Concept-Regeling veiligheid en integriteit telecommunicatie tbv internetconsultatie

Versie 6 november 2020

Verzendwijze: Elektronisch

N.B.1. Bijlagen worden i.v.m. invoering elektronische bekendmaking niet meer ter inzage gelegd maar als apart bestand naar Sdu gezonden en gelijk met de regeling bekendgemaakt.
N.B.2. Behoort bij de regeling een bijlage, dan worden daarop de regeling en artikelnummer(s) vermeld.

Ontvangen BBR	Ontvangen Postkamer	Datum verzending	Paraaf Postkamer

Regeling van de Staatssecretaris van Economische Zaken en Klimaat van , nr. WJZ/19188178, tot regels met betrekking tot aanscherping en verbetering van de beveiliging van netwerken van telecomaanbieders (Regeling veiligheid en integriteit telecommunicatie)

De Staatssecretaris 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, bedoeld in artikel 3.10, eerste lid, aanhef en onderdeel f, van de wet;
b. *kritieke onderdelen:* bij besluit van de minister aangewezen 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:* bij besluit van de minister aangewezen gegevens.

Artikel 2

1. Deze regeling is van toepassing op de kritieke onderdelen, aanpalende onderdelen, beveiligingselementen en beheeromgevingen van de netwerkaanbieder.
2. De beheersmaatregelen, genoemd in de eerste kolom, onder categorie C, nummers 1 en 2, van de bijlage, zijn 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 draagt uiterlijk 1 oktober 2022 zorg voor het treffen van noodzakelijke beheersmaatregelen als bedoeld in de eerste kolom van de bijlage.
2. De noodzakelijke beheersmaatregelen, bedoeld in het eerste lid, bestaan uit de implementatie-vereisten, genoemd in de tweede kolom van de bijlage.
3. In afwijking van het tweede lid kan de minister op aanvraag van de netwerkaanbieder ontheffing verlenen van een of meer implementatie-vereisten binnen een beheersmaatregel, bedoeld in de eerste kolom van de bijlage, indien de netwerkaanbieder naar het oordeel van de Minister heeft aangetoond dat:
    a. de implementatievereisten, genoemd in de tweede kolom van de bijlage, voor diens netwerk technisch niet geïmplementeerd kunnen worden; en
    b. de desbetreffende beheersmaatregel op een gelijkwaardige manier wordt uitgevoerd.
4. De minister beslist binnen twaalf weken na ontvangst van een aanvraag als bedoeld in het derde 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.
5. De ontheffing kan onder voorschriften of beperkingen worden 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

De 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,

De Staatssecretaris van Economische Zaken en Klimaat,

Bijlage

Beheersmaatregelen 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 strikt 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 zo snel mogelijk verifiëren en uitrollen van kritieke security patches voor software die wordt toegepast in de technische infrastructuur.	a. 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 nagestreefd. d. Indien de in onderdeel c bedoelde doorlooptijd niet haalbaar is, worden tijdelijk compenserende mitigaties getroffen**.**
3. Het actief en geautomatiseerd beschermen van beheerwerkstations die voor beheerdoeleinden worden ingezet tegen kwaadaardige malware.	a. Op beheerwerkstations zijn mechanismen actief die kwaadaardige malware geautomatiseerd detecteren en deactiveren. b. De onder a bedoelde mechanismen worden geautomatiseerd actueel gehouden ter bescherming tegen de nieuwste dreigingen en families van kwaadaardige malware.
4. Het reguleren en tot een minimum beperken van alle toegang die voor beheerdoeleinden tot apparatuur en software van de netwerkaanbieder wordt verleend door middel van een gestructureerde proces.	a. Voor het verrichten van beheerwerkzaamheden 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 die herleidbaar is 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.
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, bedoeld in onderdeel a, 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 strikt 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 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. onder a bedoelde systeem- en netwerkdata aan de hand van dreigingsindicatoren kan worden doorzocht.
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 legt contractueel de verplichting op aan beheerdienstverleners 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 legt contractueel de verplichting op aan beheerdienstverleners 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 juridische of politieke context van het land waar vandaan de beheertaken worden verricht tot specifieke beveiligingsrisico's kan leiden en treft 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 legt contractueel aan softwareleveranciers de verplichting op 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 wordt uitgerold overeenkomstig is aan de geëvalueerde software. 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 zijn 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

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 was 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 beveiligingsmaatregelen van de door netwerkaanbieders gebruikte producten en diensten.

De Taskforce heeft 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 belangen vanuit nationale veiligheid dienen te worden beschermd. Deze te beschermen belangen hebben betrekking op de gegevens die moeten 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 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

[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] Tweede Kamer, 2018-2019, 30821, nr. 92

dienen te treffen ter beveiliging van hun netwerk (hierna: beheersmaatregelen). De netwerkaanbieders zijn bij de uitwerking van de beheersmaatregelen betrokken geweest, om ervoor te zorgen dat de beheersmaatregelen uitvoerbaar zijn. Gegeven de snelle ontwikkelingen in de sector, zal de regeling of onderdelen daarvan mogelijk met enige regelmaat opnieuw moeten worden beoordeeld, waarbij de regels niet in de weg moeten staan aan verdere ontwikkelingen in techniek en doorontwikkeling van 5G netwerken.

De regeling bevat maatregelen die in lijn zijn 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 maatregelen zijn opgenomen.

Reikwijdte van de regeling
Onderhavige regeling beperkt zich tot de mobiele netwerkaanbieders. Andere telecomaanbieders die bijvoorbeeld van deze netwerken gebruik maken, maar niet in beheer hebben, vallen buiten de reikwijdte van onderhavige regeling.

De beheersmaatregelen zien toe op de kritieke onderdelen van de mobiele netwerken en de daarmee aanpalende onderdelen (artikel 2, eerste lid). Dit betreft alle systemen en de netwerkelementen die door de overheid als "kritieke onderdelen" zijn aangemerkt. Welke onderdelen behoren tot de "kritieke onderdelen", zijn aangemerkt als Departementaal vertrouwelijk[5]. Met de "aanpalende onderdelen" worden alle systemen en netwerkelementen bedoeld die zich op eenzelfde netwerksegment bevinden als een kritieke onderdeel. Tegelijk met de publicatie van deze regeling zal deze lijst met kritieke onderdelen op vertrouwelijke wijze worden gedeeld met de desbetreffende netwerkaanbieders.

De beheersmaatregelen die betrekking hebben op real-time detectie en historische opsporing van mogelijke beveiligingsincidenten (eerste kolom, onder categorie C, nummer 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 (categorie C, nummer 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. De reikwijdte van deze beheersmaatregel is dus in eerste aanleg aan de netwerkaanbieder met dien verstande dat de netwerkaanbieder de reikwijdte moet kunnen onderbouwen op basis van een uitgevoerde risicoafweging.

Bij het versleutelen van gegevens (categorie B, nummer 5) gaat het alleen om de te beschermen kritieke gegevens. Dit zijn de gegevens die vanuit nationale

[4] Tweede Kamer, vergaderjaar 2019-2020, 24095, nr. 495
[5] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013), artikel 4.

veiligheid moeten worden beschermd. Bij de beheersmaatregel (categorie B, nummer 5) is het transport bepalend. Dit kan betekenen dat het transport plaatsvindt via niet-kritieke netwerkonderdelen van de netwerkaanbieder. Tegelijk met de publicatie van deze regeling zal deze lijst met te beschermen kritieke gegevens op vertrouwelijke wijze worden gedeeld met de desbetreffende netwerkaanbieders.

De beheersmaatregelen

A. De beheersmaatregelen zijn van toepassing op een vijftal veiligheidsdomeinen. 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.

Ontheffingsmogelijkheid

De netwerkaanbieders zijn nauw betrokken geweest bij de totstandkoming van de beheersmaatregelen, dus de beheersmaatregelen zouden in beginsel moeten aansluiten op de huidige praktijk. De regeling biedt desalniettemin aan netwerkaanbieders de mogelijkheid om ten aanzien van de beheersmaatregelen een ontheffing van de Minister van Economische Zaken en Klimaat (hierna: de Minister) te verkrijgen voor één of meerdere implementatievereiste(n) (behorende bij een beheersmaatregel). In de praktijk kan de situatie zich voordoen dat een netwerkaanbieder via een alternatieve manier dan via de in de bijlage opgenomen implementatievereisten ook aan de beheersmaatregelen kan voldoen. Hierbij kan bijvoorbeeld worden gedacht aan alternatieve uitvoeringswijzen die technisch gezien beter aansluiten bij de systemen of apparatuur van de netwerkaanbieder. Dit kan betekenen dat een door de netwerkaanbieder voorgestelde alternatieve uitvoeringswijze beter aansluit op zijn huidige bedrijfsvoering, maar het kan ook betekenen dat als gevolg van innovatie en nieuwe technieken alternatieve uitvoeringswijzen mogelijk beter passend kunnen worden. Indien op een gegeven moment de indruk bestaat dat bepaalde implementatievereisten niet meer goed passend zijn als gevolg van nieuwe technologische ontwikkelingen, kan op den duur ook overwogen worden de regeling aan te passen.

Het blijft, gelet op de zorgplicht van artikel 11a.1, van de TW, 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 een vergelijkbaar beveiligingsniveau wordt behaald. Daarnaast zal de netwerkaanbieder gemotiveerd kenbaar moeten maken waarom het de desbetreffende implementatievereiste(n) technisch niet geïmplementeerd kan respectievelijk kunnen worden in diens netwerk. Eventueel kunnen aan de ontheffing voorwaarden worden verbonden.

Implementatietermijn
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. Dat zal ongeveer 1,5 jaar na publicatie van de regeling zijn. Door de regeling direct na publicatie in werking te laten treden, is 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 eisen. De toezichthouder is daarentegen tijdens de implementatiefase niet bevoegd om (tussentijds) overtredingen te constateren en te handhaven. 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 risico-analyse 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.

Reacties uit de consultatie
Er zijn reacties ingewonnen door middel van een openbare consultatie op www.internetconsultatie.nl.
PM tzt tekst aanvullen met reacties uit de consultatie

Uitvoerings- en handhaafbaarheidstoets
De uitvoerbaarheid en handhaafbaarheid zijn getoetst door de toezichthouder op de regeling, Agentschap Telecom. Onderhavige regeling is als [niet] uitvoerbaar en handhaafbaar beoordeeld.
PM de U&H-toets van AT moet nog worden uitgevoerd

Toets inzake bedrijfseffecten en administratieve lasten
Deze regeling brengt inhoudelijke nalevingskosten voor de aanbieders met zich. De aanbieders hebben een zorgplicht op grond van artikel 11.a in de Telecommunicatiewet, dus zij hebben al de nodige beveiligingsmaatregelen getroffen, zijnde een combinatie van organisatorische en technische 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 maatregelen 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, dus de aanvullende kosten die deze regeling met zich mee 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; zo geeft een netwerkaanbieder aan dat de regeldruk ook voor een belangrijk deel afhangt van de uiteindelijke implementatietermijn; een kortere implementatietermijn brengt bijvoorbeeld hogere personeelskosten met zich mee, omdat mogelijk extra personeel moet worden ingehuurd of er moet versneld worden afgeschreven op bepaalde systemen. Dit kan uiteindelijk nog extra regeldruk met zich meebrengen. Ook geven sommige netwerkaanbieders aan dat sommige nog te treffen maatregelen 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.

Notificatie
Ter voldoening aan richtlijn 2015/1535 (notificatierichtlijn) zijn de beheersmaatregelen, als nationale technische eisen, genotificeerd bij de Europese Commissie.
PM Na verwerking van de reacties uit de openbare internetconsultatie en de uitvoerings- en handhavingstoets door Agentschap Telecom zal de concept-regeling worden genotificeerd.

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 het eerste artikel van deze regeling zijn een aantal begrippen gedefinieerd. Een begripsbepaling wordt hier nader toegelicht.

Netwerkaanbieder
Het gaat hierbij om de mobiele netwerkaanbieders, die beschikken over een vergunning voor het gebruik van geharmoniseerd radiospectrum. Eerder dit 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. Mocht bij toekomstige veilingen ook andere aanbieders een vergunning zoals hier is bedoeld weten te verwerven, dan zullen zij ook aan de gestelde eisen van de regeling moeten voldoen.

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) worden inhoudelijk toegelicht in het algemeen deel van deze toelichting.

Artikel 3
Eerste lid
In het eerste lid van dit artikel is de zorgplicht voor aanbieders van openbare mobiele elektronische communicatienetwerken opgenomen om de beheersmaatregelen te treffen die zijn opgenomen in de eerste kolom van de bijlage.

Tweede lid
Ter implementatie van de beheersmaatregelen (eerste kolom van de bijlage) moet de netwerkaanbieder in ieder geval de vereisten van de tweede kolom van de bijlage uitvoeren. Als hij dat heeft gedaan, heeft hij daarmee de beheersmaatregel geïmplementeerd. De netwerkaanbieder heeft, in aanvulling op het uitvoeren van de implementatievereisten van die tweede kolom, de vrijheid om nog aanvullende maatregelen te treffen die bijdragen aan het implementeren van de beheersmaatregelen van de eerste kolom van de bijlage.

Derde lid, vierde en vijfde lid
Op grond van het derde lid kan de aanbieder een ontheffingsverzoek indienen voor een of meerdere implementatievereisten uit de tweede kolom van de bijlage (derde lid). De beleidsmatige overwegingen bij deze ontheffingsmogelijkheid worden toegelicht in het algemene deel van de toelichting. De Minister neemt binnen twaalf weken een besluit over dit verzoek. 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 een aangegeven welke termijn wel haalbaar is (vierde lid). De Minister heeft de bevoegdheid om de ontheffing onder bepaalde voorwaarden te verlenen (vijfde lid).

De Staatssecretaris van Economische Zaken en Klimaat,