Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

595

Vragen van lid **Kathmann** (PvdA) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over *het bericht dat de digitale veiligheid onvoldoende is* (ingezonden 23 september 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) en van Minister **Blok** (Economische Zaken en Klimaat), mede namens de Staatssecretaris van Infrastructuur en Waterstaat (ontvangen 3 november 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 288.

Vraag 1
Bent u bekend met het onderzoek van de DMCR en de provincie Zuid-Holland over het gebrek aan cybersecurity bij bedrijven die werken met gevaarlijke stoffen?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u zich vinden in de bevindingen van het onderzoek van de DMCR en de provincie Zuid-Holland? Zo nee, welke bevindingen deelt u niet?

Antwoord 2
DCMR heeft Fox-IT gevraagd een cybervolwassenheidsbeeld vast te stellen voor de bedrijven die vallen onder het toepassingsbereik van het Besluit risico's zware ongevallen 2015 (Brzo-bedrijven) in Zuid-Holland en Zeeland. Fox-IT heeft dat gedaan met diepte-interviews en self-assessments. Het geaggregeerde eindresultaat geeft een beeld van het implementatieniveau op een 5-punts schaal.
De bevindingen van het onderzoek geven een beeld van de situatie bij de bedrijven die deel uitmaakten van het onderzoek van DCMR.
Op basis van dat beeld kunnen wij ons vinden in de constatering dat er aanleiding is om de aandacht voor cybersecurity bij Brzo-bedrijven te vergroten.

[1] DCMR, 16 september 2021, «Meer aandacht nodig voor digitale weerbaarheid risicovolle bedrijven», https://www.dcmr.nl/actueel/nieuws/meer-aandacht-nodig-voor-digitale-weerbaarheid-risicovolle-bedrijven

ah-tk-20212022-595
ISSN 0921 - 7398
's-Gravenhage 2021

Vraag 3, 4
Hoe kan het dat bij een groot deel van de bedrijven er onvoldoende aandacht is voor cybersecurity?
Bent u het met ermee eens dat bedrijven die werken met gevaarlijke stoffen juist extra goed beveiligd moeten zijn op het digitale vlak?

Antwoord 3, 4
De digitalisering van de maatschappij en van bedrijfsprocessen in het bijzonder heeft een grote vlucht genomen. De digitale kwetsbaarheid neemt daarmee ook in de breedte van de hele maatschappij toe. Berichtgeving in de media over hacks bij bedrijven en andere organisaties dragen bij aan bewustwording over de noodzaak van een adequate digitale weerbaarheid en het daartoe treffen van de noodzakelijke beveiligingsmaatregelen.
Dit is een ontwikkelproces waarbij niet alle bedrijven al even ver zijn. Een bedrijf is primair zelf verantwoordelijk voor een veilige bedrijfsvoering en dus ook voor het treffen van adequate maatregelen met betrekking tot cybersecurity.
Zoals het Cybersecuritybeeld Nederland 2021 laat zien is ook het midden- en kleinbedrijf (mkb) steeds vaker slachtoffer van ransomware-aanvallen. De digitalisering is door deze bedrijven omarmd, maar dat geldt vaak nog niet voor het treffen van de noodzakelijke cybersecuritymaatregelen. De onderzoeksgroep van DCMR valt grotendeels in deze doelgroep. Mogelijke factoren voor onvoldoende aandacht aan cybersecurity zijn bijvoorbeeld een tekort aan relevante kennis over het onderwerp of het gebrek aan prioriteit in aandacht of financiële ruimte zolang digitale incidenten nog niet het primaire proces hebben geraakt.
Voor een bedrijf waar gewerkt wordt met gevaarlijke stoffen, kan het grote gevolgen hebben als dat bedrijf de cybersecurity niet goed op orde heeft en het doelwit wordt van digitale aanvallen. Het is dus zeker van belang dat deze bedrijven adequate maatregelen treffen ter beveiliging van hun netwerk- en informatiesystemen. Het is daarom goed dat DCMR samen met het bevoegd gezag als bedoeld in het Besluit risico's zware ongevallen 2015 (Brzo), de provincies Zuid-Holland en Zeeland, heeft onderzocht hoe het staat met de digitale weerbaarheid bij de risicovolle bedrijven in het eigen werkgebied.
De aandacht voor cybersecurity is de afgelopen jaren toegenomen maar is nog niet bij alle bedrijven op het gewenste niveau zoals ook uit het onderzoek van DCMR blijkt. Daarom is het van belang dat bedrijven hier mee aan de slag gaan. Zie verder het antwoord op vragen 5 en 6.

Vraag 5, 6
Wat doet u om de cybersecurity van deze bedrijven te vergroten?
Doet u voldoende om de cybersecurity van deze bedrijven te verbeteren? Zo ja, hoe verklaart u de bevindingen in dit onderzoek dan? Zo nee, wat gaat u meer doen om de cybersecurity van deze bedrijven te verbeteren?

Antwoord 5, 6
Zoals eerder gesteld is een bedrijf primair zelf verantwoordelijk voor een veilige bedrijfsvoering en dus ook voor het treffen van adequate maatregelen met betrekking tot cybersecurity. Vanuit omgevingsveiligheid zijn de provincies bevoegd gezag voor de Brzo-bedrijven. De Staatssecretaris van IenW is systeemverantwoordelijk voor de regelgeving Brzo (omgevingsveiligheid).
Daarnaast is er beleidsverantwoordelijkheid in het kader van bescherming van vitale processen/sectoren. De vakdepartementen kennen vanuit dit kader een beleidsverantwoordelijkheid voor aanbieders binnen deze groep bedrijven die binnen hun beleidsdomein vallen. In het geval van de olievoorziening is de Minister van EZK beleidsverantwoordelijk. De Staatssecretaris van IenW is binnen de vitale sectoren beleidsverantwoordelijk voor de «Grootschalige productie/verwerking en/of opslag van (petro)chemische stoffen» (chemiesector).
Mede naar aanleiding van de uitkomsten van het onderzoek werken het Rijk, de provincies als bevoegd gezag voor de Brzo-bedrijven en het bedrijfsleven samen om een aantal activiteiten uit te voeren om de aandacht voor cybersecurity bij deze bedrijven te versterken. De primaire focus ligt daarbij op het werken aan de bewustwording bij alle partijen, kennis opbouwen bij en delen met bedrijven en de betrokken overheidsdiensten.

Het Ministerie van Economische Zaken en Klimaat (EZK) is verantwoordelijk voor het vitale proces olievoorziening waarbinnen een deel van de onderzochte bedrijven actief is. Op dit moment onderzoekt het Ministerie van EZK of en welke van deze bedrijven, voor zover zij zich bezighouden met het beheer van oliepijpleidingen en/of met productie, opslag, transport, raffinage of behandeling van olie, bij ministerieel besluit aangewezen zullen worden als aanbieders van essentiële diensten (AED) krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni). Aangewezen bedrijven onder de Wbni hebben de plicht om beveiligingsmaatregelen te treffen met betrekking tot hun netwerk- en informatiesystemen en de plicht tot het melden van digitale incidenten met aanzienlijke gevolgen voor hun vitale dienstverlening. Het Ministerie van EZK heeft een bijbehorende toezichthouder, voor onder Wbni geschaarde partijen.
Voor zover het gaat om bedrijven binnen de onderzochte groep die als vitale aanbieder zijn of worden aangewezen geldt dat het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid tot taak heeft om deze aanbieders te informeren en adviseren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen. Daarnaast verleent het NCSC, waar nodig, ook op andere wijze bijstand aan deze aanbieders bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen. Ook verricht het NCSC analyses en technisch onderzoek ten behoeve van hiervoor beschreven dienstverlening.
De Staatssecretaris van IenW en de provincies maken in het Bestuurlijk Omgevingsberaad bestuurlijke afspraken over een versterkingsactie cybersecurity bij (Brzo)-bedrijven. Deze afspraken richten zich o.a. op het opbouwen van cybersecurity-kennis en het delen van deze kennis met bedrijven en betrokken overheidsdiensten.
Daarnaast geldt voor de onderzochte bedrijven die geen vitale aanbieder zijn binnen een vitaal proces dat zij terecht kunnen bij het Digital Trust Center (DTC), onderdeel van het Ministerie van Economische Zaken en Klimaat. Het DTC adviseert en informeert circa 1,8 miljoen niet-vitale bedrijven in Nederland over hoe zij hun digitale weerbaarheid kunnen verbeteren en jaagt de ontwikkeling van publiek-private samenwerkingsverbanden in Nederland aan, die ook deel kunnen gaan uitmaken van het zogenaamde Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden. Deze zomer is door het DTC begonnen met het proactief informeren van individuele bedrijven over digitale dreigingen.[2] Daarbij gaat het bijvoorbeeld om een beveiligingslek in bepaalde (bedrijfs)software of andere acute kwetsbaarheden. Dit gebeurt nu nog op kleine schaal. Op de langere termijn werkt het DTC toe naar een systeem dat dreigingsinformatie aan grotere groepen bedrijven kan koppelen. Het DTC biedt ook tools aan, zoals de cybersecurity basisscan voor bedrijven, om te kijken of de basisveiligheid op orde is.
Tot slot benoemen we graag dat ook in publiek-private setting cybersecurity verder wordt opgepakt. Zo werkt stichting FERM vanuit het vanuit het *Port Cyber Resilience* Programma aan het verhogen van het bewustzijn met betrekking tot cyberrisico's in de haven Rotterdam. Hierbij wordt nauw samengewerkt met onder andere het Digital Trust Center, de (zeehaven) politie, douane en DCMR.

[2] Kamerstuk 26 643 nr. 760.