
Bevordering digitale weerbaarheid bedrijven

Bevordering digitale weerbaarheid bedrijven

Aan de orde is de behandeling van:

- **het wetsvoorstel Regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven) (36270).**

De **voorzitter**:

Aan de orde is de behandeling van de Wet bevordering digitale weerbaarheid bedrijven. Ik heet de minister van Economische Zaken weer van harte welkom. Dat geldt ook voor de leden en de mensen die het debat bekijken, hier of elders. We hebben van de zijde van de Kamer vier sprekers. Het is een heugelijke dag voor mevrouw Van Meetelen, want zij gaat als laatste spreken en houdt dan haar maidenspeech. Maar ze is ook nog jarig vandaag, heb ik begrepen. Ik feliciteer haar dus alvast van harte met haar verjaardag.

Ik ben van plan om de eerste termijn te doen voor de dinerpauze. Dan gaan we drie kwartier schorsen. Er kan dan gegeten worden, maar de minister zal dan haar best moeten doen om de antwoorden voor te bereiden die zij in de termijn na de dinerpauze gaat geven.

De algemene beraadslaging wordt geopend.

De **voorzitter**:

Als eerste is het woord aan de heer Six Dijkstra, die namens Nieuw Sociaal Contract het woord gaat voeren. Gaat uw gang.

De heer **Six Dijkstra** (NSC):

Voorzitter. De fractie van Nieuw Sociaal Contract staat positief tegenover dit wetsvoorstel. Het is zinvol dat het Digital Trust Center, het DTC, wettelijk verankerd wordt en dat overheden en het bedrijfsleven dreigings- en incidentinformatie kunnen uitwisselen. Dit lijkt onze fractie een goede manier voor de overheid om bij te dragen aan de digitale veiligheid van het Nederlandse bedrijfsleven. Daarbij hebben we nog wel enkele vragen aan de minister.

De weerbaarheid van Nederland is niet alleen een sectoraal vraagstuk, maar ook een nationaal vraagstuk. We zien een risico dat de verantwoordelijkheid van de Nederlandse digitale weerbaarheid te versnipperd is. Dit vraagstuk gaat verder dan deze wet, maar de wet laat wel een klein pijnpunt zien. Het Nationaal Cyber Security Center heeft als doelgroep vitale bedrijven en het DTC heeft als doelgroep niet-vitale bedrijven. Op termijn zullen deze instanties in enige vorm samengevoegd worden. Wat zal de samenvoeging doen met de verantwoordelijkheid van de twee betrokken ministers? Dat betreft de minister van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid. In een eerdere brief is vermeld dat de minister van JenV eigenaar wordt van de nieuwe organisatie, maar daarbij blijft de minister van EZK wel medeopdrachtgever. Betekent dit dat de minister van EZK ook opdrachten kan geven met betrekking tot vitale

bedrijven of alleen met betrekking tot de niet-vitale bedrijven, die voorheen onder het DTC zouden vallen?

Daar komt bij dat: "De vakministers, in navolging van de Wbni, verantwoordelijk blijven voor het stellen van eisen aan en het toezicht op de naleving daarvan door niet-vitale aanbieders in onder hen vallende branches en sectoren." Wij vrezen dat deze verkokering als algehele trend maakt dat onder de streep niemand binnen de overheid eindverantwoordelijk is voor de digitale weerbaarheid van Nederland. Voor iedere sector en branche gelden andere toezichthouders, die ieder weer andere eisen stellen aan cyberveiligheid en op een andere manier handhaven. In het domein van de digitale weerbaarheid bestaat een grote onderlinge afhankelijkheid, bijvoorbeeld in de supplychains. Problemen in de ene sector zijn vaak ook relevant in de andere sector. Juist daarom is het zo belangrijk dat er een algemeen beeld is van de digitale weerbaarheid in alle sectoren en in de hele samenleving. Wij zijn benieuwd hoe de minister hiertegen aankijkt. Is zij het met Nieuw Sociaal Contract eens dat de verkokering van de verantwoordelijkheid voor de Nederlandse digitale weerbaarheid een risico is? Hoe wil zij voorkomen dat er onnodig met verantwoordelijkheid wordt geschoven?

Verder staat in de memorie van toelichting benoemd dat in voorkomende gevallen ook Indicators of Compromise, oftewel IoC's, gedeeld kunnen worden. Hierbij is bijvoorbeeld te denken aan IP-adressen of domeinnamen van hackerinfrastructuur. Hierop kunnen bedrijven gericht actie ondernemen. Is de minister voornemens om dit frequent te doen? Worden alle IP-adressen en domeinnamen als persoonsgegevens behandeld? Heeft het al dan niet behandelen van IoC's als persoonsgegevens nog invloed op de uitvoering en wettelijke waarborgen? En, tot slot, welk type persoonsgegeven kan onder deze wet nog meer gedeeld worden? Kunnen hier persoonsgegevens van derden, zijnde Nederlandse burgers, tussen zitten?

Ik zie uit naar de beantwoording van de minister. Dank u wel.

De voorzitter:

Dank u wel. Dan is het nu het woord aan mevrouw Martens-America. Zij voert het woord namens de VVD. Gaat uw gang.

Mevrouw Martens-America (VVD):

Voorzitter, dank. De VVD-fractie is groot voorstander van deze wet. De fractie vraagt hier al lang naar, net als veel bedrijven. Ik wil dan ook beginnen met dankwoorden voor de minister voor het ons voorleggen van deze prachtige wet. Want veel bedrijven, hardwerkende ondernemers, hebben dagelijks last van cyberaanvallen. Onze bedrijven en ondernemers, die in steeds grotere mate digitaal werken en waarvan wij vragen dat ze in steeds grotere mate digitaal werken, zijn voor venijnige cybercriminelen zeer aantrekkelijk om geld van af te troggelen. Niet alleen onze grote bedrijven hebben in steeds grotere mate te maken met cyberdreigingen, maar ook onze mkb'ers. Denk aan autogarages of de kapper om de hoek. Zij zijn doelwit voor criminelen, omdat ze doorgaans minder capaciteit in huis hebben om de digitale voordeur gesloten te houden. Dat maakt niet alleen onze individuele persoonsgegevens of de ondernemer in kwestie heel kwetsbaar, maar het raakt ook onze hele economie, want door succesvolle cyberaanvallen vloeien jaarlijks tientallen miljoenen euro's weg. Het raakt ons dus

simpelweg allemaal. Door de digitalisering en de toenemende vervlechting van systemen vervagen fysieke grenzen. Het is gewoon een nieuw fenomeen. Een cyberaanval op een ogenschijnlijk onschuldig mkb-bedrijf kan daardoor zorgen voor problemen bij een vitaal bedrijf of bij bijvoorbeeld energievoorzieningen. Een goede structurele informatiedeling is wat mijn fractie betreft dus randvoorwaardelijk voor het versterken van de hele keten.

Ik heb nog wel drie verhelderende vragen aan de minister. Eén. Wanneer het NCSC en het DTC ruimte krijgen om niet-vitale organisaties te informeren over digitale dreigingen, waar komt dan de verantwoordelijkheid uiteindelijk te liggen, ook als het bijvoorbeeld gaat over de timing van de informatiestroom richting deze bedrijven? Ik wil graag een lans breken voor één nationaal cyber protection team, waarin het NCSC en het DTC de krachten bundelen en fysiek gaan samenwerken in één gebouw. Nu weet ik dat de minister daar op dit moment druk mee is, maar ik hoor ook dat dat misschien nog wel jaren zou kunnen duren. Misschien kan de minister ons daar iets over vertellen en ook over hoe we dat zouden kunnen versnellen.

Tot slot ontslaat de komst van deze wet mkb'ers niet van hun primaire verantwoordelijkheid om hun digitale huishouding op orde te hebben. Mkb'ers zullen dus ook zelf verantwoordelijk blijven voor de preventie van digitale aanvallen. De VVD merkt echter dat de digitalisering van het mkb achterblijft en dat hier gewoon simpelweg niet altijd prioriteit aan wordt gegeven, omdat ook de mankracht er niet is. Welke rol ziet de minister voor haarzelf in het omhoog krijgen van het digitaliseringsniveau?

Dank u wel.

De **voorzitter**:

Hartelijk dank voor uw inbreng. Dan is het woord aan mevrouw Kathmann. Zij gaat het woord voeren namens de fractie GroenLinks-PvdA. Gaat uw gang.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Ik wil als eerste tegen de minister zeggen dat er een mooie wet voorligt, maar daar ga ik het niet bij laten. Het is geen kwestie van of, maar van wanneer. Dat is wat ik het meeste hoor als ik met ethisch hackers of ondernemers over digitale inbraken praat. Waar het een paar jaar geleden nog uren duurde voor een prima wachtwoord gekraakt was, gebeurt dat nu binnen een paar seconden. De hoeveelheid cyberaanvallen neemt jaarlijks toe. Het slachtofferschap van onlinecriminaliteit in Nederland is sinds 2012 met 22% toegenomen. De economische schade voor ondernemers neemt eveneens toe. Jaarlijks gaan er miljarden euro's verloren door digitale criminaliteit. Het liefst zou je alle lekken dichten en tien lagen beveiliging op elk IT-systeem inbouwen, maar dit zijn gevaren waar je niet altijd beleid op kan schrijven. Het wetsvoorstel is duidelijk over de rol die ondernemers zelf moeten oppakken en dat voelen zij ook. Het mkb heeft keer op keer bewezen hoe innovatief, weerbaar en gemotiveerd ze te werk gaan. Laat dat dus ook vooral aan hen.

Maar toch blijft cyberveiligheid een ondergeschoven kindje, want je hoort steeds vaker "mij zal het toch niet overkomen" of "heb ik wel wat te verbergen?" Bovendien zijn het weer extra kopzorgen voor ondernemers, dus is het logisch dat dat veiligheidsbeleid soms toch even blijft liggen. De insteek van deze wet is daarom ook goed. De overheid

kan en zal geen wonderen verrichten, maar gaat hooguit belangrijke informatie op tijd verstrekken. Het is aan bedrijven om daarmee te doen wat zij goedvinden en wat past bij hun bedrijf. Dat neemt niet weg dat het absoluut noodzakelijk is dat iedereen cyberveiligheid tussen de oren krijgt. Het kan je duizenden of zelfs honderdduizenden of miljoenen euro's kosten als het fout gaat. Of het kost je bedrijf gewoon de kop. Misschien is je bedrijf op zichzelf geen groot doelwit, maar werk je samen met een grote leverancier, afnemer of een lokale overheid. En opeens ben je een schakel in een groter geheel. Als jouw onderneming ten onder gaat, raakt dat een ander, gevoeliger doelwit ook. Dit is een vorm van maatschappelijke ontwrichting die voor kwaadwillende hackers maar al te aantrekkelijk is.

We zijn steeds meer verweven met elkaar in lange productieketens via talloze digitale kanalen en nog meer. Klantgegevens zijn goud waard en moeten ook als zodanig bewaakt worden. Een ransomwareaanval treft dan ook meer dan alleen het bedrijf. Ook het vertrouwen van de klant wordt geschaad en hun gegevens belanden op straat. Die verantwoordelijkheid doorleven ondernemers ook. Er is een waslijst aan maatregelen die je kan nemen: lange wachtwoorden, dubbeling op dubbeling van je bedrijfs-IT, regelmatige pentests en tweestapsverificatie. Doe dat ook als het kan. Het is net zo belangrijk als het installeren van je buitenverlichting, het slot op je deur of het leeghalen van je kassa's na een drukke dag. Maar het is nooit een totaaloplossing, want één menselijke fout kan al je goede intenties tenietdoen. Eén verkeerd mailtje, geopend op vrijdagmiddag rond een uurtje of vijf, vlak voor de borrel, en de indringer is binnen. Vervolgens heeft die het hele weekend de tijd om je leeg te roven.

Alle snuffjes om je bedrijf digitaal te versterken kunnen niet op tegen de menselijke factor. We zijn allemaal mensen; geloof het of niet. Die maken gewoon weleens een foutje. Dat doe ik ook; geloof het of niet. Toch zit er nog heel veel schaamte bij het melden van een digitaal ongeluk. Het wordt al snel een schuldvraag. Voor wie wil melden dat hij misschien op een verdacht linkje heeft geklikt, is het niet altijd duidelijk bij wie je kan melden. Een open sfeer op de werkvloer is dus nodig. Het gevoel van "je bent een held als je meldt" moet ook steeds meer doorklinken. Maar de grootste winst voor een digitaal weerbaar mkb zit 'm vooral in de bewustwording. Daarom het volgende.

We kennen allemaal wel de bedrijfshulpverlener, de bhv'er. Die kan geen gebouw blussen als het in de fik staat, maar een brandje in een prullenbak misschien wel. Een levensreddende operatie kan de bedrijfshulpverlener ook niet, maar de aed bedienen kan hij wel. Het is vaak iemand die mensen op de werkvloer kennen, vertrouwen en om hulp vragen bij een ongeluk. Daarom ben ik enorm gecharmeerd van de enige echte digitalehulpverlener. Een echt topidee is dat van sommige spelers uit de securitybranche: de zogenaamde dhv'er. In plaats van dat iedereen een beetje verantwoordelijk is, wordt iemand aangewezen als vast aanspreekpunt voor digitale ongelukken in een bedrijf. Diegene kan zichzelf opleiden en zich een uurtje of twee per week eigenaar maken van de digitale weerbaarheid. Diegene is dan het aanspreekpunt voor z'n collega's, staat in contact met de IT-afdeling of met de IT-experts op afstand en rapporteert aan het bestuur of de baas. Je bent dan misschien geen expert — dat vraagt ook niemand van je — maar je bent wel de eerste die kan inspringen als er een noodgeval is. Is de minister bekend met het concept dhv'er? Wat vindt zij ervan? Weet zij hoeveel bedrijven zo iemand hebben aangewezen? Wil zij dat aantal vergroten?

Mevrouw **Martens-America** (VVD):

Laat ik beginnen met het volgende. Ik vind het idee heel sympathiek. Ik probeer nu te zoeken naar een oplossing. Wat mensen die uit een mkb-onderneming komen weten, is dat ook het bhv-aspect als het gaat om extra regelgeving soms echt een nachtmerrie kan zijn als je een heel klein bedrijf hebt. Er moet altijd iemand aanwezig zijn en mensen moeten zich elk jaar bijscholen. Dat is niet zo makkelijk. Hoe ziet mijn collega van GroenLinks-Partij van de Arbeid dit voor zich qua uitvoering? Moet dit wettelijk verankerd worden? Wordt dit iets waar we op gaan sturen en waar we mensen ook voor kunnen beboeten? Ik ben benieuwd naar de uitvoering hiervan.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dat is een hele goede vraag. Ik ben het er ook helemaal mee eens dat die bhv af en toe ongelofelijk complex kan zijn, zeker als je een kleine ondernemer bent. Ik weet daar zelf alles van vanuit mijn eigen ervaring. Zo willen we het met die dhv'er niet aanpakken. Daarom zei ik ook: het is een idee vanuit de securitybranche zelf. Het is vooral bedoeld voor hele concrete bewustwording op de werkvloer, als je ziet dat je daar als ondernemer wel een mogelijkheid toe hebt. Dus leg het niet vast in de wet. Je kunt wel vastleggen dat je bijvoorbeeld als overheid in je communicatiekanalen het bedrijfsleven stimuleert en iedereen op de hoogte brengt van het bestaan van zo'n dhv'er, van dat ene aanspreekpunt. Het bekt lekker en het is concreet. We weten allemaal — dat laten de cijfers ons zien — dat stimuleren op een vage manier niet altijd helpt. Hoe concreter, hoe beter. Dan kunnen we allemaal stappen zetten om de miljarden aan economische schade waar mkb'ers mee te maken hebben en de kapotte bedrijven tot een minimum te beperken.

De **voorzitter**:

Mevrouw Kathmann vervolgt haar betoog.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Is de minister bekend met het dhv'er-concept? Die vraag had ik al gesteld. Wil zij het aantal vergroten? Kan zo'n dhv'er zich ergens aanmelden om gericht aangesproken te worden door het Digital Trust Center? Het hoeft een bedrijf namelijk amper iets te kosten, maar het kan de eerste stap zijn om digitale ongelukken op de werkvloer bespreekbaar te maken.

Dan de verantwoordelijke overheid. Ondernemers staan er niet alleen voor. De overheid heeft wel een rol, maar moet die duidelijk voor zichzelf en voor ondernemers afkaderen. Het lijkt me bijvoorbeeld goed om het vergroten van het aantal aangewezen digitalehulpverleners wel expliciet een doel in overheidsbeleid te maken, bijvoorbeeld in de Strategie Digitale Economie. Maar leg het bepalen van de manier waarop je dat voor elkaar krijgt in de handen van ondernemers. Zoiets kunnen we niet per motie opleggen. Zet een concreet doel als stip op de horizon en daag ondernemers uit om dat te bereiken. Help ze vervolgens waar dat nodig is. Zo zet je het mkb in eigen kracht en blijft de overheid een dienstbare partner in plaats van een schoolmeester.

Ik heb een aantal vragen. Denkt de minister dat het aantal fte en het budget van het DTC voldoende is om alle taken zoals die zijn neergelegd goed te verrichten en deze 24/7 optimaal uit te voeren? Zo ja, waar baseert de minister die veronderstelling op? Zo nee, is de minister bereid om meer budget vrij te maken? Zo niet, waarom niet?

Dan een vraag over het onderscheid tussen vitaal en niet-vitaal, waar al heel veel over gezegd is. In de digitale infrastructuur is alles natuurlijk volledig met elkaar verweven. Een hack bij een niet-vitaal bedrijf kan grote gevolgen hebben voor een vitaal bedrijf. Toch blijft de harde knip overeind: NCSC richt zich op vitaal en DTC richt zich op niet-vitaal. Met welke argumenten onderbouwt de minister de wenselijkheid van deze harde knip? Moet er niet gekeken worden naar een ander onderscheid? Wat vindt de minister van het voorstel van Cyberveilig Nederland om bijvoorbeeld te kijken naar het cybersecurityvolwassenheidsniveau?

Dan de vraag wat er nou precies in de wet is geregeld. Worden bedrijven ook geïnformeerd over mogelijke dreigingen, dus dreigingen die nog niet zijn vastgesteld? Zit in de taakstelling van het DTC ook dat de medewerkers bij het communiceren en adviseren een duidelijk handelingsperspectief geven? Er worden al digitale weerbaarheidstrainingen gegeven; daar zitten ook hele goeie tussen, maar die digitale weerbaarheidstrainingen zijn vaak best duur voor ondernemers, zeker als ze meerdere werknemers op pad willen sturen om deel te nemen aan zo'n training. Hoeveel mag een weerbaarheidstraining maximaal kosten van de minister? Wat doet de minister eraan om deze trainingen laagdrempelig beschikbaar te houden voor het mkb?

Ik kondig alvast aan — vorige week heb ik ook al gezegd dat dat geen dreigingen zijn maar een soort aankondigingen — dat ik drie moties heb klaarliggen. Eentje is bedoeld om het aantal dhv'ers bij bedrijven omhoog te krikken en om hen gericht op weg te helpen om hun taken te vervullen. Er is ook een motie die erop gericht is om het budget voor het Digital Trust Center te laten meegroeien met de hoeveelheid cyberbedreigingen in de komende jaren. Dan is er nog eentje om goeie nazorg te regelen voor werknemers en werkgevers die getroffen zijn door een cyberaanval. Je ziet nu namelijk heel vaak in die nazorg dat, ook als je de werknemer bent die op dat linkje heeft geklikt, de schuldvraag heel vaak aan de orde komt. Soms is er ook gewoon een hulpvraag waarbij juridisch advies nodig is. Hetzelfde geldt voor ondernemers die slachtoffer zijn van een cyberaanval. Vaak komen er heel veel juridische aspecten aan te pas en soms ook gewoon een beetje slachtofferhulp. Hoe ziet de minister eigenlijk die nazorg, waar is die geregeld en wat kan het DTC daarin betekenen?

Laat ik dan afsluiten met een mooie metafoor die ik gister hoorde van een gehackte ondernemer. Hij zei dat we de digitale infrastructuur als een snelweg moeten zien. In de jaren dertig legden we snelwegen aan en pas zo'n dertig jaar later kwamen we met wetgeving om alcohol achter het stuur te verbieden en gordels te verplichten. Toen nam het aantal verkeersslachtoffers drastisch af. Zo is dat nu ook met digitale infrastructuur. Laten we het ondernemers dan zo makkelijk mogelijk maken om hun gordels vast te klikken en zelf vangrails aan te leggen waar het kan. Voor een bedrijf kan dat, net als op de weg, van levensbelang zijn.

De voorzitter:

Hartelijk dank voor uw inbreng. Tot slot van de termijn van de zijde van de Kamer is het woord aan mevrouw Van Meetelen. Zoals ik al aankondigde zal zij haar maidenspeech houden en ik wens haar daar veel succes mee. Zij spreekt namens de PVV.

Mevrouw **Van Meetelen** (PVV):

Dank u, voorzitter. Goedenavond allemaal, iedereen hier aanwezig in de zaal, op de publieke tribune en iedereen die thuis kijkt. Wat een cadeau om op je verjaardag je maidenspeech te mogen houden!

Voorzitter. 1.000 jaar, de geschiedenis van de kermis gaat hier in Nederland al 1.000 jaar terug. Dat vieren wij uitgerekend dit jaar. Het waren 1.000 jaar van ontwikkeling waarin de kermis de voorloper is geweest van vele zaken, zoals de bioscoop en de theaters. De kermis stond aan de wieg van de dierentuinen en het circus. 1.000 jaar werden cultuur en tradities doorgegeven, zoals het rondreizende bestaan van het wonen in een wagen en het voortzetten van familiebedrijven. Ik ben er dan ook enorm trots op dat mijn oudste zoon — ik heb twee zonen — samen met mijn partner ons familiebedrijf voortzet, net als ik dat met mijn ouders heb gedaan. Kermisfamilies zijn vaak vele generaties terug te herleiden, zoals die van mijn partner, die al de achtste generatie poffertjesbakker is. Van sommige andere families zijn tot wel twaalf generaties terug te vinden, en dat koesteren wij als gemeenschap. Ik zeg "wij", want ook al sta ik hier nu als Tweede Kamerlid voor de grootste partij van Nederland, de PVV, ik zal altijd onderdeel blijven uitmaken van die gemeenschap waarin familie en vrienden altijd vervlochten zullen zijn door die gemeenschappelijke achtergrond: het kermisleven.

Voorzitter. Als kind opgroeien op de kermis is fantastisch. Kermiskinderen spelen immers op de kermis en welk kind wil dat nu niet? Ik heb dan ook een geweldige jeugd gehad met heel veel vriendjes op de winterschool, die jaloers waren dat wij nog een tweede school hebben en nog wel één op wielen: de Rijdende School. Deze school is uniek in zijn werkwijze en innovatie. Nergens ter wereld bestond er een rijdende school toen die in Nederland opgezet werd: een meereizende school voor kermis- en later ook circuskinderen, een voorbeeld voor inmiddels meerdere landen in Europa. Door een jarenlange expertise in afstandsonderwijs zijn ze in de coronaperiode voor winterscholen van ongekende waarde geweest voor het opzetten en implementeren van afstandsonderwijs. Een prachtig instituut!

Voorzitter. Mijn ouders en overigens ook ikzelf hebben als kermisondernemers verschillende zaken gehad. Op enig moment kochten zij een poffertjessalon en besloten zij om poffertjes in Limburg en Brabant aan de man te gaan brengen. Hier zijn ze echte pioniers in geweest, want op een paar grote gemeenten na had niemand ooit een poffertje gegeten in het mooie zuiden. Poffertjes zijn een typische kermislekkernij. Een goed poffertje bakken is echt een ambacht en kijken naar dit proces is een lust voor het oog. Het is een ambacht dat gekoesterd moet worden.

Voorzitter. Altijd reizen, altijd onderweg en toen ineens, op 12 maart 2020, vandaag exact vier jaar geleden, ook toen mijn verjaardag, kreeg heel Nederland te horen dat het land op slot ging. Dus geen start van ons seizoen, geen inkomen, niets. Een periode van financiële onzekerheid; angst voor onze toekomst maakte zich van ons meester. Ik kon daar niet bij blijven zitten wachten. Niet alleen ik, onze hele gemeenschap roerde zich en verenigde zich om op elke mogelijke wijze bij de politiek duidelijk te maken dat wij perspectief moesten krijgen en toch zeker financiële ondersteuning. Die kwam er ook, maar niet voor iedereen en niet voldoende, want er werd verschillend gekeken naar de SBI-codes bij de RVO, wat resulteerde in grote verschillen in de mate van steun en in sommige schrijnende gevallen in helemaal niets. Als kermisgemeenschap hebben wij

ettelijke acties ondernomen. Uiteindelijk vonden we daardoor in de Tweede Kamer gehoor en werd er met onze branche gesproken. Dit gaf mij een goed gevoel; dat je voor en met anderen iets voor elkaar kan betekenen en iets kan doen in het algemeen belang. Het vertegenwoordigen van mijn branche en het helpen zoeken naar oplossingen voor medeondernemers maakte dat ik mij steeds verder ging verdiepen in dossiers en de politiek daarachter.

De coronaperiode heeft mij het laatste zetje gegeven om de stap te wagen in de politiek. Ik kwam eerst op de lijst van de PVV Noord-Brabant voor de Provinciale Statenverkiezingen, alwaar ik geen zetel bemachtigde. Een paar maanden later, na vele gesprekken met mijn gezin over de vraag of ik het zou wagen, solliciteerde ik voor de Tweede Kamer. Vanaf dag één hebben ze achter mij gestaan en dat is onveranderd gebleven. Hierbij dank ik dan ook iedereen die mij de afgelopen jaren heeft geïnspireerd en gemotiveerd. Ik dank mijn gezin dat het dit zo geweldig oppakt. Dank aan al die mensen die op de PVV en op mij gestemd hebben. In het bijzonder dank aan onze fractievoorzitter Geert Wilders voor het in mij gestelde vertrouwen.

Voorzitter. Ik ben er enorm trots op dat het familiebedrijf wordt doorgezet. Maar zoals in alle bedrijven, moet er gevochten worden voor bestaanszekerheid en de voorliggende uitdagingen. Door de coronaperiode kwam er in onze branche een problematiek bovendien die er al wat langer lag, maar daarvoor nog niet echt zichtbaar was. Er kwamen ook opeens allerlei regels en problemen bij waarvan gedacht werd dat die na de coronaperiode wel weer zouden verdwijnen. Maar niets is minder waar: de regeldruk is alleen maar toegenomen, het gevecht om de beschikbare openbare ruimte wordt steeds feller en de samenleving wordt steeds harder. De druk op het ondernemerschap is onevenredig toegenomen.

Ik wil u graag even meenemen in een kleine greep van de uitdagingen waar veel ondernemers, en de kermis- en marktondernemers in het bijzonder, voor staan. De druk op het behoud van arbeidsterrein vanwege herinrichting en verstedelijking van gemeenten resulteert in verschraling of het volledig verdwijnen van kermissen, markten en overige evenementen in de binnensteden. Demografische veranderingen leiden tot spanningen en soms tot rellende jeugd. Dat resulteert in het wegblijven van welwillende bezoekers en het verzwaren van veiligheidseisen, die weer leiden tot extra restricties en kosten. De transport- en energiekosten nemen enorm toe en zijn niet meer door te berekenen in de prijzen. Ik noem ook de stikstofproblematiek en Natura 2000-gebieden waardoor sommige evenementen geen doorgang meer vinden. Door de nieuwe richtlijn voor schaarse vergunningen zien ondernemers hun inkomen ineens wegvallen en kunnen zij hun investeringen niet meer op tijd terugverdienen. Het storten en verantwoorden van contant geld bij banken en de mogelijkheid tot financieren zijn steeds moeilijker geworden. Als klap op de vuurpijl is er dan ook nog de implementatie van de zero-emissiezones die desastreus gaat uitpakken voor talloze sectoren, maar als eerste voor de ambulante handel, waar ook de kermis onder valt. Onhaalbare en onbetaalbare eisen en gebrek aan visie om hiervoor een passende oplossing te vinden, staan bovenaan het lijstje van menig ondernemer.

Voorzitter. Ondanks alles wat ik nu genoemd heb, zetten deze ondernemers door. Zij blijven kijken naar de toekomst. Zij willen de stap naar voren maken en zich verder ontwikkelen en innoveren.

Dan kom ik bij de wet waar wij vandaag het debat over hebben. Dat is een wet waarvan ik weet dat die nog niet of niet genoeg speelt bij de midden- en kleinbedrijven, laat staan bij zzp'ers. De PVV is dan ook blij met de bewustwordingscampagnes.

De PVV ziet dat er een keurmerk voor het mkb wordt opgezet en dat dit medio 2025 gereed moet zijn. De PVV is vóór keurmerken, want daarmee kan een bedrijf zich onderscheiden, maar de PVV vraagt zich wel af waarom er een keurmerk gaat komen voor het mkb terwijl er niet gehandhaafd gaat worden. Ook houdt een keurmerk in dat er een protocol moet zijn waaraan getoetst wordt, wat weer regeldruk en kosten met zich meebrengt. Kan de minister uitleggen hoe de uitvoering van het keurmerk gaat zijn en wat voor gevolgen dit heeft voor de kosten en regeldruk voor ondernemers?

De PVV vraagt zich ook af of het initiatief van het benaderen van afnemers van een door het DTC genotificeerde digitale dienstverlener bij die dienstverlener ligt, of dat wij met het DTC zelf afnemers gaan benaderen. Ik vraag dit in het kader van verantwoordelijkheid. Hoe wordt de ketenafhankelijkheid ondervangen? Als het vrijblijvend is, hoe zorgt de minister er dan voor dat die afnemers niet de dupe worden van niet-adequaat handelen? Kunnen de bedrijven die eventuele schade hebben ondervonden door nalatig handelen van zo'n dienst de weg naar de rechter maken, als bekend is dat dit bedrijf genotificeerd is?

Voorzitter. Dan heeft de PVV ook nog een vraag over de laatste regel op pagina 6; dat is de eerste alinea van de memorie van toelichting. Worden niet-vitale bedrijven al genotificeerd door het NCSC — hetgeen niet zou moeten — of staat die regel er abusievelijk in? De PVV ziet ook dat men metertijd de departementen wil samenvoegen tot één loket; hier is de PVV altijd een voorstander van geweest. Maar ook hierbij, alvast voorsortierend op de toekomst, zien we graag dat er geborgd wordt dat de non-vitale bedrijven altijd uitgezonderd blijven van extra regeldruk en kosten.

Voorzitter. Samenvattend voorziet dit voorstel in de bevoegdheid van de minister om het NCSC en het DTC gegevens met elkaar te laten uitwisselen. Notificaties volgen uit analyses, maar zijn vrijblijvend. Kan de minister een voorbeeld geven van wat dit voor een gemiddeld bedrijf gaat opleveren en eventueel gaat kosten?

Dank u, voorzitter.

(Geroffel op de bankjes)

De voorzitter:

Van harte gefeliciteerd, mevrouw Van Meetelen, nogmaals met uw verjaardag, maar ook met een prachtig pleidooi voor de erkenning van 1.000 jaar kermistraditie. U heeft hartstochtelijk gesproken over het ondernemerschap en over het bakken van poffertjes. Ik feliciteer u van harte. Uw collega's gaan u ook nog feliciteren. We gaan drie kwartier schorsen, ook voor de dinerpauze.

De vergadering wordt van 17.58 uur tot 18.52 uur geschorst.

De voorzitter:

Aan de orde is de voortzetting van het debat over de Wet bevordering digitale weerbaarheid bedrijven. We zijn toe aan de eerste termijn van de zijde van de regering. Ik geef het woord aan de minister van Economische Zaken.

Minister Adriaansens:

Dank u, voorzitter. Voordat we beginnen wil ik mevrouw Van Meetelen graag vanaf deze plek alsnog feliciteren met haar maidenspeech. Het was een heel mooie persoonlijke speech. Ik denk dat het altijd heel veel waarde toevoegt als we zien wat voor ervaring mensen meebrengen en waarom ze gemotiveerd zijn. Dank daarvoor via de voorzitter.

Voorzitter. We hebben het vandaag over het veilig werken van bedrijven in de digitale wereld. Wij willen graag dat onze bedrijven veilig digitaal kunnen werken. Daarom is het belangrijk dat we informatie kunnen delen als er bijvoorbeeld een ransomwareaanval dreigt, waarmee databestanden kunnen worden versleuteld met het doel om die later vrij te geven in ruil voor losgeld. We willen dat voorkomen. We willen dat bedrijven zich daartegen kunnen beschermen. Met het wetsvoorstel Wet bevordering digitale weerbaarheid bedrijven worden de taken en bevoegdheden van de minister van Economische Zaken geregeld om die bedrijven te kunnen informeren. Je zou bijna vragen: waarom heb je daar een wet voor nodig; dat kun je toch gewoon doen? Nee, we hebben daar een wet voor nodig, omdat je daar soms persoonsgegevens voor moet gebruiken en dat laatste vraagt om een wettelijke grondslag.

Deze wet gaat over de zogenaamde niet-vitale bedrijven. Het is makkelijker om uit te leggen wat vitale bedrijven zijn dan wat niet-vitale bedrijven zijn. Het is alles wat niet vitaal is. Vitale bedrijven bieden een dienst aan die van vitaal belang is voor de continuïteit van Nederland, zoals energie, ICT, telecom, burgerluchtvaart en de financiële sector. Al het andere is niet-vitaal en daar gaat deze wet over. Heel veel mkb'ers hebben niet-vitale bedrijven. In een aantal gevallen geldt dit ook voor zzp'ers. Zoals door een aantal leden is vermeld, is het best een uitdaging om het allemaal op orde te hebben, want de digitalisering gaat uitermate snel en niet iedereen heeft de mankracht, het geld of de tijd om zich daarin te verdiepen. Daarom is het zaak om te ondersteunen. Die vitale bedrijven vallen dus onder de wet waarover we het nu hebben ... Nee, ik moet het goed zeggen: de vitale bedrijven vallen onder de Wbni en de rest valt onder de wet waarover we het nu hebben. Dat zijn zo'n 2 miljoen bedrijven. Er zijn verschillen die maken dat we twee wetten hebben. De Wbni is een omzetting van Europese regelgeving. Dat is deze wet zeker niet. De Wbni is vooral gericht op het voorkómen van maatschappelijke ontwrichting. De wet waarover we het nu hebben, is vooral gericht op het ondersteunen en informeren van bedrijven.

Voorzitter. Dit wetsvoorstel legt mijn taken en bevoegdheden als minister vast op het terrein van digitale weerbaarheid van die niet-vitale bedrijven, zodat ik specifieke informatie met die bedrijven kan delen. Ook kan ik met dit wetsvoorstel dreigingsinformatie ontvangen, verwerken en delen met andere overheidsorganisaties en derden. Dat moet zorgvuldig gebeuren, want dreigingsinformatie kan persoonsgegevens bevatten. Om die te mogen ontvangen en verwerken, hebben we dus die grondslag nodig.

In de praktijk zal het Digital Trust Center die informatie delen en de taken uitvoeren. Dat

Digital Trust Center is in 2018 opgericht. Inmiddels is het interessant om te melden dat de informatiedienst van het Digital Trust Center sinds de start in juni 2021, toen ze echt actief werden, ruim 156.000 waarschuwingen heeft verstuurd over kwetsbare systemen bij bedrijven. Alleen al in 2023 waren dat er 140.000.

Voorzitter. Met dit wetsvoorstel kunnen we nog meer doen om bedrijven te informeren en te waarschuwen. We zijn namelijk al begonnen, maar nu kunnen we nog verder gaan. Daarom hebben we het hier vandaag over.

Voorzitter. Dan zal ik nu de vragen beantwoorden. Ik probeer dat altijd zo veel mogelijk in blokjes te doen, ook omdat men dat op prijs stelt. Het eerste blokje gaat over lasten bedrijfsleven, kosten, regeldruk. Dan de samenhang van de wetgeving, privacy en persoonsgegevens, digitale hulpverleners, en een mapje overig. Het is vanavond overzichtelijk, vermoed ik!

Allereerst een vraag van mevrouw Martens. Zij vroeg: wat gaat de minister doen om het digitaliseringsniveau van het mkb omhoog te krijgen? Wij hebben een Strategie Digitale Economie. Een van de pijlers daarvan richt zich op de versnelling van de digitalisering in het mkb. In het coalitieakkoord hebben we opgenomen dat we het groeivermogen van het mkb willen versterken. Dat doe ik onder andere door een aantal publiek-private programma's, zoals Digitale Werkplaatsen, Mijn Digitale Zaak en Smart Industry. Ik heb u in een brief van 24 oktober 2023 geïnformeerd over de voortgang van die digitale strategie.

Voorzitter. Mevrouw Van Meetelen vroeg naar het keurmerk. De ontwikkeling van het keurmerk voor het mkb voor ICT-dienstverlening is door het Centrum voor Criminaliteitspreventie en Veiligheid eind vorig jaar gestart met verschillende branches. Keurmerken zijn eigenlijk een instrument van de markt. Bedrijven gebruiken die keurmerken om zich te onderscheiden richting klanten. Het is vrijwillig om een keurmerk te halen. Er zijn dus ook geen wettelijke eisen of iets dergelijks waarop toezicht is. Het is ook nog niet bekend wat de kosten worden van het keurmerk, want daarvoor is de ontwikkeling nog niet ver genoeg.

Voorzitter. Er was ook nog een vraag van mevrouw Kathmann: hoe duur mag zo'n weerbaarheidstraining zijn? Tja, het is aan de markt om daar een goede prijs voor te bepalen en niet aan de overheid. Ik mag mij daar ook niet in mengen. Er is namelijk een wet die verhindert dat ik mij in private activiteiten meng. Maar ik verwacht dat marktpartijen met hun aanbod van weerbaarheidstrainingen rekening houden met de portemonnee, want ze willen hun dienst verkopen. Ik verwacht dus dat er een marktwerking gaat zijn.

Voorzitter, ik kom al bij het volgende blokje. Dat gaat over de taakverdeling.

Door de heer Six Dijkstra werd gevraagd naar de integratie van de organisaties. Die laat de verantwoordelijkheden onverlet. De minister van JenV wordt de verantwoordelijke voor de hele organisatie. Daarnaast heb je opdrachtgeverschap van de verschillende ministers voor de sectoren waarvoor zij verantwoordelijk zijn. Binnen die organisatie ben ik verantwoordelijk voor de informatievoorziening aan de niet-vitale bedrijven. De minister van JenV is dat op haar beurt voor de vitale bedrijven. Maar we willen natuurlijk

wel zo veel mogelijk integreren en ervoor zorgen dat er wordt samengewerkt en kennis wordt gedeeld. Daar wordt enorm op gestuurd. We willen namelijk één centrum waar al die kennis wordt gebundeld.

Er werd ook gevraagd naar een soort team. Dat wordt opgezet. Er wordt gewoon samengewerkt om te zorgen dat de goede informatie op de goede plek terechtkomt.

Voorzitter. Er werd gevraagd hoe ik kijk naar de verkokering bij de toezichthouders. We hebben een systeem waarin iedere sector eigenlijk zijn eigen toezichthouder heeft. Dat is onder andere omdat iedere toezichthouder de beveiliging, om het zo maar te zeggen, moet verinnerlijken. Kijk bijvoorbeeld naar EZK: wij hebben de RDI. Die is overigens de voorzitter van een toezichtraad waar al die toezichtsorganen in zitten om met elkaar hun kennis te delen en de vertaling te maken naar de markt. U vroeg mij of ik dat een probleem vond. Nee, niet zolang er wel goed wordt samengewerkt. Dat is wel de voorwaarde, denk ik.

Voorzitter. Wanneer krijgen het NCSC en het DTC de ruimte om niet-vitale bedrijven te informeren? Dat was een vraag van mevrouw Martens. Waar komt die verantwoordelijkheid uiteindelijk te liggen? Op het moment dat een bedrijf echt tussen wal en schip valt, dan doet het NCSC dat. Op dat moment valt dat ook onder de verantwoordelijkheid van de minister van JenV. Maar als er informatie over een vitaal bedrijf van het NCSC bij DTC komt, dan valt het onder de verantwoordelijkheid van het DTC en dus onder de verantwoordelijkheid van de minister van EZK.

Voorzitter. Er werd nog gevraagd wat nou het verschil is. Bij de vitale bedrijven is er echt sprake van maatschappelijke ontwrichting als er een cyberdreiging wordt doorgezet. Dat maakt ook echt — het is een uitvoering van een Europese regel — dat het een hele andere wet kent. Ik moet u eerlijk zeggen dat ik er zelf ook wel over heb doorgevraagd. Ik wilde weten hoe we het gingen doen: of we een aparte wet gingen inrichten of het bij dezelfde wet onder gingen brengen. Dat is altijd een keuze. Maar in dit geval is er een best goede argumentatie om het gescheiden te houden. Dat is met name omdat we willen proberen om vanuit het marktperspectief te kijken, zodat bedrijven weten waar ze aan toe zijn. Als je die bril opzet, dan is het echt logisch om deze taken, die geen uitvoering van een Europese regel zijn, in een aparte wet onder te brengen. Dat was een vraag van onder anderen mevrouw Kathmann. Zij vroeg daarover door.

Mevrouw Kathmann vroeg ook, zeg ik via de voorzitter, naar het cybervolwassenheidsniveau van Cyberveilig Nederland. Ze vroeg of dat niet een goed onderscheid zou zijn in plaats van vitaal of niet-vitaal. De beoordeling van die volwassenheid is geen ordening die we hier willen aanbrengen. Het moment kan namelijk per bedrijf verschillen. Het is dan ook heel moeilijk om bedrijven volgens die waardering goed in te delen.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dank voor de beantwoording van de vraag of cybervolwassenheid een mogelijkheid is. De minister geeft aan te kijken naar vitaal en niet-vitaal, omdat er dan gekeken wordt vanuit het marktperspectief. Ik heb daar dan wel een extra vraag bij. De markt geeft aan dat het juist voor hen niet zo goed werkbaar is, omdat alles met elkaar verweven is: een

cyberaanval op een niet-vitaal bedrijf heeft supergrote consequenties voor een bedrijf dat wél vitaal is. Als we die harde knip houden, hoe gaan we daar dan mee om?

Minister Adriaansens:

Ik denk dat dit een terechte zorg is. Van welke kant je hier ook naar kijkt, vitaal en niet-vitaal, wel bij elkaar en niet bij elkaar, het moet met name in de uitvoering goedkomen. Ik herken de alertheid. Ik denk dat we het erover hebben hoe we zorgen dat die informatie op de goede plek terecht komt. Dat vraagt een verdergaande integratie. Daarom is het ook goed dat die drie organisaties worden samengevoegd, zeg ik tegen mevrouw Kathmann via u, voorzitter. Maar we moeten wel zorgen dat dat gaat werken. De informatie moet namelijk in teams worden gedeeld. Daarbij kent iedereen zijn eigen verantwoordelijkheid in de informatieplicht die daaruit voortvloeit.

Mevrouw Kathmann (GroenLinks-PvdA):

Hoe zorgt de minister op dit moment dan dat dat werkt of gaat werken?

Minister Adriaansens:

Het is "gaat werken", want ze zijn daarmee bezig. We zullen moeten gaan monitoren en kijken of bedrijven zich goed geïnformeerd voelen. Er zijn ontzettend veel samenwerkingsverbanden waar wij contact mee hebben en waar het DTC ook contact mee heeft. Dat zijn er volgens mij een stuk of 60 op dit moment. Dat moet echt een laagdrempelige communicatie zijn over de vraag of wij de goede informatie krijgen. We zien aan de bezoeken op de website en het gebruik van de tools die worden aangeboden dat het een welkome informatie en ondersteuning is, maar het blijft een kwestie van monitoren, navragen en enquêteren: voelt u zich goed ondersteund? Het is ook met name een kwestie van daar waar het fout gaat, begrijpen waarom dat mis is gegaan. Mocht dat zitten in een gebrek aan ondersteuning, dan zou dat in een verbetercyclus gelijk moeten worden opgepakt om dat de volgende keer beter te doen. Zo zie ik het.

Voorzitter. Mevrouw Van Meetelen vroeg naar de verantwoordelijkheid van de digitale dienstverlener om de klanten te informeren over cyberdreigingen. Het DTC gaat alle bedrijven informeren waarover zij dreigingsinformatie hebben. Dat stelt hen dan in staat om zichzelf te beschermen. In de relatie tussen de ICT-gebruikende bedrijven en de ICT-leveranciers gelden een contractuele relatie en de afspraken die zij daarover maken. Als een klant schade heeft omdat de leverancier bijvoorbeeld zijn contractuele verantwoordelijkheid niet heeft genomen, dan kan zo'n klant naar de rechter stappen. Daar vallen wij als overheid buiten.

Voorzitter. Mevrouw Van Meetelen vroeg ook of de niet-vitale bedrijven gewaarschuwd worden door het NCSC. Dat worden ze dus indirect via het Digital Trust Center. Dat ontvangt dan informatie van het NCSC. Zo proberen we goed te scheiden waar de verantwoordelijkheden liggen. Ik moet zeggen dat ik in de voorbereiding op dit debat heel erg ben gestruikeld over de afkortingen. De Wbni, dus de wet waar de vitale organisaties onder vallen, regelt dat het Nationaal Cyber Security Centrum dreigings- en incidentinformatie kan delen met de zogenoemde OKTT's. Dat zijn organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten. Ik deel dit eigenlijk meer omdat ik het interessant vind dat wij overal afkortingen voor hebben, dus ik probeer in normale taal te blijven

uitleggen dat wij gewoon met elkaar moeten samenwerken en dat die organisaties daarin samen moeten optrekken.

Mevrouw **Van Meetelen** (PVV):

Dan heb ik toch nog een vraag. Begrijp ik het goed dat als er een dreiging wordt waargenomen, te allen tijde alle bedrijven waarvoor gedacht wordt dat die dreiging er kan zijn, worden geïnformeerd?

Minister **Adriaansens**:

Correct.

Mevrouw **Van Meetelen** (PVV):

Oké. Dus het is niet zo dat er op een bepaald moment één bedrijf dat is genotificeerd en dat eigenlijk zou ... Stel dat die denkt "ik doe er niks mee" of "ik doe het niet goed genoeg", dus dat er niet adequaat naar gehandeld is. Dan kunnen de onderliggende bedrijven dus eventueel een stap naar de rechter maken?

Minister **Adriaansens**:

Het DTC informeert de niet-vitale bedrijven, dus een mkb-bedrijf, dat er een dreiging is of dat er iets heeft plaatsgevonden. Soms hebben wij die informatie als overheid ook iets eerder, want dat wordt centraal doorgegeven. Dan wordt dat bedrijf geïnformeerd. Bij de niet-vitale bedrijven is het vervolgens aan het bedrijf zelf om een actie te bepalen, om zich te beschermen, om een ander beschermingsprogramma te installeren, et cetera, et cetera.

De **voorzitter**:

De minister vervolgt haar betoog.

Minister **Adriaansens**:

Dan de verhouding tot de implementatie van de NIS2-richtlijn. De vraag van mevrouw Van Meetelen ging vooral over wat het notificeren een gemiddeld bedrijf oplevert en wat het gaat kosten. Dat was volgens mij de echte vraag. Bedrijven worden gratis door het Digital Trust Center geïnformeerd over dreigingen en kwetsbaarheden. Het kost bedrijven dus niets. Het verschilt per ondernemer wat het notificeren oplevert. De Cybersecuritymonitor gaf aan dat 11% — dat is best veel — van de bedrijven met twee of meer werknemers losgeld betaalde. Dat vind ik best een indrukwekkend aantal. In ongeveer de helft van de gevallen bedraagt het losgeld meer dan 50% van de omzet. We hebben het hier echt over substantiële schade waarvan het echt de moeite waard is om te zorgen dat we dit voorkomen, zoals door een aantal van u is aangegeven.

Dan de vraag over de regeldruk. Op basis van dit wetsvoorstel is er geen regeldruk voorzien. Er worden geen eisen opgelegd aan de bedrijven. Dat is ook getoetst bij het Adviescollege toetsing regeldruk. Zij hebben dat ook aangegeven en bevestigd.

Voorzitter. Er was nog een vraag van mevrouw Van Meetelen, maar die hebben we eigenlijk net behandeld. Zij vroeg wat er gebeurt als het bedrijf geïnformeerd is. Informeert dat bedrijf vervolgens zijn klanten? Het is aan de contractuele relatie hoe ze dat vervolgens met elkaar oplossen.

Dan de vraag welke typen persoonsgegevens onder deze wet kunnen worden gedeeld. Dat was een vraag van de heer Six Dijkstra. In de basis zijn de gegevens die worden verwerkt, bedrijfsgegevens. Naast IP-adressen kunnen ook namen, e-mailadressen en telefoonnummers worden verwerkt die herleidbaar zijn tot natuurlijke personen. Die gegevens vallen dan onder de categorie gewone persoonsgegevens. Om die gegevens te mogen verwerken, is dus een wettelijke grondslag op grond van de AVG nodig.

Dan nog een vraag van de heer Six Dijkstra. Met al zijn brede ervaring in deze sector moest ik mijzelf wel verdiepen in de Indicators of Compromise, de IoC's. Dat zijn kenmerken van cyberaanvallen. Het kan dan gaan om IP-adressen van de mogelijke aanvallers. Het Digital Trust Center verwijst in de praktijk alleen naar de IoC's als deze openbaar beschikbaar zijn. IP-adressen zijn soms ook persoonsgegevens. Als het zpp'ers en dergelijke betreft, zijn ze vaak herleidbaar. Daarom is ook daarvoor weer een wettelijke basis nodig.

De heer **Six Dijkstra** (NSC):

Dank aan de minister voor deze beantwoording. Wat is de reden dat het DTC in de regel alleen openbare IoC's deelt met bedrijven en geen mogelijk vertrouwelijke of niet openbare IoC's?

Minister **Adriaansens**:

Ik zal deze vraag terugnemen voor een in-depth beantwoording in de tweede termijn, maar ik vermoed dat we geen wettelijke positie hebben om toegang tot die data te verkrijgen. Ik zal dat even checken.

De heer **Six Dijkstra** (NSC):

Dank. Ik ben daar erg benieuwd naar. Mocht er verdere integratie met het NCSC plaatsvinden, dat mogelijk ook toegang heeft tot andere data die mogelijk ook relevant kunnen zijn voor deze niet-vitale bedrijven, dan ben ik ook wel benieuwd of dat nog iets zou veranderen aan de situatie. Kunnen dan ook niet-vitale bedrijven toegang krijgen tot relevante data die via een of andere vertrouwelijke database verspreid zouden kunnen worden?

Minister **Adriaansens**:

Die vraag neem ik even mee in de rebound, als u dat goedvindt.

De **voorzitter**:

Ja hoor.

Minister **Adriaansens**:

Mevrouw Kathmann vroeg naar de digitalehulpverlener, het mooie concept van de dhv'ers. Tijdens de jaarlijkse bewustwordingscampagne van Alert Online wordt het belang van het laagdrempelig organiseren van hulp op de werkvloer onder de aandacht gebracht. Daar is het ook aan de orde gekomen. Bedrijven zijn volledig vrij in hoe ze het organiseren. Wel kunnen de dhv'ers zich aanmelden bij de onlinecommunity die het DTC bouwt. Ook via de website is informatie beschikbaar over hoe je de digitale hulp moet organiseren. Ik ben wel een beetje terughoudend over de mate waarin ik dit nog meer moet opleggen aan met name kleine bedrijven. Ik was wel gecharmeerd van het voorstel. Met enige nuance gaf mevrouw Kathmann ook aan dat dit voor een dhv'er een

heel goed instrument is, als je het zo mag noemen, maar dat het ook wel een bepaalde regeldruk of organisatiedruk met zich meebrengt. Ik heb nu dus de lijn dat we het vooral moeten stimuleren. Het zou dan interessant zijn om bijvoorbeeld te kijken hoeveel dhv'ers zich nu aanmelden bij het DTC, dus of we het op een wat zachtere manier kunnen stimuleren zonder er in deze fase te veel verplichtingen aan te verbinden. Maar dat laatste bedoelde mevrouw Kathmann volgens mij ook niet.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Nou, dat vind ik eigenlijk heel mooi om te horen, want dan zit ik op dezelfde lijn als de minister. Het voorstel vraagt eigenlijk alleen om te stimuleren, dus niet om bedrijven iets op te leggen, maar om vanuit de overheid in een beleidsbepaling neer te leggen dat we ook echt gaan stimuleren. Omdat dit ook in de branche wordt gezien als een hele concrete maatregel voor bewustwording op de werkvloer, moeten we het niet opleggen in de zin van: iedereen moet er per 2030 eentje hebben rondlopen. We leggen het stimuleren door de overheid vast, zodat we kunnen blijven roepen dat dit een goede oplossing kan zijn. Dat is eigenlijk het enige wat ons voorstel vraagt. Ik snap dat je dat bij de bedrijfshulpverlener wat steviger doet. Daar hebben we het over hartfalen. Je moet het niet bagatelliseren, maar hier hebben we het gelukkig over cybercrime. Dan kan je dat misschien ook met een wat lichtere maatregel aanpakken.

Minister **Adriaansens**:

Ik neem het voorstel graag nog eens even serieus in overweging om te kijken of we iets kunnen doen om het nog wat steviger neer te zetten via het DTC en om eens te kijken wat er dan gebeurt en of dat voldoende enthousiasme opwekt, zodat bedrijven dit model overnemen.

Mevrouw Kathmann vroeg ook naar de nazorg. Het DTC biedt geen slachtofferhulp. Er is wel algemene informatie te vinden op de website over wat je kan doen als er zich een incident heeft voorgedaan. Daarbij wordt ook verwezen naar instanties waar men heen kan. Op het moment dat we daarbij te veel maatwerk zouden gaan leveren, kan er strijdigheid ontstaan met de Wet Markt en Overheid. Inmiddels is er overigens ook een markt die hierin voorziet met commerciële cybersecuritydiensten, zoals hulp bij respons en herstel bij schade en hacks. Een bedrijf kan zich natuurlijk ook verzekeren, waarbij wordt voorzien in hulp achteraf. Dat is dus de wijze waarop dat geregeld is.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dan denk ik dat ik mijn vraag misschien niet goed heb gecommuniceerd. Waar het juist vooral over ging, is de zachte kant van zo'n cyberaanval. Als je degene bent die op dat linkje heeft geklikt op het werk, of als je die ondernemer bent die misschien wel zijn bedrijf helemaal de mist in heeft zien gaan door zo'n cyberaanval, dan heb je natuurlijk te maken met de vraag of je wel of niet verzekerd bent, of je alles terugkrijgt en wat je kunt doen om het lek te dichten. Soms is er tegenwoordig zelfs ook al hulp van je IT-specialist bij de vraag of je moet betalen of niet. Waar dit om gaat is eigenlijk ook de maatschappelijk mentale kant waar mensen mee te maken krijgen. Op de werkvloer is het vaak een schuldvraag. Daar kan ook een juridische vraag bij komen als mensen aansprakelijk worden gesteld. Dat kan ook gelden wanneer een ondernemer ten onder gaat en hij ineens allerlei rechtszaken aan zijn broek krijgt van werknemers, schuldeisers, klanten en noem maar op, met de vraag: heb je wel goed genoeg gehandeld? Die ellende zorgt er echt voor dat het leven van mensen in het moeras

draait. Het gaat er eigenlijk om of er vanuit het DTC ook aandacht is voor die kant en of mensen goed genoeg naar die hulp verwezen worden.

Minister Adriaansens:

Als het gaat om de werknemers denk ik dat bijvoorbeeld ook vertrouwenspersonen of de hr-ondersteuning daarin een rol kunnen spelen. Maar dat wordt niet bedoeld door mevrouw Kathmann. Zij heeft het echt over de ondernemer die daar zo veel ellende van kan ervaren. Ik sta wel sympathiek tegenover de aandacht die u daarvoor vraagt. Ik zal met het DTC contact opnemen over wat we daarin eventueel kunnen doen.

Voorzitter. Dan ben ik alweer bij mijn mapje "overig". Er was een vraag over het budget en de capaciteit: denkt de minister dat het aantal fte's en het budget voldoende zijn voor de taken? Het noodzakelijke budget is beschikbaar. Dat is ook besproken met de organisatie. Op de EZK-begroting is met versterking uit het vorige coalitieakkoord 8,1 miljoen per jaar beschikbaar gesteld voor de periode 2024 tot 2026. Vanaf 2027 gaat het om structureel 9 miljoen per jaar. Op basis van de plannen die er liggen en de uitvoering die gaande is, blijkt dat op dit moment voldoende te zijn.

Mevrouw Kathmann (GroenLinks-PvdA):

Ik had al aangekondigd dat er in principe wel een motie klaarligt. De onderzoeken zijn soms nog wel een beetje diffuus, maar je ziet toch af en toe echt schrikbarende toenames in het cybercrimebeeld, van 40% stijging per jaar. Als we daar echt op afstevenden, kan ik me voorstellen dat je het DTC daarin moet laten meegroeien. Aan die scenario's moeten we denken. Voor nu geeft de minister aan dat het voldoende is, maar als die scenario's waar worden, hebben we dan ook een plan B, zodat we in ieder geval de middelen voor het DTC laten meegroeien met dat cyberbeeld? Het gaat erom dat we wel op tijd klaar zijn voor die grote toename.

Minister Adriaansens:

Ik begrijp dat, want je ziet een bepaalde dreiging toenemen. Ik zou het toch praktisch willen houden. We hebben nu budget beschikbaar gesteld. Ik zou graag willen monitoren wat er aan klachten, meldingen en activiteiten plaatsvindt en op basis daarvan bezien of er een toename nodig is, want dat kan ik nu eigenlijk helemaal niet onderbouwen. Dus ik zou dat wel willen doen. Dan is even de vraag op welke wijze ik de Kamer kan meenemen in die informatie. Ik denk dat ik dat het beste kan doen bij de voortgangsrapportages rondom de uitvoering van de digitale strategie. Dan neem ik daarin een paragraaf op over de integratie van het DTC met andere organisaties, maar ook informatie over de werkwijze omtrent de kengetallen en over in hoeverre het budget toereikend is.

Mevrouw Kathmann vroeg nog of het DTC alleen kan optreden indien zich daadwerkelijk een cyberincident heeft voorgedaan, of dat het ook kan optreden als er sprake is van een mogelijke dreiging. Dit wetsvoorstel biedt de mogelijkheid om niet-vitale bedrijven te informeren over plaatsgevonden incidenten, maar ook over mogelijke bedreigingen. Er hoeft dus niet sprake te zijn van een daadwerkelijk incident.

Volgens mij ben ik dan door mijn vragen heen.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Een vraag in het verlengde van dit. Hoort het geven van een handelingsperspectief ook echt bij het communiceren met en het adviseren van niet-vitale bedrijven? Hoort dat in het advies en zit daar echt een handelingsperspectief bij?

Minister **Adriaansens**:

Er wordt dan verwezen naar organisaties die je kunnen ondersteunen. We moeten heel erg opletten dat we niet in de activiteiten treden van private organisaties, want dan zijn we gewoon niet het goede aan het doen. Er wordt dus in beginsel naar verwezen, maar er zijn ook samenwerkingsverbanden die heel erg groeien op dit moment. Ik noem de 60 samenwerkingsverbanden, waarin organisaties met elkaar ervaringen delen en expertise opbouwen. Dat is misschien ook wel de beste weg. Dat kunnen we wel stimuleren.

De **voorzitter**:

Dank voor uw inbreng in de eerste termijn. Ik stel voor dat we gelijk doorgaan met de tweede termijn, als daar bij de leden behoefte aan is. Dan kijk ik weer als eerste naar de heer Six Dijkstra. Die heeft er geen behoefte aan. Mevrouw Martens-America? Ook niet. Mevrouw Kathmann had het erover dat ze moties wilde indienen. Ja, dat wil ze ook, hoor ik. Dan gaat zij namens GroenLinks-Partij van de Arbeid het woord voeren.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Maar ik dien zeker niet alle moties in, hoor, want ik ben ook blij met een aantal toezeggingen, ook met die over de digitale hulpverlener. Maar ik ben nog niet helemaal tevreden, dus ik wil de volgende motie toch indienen.

De Kamer,

gehoord de beraadslaging,

constaterende dat cyberrisico's te vaak onbesproken blijven binnen een organisatie omdat er een stigma op heerst;

overwegende dat elke werknemer de ruimte moet hebben om laagdrempelig melding te doen als diegene een risico voor de digitale veiligheid van het bedrijf vermoedt zonder als schuldig te worden bestempeld;

van mening dat een dergelijke cultuurverandering niet vanzelf gaat maar bedrijven al veel kunnen doen door een medewerker te benoemen als digitalehulpverlener (dhv), met geringe gevolgen voor de regeldruk;

verzoekt de regering om in de Strategie Digitale Economie het vergroten van het percentage bedrijven met een aangewezen digitale hulpverlener op te nemen als doel waarop wordt gestuurd;

verzoekt de regering om deze digitale hulpverleners bij bedrijven gericht te informeren vanuit het Digital Trust Center en die zo veel mogelijk te ondersteunen bij het uitvoeren van hun takenpakket,

en gaat over tot de orde van de dag.

De voorzitter:

Deze motie is voorgesteld door het lid Kathmann.

Zij krijgt nr. 8 (36270).

Mevrouw Kathmann (GroenLinks-PvdA):

De andere motie ging inderdaad over digitale ongelukken en nazorg. Ik denk dat ik wel gewoon blij ben met de toezegging van de minister. Ik ben sowieso blij met de beantwoording van de minister en ook met deze wet, op één puntje na. Dat betreft namelijk mijn grote zorgpunt over de kosten voor zo'n digitale veiligheidstraining. Veel ondernemers geven aan: je moet zien hoeveel het ons kost als we veel werknemers succesvol door zo'n training willen sturen. Het is gewoon broodnodig, maar kijk hoeveel bedrijven echt over de kop kunnen gaan en hoe groot de risico's zijn. De minister zegt eigenlijk: de markt bepaalt. Maar wat als die prijzen dan veel te hoog zijn? Ik denk dat het echt veel meer een politieke keuze is of je daarin die sterke overheid wil zijn die ingrijpt en die die bedrijven en mkb'ers gewoon helpt om voor een redelijke prijs digitaal weerbaar te zijn.

Mevrouw Martens-America (VVD):

Ik sluit me helemaal aan bij het betoog van mevrouw Kathmann. Ik ben benieuwd naar het volgende. Misschien kunnen we samen over een jaar aan de minister vragen of ze ons een brief wil sturen met een inventarisatie van hoe het gaat. Als nou blijkt dat de mkb'ers echt met rekeningen worden opgezadeld die ze niet kunnen betalen, dan kunnen we met z'n allen opnieuw gaan kijken. Volgens mij hebben we namelijk vandaag een heel goed overleg gehad over de vraag wat we daar aan zouden kunnen doen. Want volgens mij delen we die zorg eigenlijk met z'n allen.

Mevrouw Kathmann (GroenLinks-PvdA):

Dat vind ik een goed voorstel. Het zou inderdaad fijn zijn als de minister dat zou willen monitoren en de Kamer over niet al te lange tijd zou willen laten weten hoe het daarmee staat. Volgens mij kunnen we dan inderdaad met elkaar beslissen of we daarop in willen grijpen. Ik wil ook graag mevrouw Van Meetelen feliciteren met haar verjaardag en met haar ongelofelijk mooie en inspirerende maidenspeech.

De voorzitter:

Dank voor uw inbreng. Mevrouw Van Meetelen had ook geen behoefte aan een tweede termijn. Dan zijn we ook alweer klaar met de tweede termijn. Er is één motie ingediend, maar die heeft de minister nog niet. Kan ze die gelijk beoordelen, of wil ze even schorsen? O ja, de minister had inderdaad ook nog toegezegd om een vraag te beantwoorden. We schorsen dus even voor vijf minuten.

De vergadering wordt enkele ogenblikken geschorst.

De voorzitter:

Aan de orde is de voortzetting van het debat over de Wet bevordering digitale weerbaarheid bedrijven. We zijn toe aan de tweede termijn van de zijde van de regering, waarin we ook een appreciatie krijgen van de ingediende motie. We krijgen ook nog antwoord op, geloof ik, twee vragen. De minister van Economische Zaken heeft het woord.

Minister Adriaansens:

Dank u, voorzitter. Ik wil een kleine correctie doen op mijn toezegging over de berichtgeving over de capaciteit en het budget wat betreft het DTC. Ik hou me nog steeds aan de inhoudelijke toezegging, maar we doen dat niet bij de digitale strategie, maar bij de Nederlandse Cybersecuritystrategie. Die wordt, onder regie van de minister van JenV, jaarlijks aan uw Kamer gestuurd. Dit zeg ik voor de volledigheid.

Voorzitter. Dan kom ik op de zeer technische vraag van meneer Six Dijkstra. Ja, ook niet-openbare IoC's worden gedeeld, waar dat juridisch mogelijk is. Dat moet ik voor de notulen wel even goed vermelden. Dan gaat u nu vragen wanneer dat dan zo is. Dat vermoedde ik al. Maar ik ben niet voor één gat te vangen. Soms is er sprake van bijzondere persoonsgegevens. Dan heb je ook informatie over wie er op jouw systeem zit. Wij mogen op basis van deze wet geen toegang tot dié informatie geven.

De heer Six Dijkstra (NSC):

Dank aan de minister. Dat heldert al het een en ander op. Ik ben dan wel benieuwd naar het volgende. Waar moeten we dan naar kijken als het gaat om datgene wat wel gedeeld kan worden? Is het vrij eenvoudig om, bijvoorbeeld, IP-adressen te delen? Dat is namelijk een reeks cijfers: 256⁴. In principe is alles openbaar, alleen de context is gevoelig. In welke mate is de minister ook voornemens om daar echt gebruik van te maken, om uiteindelijk het bedrijfsleven beter toe te rusten?

Minister Adriaansens:

Dit zijn best technische vragen. Ik zal 'm dus in algemene zin beantwoorden. Ik bied de heer Six Dijkstra anders heel graag aan om daar nog een keer een verdiepend gesprek over te voeren, ook met wat technisch onderlegde ambtenaren erbij. Maar in beginsel gaan wij alles doen wat nodig is om informatie over die dreiging te krijgen. We hadden al een handelend DTC, maar toen hadden we geen toegang tot IP-adressen en alles wat daarmee samenhangt, waardoor er een risico was op het gebied van toegang tot persoonsgegevens. Dat hebben we nu wel. Je moet dan wel allemaal waarborgen inregelen. Deze wet heeft als doel dat we bedrijven gaan informeren over dreigingen. Maar dan moet ik dat wel kunnen doen. Dat zou dus altijd mijn toets zijn. Op het moment dat we tegen juridische grenzen aanlopen ... Dat zeg ik even in mijn functie. Ik ga namelijk over het systeem. Ik wil dat het systeem werkt. Dus daar wil ik dan ook in de rapportage in voorzien. Als dat niet zo is, dan zult u mij zeker weer bevragen op de maatregelen die ik daarvoor zal nemen.

Voorzitter. Dan kom ik bij de motie-Kathmann op stuk nr. 8. Hoe sympathiek die motie ook is, ik moet die toch ontraden. We sturen namelijk op een doel en niet op een instrument. Het gaat om het middel dat de dhv'ers zouden kunnen bereiken, dus dat we meer weerbare bedrijven realiseren. Ik wil dat echter doen door te stimuleren, door informatiepakketten gereed te maken die recht doen aan verschillen tussen bedrijven en door daar in samenwerkingsverbanden aandacht voor te vragen. De DTC-community kan daarbij ook collegiaal advies bieden. Maar het verplicht opleggen, is niet iets wat ik wil. Ik ga het dus stimuleren, maar niet vormgeven op de manier die nu gevraagd wordt. Daarom ontraad ik deze motie.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dan wil ik graag aan de minister vragen waar zij in de motie het voorstel leest dat we het verplicht willen opleggen aan bedrijven en dat we het niet willen stimuleren.

Minister **Adriaansens**:

Ik begrijp die vraag. "Het vergroten van het percentage bedrijven" vraagt van mij om dat te gaan registreren, om dat bij te gaan houden. Ik heb daar niet echt instrumenten voor. Wat ik wél kan doen — dat gaf ik al aan — is kijken welke dhv'ers zich melden bij het DTC. Dus ik kan tellen hoeveel ervan zijn aangesloten, maar ik kan daar niet actief op sturen. Als een dhv'er niet is aangesloten bij het DTC, zou het technisch gezien nog steeds een dhv'er zijn, maar dan zit hij niet in mijn boeken, dus dan moet ik daar heel andere activiteiten op ontplooiën. Die vond ik niet heel wenselijk.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Welke activiteiten bedoelt de minister dan, welke "vele" activiteiten?

Minister **Adriaansens**:

In de een-na-laatste zin vraagt u aan mij: verzoekt de regering om in de Strategie Digitale Economie het vergroten van het percentage bedrijven met een aangewezen digitale hulpverlener op te nemen als doel waarop wordt gestuurd. Als u dat aan mij vraagt, moet ik daar actie op ondernemen. Dan moet ik dat gaan monitoren bij bedrijven. Dat creëert regeldruk. Zij moeten dat gaan registreren. Dat moet ik bijhouden. Op dat stuk ontraad ik de motie. Het stimuleren pak ik op.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Er wordt geen percentage genoemd. Er staat verhogen. Dat staat er eigenlijk. Volgens mij is dat ook het doel van stimuleren. Dan stuur je er eigenlijk op dat je een percentage verhoogt. Het is dus nu al mogelijk dat dhv'ers zich aanmelden, zegt de minister. Dan kan je in de praktijk toch aflezen aan het aantal dhv'ers dat zich aanmeldt, of het stimuleren gelukt is of niet? Dat is toch geen rocketscience?

Minister **Adriaansens**:

Dat ben ik eens met mevrouw Kathmann, maar er kunnen dan ook dhv'ers zijn die zich niet aanmelden. Die heb ik niet in het vizier. Dan vind ik het lastig om deze motie op die manier uit te voeren. Als de vraag veranderd wordt ... Maar dan moeten we 'm even gaan herformuleren. Het stimuleren van dhv heb ik toegezegd, maar ik kan niet gaan sturen op dat doel.

Mevrouw **Kathmann** (GroenLinks-PvdA):

Dan wil ik alleen nog zeggen dat we nog even de tijd zullen nemen om te kijken of we de motie zo aan kunnen passen dat de minister haar kan omarmen.

De **voorzitter**:

Oké. Dat wachten we dan even af. De minister is klaar met haar beantwoording in tweede termijn.

Minister **Adriaansens**:

Ja. Dank u, voorzitter.

De voorzitter:

Dan zijn we aan het einde van dit debat. De motie is nu formeel ontraden, zeg ik er maar even bij, maar mogelijk komt er een aangepaste versie voor de stemmingen.

De algemene beraadslaging wordt gesloten.

De voorzitter:

De stemmingen zijn voorzien op dinsdag 19 maart aanstaande. Dank aan de minister en haar ondersteuning, de leden en hun ondersteuning, de staf hier en het publiek voor zover misschien digitaal aanwezig, want ik zie ze niet meer hier op de tribune. We zijn redelijk op tijd klaar vandaag. Ik wens u allemaal een prettige avond.

Sluiting

Sluiting 19.39 uur.