders met een vestiging in Nederland. Dit volgt uit artikel 5, eerste lid, van de NIB-richtlijn. Volgens Dialogic is het .nl-domein een goede indicatie van het gericht zijn op de Nederlandse markt.[9] Een gevolg van de inperking is wel dat in Nederland gevestigde DNS-aanbieders die vooral via een niet-.nl-domein actief zijn, buiten beeld blijven. Het beeld is echter dat in Nederland gevestigde aanbieders vooral .nl-domeinnamen bedienen. Ten tweede wordt met de focus op .nl-domeinnamen aangesloten op de drempelwaarde in het Besluit ongewenste zeggenschap telecommunicatie die geldt voor aanbieders van hostingdiensten. Dat geeft eenduidigheid in de regelgeving. Alles wegende, is gekozen voor een inperking tot het .nl-domein.

Tenslotte signaleren meerdere respondenten dat een (aanzienlijk) deel van de geregistreerde of gehoste domeinen niet actief wordt gebruikt. Zij vragen deze 'geparkeerde' domeinen uit te sluiten.

Hoewel dit op zich een valide punt is, wordt hier niet voor gekozen. Het criterium zou hiermee minder duidelijk en hanteerbaar worden. Er kunnen verschillende interpretaties zijn over wanneer een domein wel of niet actief is. En omdat niet actieve domeinen snel wél actief kunnen worden, maakt dit de aanwijzing potentieel veranderlijk. Daarnaast speelt hier ook in de overweging mee, dat aansluiting op het criterium in het Besluit ongewenste zeggenschap telecommunicatie wenselijk is vanwege eenduidigheid in de regelgeving. Bovendien is al voor een relatief hoge drempelwaarde van 400.000 .nl-domeinnamen gekozen, een drempelwaarde die aanzienlijk hoger ligt dan in andere EU-lidstaten.

5.2 Regeldruk

Een respondent, een aanbieder, zegt te erkennen dat voor de continuïteit van de bedrijfsvoering het cruciaal is dat maatregelen worden getroffen op het gebied van netwerk- en informatiebeveiliging, maar dat gelet op de achtergrond (klanten stellen geen hoge eisen) het huidige beveiligingsniveau mogelijk niet conform verwachting van de Wbni is. Deze aanbieder verwacht een behoorlijke

[8] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PbEU 2019, L151).

[9] Zie het rapport 'Inventarisatie aanbieders van DNS-diensten in Nederland' van onderzoeksbureau Dialogic. Dit rapport is te vinden op https://www.rijksoverheid.nl/documenten/rapporten/2021/02/16/inventarisatie-aanbieders-van-dns-diensten-in-nederland.

regeldruk indien de zorg- en meldplicht uit de Wbni gaan gelden. Daarbij noemt deze aanbieder een aantal te nemen maatregelen.

Naar aanleiding van deze consultatiereactie en bovengenoemd advies van Adviescollege Toetsing Regeldruk, is aanvullende informatie ingewonnen bij de doelgroep, om een scherper beeld te krijgen over de verwachte extra kosten voor deze aanbieders. Naar aanleiding hiervan is de regeldrukparagraaf van deze toelichting (paragraaf 3) aangepast.

Een andere respondent stelt dat alle providers in de doelgroep al bestaande certificeringen zoals de ISO 27001 hebben. Hij vraagt om expliciet vast te leggen dat er van bestaande ISO-certificeringen van providers gebruik gemaakt zal worden, zodat niet later alsnog nieuwe regimes met bijkomende hoge kosten in beeld kunnen komen die alsnog voor hoge kosten gaan zorgen.

Hierover het volgende. AED's moeten passende technische en organisatorische maatregelen treffen ter beveiliging van hun netwerk- en informatiesystemen. Die zorgplicht is nader uitgewerkt in het Bbni. Zo hanteert de AED in elk geval een risicogebaseerde aanpak, waarbij hij zich baseert op de voor de AED relevante normen (internationaal, nationaal, sectorspecifieke of bedrijfseigen). Het Bbni stelt niet één norm of één specifieke versie daarvan verplicht. Het staat de AED daarmee vrij om het normenkader te kiezen dat het beste aansluit bij de sectorspecifieke risico's en het risicoacceptatieniveau. Uiteindelijk is het aan de toezichthouder om vast te stellen of de AED aan de zorgplicht voldoet.

5.3 Certificering

Een respondent wijst op de aankomende EU-certificeringsschema voor clouddiensten (EUCS) onder de Cyberbeveiligingsverordening[10]. Ten eerste vraagt hij om de toezegging dat niet, als gevolg van de aanwijzing in deze regeling, de facto de gehele dienst (voor alle domeinen) onder 'EUCS High' zal gaan vallen. Ten tweede vraagt hij om bevestiging dat een eventuele verplichting voor EUCS certificering voor DNS-dienstverleners zal volstaan als bewijs van conformiteit.

De zorgen van de sector over het EUCS en koppelingen hiermee vanuit (toekomstige) EU-wetgeving zijn bekend. Opgemerkt wordt dat dit geen onderwerp in deze regeling is en kan zijn. Het tweede punt is vergelijkbaar met het punt over ISO-certificering, zie hierboven.

6. Inwerkingtreding

Deze regeling treedt in werking met ingang van 1 juli 2023. Dit is in overeenstemming met het beleid inzake de vaste verandermomenten. Dit geeft de betreffende aanbieders de gelegenheid om zich voor te bereiden op de verplichtingen uit de Wbni en het Bbni die voor hen gaan gelden, zie ook paragraaf 3.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

[10] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PbEU 2019, L151).