STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 42618
5 oktober 2021

Regeling van de Minister van Economische Zaken en Klimaat van 1 oktober 2021, nr. WJZ/ 20056324, houdende nadere regels betreffende de veiligheid en integriteit van openbare elektronische communicatienetwerken en -diensten (Regeling veiligheid en integriteit telecommunicatie)

De Minister van Economische Zaken en Klimaat,

Gelet op artikel 11a.1, vierde lid van de wet en artikel 2, eerste lid, van het Besluit veiligheid en integriteit telecommunicatie;

Besluit:

Artikel 1

In deze regeling wordt verstaan onder:
a. *netwerkaanbieder:* aanbieder van een openbaar mobiel elektronisch communicatienetwerk die beschikt over vergunningen voor het gebruik van geharmoniseerd radiospectrum als bedoeld in artikel 2, onder 25, van Richtlijn (EU) 2018/1972 van het Europees parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek van elektronische communicatie (PbEU 2018, L 321) die zijn verleend met toepassing van een veiling, als bedoeld in artikel 3.10, eerste lid, aanhef en onderdeel f, van de wet;
b. *kritieke onderdelen:* door de Minister aan de netwerkaanbieder als zodanig aangemerkte en bekendgemaakte onderdelen van een openbaar elektronisch communicatienetwerk of bijbehorende faciliteiten;
c. *aanpalende onderdelen:* onderdelen van een openbaar elektronisch communicatienetwerk of bijbehorende faciliteiten die zich op eenzelfde netwerksegment bevinden als de kritieke onderdelen;
d. *netwerksegment:* onderdeel van een openbaar elektronisch communicatienetwerk dat fysiek of logisch als een afgescheiden compartiment van een openbaar elektronisch communicatienetwerk kan worden beschouwd;
e. *beheeromgevingen:* werkstations en personele en ondersteunende middelen die worden ingezet voor configuratie en beheer van kritieke onderdelen, aanpalende onderdelen of beveiligingselementen;
f. *beveiligingselementen:* beveiligingsmiddelen die ten behoeve van de in de eerste kolom van de bijlage bedoelde beheersmaatregelen worden ingezet.
g. *te beschermen kritieke gegevens:* door de Minister aan de netwerkaanbieder als zodanig aangemerkte en bekendgemaakte gegevens ter bescherming van de nationale veiligheid.

Artikel 2

1. De beheersmaatregelen in deze regeling zijn van toepassing op de kritieke onderdelen, aanpalende onderdelen, beveiligingselementen en beheeromgevingen van de netwerkaanbieder.

2. In afwijking van het bepaalde in het eerste lid zijn de beheersmaatregelen, genoemd in de eerste kolom, onder categorie C, nummers 1 en 2, van de bijlage, van toepassing op een door de netwerkaanbieder op grond van een onderbouwde risicoafweging te kiezen deel van zijn openbaar elektronisch communicatienetwerk of bijbehorende faciliteiten. Het door de netwerkaanbieder te kiezen deel omvat in ieder geval de mobile core en alle beheertoegang, zowel door intern personeel als door derde partijen tot kritieke onderdelen, aanpalende onderdelen en beveiligingselementen.

3. In afwijking van het bepaalde in het eerste lid is de beheersmaatregel, genoemd in de eerste kolom, onder categorie B, nummer 5, van de bijlage, van toepassing op het transport van te beschermen kritieke gegevens ongeacht het netwerkonderdeel waarover dat transport plaatsvindt.

Artikel 3

1. De netwerkaanbieder voldoet op uiterlijk 1 oktober 2022 aan de beheersmaatregelen, genoemd in de eerste kolom van de bijlage, door implementatie van de implementatievereisten, genoemd in de tweede kolom van de bijlage.

2. In afwijking van het eerste lid kan de Minister op aanvraag van de netwerkaanbieder ontheffing verlenen van één of meer implementatievereisten van een beheersmaatregel, indien de netwerkaanbieder naar het oordeel van de Minister heeft aangetoond dat met een door de netwerkaanbieder genoemde alternatieve uitvoeringswijze voor de desbetreffende beheersmaatregel tenminste een vergelijkbaar beveiligingsniveau wordt bereikt.

3. De Minister beslist binnen twaalf weken na ontvangst van een aanvraag als bedoeld in het tweede lid. Indien de Minister niet binnen twaalf weken een besluit op de aanvraag kan nemen, stelt de Minister de aanvrager daarvan in kennis en noemt daarbij een termijn waarbinnen de beschikking wel tegemoet kan worden gezien.

4. De ontheffing wordt onder voorschriften of beperkingen verleend.

Artikel 4

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Artikel 5

Deze regeling wordt aangehaald als: Regeling veiligheid en integriteit telecommunicatie.

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

's-Gravenhage, 1 oktober 2021

De Minister van Economische Zaken en Klimaat,
S.A. Blok

BIJLAGE

Beheersmaatregelen en implementatievereisten als bedoeld in artikel 3, eerste lid.

Beheersmaatregel	Implementatievereisten
Categorie A: Veilige configuratie van technische apparatuur	
1. Het minimaliseren en afschermen van de functionaliteit van technische systemen conform erkende practices en richtlijnen.	a. Functies en software applicaties die niet noodzakelijk zijn voor de correcte werking van een systeem of netwerkelement worden verwijderd of gedeactiveerd. b. Het gebruik van netwerkpoorten, -protocollen en -diensten is slechts toegestaan als daaraan een gevalideerde bedrijfstoepassing ten grondslag ligt. c. Besturingssystemen, software omgevingen en netwerkapparaten worden, voor zover beschikbaar, geconfigureerd conform CIS benchmarks.
2. Het verifiëren en uitrollen van kritieke security patches voor software die wordt toegepast in de technische infrastructuur.	a. Door leveranciers ter beschikking gestelde kritieke security patches worden structureel op instanties van de betreffende software uitgerold. b. Een kritieke security patch wordt slechts dan geïnstalleerd als de integriteit en de bron waarvan deze afkomstig is met succes zijn geverifieerd. c. Bij het verifiëren en uitrollen van kritieke security patches wordt een zo kort mogelijke doorlooptijd gerealiseerd. d. Indien de in onderdeel c bedoelde doorlooptijd niet haalbaar is, worden tijdelijk compenserende mitigaties getroffen om de risico's zoveel mogelijk te beperken.
3. Het actief en geautomatiseerd beschermen van beheerwerkstations die voor beheerdoeleinden worden ingezet tegen malware.	a. Op beheerwerkstations zijn mechanismen actief die kwaadaardige malware geautomatiseerd detecteren en deactiveren. b. De onder a bedoelde mechanismen worden geautomatiseerd actueel gehouden.
4. Het door middel van een gestructureerd proces reguleren en tot een minimum beperken van toegang voor beheerdoeleinden van apparatuur en software van de netwerkaanbieder.	a. Voor toegang om beheerwerkzaamheden te verrichten wordt uitsluitend gebruik gemaakt van persoonsgebonden accounts die specifiek voor dat doel zijn uitgegeven. b. Toegangsrechten van beheerpersoneel worden beperkt tot functies en gegevens die de desbetreffende medewerker aantoonbaar nodig heeft ter vervulling van de rol of taak. c. Alle accounts en toegangsrechten die voor beheerdoeleinden zijn uitgegeven, worden periodiek op juistheid en noodzaak geëvalueerd en geactualiseerd. d. Alle beheertoegang vereist Multi Factor Authenticatie. De beheertoegang is herleidbaar naar individuele medewerkers.
5. Het onderhouden van een actuele inventaris van technische assets en het actief toezien op het voorkomen van toelating van ongeautoriseerde hardware en software in de technische infrastructuur.	a. Er is een actuele inventaris van hardware en software assets die geautoriseerd in bedrijf zijn in de technische infrastructuur van de netwerkaanbieder. b. In de inventaris van hardware en software assets zijn zowel de functionele beschrijvingen als de eigenaren van alle technische assets geregistreerd. c. De netwerkaanbieder ziet er actief op toe dat zich in de technische infrastructuur geen ongeautoriseerde apparatuur bevindt. d. De netwerkaanbieder ziet er actief op toe dat in de technische infrastructuur geen ongeautoriseerde software applicaties actief zijn.
Categorie B: Veilige configuratie van netwerken	
1. Het structureel opdelen van de technische netwerkinfrastructuur in fysiek of logisch afgescheiden zones waarvan de buitengrenzen actief worden beschermd.	a. De technische infrastructuur is aan de hand van door de netwerkaanbieder vastgestelde criteria, classificaties of vertrouwensniveaus in fysiek of logisch afgescheiden segmenten opgedeeld. b. De netwerkaanbieder onderhoudt een actueel overzicht van alle technische koppelingen met betrekking tot netwerksegmenten onderling en met betrekking tot externe technische netwerken. c. De netwerkaanbieder hanteert een eenduidig beleid ten aanzien van verkeersstromen die op de grens met externe technische infrastructuren zijn toegestaan. d. Het onder c bedoelde beleid en de uitvoering ervan worden periodiek op juistheid en volledigheid geëvalueerd en geactualiseerd.

Beheersmaatregel	Implementatievereisten
2. Het uitsluitend verlenen van toegang tot apparatuur en software van de netwerkaanbieder aan derde partijen die uitbestede beheertaken verrichten via een afgeschermde virtual desktop omgeving.	a. Alle beheertoegang door personeel van derde partijen verloopt via een specifiek voor dat doel ingerichte virtual desktop omgeving. b. Toegang tot de virtual desktop omgeving wordt uitsluitend verleend vanaf werkstations die conform security richtlijnen van de netwerkaanbieder zijn geconfigureerd en die configuratie voorafgaand technisch is geverifieerd. c. Toegang tot de virtual desktop omgeving vereist Multi Factor Authenticatie (MFA), niet zijnde het gebruik van SMS, waarbij de authenticatiemiddelen aan individuele medewerkers van de derde partij worden uitgereikt. d. De virtual desktop omgeving beperkt de toegang tot systemen en netwerkelementen waarop de derde partij beheerwerkzaamheden moet verrichten.
3. Het gericht beschermen met cryptografische technieken van netwerkverbindingen die voor beheerdoeleinden worden ingezet.	a. Op netwerkverbindingen waarover beheertaken worden verricht, wordt zowel de vertrouwelijkheid als de integriteit van de gegevensuitwisseling cryptografisch beschermd met een beveiligingssterkte van minimaal 112 bits. b. De cryptografische sleutels die voor de versleuteling worden ingezet, worden per sessie, per vastgestelde tijdeenheid of per vastgesteld aantal datablokken vernieuwd. c. Bij gebruik van (3)TDES worden maximaal 2^20 datablokken met dezelfde cryptografische sleutels vercijferd. d. Gebruik van (3)TDES wordt uiterlijk 31 december 2023 uitgefaseerd.
4. Het uitsluitend verrichten van bedrijfsinterne beheertaken vanaf afgescheiden beheerwerkstations met geminimaliseerde communicatievoorzieningen.	a. Bedrijfsinterne beheerwerkstations van waaraf beheerwerkzaamheden worden verricht, worden gescheiden van reguliere werkplekken. b. De netwerkaanbieder ziet er op toe dat bedrijfsinterne beheerwerkstations geen toegang hebben tot openbare communicatienetwerken en – diensten.
5. Het cryptografisch beschermen van te beschermen kritieke gegevens bij transport door technische infrastructuren.	a. Te beschermen kritieke gegevens worden bij transport met minimaal 112 bits sterkte versleuteld. b. De cryptografische sleutels die voor de versleuteling, bedoeld in onderdeel a, worden ingezet, worden per sessie, per vastgestelde tijdeenheid of per vastgesteld aantal datablokken vernieuwd. c. Gebruik van (3) TDES wordt uiterlijk 31 december 2023 uitgefaseerd en tot die tijd wordt bij dit gebruik verzekerd dat maximaal 2^20 datablokken met dezelfde sleutel worden vercijferd. d. Met uitzondering van signaleringsverkeer ziet de netwerkaanbieder erop toe dat de versleuteling, bedoeld in onderdeel a, in alle gevallen end-to-end is.
Categorie C: Bewaking van technische infrastructuur	
1. Het onderhouden van voorzieningen voor near real-time detectie van mogelijke beveiligingsincidenten die een passende risico-gedreven doorsnede van de technische infrastructuur bestrijken en de netwerkaanbieder aantoonbaar in staat stellen om de aanwezigheid van geavanceerde dreigingsactoren waar te nemen.	a. De technische infrastructuur van de netwerkaanbieder wordt actief bewaakt met security monitoring oplossingen die geautomatiseerd en in real-time melding maken van mogelijke security incidenten. b. Alarmen en waarnemingen afkomstig uit de security monitoring, bedoeld in onderdeel a, worden tijdig en vervolgens structureel geanalyseerd en opgevolgd. c. Security monitoring oplossingen zijn aantoonbaar geconfigureerd om bijvoorbeeld lateral movement technieken, data exfiltratie en misbruik van accounts met hoge toegangsrechten te detecteren. d. Configuraties van security monitoring oplossingen worden structureel getoetst op het vermogen om geavanceerde dreigingsactoren waar te nemen.
2. Het onderhouden van voorzieningen om historische manifestaties van geavanceerde dreigingen en aanvalsvectoren in de technische infrastructuur op te sporen.	a. De netwerkaanbieder onderhoudt een structurele historie van systeem- en netwerkdata met een retentietijd van minimaal drie maanden. b. De data, bedoeld in onderdeel a, omvatten in elk geval een selectie van logbestanden van systemen en netwerkelementen, DNS en netflow-gegevens en packet captures van netwerkverkeer die de netwerkaanbieder met risicoafwegingen kan onderbouwen. c. De netwerkaanbieder beschikt over analytische oplossingen waarmee de data, bedoeld in onderdeel a, met gebruik van dreigingsindicatoren kunnen worden doorzocht.

Beheersmaatregel	Implementatievereisten
3. Het actief toetsen van de technische infrastructuur op mogelijke kwetsbaarheden en het structureel opvolgen van bevindingen die daaruit voortvloeien.	a. De netwerkaanbieder verzamelt structureel rapportages over kwetsbaarheden in de hardware en software die in de technische infrastructuur worden ingezet. b. De netwerkaanbieder past een combinatie van geautomatiseerde vulnerability scans, penetratietesten en red team oefeningen toe om kwetsbaarheden in de technische infrastructuur op te sporen. c. De netwerkaanbieder hanteert een structurele en geformaliseerde proces om kwetsbaarheden die door middel van de activiteiten, bedoeld in onderdeel b, aan het licht zijn gekomen te analyseren, prioriteren en indien noodzakelijk deze op te lossen.
Categorie D: Security assurance op software en beheerdiensten	
1. Het opleggen van vergelijkbare beveiligingsverplichtingen aan beheerdienstverleners die uitbestede beheertaken verrichten in de technische infrastructuur en in de fysieke werkomgeving van de netwerkaanbieder.	a. De netwerkaanbieder komt contractueel met de beheerdienstverlener overeen dat in de technische en fysieke werkomgeving die voor dienstverlening aan de netwerkaanbieder worden ingezet beveiligingsmaatregelen worden getroffen die overeenkomen met de op dat moment geldende beveiligingsmaatregelen van de netwerkaanbieder. b. De netwerkaanbieder komt contractueel met de beheerdienstverleners overeen dat kwetsbaarheden en vermoedens van beveiligingsincidenten in de werkomgeving, bedoeld in onderdeel a, terstond worden gemeld aan het beveiligingsaanspreekpunt van de netwerkaanbieder. c. Voor zover uitbestede beheertaken geheel of gedeeltelijk buiten Nederland worden verricht, brengt de netwerkaanbieder structureel in kaart in hoeverre de door de overheid vastgestelde en richting netwerkaanbieder gecommuniceerde juridische of politieke context van het land waar vandaan de beheertaken worden verricht tot specifieke beveiligingsrisico's kan leiden en treft vervolgens passende maatregelen om deze te beheersen.
2. Het opleggen van de contractuele verplichting aan toeleveranciers dat bij de ontwikkeling en levering van software oplossingen gangbare beveiligingspractices worden toegepast.	De netwerkaanbieder komt contractueel met de softwareleveranciers overeen dat: a. een Secure Software Development Life-Cycle (SSDLC) wordt toegepast die aantoonbaar conformeert aan een erkende standaard of richtlijn; b. software, inclusief generieke componenten, op het moment van ingebruikname volledig is gepatcht, voldoet aan door de netwerkaanbieder vastgestelde hardening vereisten en is opgewaardeerd naar versies waar nog actief support op wordt verleend; c. terstond melding wordt gemaakt van kwetsbaarheden in de geleverde software en dat wordt voorzien, conform vastgestelde oplostijden en al naar gelang de ernst van de kwetsbaarheid, in updates of patches om die kwetsbaarheden te verhelpen.
3. Het uitsluitend in productie nemen van software die met succes een onafhankelijke beveiligingsevaluatie of penetratietest heeft ondergaan.	a. Op softwareproducten wordt voorafgaand aan uitrol een passende technische beveiligingsevaluatie of penetratietest verricht, door de netwerkaanbieder of door een onafhankelijke derde partij. b. De netwerkaanbieder legt de verplichting op aan de softwareleveranciers dat wordt aangetoond dat productiesoftware die in de infrastructuur van de netwerkaanbieder wordt uitgerold overeenkomstig is aan de geëvalueerde software, bedoeld in onderdeel a. c. De netwerkaanbieder stuurt actief op opvolging van bevindingen uit de beveiligingsevaluatie, bedoeld in onderdeel a, en neemt het software product in gebruik op voorwaarde dat eventuele bevindingen, die naar hun aard dusdanig ernstig en/of urgent zijn, dienen te worden opgelost.
4. Het structureel beoordelen van beheerdienstverleners en softwareleveranciers op naleving van contractuele beveiligingsafspraken.	a. De netwerkaanbieder toetst structureel en met passende instrumenten de naleving van contractuele beveiligingsafspraken. b. Indien er tekortkomingen worden geconstateerd, komt de netwerkaanbieder met de desbetreffende beheerdienstverlener of softwareleverancier een verbeterplan met tijdlijnen overeen.
Categorie E: Human resource security	
1. Het gericht uitvoeren van een programma om het beveiligingsbewustzijn van bedrijfsintern beheerpersoneel te verhogen.	a. De netwerkaanbieder voert voor beheerpersoneel een gericht bewustzijnsprogramma uit met betrekking tot spear-phishing. b. De netwerkaanbieder verricht periodiek onaangekondigde spear-phishing campagnes om te toetsen of het personeel die campagnes herkent en conform interne beleidsregels reageert.
2. Het structureel screenen van personeel van derde partijen die uitbestede beheertaken verrichten alvorens hen toegang wordt verleend tot apparatuur en software van de netwerkaanbieder.	Personeel van een derde partij dat uitbestede beheertaken verricht: a. is op persoonsgegevensniveau bij de netwerkaanbieder bekend en geadministreerd; b. heeft voorafgaand aan het verkrijgen van toegang aantoonbaar een passend en schriftelijk bekrachtigde achtergrondonderzoek ondergaan.

TOELICHTING

I. Algemeen

1. Inleiding

Deze regeling bevat aanvullende beveiligingsmaatregelen voor aanbieders van mobiele communicatienetwerken, zoals aangekondigd in het Besluit veiligheid en integriteit telecommunicatie[1], om de weerbaarheid van hun huidige netwerken te verhogen in het licht van actuele dreigingen.

De interdepartementale Tasforce Economische Veiligheid[2] (hierna: Taskforce) heeft onderzocht of de huidige beveiligingsmaatregelen die de aanbieders van mobiele netwerken op grond van de in artikel 11a.1 van de Telecommunicatiewet (hierna: Tw) opgenomen zorgplicht nemen, voldoende zijn, gelet op het actuele dreigingsbeeld. Aanleiding hiervoor waren de waarschuwingen van de inlichtingen- en veiligheidsdiensten voor infiltratie van statelijke actoren ten behoeve van spionage in de telecomsector. De Taskforce heeft geconcludeerd dat aanvullende maatregelen nodig zijn, zowel ten aanzien van beveiligingsmaatregelen als ten aanzien van de door netwerkaanbieders gebruikte producten en diensten.

De Taskforce heeft in 2019 met medewerking van de netwerkaanbieders van mobiele telecommunicatienetwerken door de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (hierna: TNO) een risicoanalyse laten uitvoeren naar de kwetsbaarheid van hun netwerken voor misbruik van producten en diensten (apparatuur, programmatuur, beheer en aanverwante dienstverlening). Hierbij is in kaart gebracht welke maatregelen de netwerkaanbieders reeds treffen om de beveiliging van hun netwerk te verhogen in het licht van de huidige dreiging en is onderzocht welke aanvullende maatregelen nodig zijn om de weerbaarheid van het huidige netwerk te verhogen in het licht van dit dreigingsbeeld. Om tot de juiste maatregelen te komen heeft de Taskforce eveneens gekeken welke gegevens vanuit nationale veiligheid dienen te worden beschermd, de zogeheten kritieke gegevens.

Bij kamerbrief van 1 juli 2019[3] heeft de regering aangekondigd dat mobiele netwerkaanbieders zullen worden verplicht om die aanvullende beveiligingsmaatregelen te nemen om weerbaarheid tegen de hierboven genoemde dreiging te verhogen.

Het Besluit veiligheid en integriteit telecommunicatie (hierna: besluit) vormt de basis voor de maatregelen die ter uitwerking van de rapportage van de Taskforce dienen te worden genomen. In dit besluit is in artikel 2, eerste lid, een grondslag opgenomen om bij ministeriële regeling nadere regels te kunnen stellen met betrekking tot de artikel 11a.1 van de Tw bedoelde technische en organisatorische maatregelen en het stellen van technische en organisatorische eisen aan aanbieders van openbare elektronische communicatienetwerken en/of openbare elektronische communicatiediensten.

Deze regeling bevat de door TNO opgestelde aanvullende organisatorische en technische maatregelen die aanbieders van mobiele telecommunicatienetwerken dienen te treffen ter beveiliging van hun netwerk (hierna: beheersmaatregelen).

De in de regeling opgenomen beheersmaatregelen zijn in lijn met de technische maatregelen die in de Europese toolbox[4] zijn genoemd. De toolbox is het gemeenschappelijk instrumentarium van mitigerende beveiligingsmaatregelen die lidstaten kunnen nemen om de veiligheidsrisico's bij 5G te beheersen en is 29 januari 2020 door de Europese Commissie gepubliceerd. Zonder hierbij uitputtend te zijn, worden in de toolbox ook beveiligingsmaatregelen genoemd, zoals configuratie van apparatuur, strikte toegangsregels (inclusief toegangsrechten van derde partijen), het versterken van de integriteit van software en patch management, die eveneens in deze regeling als beheersmaatregelen zijn opgenomen.

2. Reikwijdte van de regeling

Onderhavige regeling beperkt zich tot mobiele netwerkaanbieders. Andere telecomaanbieders die

---

1 Staatsblad 457, jaargang 2019; Besluit van 28 november 2019, houdende nadere regels betreffende de veiligheid en integriteit van openbare elektronische communicatienetwerken en -diensten.
2 De Taskforce Economische Veiligheid (TFEV) is 21 februari 2019 opgericht onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).
3 Kamerstukken II, 2018–19, 30 821, nr. 92.
4 Kamerstukken II, 2019–20, 24 095, nr. 495.

bijvoorbeeld van deze netwerken gebruik maken, maar niet in beheer hebben, vallen buiten de reikwijdte van de regeling.

De beheersmaatregelen hebben betrekking op de kritieke onderdelen van de mobiele netwerken en de daarmee aanpalende onderdelen (artikel 2, eerste lid). Hierbij gaat het om systemen en netwerkelementen die door de overheid als 'kritieke onderdelen' zijn aangemerkt. De kritieke onderdelen zijn door de overheid gerubriceerd als 'Departementaal vertrouwelijk'[5]. De lijst met kritieke onderdelen is in december 2020 met de desbetreffende netwerkaanbieders op vertrouwelijke wijze gedeeld. Met de 'aanpalende onderdelen' worden alle systemen en netwerkelementen bedoeld die zich op eenzelfde netwerksegment bevinden als een kritieke onderdeel.

De beheersmaatregelen die betrekking hebben op real-time detectie en historische opsporing van mogelijke beveiligingsincidenten (eerste kolom, onder categorie C, nummers 1 en 2, van de bijlage) en de beheersmaatregel die betrekking heeft op het cryptografisch beschermen (versleutelen) van kritieke gegevens bij transport door technische infrastructuren (eerste kolom, onder categorie B, nummer 5, van de bijlage) kennen een afwijkende reikwijdte (artikel 2, tweede en derde lid).

Het gaat bij detectie en opsporing (eerste kolom, categorie C, nummers 1 en 2) om een doorsnede van de technische infrastructuur die met risicoafwegingen kan worden onderbouwd en die in elk geval de mobile core en alle beheertoegang (zowel door intern personeel als door derde partijen) tot de kritieke onderdelen, aanpalende onderdelen en de beveiligingselementen omvatten. Het bepalen van de reikwijdte van deze beheersmaatregel is dus in eerste instantie aan de netwerkaanbieder met dien verstande dat de netwerkaanbieder de reikwijdte moet kunnen onderbouwen op basis van een uitgevoerde risicoafweging.

Voor de reikwijdte van de beheersmaatregel voor het versleutelen van gegevens (eerste kolom, categorie B, nummer 5) is het transport van te beschermen kritieke gegevens bepalend (gegevens die vanuit nationale veiligheid moeten worden beschermd). Dit kan betekenen dat het transport plaatsvindt via niet-kritieke netwerkonderdelen van de netwerkaanbieder, omdat kritieke gegevens ook over niet-kritieke onderdelen getransporteerd kunnen worden. Om dezelfde reden als de rubricering van de kritieke onderdelen zijn ook de te beschermen kritieke gegevens gerubriceerd als Departementaal Vertrouwelijk. Tegelijk met de publicatie van deze regeling zal de lijst met de kritieke gegevens op vertrouwelijke wijze worden gedeeld met de desbetreffende netwerkaanbieders.

3. De beheersmaatregelen

De beheersmaatregelen zijn te verdelen in een vijftal veiligheidsdomeinen.

A. Veilige configuratie van technische apparatuur: het doel van deze beheersmaatregelen is om te waarborgen dat bij de netwerkaanbieder bekend is welke informatieverwerkende assets direct of indirect van invloed kunnen zijn op de vertrouwelijkheid van de te beschermen kritieke gegevens en deze assets te beschermen tegen ongeautoriseerde toegang en andere (geavanceerde) vormen van digitaal misbruik.
B. Veilige configuratie van netwerkinfrastructuur: het doel van deze beheersmaatregelen is om de vertrouwelijkheid van te beschermen kritieke gegevens en de bescherming van te beschermen verwerkende faciliteiten in de netwerken van aanbieders te waarborgen.
C. Bewaking van technische infrastructuur (monitoring): het doel van deze beheersmaatregelen is te waarborgen dat kwetsbaarheden en incidenten die impact kunnen hebben op de van overheidswege vastgestelde te beschermen belangen tijdig worden herkend en opgelost.
D. Security assurance op software en beheerdiensten: het doel van deze beheersmaatregelen is om passende waarborgen te verkrijgen ten aanzien van de beveiliging van producten en diensten van derde partijen die direct of indirect van invloed kunnen zijn op de van overheidswege vastgestelde te beschermen belangen.
E. Human resource security: het doel van deze beheersmaatregelen is te waarborgen dat zowel intern als extern beheerpersoneel bekend is bij de netwerkaanbieder en uit oogpunt van veiligheid en betrouwbaarheid geschikt is voor het verrichten van (gevoelige en/of kritieke) beheerwerkzaamheden.

4. Ontheffingsmogelijkheid

De netwerkaanbieders zijn nauw betrokken geweest bij zowel de risicoanalyse van de Taskforce als de totstandkoming van de beheersmaatregelen, dus de beheersmaatregelen sluiten in beginsel aan op de huidige praktijk van de netwerkaanbieders. De regeling biedt desalniettemin aan netwerkaanbieders de mogelijkheid om ten aanzien van de beheersmaatregelen een ontheffing van de Minister van

[5] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013), artikel 4.

Economische Zaken en Klimaat (hierna: de Minister) te verkrijgen voor één of meerdere implementatievereiste(n) (behorende bij een beheersmaatregel) (artikel 3, tweede lid). Met de regeling wordt immers de zorgplicht – zoals die in de artikel 11.a., van de Tw is opgenomen – op een gedetailleerder niveau ingevuld dan sinds de introductie van de zorgplicht in 2012 is gedaan. Hoewel de regeling ruimte biedt aan aanbieders om hun eigen uitvoeringswijze te kiezen, kan een dergelijke mate van gedetailleerdheid in de weg staan aan voornamelijk het meegaan met de snelle technologische ontwikkelingen in de mobiele telecommunicatiesector. De nodige flexibiliteit in het stelsel, in de vorm van de mogelijkheid om via een ontheffing van bepaalde implementatievereisten van een beheersmaatregel op een alternatieve wijze aan de desbetreffende beheersmaatregel te voldoen, wordt daarom wenselijk geacht. Het blijft, gelet op de zorgplicht van artikel 11a.1, van de Tw en de dreigingen voor de nationale veiligheid, van belang dat ook bij een alternatieve uitvoeringswijze de continuïteit, integriteit en veiligheid van het netwerk en de dienstverlening zo goed mogelijk worden gewaarborgd. Een ontheffingsaanvraag wordt om die reden slechts verleend als met een door de netwerkaanbieder voorgestelde alternatieve uitvoeringswijze minimaal een vergelijkbaar beveiligingsniveau als het beveiligingsniveau van de beoogde beheersmaatregel wordt behaald. Aan de ontheffing zal in ieder geval het voorschrift worden verbonden dat de beheersmaatregel conform de voorgestelde alternatieve wijze wordt uitgevoerd. Daarnaast kunnen er ook andere voorschriften of beperkingen aan de ontheffing worden verbonden (artikel 3, vierde lid).

5. Noodzakelijkheid, proportionaliteit, en geschiktheid

De beheersmaatregelen die in deze regeling zijn opgenomen worden noodzakelijk, proportioneel, en geschikt geacht. Met betrekking tot de noodzaak kan worden geconcludeerd, zoals reeds opgemerkt in paragraaf 1, dat uit de risicoanalyse van de Taskforce is gebleken dat de beheersmaatregelen, zoals opgenomen in deze regeling, in aanvulling op de huidige beveiligingsmaatregelen, van de netwerkaanbieders nodig zijn om de weerbaarheid van de huidige netwerken te verhogen in het licht van de actuele dreiging van spionage door statelijke actoren. Bij de uitwerking van de concrete maatregelen is telkens beoordeeld of de maatregelen een afdoende antwoord zouden kunnen zijn op de geïnventariseerde risico's, waarbij, mede door betrokkenheid van de netwerkaanbieders, tegelijkertijd is gekeken in hoeverre de maatregelen aansluiten bij de huidige praktijk van de netwerkaanbieders en in hoeverre deze ook in de praktijk zouden kunnen worden uitgevoerd door de aanbieders. Daarmee worden de beheersmaatregelen als proportioneel geacht in het licht van de actuele dreiging en gaan de maatregelen niet verder dan nodig is om het gestelde doel te bereiken.

6. Implementatietermijn en evaluatie

Er is voor gekozen om de regeling direct na publicatie in werking te laten treden. De beheersmaatregelen moeten echter uiterlijk op 1 oktober 2022 door de aanbieders zijn geïmplementeerd. Door de regeling direct na publicatie in werking te laten treden, is Agentschap Telecom (hierna: AT) (de toezichthouder) bevoegd om de implementatie door de netwerkaanbieders te monitoren. Hoewel de netwerkaanbieders betrokken zijn geweest bij de totstandkoming van deze regeling kan de toezichthouder daar waar nodig in dialoog met de netwerkaanbieders treden over de juiste interpretatie van de gestelde implementatievereisten. De toezichthouder is daarentegen tijdens de implementatiefase niet bevoegd om (tussentijds) overtredingen van deze regeling te constateren en te handhaven. Dit laat onverlet dat als de toezichthouder een andere overtreding constateert van hoofdstuk 11a van de Tw hij uiteraard wel handhavend kan optreden. Bij het vaststellen van de implementatietermijn is gestreefd naar het vinden van een balans tussen enerzijds het spoedig mitigeren van de risico's zoals die in de door TNO uitgevoerde risicoanalyse zijn geïdentificeerd en anderzijds rekenschap geven aan het feit dat dit een stevig pakket aan maatregelen is die veel inspanningen van de aanbieders zal vergen om de vereiste aanpassingen in de bedrijfsvoering (inclusief relevante systemen) door te voeren.

Ik ben me ervan bewust dat de situatie kan ontstaan dat de in de regeling opgenomen maatregelen niet langer toereikend zijn om risico's voor de nationale veiligheid, die aan veranderingen onderhevig zijn, in de toekomst blijvend en tot een aanvaardbaar niveau te reduceren. Daarom wordt in samenwerking tussen aanbieders en overheid een structurele aanpak ingericht om ontwikkelingen in dreiging en techniek in samenhang te bezien. Als zodanig is er een continue mogelijkheid om de maatregelen in samenspraak met de mobiele aanbieders te evalueren en zo nodig de regeling hierop aan te passen. Afgezien van de evaluatie van de regeling in het licht van de actuele dreiging wordt de werking van de regeling twee jaar na inwerkingtreding geëvalueerd. Bij deze evaluatie zal in ieder geval worden gekeken naar de effectiviteit en doeltreffendheid van de systematiek van de regeling.

7. Reacties uit de consultatie

Er zijn reacties ingewonnen door middel van een openbare consultatie op www.internetconsultatie.nl.

Tijdens de consultatie zijn negen reacties ingediend: vijf openbaar (T-Mobile, Internet Society, Huawei, Nokia, I River) en vier niet-openbaar.

Systematiek en evaluatietermijn

Meerdere partijen zijn ingegaan op de onderliggende systematiek van de regeling. Enerzijds is door bepaalde partijen aangegeven dat de regeling een statische en gedetailleerd ingevulde 'rules based approach' zou betreffen, in plaats van een gewenste 'principle based approach', bij voorkeur stoelend op een internationaal erkende, brede en open norm, die meer ruimte biedt aan de aanbieders om zelfstandig invulling te geven aan de implementatievereisten. Anderzijds heeft een partij aangegeven dat ze de beheersmaatregelen juist te generiek vindt om effectief te zijn, vanwege het gebruik van bewoordingen zoals 'minimaliseren', 'zo snel mogelijk', of 'actief toezien'. Hierdoor is niet vast te stellen wanneer is voldaan aan de beheersmaatregelen.
Ik kies in dit geval bewust voor de huidige systematiek. Zoals in de paragrafen 1 en 6 van de toelichting is aangegeven, worden de in deze regeling opgenomen aanvullende maatregelen noodzakelijk geacht vanwege geconstateerde dreigingen ten aanzien van de nationale veiligheid. De overheid heeft een lijst met kritieke gegevens vastgesteld in de nationale telecominfrastructuur, welke afzonderlijk wordt gedeeld met de netwerkaanbieders. Op basis van de resultaten van de door de TFEV uitgevoerde risicoanalyse is er voor gekozen niet één algemene erkende standaard te hanteren die door de individuele aanbieders zou kunnen worden geïnterpreteerd en waar ze zelf invulling aan zouden kunnen geven. Aanbieders hanteren immers hun eigen, verschillende, interne normen en daarmee samengaande security policies. Ook corresponderen de in de regeling opgenomen maatregelen wel degelijk met internationale normen, zoals de ISO27002:2013 en NIST SP 800-53. Daar komt bij dat deze internationale standaarden referentiekaders zijn en daarbij veel ruimte voor interpretatie bieden, met mogelijk verschillende beveiligingsniveaus tot gevolg. Met het pakket aan specifieke beheersmaatregelen is daarom gestreefd naar meer duidelijkheid door het specifieker vastleggen van een bepaald beveiligingsniveau.
Wel kies ik ervoor, mede gelet op het verzoek van meerdere partijen om de regeling 2 jaar na inwerkingtreding te evalueren op in ieder geval de doeltreffendheid en effectiviteit van de gekozen systematiek.

Ontheffingsmogelijkheid

Met betrekking tot artikel 3, derde lid, onderdeel a (zoals geconsulteerd), van de regeling, hebben partijen opgemerkt dat het op zich 'technisch' altijd mogelijk is om aan implementatievereisten te voldoen. Hierdoor zou er in de praktijk geen goed gebruik kunnen worden gemaakt van de ontheffingsmogelijkheid. Partijen geven aan dat een ontheffing mogelijk moet zijn wanneer een implementatievereiste eerder als disproportioneel dan wel onvoldoende effectief of efficiënt wordt beschouwd, waarbij een alternatieve implementatie voorhanden is die het vereiste beveiligingsniveau van de beheersmaatregel borgt. Hierbij wordt dus gevraagd naar een oplossing die meer ruimte zou moeten bieden om aan de netwerkaanbieder een ontheffing te kunnen verlenen. Gelet op deze opmerking heb ik artikel 3, derde lid, onderdeel a (zoals geconsulteerd), van de regeling, laten vervallen.

Met betrekking tot artikel 3, derde lid, onderdeel b (zoals geconsulteerd), van de regeling, hebben meerdere partijen opgemerkt dat niet van belang is of de desbetreffende beheersmaatregel op een gelijkwaardige manier wordt uitgevoerd, maar dat relevant is of een voldoende niveau van beveiliging kan worden bereikt binnen de doelstelling van de maatregel. Gelet op deze opmerking heb ik de formulering van dit onderdeel aangepast. Gegeven de doelstelling van de regeling is het logisch dat een vergelijkbaar beveiligingsniveau als voorwaarde aan de verlening van een ontheffing wordt verbonden. Nu artikel 3, derde lid, onderdeel a (zoals geconsulteerd), van de regeling, is komen te vervallen en het eerste en tweede lid (zoals geconsulteerd) zijn samengevoegd tot het eerste lid, is de hiervoor bedoelde formulering opgenomen in artikel 3, tweede lid, van de regeling.

Reikwijdte regeling

Meerdere partijen vragen zich af of de in maatregelen overeenkomstig van toepassing zijn op het niet-mobiele netwerk. Dit is niet het geval. De maatregelen gelden alleen voor de mobiele netwerken en systemen. Een partij vraagt of de regeling ook van toepassing is op installaties op zee. Dit is het niet geval. De regeling is van toepassing op aanbieders van een openbaar mobiel elektronisch communicatienetwerk die beschikken over vergunningen voor het gebruik van geharmoniseerd radiospectrum als bedoeld in artikel 2, onder 25, van Richtlijn (EU) 2018/1972, die zijn verleend met toepassing van een veiling, bedoeld in artikel 3.10, eerste lid, aanhef en onderdeel f, van de Tw. Vergunningen voor installaties op zee zijn echter verleend met een procedure zoals bedoeld in artikel 3.10, eerste lid, aanhef en onderdeel b, van de Tw.

Implementatietermijn

Ten aanzien van de implementatietermijn hebben verschillende partijen, aangegeven dat een langere implementatietermijn nodig dan wel wenselijk is. Hoewel meerdere aanbieders een deel van de beheersmaatregelen reeds heeft uitgevoerd, is de termijn tot aan 1 oktober 2022 te kort is om aan alle beheersmaatregelen te voldoen. Men vraagt hierbij om een langere implementatietermijn in acht te nemen, namelijk 2 jaar. Er wordt hierbij ook aangegeven dat er nog geen zicht is in de wijze waarop AT toezicht zal houden. Gegeven het belang voor de nationale veiligheid van een snelle implementatie van de in deze regeling opgenomen beheersmaatregelen wordt de implementatietermijn niet uitgesteld. Daarbij weeg ik ook mee dat de aanbieders al vanaf mei 2020[6] bekend zijn met de komst van deze beheersmaatregelen en bijbehorende implementatievereisten, waardoor zij (reeds) de benodigde voorbereidingen hebben kunnen treffen. Met betrekking tot de opmerking die is gemaakt over het toezicht verwijs ik naar paragraaf 6 van de toelichting en daarnaast zal ook hieronder nader worden ingegaan op dit onderwerp.

Toezicht

Meerdere partijen geven aan dat de wijze waarop AT toezicht zal houden ook effect kan hebben op de implementatie(wijze). Er wordt ook gevraagd naar het toetsingskader van AT. Een toetsingskader definieert welke aspecten van de regeling worden gemonitord en welke verwachtingen aan de aanbieders worden gesteld. Uitgangspunt is dat aan alle beheersmaatregelen, via de bijbehorende implementatievereisten, wordt voldaan, rekening houdend met eventueel aangevraagde en verleende ontheffingen.

Vergoeding van de kosten/compensatie

Meerdere partijen hebben verzocht om vergoeding van kosten die zij moeten maken voor het uitvoeren van de regeling. Uitgangspunt in het nadeelcompensatierecht is dat eenieder die nadeel lijdt als gevolg van de rechtmatige uitvoering van een publiekrechtelijke taak of bevoegdheid, waaronder het stellen van algemeen verbindende voorschriften, dat nadeel in beginsel zelf dient te dragen. Nadeelcompensatie is aan de orde als sprake zou zijn van schade die uitgaat boven het normale maatschappelijke risico en die een benadeelde in vergelijking met anderen onevenredig zwaar treft. Bij de uitvoering van deze regeling wordt niet aan genoemde criteria voldaan. Ik zie dan ook geen aanleiding om over te gaan tot compensatie.

Sancties

Een partij vraagt ook naar de maximale sancties die kunnen worden opgelegd. Ik verwijs hiervoor naar artikel 15.4 van de Tw.

Vertrouwelijkheid kritieke onderdelen

Meerdere partijen geven aan dat zij niet weten op welke netwerkonderdelen de regeling van toepassing is vanwege de vertrouwelijkheid van de zogenoemde kritieke onderdelen. Er wordt om deze informatie gevraagd, zodat het mogelijk wordt om met de overheid discussie te voeren over de beheersmaatregelen. Vanwege de gerubriceerde status van deze informatie kan ik echter niet aan dit verzoek tegemoet komen.

Reacties op specifieke implementatievereisten

Software assurance

Meerdere partijen gaan in op beheersmaatregelen over de security assurance op software en beheersdiensten, zoals genoemd in categorie D van de bijlage. Er wordt aangegeven dat aansluiting moet worden gezocht bij het certificeringsproces zoals die in het concept- Uitvoeringswet cyberbeveiligingsverordening is opgenomen. Partijen geven aan dat het niet gewenst is dat er product- en software assessments moeten plaatsvinden voor ieder product, operator en land en dat er geen verplichte pentesten moeten plaatsvinden. Er wordt voorgesteld dat de assessments ook internationaal, bijvoorbeeld op EU-niveau, zouden kunnen worden uitgevoerd. Meerdere partijen verwijzen hierbij naar de NESAS certificering (Network Equipment Security Assurance Scheme) zoals die door

[6] Op 27 mei 2020 is het TNO-eindrapport waarin de maatregelen staan zoals die in de bijlage zijn opgenomen gedeeld met de aanbieders.

de 3GPP[7] en de GSMA[8] worden ontwikkeld, waarbij compliance ook wordt bepaald door onafhankelijke derde partijen. Er wordt door een partij voorgesteld om aan te sluiten bij de huidige praktijk, waarbij software op een continue manier wordt ontwikkeld, getest en geïntegreerd.

Ten aanzien van de ingebruikname van software is in maatregel in de tweede kolom van de bijlage, categorie D, nummer 3, onderdeel a, opgenomen dat software producten voorafgaand aan uitrol een passende (technische) security evaluatie of penetratietest wordt verricht, hetzij door de organisatie zelf of door een van de leverancier onafhankelijke derde partij. Deze maatregel kan voor mobiele netwerkapparatuur worden ingevuld middels onafhankelijke certificering tegen bijvoorbeeld het door de partijen genoemde NESAS Schema dat door de GSMA en 3GPP is gelanceerd.

Ten aanzien van de maatregel tweede kolom, categorie D, nummer 3, onderdeel c, van de bijlage, over het oplossen van bevindingen die uit de beveiligingsevaluatie van software naar voren is gekomen, geeft een partij aan dat het oplossen van alle bevindingen niet altijd nodig zal zijn. In de praktijk zullen niet alle bevindingen zeer ernstig zijn of om een dusdanig urgent karakter hebben dat direct om een oplossing vraagt en kan het moeten oplossen van alle bevindingen tot vertraging van de ingebruikname van software leiden. De partij vraagt aan de wetgever om hier rekening mee te houden. Hierop is maatregel D3, onderdeel c, aangepast door de mogelijkheid te creëren dat ernst en/of urgentie kunnen worden meegewogen bij het al dan niet oplossen van de bevindingen.

Real time detectie

Meerdere partijen hebben ten aanzien van de maatregel eerste kolom, categorie C, nummer 1, van de bijlage, over detectie van mogelijke beveiligingsincidenten aangegeven dat de ‘real time’ detectie niet altijd haalbaar of reëel is en een onnodige verzwaring is van het vereiste. Naar aanleiding van de suggestie van meerdere partijen is ‘real time’ vervangen door ‘near real time’.

Patchmanagement

Een partij vraagt ten aanzien van beheersmaatregel tweede kolom, categorie C, nummer 2c, van de bijlage, ten aanzien van het zo snel mogelijk verifiëren en uitrollen security patches voor software wat er wordt bedoeld met ‘zo snel mogelijk’. Deze partij schrijft in haar reactie terecht dat patches doorgaans een hoge graad van urgentie hebben en worden in de praktijk vaak al zo snel mogelijk worden uitgerold. In de regeling zal niet worden verabsoluteerd wat met ‘zo snel mogelijk’ wordt bedoeld. Het uitgangspunt is ‘zo snel mogelijk’, maar dat dient wel op een verantwoorde manier te geschieden. Het kan bijvoorbeeld nodig zijn om eerst te testen of de continuïteit van de dienstverlening niet in gevaar komt. Het is noodzakelijk om aan de netwerkaanbieders ruimte te bieden om hierin de juiste afwegingen te maken.

8. Uitvoerings- en handhaafbaarheidstoets

De uitvoerbaarheid en handhaafbaarheid zijn getoetst door AT. Onderhavige regeling is als uitvoerbaar en handhaafbaar beoordeeld, mits een oplossing wordt gevonden voor het onderstaande.
AT merkt op dat de regeling geen voorzieningen lijkt te hebben getroffen voor (potentiële) nieuwe vergunninghouders waarvoor de regeling ook zou moeten gelden. Daarbij wijst het agentschap specifiek op de vertrouwelijkheid van de kritieke netwerkonderdelen en de kritieke gegevens alsmede op de implementatietermijn die ook op nieuwe netwerkaanbieders van toepassing lijkt te zijn. Hierover merk ik het volgende op. Zodra een aanbieder voldoet aan de definitie van netwerkaanbieder zoals bedoeld in artikel 1 van de regeling, is de regeling op deze aanbieder van toepassing. Als gevolg hiervan zal een potentiële nieuwe vergunninghouder tijdig worden geïnformeerd over de kritieke onderdelen en kritieke gegevens. Dit betekent dat een potentiële nieuwkomer tijdig moet worden geïnformeerd over de kritieke onderdelen en de kritieke gegevens. Op dit moment kan de situatie voor potentiële nieuwe vergunninghouders nog niet volledig worden overzien, bijvoorbeeld ten aanzien van de uitrol en ingebruikname van het netwerk. Mocht daar meer zicht op zijn, dan zal worden bezien hoe hiermee in het licht van deze regeling moet worden omgegaan.

9. Toets inzake bedrijfseffecten en administratieve lasten

Deze regeling brengt inhoudelijke nalevingskosten voor de netwerkaanbieders met zich. De netwerkaanbieders hebben een zorgplicht op grond van artikel 11.a van de Tw, dus zij hebben al de nodige beveiligingsmaatregelen getroffen, zijnde een combinatie van organisatorische en technische

[7] 3rd Generation Partnership Project (3GPP) waarin meerdere telecommunicatie- standaardaardisatie organisaties zijn verenigd (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
[8] Mondiale belangenorganisatie van de mobiele telecomsector.

maatregelen. Voor de continuïteit van hun eigen bedrijfsvoering is het cruciaal dat beveiligingsmaatregelen worden getroffen, want zonder afdoende maatregelen is men zeer kwetsbaar voor tal van dreigingen, zoals cybercrime, stroomstoringen en menselijke fouten. De netwerkaanbieders hebben dus al veel investeringen gedaan ter beveiliging van hun systemen om zodoende incidenten en – als gevolg daarvan – mogelijk grote schadeposten zo veel mogelijk te voorkomen. Deze regeling betekent een nadere invulling en aanscherping van die zorgplicht. Dat betekent dat de netwerkaanbieders extra beheersmaatregelen zullen treffen, maar dat per netwerkaanbieder wel kan verschillen wat er nog moet worden gedaan om aan de gestelde eisen te kunnen voldoen, want het is ook afhankelijk van wat de reeds gedane investeringen. Met het oog op de berekening van de regeldruk is aan de netwerkaanbieders gevraagd een inschatting te maken van de regeldruk (de aanvullende kosten die deze regeling met zich gaat brengen) en om deze kosten uit te splitsen in eenmalige kosten en structurele kosten (jaarlijks terugkerende kosten). Het gaat hierbij om investeringen om processen en systemen aan te passen, maar ook uiteenlopende kosten zoals personeelskosten, toezichtskosten (kosten die gemoeid zijn met de interactie met de toezichthouder) en jaarlijkse onderhoudskosten etc. De netwerkaanbieders hebben een inschatting gemaakt van de regeldruk: tezamen bedragen de eenmalige investeringen ca 17 à 21 mln, de structurele jaarlijkse kosten bedragen ca 8 à 10 mln. De netwerkaanbieders hebben in hun reactie aangegeven dat er de nodige onzekerheden zijn in de berekeningen. Een netwerkaanbieder geeft aan dat de regeldruk ook voor een belangrijk deel afhangt van de uiteindelijke implementatietermijn. Een kortere implementatietermijn brengt bijvoorbeeld hogere personeelskosten met zich, omdat mogelijk extra personeel moet worden ingehuurd of er moet versneld worden afgeschreven op bepaalde systemen. Dit kan uiteindelijk nog extra regeldruk met zich brengen. Ook geven sommige netwerkaanbieders aan dat sommige nog te treffen beheersmaatregelen en de daaruit voortvloeiende kosten op een bredere domein van hun netwerk en/of diensten betrekking zal hebben dan in artikel 2 van de regeling is aangegeven, omdat die onderdelen onlosmakelijk met elkaar zijn verbonden, wat betekent dat die kostenposten op dat bredere domein zien.

10. Notificatie

Ter voldoening aan richtlijn 2015/1535 (notificatierichtlijn) zijn de beheersmaatregelen, als nationale technische eisen, genotificeerd bij de Europese Commissie. De Europese Commissie heeft in haar reactie[9] Nederland erop gewezen dat 'het belangrijk is om de EU-toolbox[10] volledig te blijven toepassen als een gecoördineerde EU-aanpak om versnippering van de reacties en uiteenlopende interpretaties van de risicobeoordeling tussen de lidstaten te voorkomen. Het is van groot belang dat de lidstaten zorgen voor een snelle tenuitvoerlegging van doeltreffende en passende risicobeperkende maatregelen in overeenstemming met de EU-toolbox.'
Overeenkomstig artikel 5, lid 3 van Richtlijn (EU) 2015/1535 zal de vastgestelde regeling aan de Commissie worden meegedeeld.

11. Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt gepubliceerd. Hiermee wordt afgeweken van de vaste verandermomenten, zoals opgenomen in het kabinetsbeleid inzake vaste verandermomenten (Kamerstukken II 2009/10, 29 515, nr. 309). Het kabinetsbeleid biedt de mogelijkheid af te wijken van vaste verandermomenten indien nodig voor nood- en spoedregelgeving. In het licht van het actuele dreigingsbeeld dient deze regeling zo spoedig mogelijk in werking te treden.

II Artikelen

Artikel 1

In dit artikel is een aantal begrippen gedefinieerd. Eén begripsbepaling wordt hier nader toegelicht.

Netwerkaanbieder

Het gaat hierbij om mobiele netwerkaanbieders, die beschikken over een vergunning voor het gebruik van geharmoniseerd radiospectrum. Vorig jaar heeft er een veiling van frequenties voor mobiele communicatie (de multibandveiling 2020) plaatsgevonden. Aan de veiling hebben de drie huidige marktpartijen (KPN, T-Mobile NL en VodafoneZiggo) deelgenomen en frequenties verworven. Mochten bij toekomstige veilingen ook andere aanbieders een vergunning zoals hier is bedoeld weten te

[9] Mededeling van de Commissie – TRIS/(2021) 03 219, 13 september 2021.
[10] Kamerstukken II, 2019–20, 24 095, nr. 495.

verwerven, dan zullen zij ook aan de gestelde eisen van de regeling moeten voldoen. Zie hierover ook paragraaf 8 over de uitvoerings- en handhaafbaarheidstoets.

Artikel 2

In dit artikel wordt bepaald op welke onderdelen van het netwerk de beheersmaatregelen betrekking hebben. De desbetreffende onderdelen van het netwerk (eerste en tweede lid) alsmede het transport van te beschermen kritieke gegevens (derde lid) zijn inhoudelijk toegelicht in het algemeen deel van de toelichting.

Artikel 3

Eerste lid

In het eerste lid wordt de verplichting opgelegd aan netwerkaanbieders om voor 1 oktober 2022 aan de in deze regeling opgenomen beheersmaatregelen te voldoen.

Om aan de beheersmaatregelen van de eerste kolom van de bijlage te voldoen, moet de netwerkaanbieder in ieder geval de vereisten van de tweede kolom van de bijlage implementeren. Als hij dat heeft gedaan, heeft hij daarmee aan de verplichting voldaan om de beheersmaatregel te implementeren. De netwerkaanbieder heeft, in aanvulling op het uitvoeren van de implementatievereisten van die tweede kolom, echter de vrijheid om aanvullende maatregelen en/of handelingen te treffen die bijdragen aan het behalen van het beveiligingsniveau van de desbetreffende beheersmaatregel van de eerste kolom van de bijlage.

Tweede, derde en vierde lid

Op grond van het tweede lid kan de aanbieder een ontheffingsverzoek indienen voor één of meerdere implementatievereisten uit de tweede kolom van de bijlage. De beleidsmatige overwegingen bij deze ontheffingsmogelijkheid zijn toegelicht in het algemeen deel van de toelichting. De Minister neemt binnen twaalf weken een besluit over dit verzoek (derde lid). Indien de Minister voorziet dat het niet haalbaar is om binnen de termijn van twaalf weken een besluit te nemen, dan wordt de netwerkaanbieder hierover ingelicht en wordt aangegeven welke termijn wel haalbaar is (derde lid). De Minister verleent de ontheffing in ieder geval onder

de voorwaarde dat alternatieve uitvoeringswijze waarmee voor de desbetreffende beheersmaatregel in ieder geval een gelijkwaardig beveiligingsniveau wordt bereikt ook daadwerkelijk wordt uitgevoerd (vierde lid).

De Minister van Economische Zaken en Klimaat,
S.A. Blok