Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Minister van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
3045609

Datum 7 oktober 2020
Onderwerp Antwoorden op Kamervragen "hack Apollo Vredestein toont zwakke cyberbeveiliging”

In antwoord op uw brief van 2 september 2020 delen we u mede namens de minister van Economische Zaken en Klimaat mee dat de schriftelijke vragen van de leden Van den Berg en Amhaouch (beiden CDA) aan de ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat en de staatssecretaris van Economische Zaken en Klimaat over het bericht 'Hack bij Apollo Vredestein toont zwakke cyberbeveiliging Nederlandse bedrijven' en het bericht 'Overheid wist wie kwetsbaar was, maar liet bedrijven toch gehackt worden' worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

De Staatssecretaris van Economische Zaken en Klimaat,

Mona Keijzer

Vragen van de ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat op de schriftelijke vragen van de leden Van den Berg en Amhaouch (beiden CDA) over het bericht 'Hack bij Apollo Vredestein toont zwakke cyberbeveiliging Nederlandse bedrijven' en het bericht 'Overheid wist wie kwetsbaar was, maar liet bedrijven toch gehackt worden' (ingezonden 2 september 2020, nr. 2020Z15381)

Vraag 1
Bent u bekend met het bericht 'Hack bij Apollo Vredestein toont zwakke cyberbeveiliging Nederlandse bedrijven' en het bericht 'Overheid wist wie kwetsbaar was, maar liet bedrijven toch gehackt worden'?

Antwoord 1
Ja.

Vraag 2
In hoeverre deelt u de zorgen van IT-experts over de informatiebeveiliging bij Nederlandse bedrijven? Klopt het dat veel bedrijven nog onvoldoende zijn beschermd tegen cybercriminaliteit en kwetsbaar zijn voor bijv. hacks en gijzelsoftware? Hoezeer ziet u daarbij verschil tussen grote, middelgrote (tot 250 werknemers) en kleine bedrijven (minder dan 25 werknemers)?

Antwoord 2
Het kabinet is zich zeer bewust van de risico's op het gebied van digitale dreigingen. Cybersecurity is daarom een prioriteit van dit kabinet, dat hierin extra investeert. De aanpak is vormgegeven in de Nederlandse Cyber Security Agenda uit 2018. Er zijn sindsdien al veel belangrijke maatregelen in gang gezet bij de overheid, (vitale) bedrijven en andere organisaties. Deze maatregelen richten zich op preventie, maar ook op onze respons op digitale incidenten. Voor een overzicht van concrete stappen die zullen worden gezet om Nederland digitaal veilig te houden verwijs ik u graag in het bijzonder naar de tabel 'Versterking Cybersecuritystelsel: Respons en Weerbaarheid' in de kabinetsreactie op het WRR rapport 'Voorbereiden op digitale ontwrichting'[1] en de beleidsreactie op het Cyber Security Beeld Nederland 2020[2].

De digitale weerbaarheid is ondanks die inzet nog niet overal op orde. Daarom blijven partijen kwetsbaar voor cyberincidenten zoals hacks of gijzelsoftware. Kleinere MKB-ers hebben de basis nog niet altijd goed op orde of hebben geen maatregelen getroffen.
Grotere bedrijven hebben meer met incidenten te maken dan kleinere ondernemers. Een groter werknemersbestand en complexere ICT-infrastructuur spelen hierbij een belangrijke rol. Dit vergroot het aanvalsoppervlak[3].

Voor elk bedrijf zijn, ongeacht de grootte, goede beveiligingsmaatregelen en preventie van belang. Daarom zal de inzet om de digitale weerbaarheid van de Nederlandse samenleving te borgen en te verbeteren, zoals uiteengezet in bovengenoemde documenten, de komende jaren over de hele breedte moeten worden voortgezet om de ontwikkelingen bij te kunnen houden.

Vraag 3

[1] Kamerstukken II, 2019/20, 26643, nr. 673

[2] Kamerstukken II, 2019/20, 26643, nr. 695

[3] Dit komt naar voren in het CSBN 2020 en de CBS Cybersecuritymonitoren 2018/2019

Welke kwetsbaarheden t.a.v. cyberbeveiliging komen bij bedrijven het meest voor? Deelt u de analyse van Deloitte Cyber Risk Services dat cybercriminelen "hun doelwit vaak niet kiezen aan de hand van de branche waarin een bedrijf zit, maar aan de hand van de gebruikte technologie"? Hoe kan in uw ogen het bedrijfsleven zich hier het beste tegen beschermen? Zijn er sectoren waarin het aantal cyberaanvallen (of pogingen daartoe) groter is dan in andere sectoren? Indien ja, welke?

Antwoord 3
Kwetsbaarheden komen voor in verschillende verschijningsvormen en kunnen door kwaadwillenden misbruikt worden. Veel voorkomende vormen van cybercriminaliteit zijn phishing, plaatsen van gijzelsoftware en malware, met als mogelijk gevolg uitval van diensten, vernietiging van data en datalekken. Essentiële onderdelen van een goede aanpak voor cyberveiligheid in het bedrijfsleven zijn onder meer: inventarisatie van kwetsbaarheden, tijdig uitvoeren van updates, toegangsmanagement, het gebruik van veilige instellingen. Naast eigen maatregelen kunnen ondernemingen een cybersecuritybedrijf in de arm nemen om adequate maatregelen te treffen.

De analyse van Deloitte deel ik over het algemeen. Het lijkt er minder toe te doen in welke bedrijfstak een bedrijf actief is. Uit het CSBN 2020 blijkt dat uiteenlopende sectoren en organisaties doelwit zijn van digitale aanvallen. Dit komt overeen met de uitkomsten van de Cybersecurity monitor 2019 van het CBS. Daaruit blijkt namelijk dat incidenten ongeveer gelijk plaatsvinden voor alle bedrijfstakken. Vaak is financieel gewin een beweegreden om een (cyber)delict te plegen. Bij maximaal financieel gewin als beweegreden kan de kwetsbaarheid van een bedrijf (bij het personeel, technologie of netwerk) een groter risico vormen om slachtoffer te worden dan de branche waarin het bedrijf opereert. De karakteristieken van het internet geven criminelen immers de mogelijkheid om vele potentiele slachtoffers tegelijkertijd te benaderen.
Daarentegen kan ook het verkrijgen van bedrijfsgevoelige informatie een beweegreden zijn om een cybercrime delict te plegen. In dit geval is de branche waarin een bedrijf opereert wel van belang.

Vraag 4
Is bekend hoeveel (cyber)veiligheidsincidenten bij bedrijven zich dit jaar in Nederland hebben voorgedaan? Geldt hiervoor een meldplicht? Zo ja, hoe krijgt een dergelijke melding opvolging en wordt er lering uit getrokken? Zo nee, denkt u dat een meldplicht meerwaarde kan hebben? Hoe vaak is het tot dusver voorgekomen dat de overheid heeft ingegrepen ingeval bedrijven kwetsbaar bleken op het gebied van (cyber)beveiliging, en op welke manieren?

Antwoord 4
Er is geen volledig beeld van het aantal incidenten of het aantal keren dat de overheid heeft ingegrepen dat zich in het afgelopen jaar bij bedrijven in Nederland heeft voorgedaan.

Voor vitale aanbieders, die krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) zijn aangewezen als aanbieder van essentiële dienst (AED), geldt een wettelijke meldplicht in geval van digitale incidenten met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening bij zowel het Nationaal Cyber Security Centrum (NCSC) als de (sectorale) toezichthouder. Daarnaast geldt ook voor vitale aanbieders, die krachtens de Wbni zijn aangewezen als andere vitale aanbieder (AAVA) een meldplicht voor incidenten met (potentiële) aanzienlijke gevolgen voor de dienstverlening bij het NCSC.
Bij een melding van een bovenbedoeld incident zal het NCSC, gelet op zijn wettelijke taken in de Wbni, de betrokken vitale aanbieder waar nodig adviseren en anderszins bijstaan teneinde de continuïteit van zijn diensten te waarborgen en herstellen. Informatie betreffende een gemeld incident, die relevante

dreigingsinformatie bevat voor bijvoorbeeld andere vitale aanbieders, wordt bovendien in het kader van de wettelijke taakuitoefening, door het NCSC met die andere aanbieders gedeeld, zodat daarmee de kans op soortgelijke incidenten bij andere aanbieders kan worden verkleind. De toezichthouders houden toezicht op de naleving van wettelijke voorschriften, waaronder die betreffende de meldplicht. De toezichthouder kan indien nodig ook ingrijpen bij niet-naleving van de meld- en zorgplicht.

Naast de meldplicht voor bovenbedoelde vitale aanbieders bevat de Wbni ook een meldplicht van incidenten met aanzienlijke gevolgen voor de dienstverlening voor digitale dienstverleners (cloudcomputerdiensten, online marktplaatsen en online zoekmachines) bij zowel de (sectorale) toezichthouder als het CSIRT voor digitale diensten. Voor andere niet-vitale aanbieders geldt op zich geen wettelijke meldplicht van incidenten. Hoewel een incident of aanval voor een individueel bedrijf grote gevolgen kan hebben, is met name ook de maatschappelijke impact daarvan bij een niet-vitale aanbieder minder groot dan bij vitale aanbieders. Uiteraard kunnen deze bedrijven wel ook aangifte doen als zij slachtoffer zijn van cybercriminaliteit. Ook worden deze bedrijven aangemoedigd om op vrijwillige basis incidenten door te geven aan onder meer het DTC en de fraudehelpdesk, en kunnen zij incidenten met aanzienlijke gevolgen ook melden bij het NCSC. Op basis hiervan kunnen, binnen de geldende wettelijke kaders, bijvoorbeeld waar nodig ook andere organisaties gewaarschuwd worden.

Vraag 5
Wat zijn de redenen waarom veel bedrijven nog onvoldoende zijn beschermd tegen cybercriminelen? Heeft dit in uw ogen te maken met bewustzijn, liggen hier financiële motieven aan ten grondslag, of anderszins?

Antwoord 5
Uit verschillende onderzoeken en gesprekken van het DTC met ondernemers komt naar voren dat voor een deel te maken heeft met bewustzijn. Een deel van de ondernemers weet onvoldoende van het onderwerp af of weten niet waar ze de informatie kunnen halen en welke tools ze goed kunnen inzetten.
Er kan ook een bewuste (bedrijfseconomische) keuze voor een bedrijf aan ten grondslag liggen: cybersecurity vergt capaciteit en investeringen en dergelijke investeringsbeslissingen moeten bedrijven afwegen tegen de eventuele risico's en schade die een incident kan veroorzaken.

Vraag 6
Welke maatregelen neemt het kabinet om de cyberbeveiliging bij Nederlandse bedrijven te verhogen? Betreft dit dwingende of vrijwillige maatregelen? Hoe kan de overheid ondernemers helpen de juiste maatregelen te nemen? Past dit binnen de reikwijdte van het MKB-Actieplan? Bent u over dit thema in gesprek met ondernemers(organisaties)?

Antwoord 6
In vraag 2 en 4 is reeds ingegaan op de bredere strategische inzet voor cybersecurity vanuit de NCSA, en de wettelijke kaders betreffende het melden van incidenten.

Het NCSC heeft wettelijk primair tot taak om vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid te informeren en adviseren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen en ook overigens bij te staan bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen. Voor het opvolgen van adviezen of het gebruik maken van bijstand van het NCSC geldt dat dit vriiwillig is. Daarnaast heeft het NCSC ook tot taak om dreigingsinformatie, die in het kader van de primaire taakuitoefening is verkregen, waar nodig te delen met bijvoorbeeld andere bij ministeriële regeling aangewezen computercrisisteams.

Voor het niet-vitale bedrijfsleven is er het Digital Trust Center (DTC) dat informatie verstrekt over de noodzaak van bescherming en dat ook tools (zoals de basisscan cyberweerbaarheid) en adviezen beschikbaar stelt, zodat zij zich beter tegen cyberincidenten kunnen beschermen. Het DTC heeft wel een inspanningsverplichting om ondernemers te bereiken met concrete informatie en adviezen, maar bedrijven hebben een eigen verantwoordelijkheid. Het is aan de bedrijven zelf om deze adviezen op te volgen. Het DTC stimuleert de samenwerking tussen de bedrijven zodat bedrijven elkaar kunnen helpen de weerbaarheid te vergroten. Op dit moment zijn er 29 van dergelijke samenwerkingsverbanden bij het DTC aangesloten en verdere groei is voorzien.

Om het bewustzijn en de actiebereidheid van het bedrijfsleven te verhogen worden door JenV en EZK (doelgroepgerichte) bewustwordingscampagnes breed ingezet op preventie van cybercrime (zoals "Eerst checken dan klikken" en "Doejeupdates"). De overheid helpt hiermee ondernemers om veilig digitaal te ondernemen.
Specifiek voor het MKB is er het actieplan MKB. Daarmee ondersteunt de overheid ondernemers uit het midden- en kleinbedrijf (mkb) bij grote uitdagingen, zoals digitalisering, personeel en financiering. Een onderdeel daarvan is het verhogen van de cyberweerbaarheid.

In het Nationaal Platform Criminaliteitsbeheersing (NPC) werken overheid en bedrijfsleven nauw samen om criminaliteit te voorkomen en terug te dringen. Het NPC heeft onder andere cyber(security) als onderwerp geprioriteerd in het actieprogramma 'Veilig Ondernemen 2019-2022'. Dit actieprogramma dient ter versterking van de digitale veiligheid in het MKB. Daarnaast worden er ook dit jaar weer (digitale) bijeenkomsten georganiseerd door Platforms Veilig Ondernemen om de bewustwording in het MKB te vergroten.

Verder ondersteunt het Ministerie van JenV, in samenwerking met het DTC (ministerie van EZK) en het ministerie van BZK, initiatieven van gemeenten en regionale samenwerkingsverbanden Veiligheid en Platforms Veilig Ondernemen (PVO) gericht op het vergroten van de cyberweerbaarheid van bedrijven. Eind oktober worden deze initiatieven geformaliseerd in een City Deal. In deze City Deal ontwikkelen interbestuurlijke partners, het bedrijfsleven en kennisinstellingen nieuwe aanpakken om de doelgroepen beter te bereiken en gedragsverandering te bewerkstelligen. Binnen deze City Deal wordt tevens de verbinding gelegd met het actieprogramma 'Veilig Ondernemen 2019-2022'. Dit actieprogramma dient ter versterking van de digitale veiligheid in het MKB.

Vraag 7
Klopt de berichtgeving dat een cybercrimineel eerder dit jaar verschillende Nederlandse bedrijven en buitenlandse organisaties heeft gehackt, waardoor wachtwoorden van medewerkers op straat zijn komen te liggen, het ministerie van Justitie en Veiligheid hiervan tevoren voor was gewaarschuwd, maar niets deed omdat het Nationaal Cyber Security Center (NCSC) organisaties buiten het wettelijk mandaat ligt, t.w. de Rijksoverheid en bedrijven in 'vitale sectoren', niet kan informeren? Hoezeer deelt u de mening met de Stichting Digitale Infrastructuur Nederland dat de nationale veiligheid niet wordt gediend met dit beleid?

Antwoord 7
Het NCSC informeert zijn primaire doelgroep (Rijk, vitaal) gericht over voor hun relevante digitale dreigingen. Daarnaast informeert het NCSC het brede publiek door het uitbrengen van algemene beveiligingsadviezen over kwetsbaarheden. Deze adviezen zijn voor iedereen toegankelijk en terug te vinden op de website van het NCSC. Het NCSC is bekend met bedoelde buitgemaakte gegevens door misbruik van een kwetsbaarheid in Pulse Secure VPN-software. Het NCSC heeft eerder een beveiligingsadvies uitgebracht voor deze kwetsbaarheid met inschaling

kans op misbruik Hoog en vervolgschade Hoog.[4] Het is primair ieders eigen verantwoordelijkheid om deze adviezen op te volgen.

Zoals hierboven in het antwoord op vraag 6 is vermeld, heeft het NCSC primair als wettelijke taak om vitale aanbieders en onderdelen van de rijksoverheid te informeren en adviseren over en bij te staan bij dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen. Doel hiervan is het voorkomen of beperken van de uitval van voor de samenleving vitale diensten en daarmee de risico's op maatschappelijke ontwrichting weg te nemen.
Daarnaast heeft het NCSC, voor zover noodzakelijk ter voorkoming van nadelige maatschappelijke gevolgen, krachtens de wet als taak om informatie over dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen van andere organisaties (waaronder ook persoonsgegevens), die is verkregen bij analyses ten behoeve van de primaire taak, door te verstrekken aan bijvoorbeeld andere bij ministeriele regeling aangewezen computercrisisteams.
In de genoemde casus m.b.t. Pulse Secure VPN-software bestond, gezien de aard van de gegevens, ten tijde van het incident geen mogelijkheid voor het NCSC om de betreffende dreigingsinformatie rechtmatig via het Landelijk Dekkend Stelsel met schakelorganisaties te delen, teneinde die organisaties in staat te stellen die dreigingsinformatie aan hun achterban te verstrekken. Inmiddels zijn bijvoorbeeld verschillende computercrisisteams bij ministeriële regeling aangewezen, waaraan voor hun achterbannen relevante dreigingsinformatie, met inbegrip ook van persoonsgegevens, kan worden gedeeld.
Het DTC is opgericht ter verhoging van de digitale weerbaarheid van bedrijven in Nederland die geen vitale aanbieder zijn. Het DTC maakt deel uit van het Landelijk Dekkend Stelsel. Momenteel wordt door het Ministerie van EZK gewerkt aan het laten voldoen van het DTC aan de voorwaarden waardoor het DTC krachtens de Wbni aangewezen zou kunnen worden als organisatie waaraan het NCSC concrete dreigingsinformatie die betrekking heeft op het niet-vitale bedrijfsleven kan delen. Het DTC zou dan de bedrijven over de dreigingsinformatie kunnen informeren. Het Ministerie van EZK is bezig met de voorbereidende werkzaamheden hiervoor en hun streven is dat deze nieuwe dienstverlening begin volgend jaar kan starten.
In bovenvermelde kabinetsreactie op het WRR-rapport is als een van de verschillende maatregelen opgenomen dat wordt geïnventariseerd welke wettelijke bevoegdheden de overheid heeft bij digitale crisissituaties, zodat kan worden bezien waar eventuele aanvullingen nodig zijn.

Vraag 8
In hoeverre onderkent u het risico dat cybercriminelen ook niet-vitale bedrijven grote schade kunnen toebrengen en deze als leveranciers van de vitale sector ook weer vitale bedrijven kunnen beschadigen? Wat kunt en gaat u doen dit risico te mitigeren?

Antwoord 8
De impact van incidenten in de vitale infrastructuur, de snelheid van technologische ontwikkelingen, de verandering van (cyber)dreigingen en de toenemende onderlinge verwevenheid van vitale infrastructuur maakt dat het kabinet blijvende aandacht heeft voor het verhogen en borgen van de weerbaarheid van de vitale infrastructuur. De primaire verantwoordelijkheid voor de continuïteit en weerbaarheid van vitale processen ligt bij de vitale aanbieders zelf. Daarbij hoort het verkrijgen van inzicht in dreigingen en kwetsbaarheden, risico's en het ontwikkelen en onderhouden van capaciteiten waarmee de weerbaarheid van vitale processen wordt verhoogd en geborgd. Aandacht voor risico's die kunnen ontstaan in de leverancierskeketen (inclusief niet-vitale bedrijven) maakt hier onderdeel van uit. In 2018 is voor veilige inkoop en aanbesteding binnen het Rijk een instrumentarium ontwikkeld en ingevoerd door het kabinet. Dit instrumentarium is ook beschikbaar gesteld voor de vitale

[4] https://advisories.ncsc.nl/advisory?id=NCSC-2019-0353

infrastructuur en biedt daarmee een middel voor vitale aanbieders om risico's voor de nationale veiligheid in de toeleveranciersketen in kaart te brengen voordat een opdracht wordt aanbesteed of gegund.

Vraag 9
Hoe gaat u ervoor zorgen dat cyberbeveiliging zowel in het vitale als niet-vitale bedrijfsleven, maar ook binnen de overheid, structureel geborgd wordt én blijft?

Antwoord 9
Zoals reeds aangegeven in de antwoorden op vragen [2, 4 en 7] wordt er structureel ingezet op het verhogen van cybersecurity en heeft het kabinet hier ook in geïnvesteerd.

De overheid treft continu maatregelen om haar digitale dienstverlening blijvend veilig aan te bieden en investeert in de digitale weerbaarheid en herstelvermogen van de openbare sector. Dat betekent aandacht voor preventieve maatregelen, goede detectie van aanvallen en een adequate respons. Het vergroten van de feitelijke veiligheid en oefenen met herstel na een mogelijk ontwrichtende incident hebben daarbij de nadruk. Ik heb uw Kamer in meer detail geïnformeerd in de Agenda Digitale Overheid, NL DIGIbeter[5] en in de Strategische I-agenda Rijksdienst 2019-2021, editie 2020[6].

[5] *Kamerstukken II* 2019/20, 26643, nr. 700
[6] *Kamerstukken II* 2019/20, 26643, nr. 683