Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

36 764 Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet)

Nr. 7 **VERSLAG**

Vastgesteld 8 september 2025

De vaste commissie voor Digitale Zaken, belast met het voorbereidend onderzoek van bovenstaand wetsvoorstel, heeft de eer als volgt verslag uit te brengen van haar bevindingen.

Onder het voorbehoud dat de regering op de gestelde vragen tijdig en genoegzaam zal hebben geantwoord, acht de commissie de openbare beraadslaging over dit wetsvoorstel voldoende voorbereid.

Inhoudsopgave **blz.**

kst-36764-7
ISSN 0921 - 7371
's-Gravenhage 2025

I. ALGEMEEN DEEL

1. Inleiding

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de Cyberbeveiligingswet (Cbw). Over de wet en alle aanhangige stukken hebben deze leden vragen en opmerkingen.

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de Cyberbeveiligingswet. Deze leden delen het doel van het wetsvoorstel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de EU te bereiken, teneinde de werking van de interne markt te verbeteren. Zij stellen nog enkele vragen.

De leden van de NSC-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel ter implementatie van de Europese NIS2-richtlijn via de Cyberbeveiligingswet. Deze leden onderschrijven het belang van versterkte digitale weerbaarheid, vooral voor vitale processen en essentiële diensten. Zij merken op dat digitalisering diep doordringt in alle sectoren van de samenleving en daarmee de afhankelijkheid van goed functionerende en veilige digitale systemen vergroot. Daarom achten deze leden het van groot belang dat het wetgevend kader helder en werkbaar is. Tegelijkertijd constateren zij dat het wetsvoorstel op een aantal punten nadere toelichting of verduidelijking behoeft. Zij hebben in dat kader de volgende vragen en opmerkingen De leden van de voornoemde fractie wijzen op de recente datadiefstal bij laboratorium Clinical Diagnostics in Rijswijk. Dit onderstreept opnieuw de kwetsbaarheid van onze digitale infrastructuur. Deze gevoelige informatie omvat onder andere persoonsgegevens die gedeeld zijn met het laboratorium, wat voor de betrokkenen niet alleen een ernstige inbreuk op de privacy betekent, maar ook verhoogde risico's op phishing en identiteitsfraude met zich meebrengt. Dit incident werpt een urgent licht op de noodzaak van strengere en effectievere wetgeving op het gebied van cyberbeveiliging. De Cyberbeveiligingswet roept in dit kader belangrijke vragen op over de reikwijdte, handhaving en effectiviteit ervan, zeker wanneer gevoelige medische gegevens op zo'n grote schaal kunnen lekken. De leden van deze fractie vragen in hoeverre de huidige Cyberbeveiligingswet voldoende bescherming biedt tegen datalekken binnen organisaties die gevoelige medische gegevens verwerken. Vallen die altijd binnen deze wet?

De leden van de D66-fractie hebben met interesse kennisgenomen van de Cyberbeveiligingswet. Deze leden onderschrijven het belang van een hoog niveau van digitale weerbaarheid en de implementatie van de NIS2-richtlijn. Zij constateren wel dat hier sprake is van een grote stelselherziening met een omvangrijke uitbreiding van reikwijdte en verplichtingen. Daar hebben deze leden enkele vragen over.

De leden van de CDA-fractie hebben kennisgenomen van het wetsvoorstel en hebben hierover nog enkele vragen.

De leden van de SP-fractie hebben de Cyberbeveiligingswet gelezen en hebben hier nog enkele vragen over. Kan de regering allereerst meer ingaan op het advies van de Raad van State voor zover het gaat over de taakverdeling tussen de vakministers en de zelfstandige bestuursorganen (zbo's)? En kan de regering iets zeggen over de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)? Eerder is er bewust voor gekozen om al het toezicht bij de ANVS te leggen, maar nu krijgt de Minister van Infrastructuur en Waterstaat (I&W) ook een deel van dat toezicht. Kan de regering aangeven of er nog andere zbo's zijn waar zo'n situatie kan voorkomen?

De leden van de SP-fractie vragen tevens waarom de Autoriteit Persoonsgegevens (AP) tot op heden nog geen middelen heeft ontvangen om haar taak (samen met andere toezichthouders toezicht houden op de Cyberbeveiligingswet) uit te voeren. Daarbij houdt de AP toezicht op alle organisaties en sectoren en kan zij de samenwerking tussen de verschillende toezichthouders bevorderen. De AP geeft aan structureel circa twee miljoen euro nodig te hebben. Is de regering bereid de AP alsnog van deze middelen te voorzien?

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van onderhavig wetsvoorstel. Deze leden merken op dat de Afdeling advisering van de Raad van State adviseert om nader in te gaan op de wijze waarop invulling wordt gegeven aan de coördinerende taak van de Minister van Justitie en Veiligheid (J&V). Uit het nader rapport blijkt niet of de memorie van toelichting is aangevuld op dit punt. Ook wordt niet ingegaan op welke zbo's belast zijn met toezichts- en handhavingstaken, ondanks het advies van de Raad van State hierover. Kan de regering alsnog uitgebreider op beide zaken ingaan?

2. De NIS2-richtlijn

2.1. Kern van de richtlijn

De leden van de CDA-fractie vragen wat de reden is voor de keuze om uit te gaan van minimumharmonisatie, terwijl een van de problemen van de NIS1-richtlijn was dat er teveel verschillen tussen lidstaten ontstonden. In dat kader vragen deze leden of de regering een compleet overzicht wil delen van alle onderdelen van het wetsvoorstel die verder gaan dan de minimumeisen van de richtlijn.

De leden van de GroenLinks-PvdA-fractie hebben vragen over tekortkomingen van de NIS1-richtlijn. Volgens de regering bestaan er te veel verschillen tussen de implementatie in lidstaten. Kan de regering enkele problematische tegenstrijdigheden tussen lidstaten noemen, die de komst van de NIS2-richtlijn rechtvaardigen? Kan de regering ook toelichten in welke mate Nederland de NIS1-richtlijn heeft geïmplementeerd?

De leden van de GroenLinks-PvdA-fractie merken op dat Nederland de NIS2-richtlijn te laat implementeert in nationale wetgeving. Deze leden vragen de regering om duidelijk te maken of dit gevolgen heeft voor de cyberveiligheid van entiteiten, aangezien Nederland in de tussentijd geen gelijkgestemde wetgeving heeft met andere landen. Kan de regering de trage implementatie en de gevolgen daarvan nader toelichten? Op welke termijn verwacht de regering deze wet wel volledig te hebben ingevoerd?

2.2. Belangrijkste onderdelen van de richtlijn

De leden van de D66-fractie vragen de regering uiteen te zetten welke onderdelen van de huidige nationale wetgeving tekortschoten en waarom de gekozen verzwaringen noodzakelijk zijn, mede in het licht van het advies van het Adviescollege Toetsing Regeldruk (ATR) waarin gesteld wordt dat er geen aanleiding is om te kiezen voor zwaardere eisen dan de minimumeisen van de richtlijn.

2.3. Verhouding tot de CER-richtlijn en de Wwke

De leden van de GroenLinks-PvdA-fractie erkennen het belang van coherentie tussen de Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet. Echter vragen deze leden of de koppeling tussen de

twee wetten strikt noodzakelijk is geweest, of andere lidstaten dezelfde keuze maken, en of dit heeft geleid tot vertraging.

De leden van de VVD-fractie begrijpen dat de NIS2-richtlijn regelt dat entiteiten die uit hoofde van de CER-richtlijn worden aangewezen als kritieke entiteit, ook onder het toepassingsbereik van de NIS2-richtlijn vallen en automatisch als essentiële entiteit in de zin van de NIS2-richtlijn kwalificeren. Andersom geldt dat echter niet: een essentiële entiteit kwalificeert niet automatisch als kritieke entiteit, omdat kritieke entiteiten eerst als zodanig moeten worden aangewezen. Kan de regering nader toelichten waarom hiervoor gekozen? Welke lidstaatopties zijn er mogelijk onder het bereik van de NIS2 en de CER-richtlijn bij het aanwijzen of kwalificeren van een essentiële entiteit of kritieke entiteit? Kan de regering nader schematisch uitleggen welke ruimte lidstaten hebben bij de beoordeling hiervan?

2.4. Verhouding tot de DORA

De leden van de GroenLinks-PvdA-fractie lezen dat de samenhang met de Digital Operational Resilience Act (DORA) ervoor zorgt dat financiële instellingen gemakkelijk in het NIS2-regime vallen. Vanuit dit oogpunt valt het hen echter op dat de Minister van Financiën als bevoegde entiteit wordt aangewezen. Is een andere rolverdeling verkend, bijvoorbeeld door de Minister van Justitie en Veiligheid als één centraal aanspreekpunt aan te wijzen? Graag vernemen deze leden wat de specifieke bevoegdheden van de Minister van Financiën behelzen.

3. Nationale context

De leden van de GroenLinks-PvdA-fractie onderschrijven het belang van een brede maatschappelijke aanpak voor cyberveiligheid. Cyberveiligheid moet doorleefd worden in de hele structuur en cultuur van organisaties die het land draaiende houden. Deze leden vragen om een beknopte uiteenzetting van de doelstellingen uit artikel 7 van de NIS2-richtlijn en wat het antwoord op deze is zoals beschreven in de Nederlandse Cybersecuritystrategie (NLCS). Is het doel om beter zicht te hebben op cyberincidenten, -dreigingen en -risico's volledig afgedekt met de komst van de Cyberbeveiligingswet? Zij vragen de regering daarnaast om duidelijk te maken hoe abstract of concreet deze nationale strategie hoort te zijn volgens de NIS2-richtlijn, wetende dat de strategie nog per sector moet worden uitgewerkt.

4. Gemaakte implementatiekeuzes op hoofdlijnen

De leden van de GroenLinks-PvdA-fractie kunnen zich vinden in het besluit om de NIS2-richtlijn om te zetten in één centrale wet. Deze leden vragen de regering of zij een analyse heeft gemaakt om te bezien of er alsnog aanpassingen in sectorale wetgeving of samenhangend beleid noodzakelijk zijn voor een effectieve werking van de Cyberbeveiligingswet. Zo ja, waarom is er gekozen om niet gelijktijdig aan de Cyberbeveiligingswet ook samenhangende wetgeving aan te passen? Zo nee, met welke zekerheid kan de regering dan zeggen dat er geen tegenstrijdigheden of onduidelijkheden bestaan tussen de Cyberbeveiligingswet en andere wetgeving?

De leden van de GroenLinks-PvdA-fractie vragen wat de voor- en nadelen zijn van het aanwijzen van vakministers als verantwoordelijk binnen hun sectoren. Over het algemeen achten zij het wenselijk dat coördinerende taken helder en centraal belegd zijn. Is er, gezien de centrale en coördinerende rol van de Minister van Justitie en Veiligheid, niet veel voor te

zeggen om deze Minister als eindverantwoordelijk aan te wijzen voor alle sectoren? Deze leden vragen of dit de samenwerking en informatie-uitwisseling tussen sectoren kan verbeteren. Bovendien merken zij op dat de coördinerende Staatssecretaris voor Digitalisering en Koninkrijksrelaties geen rol heeft in deze wet. Heeft de regering overwogen om de Minister van Binnenlandse Zaken, gedelegeerd aan de relevante Staatssecretaris, als coördinerend aan te wijzen?

De leden van de CDA-fractie constateren dat de reikwijdte van de richtlijn is uitgebreid ten opzichte van de NIS1-richtlijn. Deze leden vragen of de regering nader wil ingaan op de gemaakte keuzes in Europees verband. Zij vragen of is overwogen de reikwijdte nog verder uit te breiden en om welke sectoren het dan ging. Ook vragen de leden van de CDA-fractie wat de inzet van de regering was op dit punt, en in hoeverre deze inzet is overgenomen.

5. Gevolgen

5.1. Essentiële entiteiten en belangrijke entiteiten

5.1.1. Essentiële entiteiten en belangrijke entiteiten

De leden van de GroenLinks-PvdA-fractie lezen over het onderscheid tussen essentiële en belangrijke entiteiten. Kan de regering beeldend maken wat het onderscheid tussen beide categorieën is, door enkele voorbeelden te noemen van zowel essentiële als belangrijke entiteiten? Kan de regering daarbij onderbouwen op basis van welke kwalificaties deze entiteiten in een van de twee categorieën is geplaatst? Deze leden vragen de regering ook om voorbeelden te noemen van entiteiten die in meerdere sectoren actief zijn en te maken krijgen met verschillende sectorale verplichtingen en aanspreekpunten. Bovendien zien zij het risico dat entiteiten die in meerdere sectoren werken, in geval van crisis alsnog de weg niet kunnen vinden naar de juiste instantie. De leden vragen aan de regering om nader toe te lichten hoe entiteiten in meerdere sectoren worden geacht hun zorgplicht en meldplicht uit te voeren.

De leden van de GroenLinks-PvdA-fractie voorzien mogelijke grijze gebieden als het aankomt op entiteiten die niet per wet als essentieel of belangrijk kunnen worden bestempeld. Hiervoor wordt de nationale vitaalbeoordeling gebruikt als methodiek. Het is voor deze leden echter niet duidelijk hoe deze beoordeling en de aanwijzing in de praktijk zal werken. Zij vragen de regering dan ook om beter duidelijk maken hoe dit aanwijzingsproces werkt, zodat het helder is hoe de beoordeling op basis van criteria wordt uitgevoerd, wie daarvoor verantwoordelijk is en wat er verwacht wordt van de desbetreffende entiteit. Zij vragen de regering om duidelijk te maken hoe de rollen verdeeld zijn tussen de vakminister en de Minister van Justitie en Veiligheid.

De leden van de VVD-fractie constateren dat het uitvoeren van de vitaalbeoordeling en de aanwijzing van entiteiten in de eerste plaats een verantwoordelijkheid is van de vakminister, in overleg met de Minister van Justitie en Veiligheid (J&V) als coördinerend bewindspersoon voor de bescherming van de vitale infrastructuur en cybersecurity. Kan de regering nader toelichten hoe dit afstemmen efficiënt in de praktijk zal werken? Wat is de procedure bij mogelijke beleidsconflicten tussen de vakminister en de Minister van J&V in zijn rol als coördinerend bewindspersoon? Deze leden vragen een uitgebreide toelichting op de coördinerende rol van de Minister van J&V en hoe die in de praktijk zal worden vormgegeven.

5.1.2. Overheidsinstanties

De leden van de GroenLinks-PvdA-fractie staan achter de keuze om de NIS2-richtlijn toe te passen op medeoverheden. Echter, deze leden hebben twijfels over de capaciteit van gemeenten, provincies en waterschappen om zich voldoende voor te bereiden op de Cyberbeveiligingswet. Welke duidelijkheid verschaft de regering aan medeoverheden over de nodige voorbereiding? Zij wijzen op nieuwe verplichtingen, (voorbereidings-)budget, aanvullende capaciteit en dergelijke waar medeoverheden zich op moeten kunnen voorbereiden. De leden vragen aan de regering om aan te tonen dat zij medeoverheden hier adequaat over hebben geïnformeerd en welke middelen de regering beschikbaar heeft gesteld voor het steunen van overheidsorganisaties.

De leden van de GroenLinks-PvdA-fractie merken op dat criterium A wijst op het algemene belang dat een overheidsdienst moet dienen. Echter zijn veel overheidsdiensten in de jaren geliberaliseerd, denk aan de Nederlandse Spoorwegen (NS), die zowel een essentiële overheidsdienst vervullen als opereren onder marktomstandigheden. Voldoen dergelijke entiteiten aan criterium A? Acht de regering het wenselijk om dit soort organisaties wel of niet als overheidsinstanties aan te merken?

De leden van de GroenLinks-PvdA-fractie merken op dat criterium C alleen toeziet op organisaties met een meerderheidsaandeel van de overheid. Deze leden vragen aan de regering om te onderbouwen waarom dit criterium niet van toepassing is op organisaties die voor een aanzienlijk deel, maar minder dan 50%, gefinancierd worden door de overheid. Is er bij deze organisaties niet evengoed sprake van een bijzonder algemeen belang?

De leden van de GroenLinks-PvdA-fractie merken op dat het Ministerie van Defensie niet onder het bereik van de NIS2-richtlijn valt. Hoewel de uitzonderlijke positie van dit departement begrijpelijk is, vragen deze leden om een nadere onderbouwing waarom deze buiten de reikwijdte valt van dit criterium en hoe onder welk cyberveiligheidsregime het departement wél valt.

5.1.3. Onderwijsinstellingen

De leden van de GroenLinks-PvdA-fractie lezen dat de Minister van Onderwijs, Cultuur en Wetenschap (OCW) de bevoegdheid krijgt om onderwijsinstellingen aan te wijzen als essentiële of belangrijke entiteit. Deze leden vragen de regering om helder te formuleren wanneer de Minister van OCW deze bevoegdheid inzet. Welke instellingen zullen per direct aangewezen worden als zodanig? Welke andere voorwaarden zijn er verbonden aan deze aanwijzing? Bovendien lezen zij dat er «intensief overleg [is] gevoerd met alle betrokken stakeholders.» Graag vernemen de leden welke instellingen dit betreft en of deze unaniem instemden met het voorstel. Zijn er in deze gesprekken concessies gedaan vanuit de regering?

De leden van de GroenLinks-PvdA-fractie merken op dat ziekenhuizen en zorginstellingen niet onder het toepassingsbereik van de NIS2-richtlijn vallen. Dit zijn echter cruciale organisaties die het algemene belang dienen. Biedt de NIS2-richtlijn de ruimte om ziekenhuizen en zorginstellingen standaard als essentiële of belangrijke entiteit aan te wijzen en zo ja, heeft de regering deze mogelijkheid overwogen?

De leden van de D66-fractie zijn geschokt door recente cyberaanvallen op onderwijsinstellingen. Deze leden achten het zeer noodzakelijk om de cyberveiligheid van onderwijsinstellingen te versterken. Zij vragen de regering wel om nader te motiveren waarom onderwijsinstellingen worden aangewezen onder de Cyberbeveiligingswet, terwijl dit in de richtlijn optioneel is en andere lidstaten deze keuze niet maken en welke andere opties de regering heeft overwogen om cyberveiligheid van onderwijsinstellingen te versterken.

De leden van de D66-fractie vragen of de regering onderkent dat er al een sectorbreed systeem van bestuurlijke afspraken, audits en samenwerking via SURF bestaat, waarmee de cyberweerbaarheid van onderwijsinstellingen de afgelopen jaren is versterkt. Acht de regering het voldoende proportioneel en doeltreffend om een nieuw systeem op te tuigen in plaats van het huidige systeem te verbeteren? Deze leden vragen tevens hoe wordt voorkomen dat bestaande governance en toezichtstructuren, zoals de externe audits, de rol van de Raden van Toezicht en het toezicht conform de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) moeten worden vervangen door nieuwe en nog niet bewezen inspectiestructuren, waardoor dubbele toezichtlagen ontstaan. Hoe verhouden nieuwe verplichtingen zich tot de bestaande verantwoordelijkheden van bestuurders en Raden van Toezicht?

Daarnaast constateren de leden van de D66-fractie dat de invoering van de Cyberbeveiligingswet voor onderwijsinstellingen aanzienlijke administratieve verplichtingen en extra kosten met zich meebrengt, terwijl de meerwaarde in termen van veiligheid ten opzichte van de huidige systematiek vooralsnog onduidelijk is. Hoe wordt geborgd dat deze lasten in verhouding staan tot de verwachte veiligheidswinst? Welke middelen stelt de regering beschikbaar om de extra uitvoerings- en financieringslasten voor instellingen en SURF op te vangen, mede gezien de structurele bezuinigingen op de onderwijsbegroting en het feit dat instellingen momenteel zelfs bijdragen aan de kosten van SURF en de Inspectie van het Onderwijs? Ook vragen deze leden hoe de regering de claim van onderwijsinstellingen beoordeelt dat de termijnen die nu gesteld zijn voor onderwijsinstellingen «volstrekt onhaalbaar» zijn.

Daarbij vragen de leden van de D66-fractie expliciet om te reflecteren op de indruk die in overleg met het Ministerie van OCW is ontstaan dat het hoger onderwijs niet onder deze wet zou vallen en dat er door het Ministerie van OCW niet is ingezet op voorbereiding voor implementatie van deze wet.

De leden van de CDA-fractie constateren dat de keuze is gemaakt om hoger onderwijsinstellingen onder het toepassingsbereik van de richtlijn te brengen. Deze leden lezen dat dit met name ziet op kritieke onderzoeksactiviteiten. Zij vragen of de regering deelt dat het per instelling en soort onderwijs (hoger beroepsonderwijs en universiteiten) verschilt in hoeverre sprake is van kritieke onderzoeksactiviteiten. De leden vragen daarom of er mogelijkheden zijn om het begrip «onderwijsinstellingen» nader te specificeren zodat het toepassingsbereik echt gericht wordt op instellingen die kritieke onderzoeksactiviteiten verrichten. Deze leden vragen verder of de regering nader wil ingaan op de vraag wat wel en niet onder kritieke onderzoeksactiviteiten wordt verstaan. Zij vragen of inmiddels al duidelijk is of de Minister van OCW gebruik zal maken van deze nieuwe bevoegdheid en wat hiervan de financiële implicaties zijn.

5.2. Zorgplicht

5.2.1. Inleiding

De leden van de GroenLinks-PvdA-fractie hebben begrip voor de keuze om uit te gaan van een interne risicobeoordeling. Echter, deze leden vinden de aanname dat entiteiten goed inzicht hebben in hun eigen dienstverlening en systemen te kort door de bocht. Zij vrezen dat niet alle entiteiten beschikken over de nodige IT-kennis, of dit hebben uitbesteed aan derden. Daarom vragen de leden aan de regering of er in bijzondere gevallen ook onafhankelijke risicobeoordelingen kunnen worden uitgevoerd. Heeft de regering een plan om entiteiten met onvoldoende interne IT-kennis te ontzien en de risicobeoordeling bij een onafhankelijke instantie te beleggen? Is het borgen en versterken van de IT-kennis binnen organisaties ook een doel van de NIS2-richtlijn?

5.2.2. Beveiliging van netwerk- en informatiesystemen

De leden van de GroenLinks-PvdA-fractie volgen de technologieneutrale definitie van «netwerk- en informatiesystemen.» Deze leden zetten echter een vraagteken bij de definitie van «digitale weerbaarheid.» Is het volgens de regering te kwantificeren wanneer een entiteit voldoende digitaal weerbaar is? Zij leden vragen een heldere definitie van dit begrip.

5.2.3. De maatregelen

De leden van de GroenLinks-PvdA-fractie moedigen het gebruik van de best beschikbare standaarden en technieken aan. Deze leden vragen de regering wel om te verhelderen hoe de effectiviteit van maatregelen wordt gemeten: is dit mede op basis van analyses van casussen waarin bepaalde maatregelen effectief een aanval of storing hebben voorkomen? Bovendien vragen zij hoe de kans op incidenten en de mogelijke maatschappelijke en economische gevolgen daarvan worden vastgesteld. Is hier een standaardmethodiek voor die voor alle sectoren van toepassing is?

De leden van de GroenLinks-PvdA-fractie vragen hoe de evenredigheid van maatregelen wordt vastgesteld. Gezien de risicobeoordeling bij entiteiten zelf wordt belegd, bestaat de kans dat evenredigheid subjectief wordt geïnterpreteerd. Welke waarborgen bouwt de regering in om ervoor te zorgen dat evenredigheid zo objectief als mogelijk wordt vastgesteld?

De leden van de GroenLinks-PvdA-fractie zien de groeiende afhankelijkheid van een selecte groep niet-Europese techleveranciers als één van de belangrijkste dreigingen voor onze cyberveiligheid en weerbaarheid. Wordt onder de NIS2-richtlijn expliciet aandacht gevraagd voor het terugdringen van deze afhankelijkheden en het bevorderen van de strategische autonomie? Kortom, geldt het diversificeren van de eigen IT-systemen en het afbouwen van afhankelijkheden als een legitieme cyberveiligheidsmaatregel? Deze leden vragen de regering om toe te lichten hoe de NIS2-richtlijn de strategische autonomie bevordert.

De leden van de D66-fractie vragen de regering om te reageren op de zorgen vanuit NLdigital en het bedrijfsleven met betrekking tot het laat toegevoegde artikel 18 van het Cyberbeveilingsbesluit, met een grondslag enkel in de memorie van toelichting, waarin de zorgplicht wordt uitgebreid en te reageren op het door hen aangedragen alternatief. Deze leden vragen daarbij hoe deze Nederlandse uitbreiding zich verhoudt tot het streven naar een Europees gelijk speelveld en welke impact de regering

verwacht op het Nederlandse vestigingsklimaat voor internationale techbedrijven.

5.3. Governance

5.3.1. Inleiding

De leden van de GroenLinks-PvdA-fractie vinden het essentieel dat bestuursleden van entiteiten doordrongen zijn van het belang van cyberveiligheid. Deze leden constateren echter dat er in veel instanties te weinig interne kennis en kunde is op het gebied van IT, wat bestuurlijk overleg over cyberveiligheid bemoeilijkt. Zij wijzen op het nut van een «cyberjaarverslag,» een gestandaardiseerd jaarlijks inzicht in de stand van de IT en het voldoen aan digitale wetgeving. De leden vragen de regering om de aangenomen motie van het lid Kathmann (Kamerstuk 26 643, nr. 1342), die oproept om het invoeren van een cyberjaarverslag te verkennen, te betrekken bij de implementatie van de Cyberbeveiligingswet. Zij menen dat het cyberjaarverslag bijdraagt aan een beter en bruikbaar inzicht in de IT voor bestuurders van organisaties.

5.3.2. Training

De leden van de GroenLinks-PvdA-fractie prijzen de inzet op het trainen van bestuurders. Deze leden vragen de regering of zij een verkenning heeft uitgevoerd of er voldoende cursusaanbieders en -materiaal beschikbaar is om te voldoen aan deze bepaling. Aan welke organisatie of toezichthouder moeten bestuurders aantonen dat zij deze trainingen hebben gevolgd en hun certificaten vernieuwen?

5.3.3. Normadressaat

5.3.3.1 Bestuur van essentiële entiteiten en belangrijke entiteiten, niet zijnde overheidsinstanties

De leden van de GroenLinks-PvdA-fractie begrijpen de keuze om beveiligingsmaatregelen alleen met goedkeuring van het dagelijks bestuur te laten vaststellen en om alle bestuursleden te laten voldoen aan de opleidingsverplichting. De kennis over IT en cyberveiligheid dient breed gedragen te worden. Het risico bestaat echter dat de brede opleidingsverplichting de kennis kan verwateren. Biedt de NIS2-richtlijn de kans voor besturen om één bestuurslid als eindverantwoordelijke op het gebied van IT en cyberveiligheid aan te wijzen, zodat deze beschikt over diepere specialistische kennis, in plaats van dat alle bestuursleden enkel over algemene kennis beschikken? Deze leden zijn benieuwd of de regering deze benadering heeft overwogen.

5.3.3.2 Bestuur van overheidsinstanties

De leden van de GroenLinks-PvdA-fractie missen in de rolverdeling binnen overheidsorganisaties duidelijkheid over de rol van de volksvertegenwoordiging. Gemeenten, provincies en het Rijk hebben immers verantwoording af te leggen aan de controlerende macht. Deze leden vragen de regering daarom om toe te lichten op welke wijze de volksvertegenwoordiging dient te worden geïnformeerd (al dan niet vertrouwelijk) over de maatregelen die volgen uit de NIS2-richtlijn. Zij benadrukken het belang van transparantie en medezeggenschap over politieke keuzes inzake digitalisering en cyberveiligheid. Op welke manier kunnen raadsleden, Statenleden en Kamerleden de genomen maatregelen controleren en (bij)sturen?

5.4. Meldplicht

De leden van de GroenLinks-PvdA-fractie vragen de regering om een overzicht van alle (beoogde) sectorale Computer Security Incident Response Teams (CSIRT's) die volgen uit de NIS2-richtlijn.

De leden van de GroenLinks-PvdA-fractie zijn van mening dat melden van incidenten, groot en klein, zo veel als mogelijk gestimuleerd moeten worden. Deze leden vragen daarom of de meldplicht bij significante incidenten niet als nadeel heeft dat kleine incidenten, die alsnog grote gevolgen blijken te hebben, niet (op tijd) worden gemeld. Heeft de regering overwogen om de meldplicht te verbreden of de drempelwaarden te verlagen? Zij ontvangen graag meer informatie over deze afweging en hoe mogelijke alternatieve invullingen van de meldplicht zijn ontvangen door de betrokken sectoren. De leden ontvangen daarnaast graag, wanneer dat beschikbaar is, informatie over de vastgestelde drempelwaarden per sector. Hoe komen deze drempelwaarden tot stand en wat voor overleg gaat hieraan vooraf met belanghebbenden? Deze leden achten het van belang dat deze waarden en de afweging hiervan openbaar en controleerbaar zijn.

De leden van de GroenLinks-PvdA-fractie vinden het onduidelijk waarom de regering enkel streeft naar het invoeren van een dubbele meldplicht aan het CSIRT die slechts één handeling van de betrokken entiteit vergt. Waarom is dit een streven en geen doel? Graag een toelichting over welke drempels er in de weg staan om dit technisch zo in te richten dat één handeling afdoende is.

De leden van de CDA-fractie constateren dat voor essentiële entiteiten en belangrijke entiteiten een dubbele meldplicht geldt. Deze leden vragen of de regering kan garanderen dat voor deze entiteiten een centraal loket wordt ingericht, direct vanaf het moment dat de wet in werking treedt, zodat entiteiten niet met onnodige lasten worden opgezadeld.

De leden van de CDA-fractie vragen ook of de regering nader wil ingaan op de gevolgen in de praktijk van de nieuwe meldplicht. Deze leden vragen of de regering kan inschatten hoeveel extra meldingen zullen worden gedaan als gevolg van de nieuwe meldplicht. Ook vragen zij of de CSIRT's en toezichthoudende instanties in staat zijn een toename van meldingen te behandelen, en welke keuzes daarin worden gemaakt.

5.5. CSIRT

5.5.1. Aanwijzing CSIRT's

De leden van de GroenLinks-PvdA-fractie vragen de regering om helder uit te leggen hoe de structuur van een CSIRT er in de praktijk uit zal zien. Deze leden vragen de regering om in duidelijke taal uit te leggen over welke capaciteit, structuur en kennis een CSIRT zal moeten beschikken.

5.5.2. Verwerking van gegevens door het CSIRT

De leden van de GroenLinks-PvdA-fractie erkennen het belang van een snelle en volledige informatie-uitwisseling door CSIRT's. Deze organisaties kunnen enkel hun werk uitvoeren door te beschikken over belangrijke en gevoelige data. Dat roept bij deze leden de vraag op of CSIRT's zelf ook niet moeten voldoen aan relevante cyberveiligheidseisen, zoals voorgeschreven aan entiteiten die onder de NIS2-richtlijn vallen. Als het CSIRT platligt, heeft dat immers ook gevolgen voor de digitale

weerbaarheid. Hoe wordt de cyberveiligheid van CSIRT's gewaarborgd en wie ziet daarop toe?

5.5.3. Rol NCSC

De leden van de GroenLinks-PvdA-fractie vragen de regering om te specificeren welk «groot deel van de entiteiten die onder het toepassingsbereik van de Cyberbeveiligingswet vallen» vermoedelijk onder het Nationaal Cyber Security Centrum (NCSC) zal vallen als nationale CSIRT.

De leden van de D66-fractie vragen of de regering kan reageren op de behoefte vanuit G4 gemeenten waarbij burgemeesters rechtstreeks gegevens van het NCSC kunnen ontvangen, omdat zij die gegevens nodig achten om de lokale impact van cyberdreigingen en veiligheidsincidenten te kunnen duiden. Kan de regering toelichten of, en zo ja, welke mogelijkheden voor zulke gegevensdeling reeds bestaan in bestaande wet- en regelgeving? Of moet er in de Cyberbeveiligingswet een expliciete wettelijke grondslag worden opgenomen?

5.5.4. Samenwerking tussen CSIRT's

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen hoe en waar de samenwerkingsprotocollen tussen CSIRT's worden gepubliceerd. Deze leden hechten belang aan het openbaar maken van deze protocollen.

5.6. Handhaving

5.6.1. Handhaving van verplichtingen uit Cbw, uitvoeringshandelingen en gedelegeerde handelingen

De leden van de GroenLinks-PvdA-fractie zijn van mening dat het nog onduidelijk is wanneer er sprake is van «effectief toezicht» zoals bedoeld in artikel 32 van de NIS2-richtlijn. Deze leden vragen de regering om dit te definiëren. Daarnaast vragen zij aan de regering om duidelijk te maken wanneer geldboeten aan een entiteit zouden worden opgelegd. Wat gebeurt er met de inkomsten uit boetes die worden opgelegd aan entiteiten? Volgens de leden van de moet de regering overwegen om deze boetes standaard terug te investeren in de cyberveiligheid van Nederland. Zij horen graag de reactie van de regering.

5.6.2. Bestuursrechtelijke handhaving

5.6.3. Differentiatie in het toezicht

De leden van de GroenLinks-PvdA-fractie hebben begrip voor het aanbrengen van differentiatie in toezicht op verschillende sectoren. Wel waken deze leden ervoor dat dit niet mag leiden tot een feitelijk betere of slechtere mate van toezicht, afhankelijk van sectoren. Zij vragen de regering hoe dit risico wordt voorkomen.

5.6.4. Handhavingsinstrumentarium

De leden van de GroenLinks-PvdA-fractie vragen de regering om duidelijk te maken welke eisen er worden gesteld aan de onafhankelijke organisaties die beveiligingsscans en audits uitvoeren bij essentiële en belangrijke entiteiten. Deze leden wijzen erop dat de organisaties die deze onderzoeken doen betrouwbaar moeten zijn. Is het uitgesloten dat niet-Europese organisaties deze onderzoeken uitvoeren? Gezien de gevoeligheid van de onderzoeken achten deze leden dit wenselijk.

Bovendien vragen zij of de methodiek voor audits en scans wordt gestandaardiseerd, en zo ja, volgens welke standaardmethodiek deze plaatsvinden.

De leden van de CDA-fractie constateren dat de Raad van State heeft geadviseerd om in kaart te brengen welke zelfstandige bestuursorganen (zbo's) belast zijn met toezichts- en handhavingstaken gericht op veiligheid, en om in de toelichting aan te geven hoe wordt voorkomen dat de uitoefening van deze taken in de praktijk tot problemen leidt, doordat zij overlapt met taken die zijn toebedeeld via het wetsvoorstel. Deze leden vragen of de regering alsnog specifiek wil ingaan op dit punt en ook om dit overzicht te delen.

5.6.5. Bepalen einddatum, verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur

5.6.5.1 Implementatie van artikel 32, vijfde lid, NIS2-richtlijn

De leden van de GroenLinks-PvdA-fractie vragen om een nadere onderbouwing welke organisaties bedoeld worden met «certificerings- of vergunningsinstanties.»

5.6.5.2 Bepaling einddatum door toezichthoudende instantie

De leden van de GroenLinks-PvdA-fractie vinden het van belang dat het vaststellen van een einddatum, waarop maatregelen getroffen moeten zijn om overtredingen te voorkomen, op een transparante wijze gebeurt. Kan de regering toelichten hoe toezichthoudende instanties geacht worden deze einddatum vast te stellen, en aan welke instantie zij dit moeten motiveren? Wordt hiervoor een afwegingskader per sectorale toezichthouder opgesteld, al dan niet in samenspraak met betrokken entiteiten? Deze leden benadrukken dat sancties en ingrepen als doel moeten hebben om de cyberveiligheid feitelijk te verbeteren. Het is dus wenselijk dat entiteiten niet verrast worden door handhaving en vroegtijdig worden gewezen op realistische verbeterpunten.

5.6.5.3 Verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur

De leden van de GroenLinks-PvdA-fractie onderstrepen dat het schorsen van leden uit een bestuur een zeer zwaarwegend middel is. Deze leden vragen de regering om een scenario te schetsen waarin deze maatregelen doeltreffend en proportioneel zou zijn.

5.6.6. Bestuurlijke boete

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen welke mogelijkheden entiteiten hebben om bezwaar te maken tegen een boetebesluit. Tevens vragen de leden hoe de hoogte van het boetemaximum is onderbouwd. Deze leden merken op dat de regering het boetemaximum bij overige overtredingen niet evenredig vindt. Kan de regering kort toelichten dat dit boetemaximum in geen geval evenredig is? Verder merken deze leden op dat entiteiten zwaar beboeten mogelijk als gevolg heeft dat, door de hoogte van de boete, de continuïteit bij een dienstverlenende entiteit in gevaar kan komen. Kan de regering toelichten hoe wordt voorkomen dat een hoge boete leidt tot haperingen in de dienstverlening?

5.6.7. Overtrederschap

De leden van de GroenLinks-PvdA-fractie merken op dat overtredingen van de Cyberbeveiligingswet kunnen leiden tot handhaving jegens individuen, zoals bestuursleden. Deze leden vragen de regering om te bevestigen of dit inderdaad het geval is, en zo ja, om te onderbouwen dat bestraffen op persoonlijke titel effectief leidt tot betere cyberveiligheid.

5.6.8. Samenwerking toezichtoudende instanties

De leden van de GroenLinks-PvdA-fractie erkennen het belang van een goede samenwerking tussen toezichthouders. Deze leden vragen aan de regering op welke wijze de samenwerkafspraken tussen toezichthouders worden vastgesteld en waar en wanneer deze worden gepubliceerd.

5.7. Registratie

De leden van de GroenLinks-PvdA-fractie hebben twijfels over de registratieplicht van de NIS2-richtlijn. Deze leden stellen dat het opbouwen van een lijst met relevante entiteiten ook leidt tot een nieuwe, gevoelige dataset. Onderschrijft de regering dat een dergelijk overzicht gevoelige informatie betreft? Zij vinden het niet duidelijk beschreven hoe de vertrouwelijke en veilige toegang tot het register door CSIRT's wordt geregeld. De regering spreekt van een «technische oplossing» die dit moet waarborgen. Welke techniek betreft dit en is deze waterdicht?

De leden van de GroenLinks-PvdA-fractie lezen dat cloudcomputing-diensten en socialenetwerkdiensten vallen onder de reikwijdte van de NIS2-richtlijn. Dit betreft echter veelal niet-Europese bedrijven die diensten verlenen aan Nederlandse en Europese instanties. Daarom vragen deze leden om helder te maken welke verplichtingen (kunnen) worden opgelegd aan bedrijven die essentiële ICT en communicatiemogelijkheden verlenen, maar niet onder Europese jurisdictie vallen. Zij vinden het gerechtvaardigd om niet-Europese bedrijven zoveel als mogelijk aan de NIS2-richtlijn te laten voldoen.

5.8. Toepassing in Caribisch deel van het Koninkrijk

De leden van de GroenLinks-PvdA-fractie zijn teleurgesteld over het niet meenemen van Caribisch Nederland onder het bereik van de Cyberbeveiligingswet. Deze leden vragen de regering om veel duidelijker te stellen waarom dit nu niet mogelijk is, en welke randvoorwaarden er nodig zijn om dit wel mogelijk te maken. Hierin achten zij het waardevol om hardop de ambitie uit te spreken dat Caribisch Nederland op termijn wordt opgenomen in de Cyberbeveiligingswet. De formulering van de regering is momenteel te vrijblijvend en leidt niet tot een verbetering van de cyberveiligheid in het Caribische deel van het Koninkrijk.

5.9. Rechtsbescherming en vereisten aan besluiten

De leden van de GroenLinks-PvdA-fractie erkennen het belang van openbaarheid over overtredingen. Echter ligt het risico van reputatieschade voor entiteiten op de loer, met nadelige effecten voor de integriteit en het vertrouwen in deze entiteiten. Deze leden benadrukken dat hiermee het ontwrichtende effect van cyberaanvallen alsnog tot uiting kan komen. Daarom horen zij graag van de regering of er scenario's zijn waarin het niet openbaren van overtredingen de voorkeur heeft.

6. Verhouding tot het hoger recht

6.1. Inleiding

6.2. Gegevensverwerkingen

De leden van de GroenLinks-PvdA-fractie lezen dat CSIRT's geacht worden om gevoelige informatie onderling uit te wisselen. Deze leden vragen de regering om een toelichting over de technische maatregelen die getroffen zullen worden om de vertrouwelijkheid van deze communicatie te waarborgen.

6.3. EVRM

6.3.1. Beperking moet legitiem doel dienen en noodzakelijk zijn

De leden van de GroenLinks-PvdA-fractie waarschuwen dat bevoegdheden die gaan over het verzamelen van gevoelige informatie aan stevige kaders gebonden moeten zijn. Dit voorkomt zogenaamde «mission creep», waarin het doel waarvoor informatie wordt verzameld en verwerkt verwatert. Deze leden vragen de regering om uit te leggen dat hier geen sprake van kan zijn.

De leden van de VVD-fractie lezen dat ter bevordering van grensoverschrijdende samenwerking het nodig is dat iedere lidstaat een centraal contactpunt aanwijst dat verantwoordelijk is voor het leggen van verbindingen op het niveau van de EU, en meer in het bijzonder het informeren van andere lidstaten in geval van incidenten van grensoverschrijdende consequenties. In Nederland is de Minister van Justitie en Veiligheid aangewezen als het centrale contactpunt. Hoe vindt dit contact nu in de praktijk plaats, door welke organisatie en wat is de huidige wettelijke grondslag daarvoor? Deze leden vragen hoe binnen het Ministerie van Justitie en Veiligheid deze taak wordt belegd, waarom hiervoor is gekozen en hoe in de praktijk overlap wordt voorkomen met andere centrale contactpunten.

6.3.1.1 Dringende maatschappelijke behoefte

De leden van de GroenLinks-PvdA-fractie vragen of de afstemming tussen vakministers en de coördinerende Minister van Justitie en Veiligheid niet zal leiden tot onnodig veel overdrachten van gevoelige data. Hierdoor ontstaan er meerdere datapunten die elk het risico op een lek kunnen vergroten. Heeft de regering passende maatregelen getroffen om in het schakelen tussen sectoren, vakministers en het centrale contactpunt geen extra risico te lopen op datalekken?

6.3.1.2 Proportionaliteit

De leden van de GroenLinks-PvdA-fractie zijn kritisch op het aanleggen van een register met IP-adressen. Deze leden vragen om een nadere onderbouwing van de noodzaak hiervan. Tevens willen zij weten welke beveiligingsmaatregelen worden genomen om dit register zo goed mogelijk te beschermen.

6.4. Avg

De leden van de GroenLinks-PvdA-fractie vragen de regering op welke wijze de Autoriteit Persoonsgegevens (AP) is betrokken bij de totstandkoming van deze paragraaf. Kan de toezichthouder zich vinden in de uiteindelijke formulering?

6.4.1. Opslagbeperking

De leden van de GroenLinks-PvdA-fractie benadrukken het belang van wettelijke bewaartermijnen. Deze leden lezen dat deze termijnen zullen aansluiten op sectorale wetgeving. Kan de regering aangeven of er wezenlijke verschillen zijn in de bewaartermijnen die gehanteerd worden in verschillende sectoren? Zo ja, zijn deze verschillende bewaartermijnen gerechtvaardigd? Zij willen weten of het hanteren van één bewaartermijn voor alle data-opslag van CSIRT's mogelijke voordelen heeft.

De leden van de GroenLinks-PvdA-fractie vinden het niet duidelijk omschreven waarom de CSIRT bijzondere persoonsgegevens moet kunnen analyseren. Deze leden vragen de regering om nader toe te lichten waarom een uitzondering van bijzondere persoonsgegevens niet mogelijk is.

7. Verhouding tot nationale regelgeving

7.1. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen welke rol de coördinerende Staatssecretaris voor Digitalisering en Koninkrijksrelaties heeft voor het naleven van de NIS2-richtlijn bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

7.2. Ministerie van Economische Zaken

De leden van de GroenLinks-PvdA-fractie wijzen er op dat mkb'ers, die in een toeleveringsketen zitten met essentiële en belangrijke entiteiten, ook beschikken over informatie die ze mogelijk een doelwit maken voor kwaadwillenden. Welke maatregelen treft de regering om dit risico te mitigeren en ook deze bedrijven weerbaar te maken?

De leden van de NSC-fractie vragen de regering op welke wijze de samenwerking tussen de Cyberbeveiligingswet en de Wet bevordering digitale weerbaarheid (Wbdw) wordt geborgd. Wordt er voorzien in een geïntegreerd meld- en toezichtkader voor organisaties die onder beide wetten vallen? Daarnaast vragen deze leden hoe wordt voorkomen dat organisaties met dubbele toezichthouders te maken krijgen en of het risico van overlappende verplichtingen voldoende wordt ondervangen.

7.3 Ministerie van Volksgezondheid, Welzijn en Sport

De leden van de GroenLinks-PvdA-fractie benadrukken dat de Inspectie Gezondheidszorg en Jeugd (IGJ) een essentiële taak heeft om de cyberveiligheid van de zorgsector te controleren. Het is echter niet duidelijk of de IGJ beschikt over de capaciteit om dit naar wens te doen. Graag vernemen zij welke extra belasting de IGJ krijgt onder de NIS2-richtlijn en of de IGJ daarin tegemoet wordt gekomen.

8. Gevolgen

8.1. Gevolgen voor burgers en bedrijven

8.1.1. Inleiding

De leden van de GroenLinks-PvdA-fractie vragen aan de regering hoe zij tot de inschatting is gekomen dat 8.100 entiteiten onder de Cyberbeveiligingswet zullen vallen. Worden deze 8.100 entiteiten op de hoogte gesteld van hun mogelijke aanwijzing als essentiële of belangrijke entiteit?

De leden van de NSC-fractie vragen de regering of uit artikel 8, eerste lid, onderdeel h, van de Cyberbeveiligingswet voldoende duidelijk blijkt dat wordt gedoeld op gemeenschappelijke regelingen als bedoeld in de Wet gemeenschappelijke regelingen. Voorts vragen deze leden of het voldoende helder is dat niet de regeling zelf, maar de bij die regeling ingestelde openbare lichamen, bedrijfsvoeringsorganisaties en gemeenschappelijke organen als entiteiten onder de Cyberbeveiligingswet vallen.

8.1.2. Zorgplicht

De leden van de GroenLinks-PvdA-fractie zijn kritisch op het feit dat de cyberveiligheidsmaatregelen in algemene maatregelen van bestuur (AMvB) worden beschreven. Deze leden vragen de regering waarom deze uitwerking in lagere regelgeving wordt gedaan en hoe daarbij de betrokkenheid van de volksvertegenwoordiging en de entiteiten zelf wordt gewaarborgd.

De leden van de GroenLinks-PvdA-fractie hebben zorgen over de hoge regeldruk voor entiteiten. Die moeten allemaal de gelegenheid hebben om zich goed voor te bereiden op de nieuwe regelgeving. Kan de regering toelichten hoe zij (potentiële) entiteiten heeft geholpen bij het treffen van voorbereidingen voor deze wet?

De leden van de CDA-fractie lezen dat voor entiteiten die niet reeds onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen de schatting is dat zij een toename van 22% aan ICT-beveiligingskosten nodig hebben om aan de zorgplicht te voldoen. Deze leden vinden dit een stevige toename. Zij vragen of de regering met een voorbeeld wil verduidelijken hoe dit er in de praktijk voor een dergelijke entiteit uitziet. De leden vragen ook of het uiteindelijke voorstel, dat op punten afwijkt, leidt tot een extra toename van kosten en zo ja, hoeveel.

8.1.3. Meldplicht

De leden van de GroenLinks-PvdA-fractie hebben vragen over twee aannames. Ten eerste vragen zij de regering om de verwachting van circa 1.000 incidenten per jaar te onderbouwen. Ten tweede vragen zij om een onderbouwing voor de gemiddelde 480 minuten die voorzien zijn voor het oplossen van een incident.

8.1.4. Overige verplichtingen

De leden van de GroenLinks-PvdA-fractie vragen aan de regering of het bijhouden van een database met domeinnaamregistraties geen onnodige cyberveiligheidsrisico's creëert. Hoe waarborgt de regering dat dit register goed is beveiligd?

8.1.5. Toezichtslasten

De leden van de GroenLinks-PvdA-fractie plaatsen een kanttekening bij de vierjaarlijkse steekproefsgewijze audit. Deze leden vragen de regering waarom deze frequentie is gekozen, en geen hogere of lagere frequentie. Het lijkt deze leden verstandig om, indien mogelijk, vaker deze audits uit te voeren.

De leden van de GroenLinks-PvdA-fractie vragen ook aan welke eisen de onafhankelijke en gekwalificeerde deskundige, die de audits uitvoert, moet voldoen. Is er sprake van één standaardmethodiek voor een audit?

8.2. Financiële gevolgen voor de overheid

De leden van de GroenLinks-PvdA-fractie zijn bezorgd over de beschikbare IT-kennis op de arbeidsmarkt en binnen de overheid. Deze leden lezen dat het aantrekken van werknemers voor de CSIRT's de schaarste en kosten verder zal verhogen. Hoe waarborgt de regering dat het inrichten van de CSIRT's niet leidt tot een verzwakking van de IT-capaciteit en -kennis waar overheidsinstanties en entiteiten over beschikken?

9. Adviezen, consulatie en uitvoerings- en handhaafbaarheidstoetsen

De leden van de ChristenUnie-fractie merken voorts op dat in de memorie van toelichting niet wordt ingegaan op het advies van het Interprovinciaal Overleg (IPO) om de uitkomsten van de impactanalyse van de provincies mee te nemen in het vervolg van het wetgevingstraject. Hoe kijkt de regering naar dit advies?

9.1. Advies AP

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen waarom bevoegde autoriteiten een bewaartermijn van 60 maanden opgelegd krijgen en de CSIRT een termijn van 12 maanden. Waaruit volgt dat dit tijdsbestek proportioneel is?

9.2. Advies ATR

De leden van de GroenLinks-PvdA-fractie vragen de regering om een onderbouwing voor de termijn van vier jaar voor de evaluatiebepaling. Deze leden begrijpen dat één jaar kortdag is, maar horen graag waarom twee of drie jaar geen opties zijn. Het is voor deze leden van belang dat we snel kunnen reageren mocht blijken dat delen van de Cyberbeveiligingswet niet naar behoren werken.

De leden van de VVD-fractie vragen naar aanleiding van het advies van het Adviescollege toetsing regeldruk (ATR) toe te lichten dat er op geen enkele wijze gekozen is voor zwaardere eisen dan de minimumvoorschriften uit de NIS2-richtlijn. Ook vragen ze de mkb-toets of de AMvB tijdig kan worden gedeeld met de Kamer en waarom niet is gekozen ook om een mkb-toets op het wetsvoorstel uit te voeren. Deze leden lezen voorts dat er handreikingen zullen worden gepubliceerd die begeleiding bieden bij de implementatie van de vereisten die de Cyberbeveiligingswet bevat. Kan de regering concretiseren hoe deze handreikingen eruit zien en toezeggen dat deze na aanname van het wetsvoorstel door de Tweede Kamer zo snel mogelijk worden gepubliceerd? Wordt hierin ook aandacht besteed aan de samenloop met de implementatie van de CER-richtlijn?

De leden van de VVD-fractie benadrukken het belang van voldoende informatie, aangezien het onderhavige wetsvoorstel, ook in samenhang met het wetsvoorstel tot implementatie van de CER-richtlijn, ervoor kan zorgen dat entiteiten onder de verantwoordelijkheid vallen van verschillende Ministers, vervolgens te maken krijgen met verschillende Computer Security Incident Response Teams (CSIRT's), verschillende toezichthouders, verschillende AMvB's en ministeriële regelingen. Dat brengt voor de uitvoerbaarheid, handhaafbaarheid, werklast en regeldruk gevolgen met zich mee. Welke aanvullende maatregelen treft de regering in aanloop naar inwerkingtreding van de twee wetsvoorstellen om zoveel mogelijk helderheid en duidelijkheid te verschaffen?

De leden van de NSC-fractie lezen dat het ATR adviseert om het nut en de noodzaak van het wetsvoorstel Cyberbeveiligingswet in de memorie van toelichting beter te onderbouwen, door te verduidelijken op welke onderdelen de bestaande wetgeving tekortschiet. Deze leden vragen de regering hoe en waar in paragraaf 2.2 van de memorie van toelichting de onderbouwing is opgenomen dat de bestaande wetgeving tekortschiet. Zij vragen de regering hierbij concrete voorbeelden te geven van bestaande lacunes die met dit wetsvoorstel worden geadresseerd.

9.3. Digitale sector

9.3.1. Database met domeinregistratiegegevens

De leden van de GroenLinks-PvdA-fractie vragen aan de regering per wanneer afspraken worden gemaakt met de sector over de procedure rondom verificatie van domeinregistratiegegevens.

9.4. Zorgplicht

De leden van de GroenLinks-PvdA-fractie uiten hun twijfel over het per AMvB vastleggen van maatregelen in het kader van de zorgplicht. Hoe zorgt de regering ervoor dat zowel de Tweede Kamer als de sector betrokken blijven bij het opstellen van deze AMvB?

9.5. Governance

De leden van de GroenLinks-PvdA-fractie vernemen graag of de onduidelijkheden rondom de definities van bestuur reeds zijn weggenomen. Bevestigen de organisaties die hier kanttekeningen bij plaatsten dat dit nu voldoende duidelijk is?

9.6. Meldplicht

De leden van de GroenLinks-PvdA-fractie vernemen graag van de regering aan welke randvoorwaarden voldaan moet worden om één meldportaal in te richten voor verschillende wetgeving. Is dit volgens de regering wenselijk?

9.7. Handhaving

De leden van de GroenLinks-PvdA-fractie lezen dat toezichthouders een afwegingskader zullen hanteren voor het inzetten van hun handhavingsmaatregelen. Op welke wijze wordt deze vastgesteld en gepubliceerd? Deze leden hechten belang aan tijdige openbaarmaking van de afwegingskaders, om de rechtszekerheid van entiteiten te vergroten.

9.8. Overige opmerkingen

De leden van de GroenLinks-PvdA-fractie merken op dat er bezwaren zijn gemaakt tegen het gebrek aan een uitvoeringstoets naar het Cyberbeveiligingsbesluit. Daarmee blijven de gevolgen van de praktische uitwerking van de Cyberbeveiligingswet ongewis. Kan de regering toezeggen alsnog een nadere uitvoeringstoets uit te voeren, zodat entiteiten en medeoverheden meer zekerheid hebben vooraf aan de inwerkingtreding van de Cyberbeveiligingswet en het daarbij behorende besluit?

9.9. Advies Raad voor de rechtspraak

De leden van de VVD-fractie vragen of de regering nader kan toelichten waarom is gekozen voor concentratie van beroepszaken bij de rechtbank Rotterdam voor de gezondheidszorgsector, terwijl dat in andere sectoren niet het geval is? Deze leden vernemen graag een reactie van de regering.

10. Overgangsrecht en inwerktreding

De leden van de CDA-fractie vragen waarom het advies van het ATR om één jaar na invoering een invoeringstoets uit te voeren niet is overgenomen. Deze leden vragen of de regering deelt dat een evaluatie na vijf jaar iets anders is dan een invoeringstoets. Zij vragen tevens of de regering deelt dat een invoeringstoets van meerwaarde is, gezien de complexe aard van de wet en de aanzienlijke administratieve lasten die de wet met zich mee brengt.

II. ARTIKELSGEWIJZE TOELICHTING

Artikel 3

De leden van de GroenLinks-PvdA-fractie vragen de regering om de afweging te duiden tussen het vastleggen van maatregelen per AMvB, in plaats van deze wettelijk vast leggen. Welke voor- en nadelen heeft deze werkwijze?

Artikel 5

De leden van de GroenLinks-PvdA-fractie vragen de regering of de uitgezonderde organisaties momenteel voldoen aan een adequate mate van beveiliging. Deze leden benadrukken dat de cyberveiligheid van deze organisaties van essentieel belang is en dat een hoog niveau van veiligheid betracht moet worden.

Artikel 4, eerste lid

De leden van de NSC-fractie lezen in artikel 4.1 dat sectorale regels geregeld kunnen worden via AMvB's. Deze leden vragen de regering hoe wordt gewaarborgd dat sectorale regels die via AMvB's worden vastgesteld op een transparante en toegankelijke wijze tot stand komen. Zij vragen daarnaast hoe betrokken organisaties invloed kunnen uitoefenen op de totstandkoming van sectorspecifieke verplichtingen. Tevens vragen zij hoe de regering voorkomt dat grote verschillen ontstaan in uitvoerbaarheid en proportionaliteit tussen sectoren.

Artikel 11

De leden van de GroenLinks-PvdA-fractie vragen de regering of zij heeft overwogen de bevoegdheid tot het benomen van essentiële entiteiten binnen het hoger onderwijs bij de Minister van Justitie en Veiligheid te beleggen.

Artikel 11 & 13

Deze artikelen bevatten een grondslag voor de Minister van Onderwijs, Cultuur en Wetenschap (OCW) om via een besluit of een regeling het hoger onderwijs onder de werking van de Cyberbeveiligingswet te brengen. De oud-minister van OCW heeft in het voorjaar van 2025 al aangekondigd gebruik te maken van deze regeling. De leden van de NSC-fractie vragen de regering waarom het hoger onderwijs niet direct in

de wet is opgenomen als sector onder de werking van de Cyberbeveiligingswet. Zij vragen of overwogen is om het hoger onderwijs wettelijk als essentiële entiteit aan te merken, gezien de eerder aangekondigde voornemens van de Minister van OCW.

Artikel 14

De leden van de GroenLinks-PvdA-fractie vragen de regering of de NCSC beschikt over voldoende capaciteit en kennis om hun taken naar behoren uit te voeren. Weegt de capaciteit van het NCSC mee in de keuze om vakministers verantwoordelijk te maken voor hun eigen sectoren, in plaats van de Minister van Justitie en Veiligheid?

Artikel 16

De leden van de GroenLinks-PvdA-fractie vragen de regering welke gevolgen artikel 16 heeft op de bestaande schakelorganisaties, de zogenaamde «OKTT»-organisaties. Het is hen onduidelijk hoe de Cyberbeveiligingswet de bewezen effectieve manier van samenwerking met OKTT's beïnvloedt. Ziet de regering de mogelijkheid om de werkzaamheden van OKTT's door te zetten en in te passen in het regime dat voortvloeit uit de Cyberbeveiligingswet? De leden vragen om zo snel mogelijk inzicht te bieden in welke organisaties als «relevante partijen» worden aangewezen per AMvB.

De leden van de NSC-fractie lezen dat op grond van de Wbni bepaalde organisaties zijn aangewezen als partijen met een objectief kenbare taak (OKTT) om andere organisaties of het publiek te informeren over dreigingen en incidenten betreffende netwerk- en informatiesystemen, of als CSIRT. Deze leden willen de regering vragen om uiteen te zetten waarom deze aanwijzingen met de Cyberbeveiligingswet worden ingetrokken. Welke belemmeringen ziet de regering om de deling van dreigings- en incidentinformatie via OKTT's te continueren?

Ook vragen de leden van de NSC-fractie of de regering erkent dat informatiedeling een belangrijke preventieve werking heeft en daarom zo proactief mogelijk moet plaatsvinden, ongeacht of de betrokken partijen onder de Cyberbeveiligingswet vallen. Is de regering zich ervan bewust dat het schrappen van de OKTT-status het proactieve karakter van informatiedeling voor een belangrijke doelgroep ontneemt? Acht de regering het, vanuit het perspectief van robuustheid, verstandig om bestaande structuren voor informatiedeling te behouden? Kan de regering toelichten onder welke voorwaarden organisaties die op grond van de Wbni als OKTT zijn aangewezen, kunnen worden aangemerkt als «relevante partij»? Welke definitie hanteert de regering voor «relevante partij»? Waarom is er niet voor gekozen om wettelijk vast te leggen dat bestaande OKTT's altijd als «relevante partij» kwalificeren? Waarom is ervoor gekozen om de kwalificatie-eisen voor «relevante partij» niet nader te specificeren in een AMvB?

De leden van de NSC-fractie vragen de regering om nader toe te lichten waarom niet is gekozen om de Wbdw zodanig te wijzigen dat OKTT's dreigings- en incidentgegevens van het NCSC kunnen blijven ontvangen, zodat zij hun informatievoorzienende rol richting het mkb kunnen blijven vervullen?

De leden van de D66-fractie vragen of de regering kan aangeven op welke manier zij uitvoering gaat geven aan artikel 16, tweede lid, onderdeel e en artikel 16, derde lid over het proactief en niet-intrusief scannen van

netwerk- en informatiesystemen met het oog op het opsporen van kwetsbare of onveilig geconfigureerde systemen.

De leden van de D66-fractie constateren dat de bestaande aanwijzing van organisaties die objectief kenbaar tot taak hebben om dreigingsinformatie te delen (OKTT's) vervalt en wordt vervangen door de categorie «relevante partijen». Deze leden vragen op welke gronden besloten is de OKTT-systematiek los te laten, welke criteria gelden exact voor aanwijzing als «relevante partij», waarom er niet voor is gekozen bestaande OKTT's bij wet automatisch onder deze nieuwe categorie te laten vallen en waarom er niet voor is gekozen de eisen voor «relevante partijen» bij AMvB te definiëren, zodat vooraf helder is wie kwalificeert? Is de regering zich ervan bewust dat door de OKTT-status te schrappen, het proactieve karakter van informatiedeling voor een doelgroep komt te vervallen?

Artikel 19

De leden van de GroenLinks-PvdA-fractie vragen de regering of er, door de spreiding van verantwoordelijkheden over vakministers, aanleiding is om ook Cyberbeveiligingsstrategieën per sector vast te stellen, bovenop de nationale strategie.

Artikel 21

De leden van de GroenLinks-PvdA-fractie achten de bevoegdheid om entiteiten op te dragen om specifieke leveranciers te weren een zwaar middel. De proportionaliteit van deze maatregel vraagt om een zorgvuldige uitwerking en toelichting over hoe, wanneer en waarom de regering over zou gaan tot deze beslissing. Kan de regering een scenario schetsen waarin deze bevoegdheid wordt ingezet? Deze leden sporen de regering aan om dit de verduidelijken en begrenzing van dit artikel zo snel mogelijk per AMvB vast te leggen, zodat helderheid bestaat over de bedoeling en handhaving van dit artikel.

Artikel 33

De leden van de GroenLinks-PvdA-fractie vragen de regering of meldingen in het kader van artikel 33 op dezelfde manier verlopen als bij artikelen 25 t/m 29.

OVERIG

De leden van de VVD-fractie vinden het belangrijk dat er in de praktijk geen verdere versnippering plaatsvindt bij zelfstandige bestuursorganen zoals toezichthouders naar aanleiding van de implementatie van het wetsvoorstel. Welke maatregelen neemt de regering om in de praktijk overlapping en versnippering tussen taken en bevoegdheden van toezichthouders te voorkomen, en welke afspraken zijn er al gemaakt tussen toezichthouders in aanloop naar de indiening van het wetsvoorstel en welke afspraken worden er in de komende periode hierover nog gemaakt? Wie is verantwoordelijk voor het toezicht op de naleving van het maken van afspraken tussen toezichthouders onderling?

De leden van de NSC-fractie vragen de regering waarom in de toelichting bij het wetsvoorstel beperkt aandacht wordt besteed aan het grensoverschrijdende karakter van cyberdreigingen. Deze leden vragen welke wettelijke ruimte er is om dreigings- en incidentinformatie te delen met buitenlandse (niet-EU) CERT's, multilaterale partners zoals de NAVO, en private samenwerkingspartners.

De leden van de NSC-fractie vragen de regering hoe wordt gewaarborgd dat Nederland bij internationale cyberincidenten snel en effectief kan schakelen met relevante partijen buiten de EU. Deze leden vragen tevens hoe de aansluiting wordt geborgd met niet-EU-certificeringsinstanties, internationale normenkaders en buitenlandse CERT's.

De leden van de CDA-fractie hebben nog enkele vragen over het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten. Deze leden vragen of de regering kan aangeven wat de reden is geweest om de interventiebevoegdheid van vakministers – om aan bedrijven de verplichting op te leggen om producten of diensten van specifieke leveranciers te weren dan wel te verwijderen – te introduceren in een AMvB.

De leden van de CDA-fractie vragen waarom de regering dit onderdeel heeft toegevoegd na de internetconsultatieronde, waardoor het bedrijfsleven hier geen zienswijze op heeft kunnen geven. Deze leden vragen op welke manier overleg en informatievoorziening tussen de vakministers en het bedrijfsleven geborgd is met de voorgestelde interventiebevoegdheid. Zij vragen wat het effect is op de eisen die zijn gesteld rondom het opmaken van een risicoanalyse. Verder vragen zij of de regering kan ingaan op de wijze waarop de interventiebevoegdheid kan worden ingezet en wat de eisen hiervoor zijn.

De leden van de CDA-fractie vragen of het in lijn is met de wettelijke waarborgen om de interventiebevoegdheid onder te brengen in een AMvB, in plaats van in het wetsvoorstel zelf. Deze leden vragen of de regering in dat licht ook kan reflecteren op artikel 21 van de Cyberbeveiligingswet en artikel 15 van de Wwke.

De voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller