AH 2981

2021Z05959

Antwoord van minister Grapperhaus (Justitie en Veiligheid), mede namens minister Schouten (Landbouw, Natuur en Voedselkwaliteit) (ontvangen 28 mei 2021)

Zie ook Aanhangsel Handelingen, vergaderjaar 2020-2021, nr. 2613

Vraag 1

Bent u bekend met het artikel 'Oproep na kaashack: bestempel voedselvoorziening als vitale infrastructuur'?[1]

Antwoord op vraag 1

Ja.

Vraag 2

Wat zijn de voor- en nadelen van de voedselvoorziening als vitale infrastructuur te benoemen?

Antwoord op vraag 2

Bij het identificeren van vitale infrastructuur gaat het niet om een afweging waarbij voor- en nadelen leidend zijn. Dit gebeurt aan de hand van vooraf vastgestelde criteria (zie hiervoor het antwoord op vraag 4) op basis waarvan processen al dan niet als vitaal worden aangemerkt middels een vitaliteitsbeoordeling. Uitgangspunt is hierbij dat uitval of verstoring van het proces tot ernstige maatschappelijke ontwrichting kan leiden. Binnen een als vitaal aangemerkt proces kunnen aanbieders die een belangrijke rol vervullen als vitale aanbieders worden aangemerkt. Rechten en plichten voor deze vitale aanbieders volgen bijvoorbeeld uit de Wet beveiliging netwerk- en informatiesystemen (Wbni) of uit sectorale wetgeving.

Vraag 3

[1] NOS, 12 april 2021, 'Oproep na kaashack: bestempel voedselvoorziening als vitale infrastructuur', https://nos.nl/artikel/2376492-oproep-na-kaas-hack-bestempel-voedselvoorziening-als-vitaleinfrastructuur.html

Wat voor hulp biedt het Nationaal Cyber Security Centrum (NCSC) aan bedrijven die als vitale infrastructuur worden gezien?

Antwoord op vraag 3

Het Nationaal Cyber Security Centrum (NCSC) heeft krachtens de Wbni primair tot taak om vitale aanbieders en andere aanbieders die deel uitmaken van de rijksoverheid te informeren en adviseren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen, waar nodig op andere wijze bijstand te verlenen bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen, en ten behoeve daarvan analyses en technisch onderzoek te verrichten.

Het NCSC werkt hiertoe voortdurend aan de eigen informatiepositie. Dit gebeurt onder meer door het bevorderen van meldingen van organisaties uit bovengenoemde doelgroep van het NCSC (Rijk en vitaal) en het aangaan van samenwerkingsrelaties met andere organisaties.

Vraag 4

Wat zijn de criteria om een bedrijf te kenmerken als vitale infrastructuur?

Antwoord op vraag 4

De Nederlandse vitale infrastructuur wordt gevormd door processen die zo vitaal zijn voor het functioneren van onze samenleving, dat verstoring ervan grote gevolgen voor onze samenleving heeft.[2] De verantwoordelijke vakdepartementen beoordelen of en welke processen vitaal zijn. Dit gebeurt in elk geval om de 4 jaar, maar ook wanneer maatschappelijke ontwikkelingen, zoals veranderende dreigingen of risico´s, daar aanleiding toe geven. Bij deze vitaliteitsbeoordelingen worden vooraf centraal opgestelde impactcriteria gehanteerd. Op hoofdlijnen is bepalend dat uitval of verstoring van het proces tot ernstige maatschappelijke ontwrichting kan leiden. Meer concreet wordt getoetst op basis van criteria als grootschalige economische schade, fysieke gevolgen en cascade effecten. Deze criteria zijn ontwikkeld aan de hand van Europese richtlijnen en een nationale beoordelingssystematiek.

Vraag 5

[2] Kamerstuk 30821, 81

Wat vindt u van de oproep om de voedselvoorziening toe te voegen aan de lijst met bedrijven die worden gezien als vitale infrastructuur?

Antwoord op vraag 5

Ik begrijp die oproep, want voedselvoorziening is vanzelfsprekend heel belangrijk voor onze samenleving. Een objectieve vitaliteitsbeoordeling bepaalt, zoals hierboven vermeld, of een proces wordt aangemerkt als vitaal proces en daarmee deel uitmaakt van de vitale infrastructuur. Elke vier jaar wordt de vitaliteitbeoordeling van processen in elk geval opnieuw doorlopen, zodat nieuwe ontwikkelingen in sectoren of in dreigingen kunnen worden meegenomen. Een dergelijke vitaliteitsbeoordeling van de voedselvoorziening vindt in het kader hiervan later dit jaar plaats door het verantwoordelijke ministerie (Landbouw, Natuur en Voedselkwaliteit). Hierbij moet wel opgemerkt worden dat hoewel voedselvoorziening heel belangrijk is, een proces pas vitaal is als de uitval van een individuele aanbieder leidt tot grootschalige gevolgen.

Vraag 6

Deelt u de verwachting van IT-beveiligingsexperts, dat hackaanvallen op de voedselvoorziening vaker voor zullen komen? Zo nee, waarom niet?

Vraag 7

Kunt u reflecteren op het bericht dat ethische hackers aangeven dat de digitale veiligheid van de voedselvoorziening niet op orde is?

Antwoord op vraag 6 en 7

In het Cybersecuritybeeld Nederland (CSBN 2020)[3] wordt geconstateerd dat de digitale dreiging inmiddels een permanent karakter heeft gekregen. Afpersing via ransomware, waar volgens het artikel van de NOS in dit geval sprake van is, is bijvoorbeeld nog altijd een aantrekkelijk verdienmodel voor criminele actoren, en kan leiden tot financiële maar ook maatschappelijke schade. Daarbij richten ze zich

[3] Kamerstuk 26643, 695

op organisaties waarvan zij verwachten dat die de mogelijkheid hebben om grotere geldbedragen te betalen of waarvoor bedrijfscontinuïteit en een belangrijke rol speelt. In de voedselvoorziening kan dit het geval zijn.

Op dit moment is mij geen beeld van de digitale veiligheid van specifiek de voedselvoorziening bekend. In algemene zin constateert het CSBN 2020 wel dat de weerbaarheid tegen digitale dreigingen nog niet overal op orde is. Bij veruit de meeste digitale aanvallen wordt nog steeds gebruik gemaakt van eenvoudige methoden. Het nemen van basismaatregelen kan helpen om barrières op te werpen of schade te beperken.

Vraag 8

Wat vindt u van de uitspraak dat de pakkans bij hacken laag is? Wat is de reden van de lage pakkans?

Antwoord op vraag 8

Uit voorlopige cijfers blijkt dat het aantal geregistreerde gevallen van computervredebreuk stijgt[4]. Al eerder heb ik uw Kamer geïnformeerd over de uitdagingen bij opsporing in het digitale domein[5]. Het internet is inherent grensoverschrijdend en biedt veel schaalvoordelen. Daders kunnen gemakkelijk in verschillende landen veel slachtoffers maken. Verder zijn online de mogelijkheden tot anonimisering groot, wat het moeilijker maakt de identiteit van verdachten te achterhalen. Het Team High Tech Crime van de Politie en het Landelijk Parket signaleren een toename in de (technische) complexiteit van opsporingsonderzoeken. Dit beïnvloedt de duur en benodigde capaciteit voor opsporingsonderzoeken.

Aangezien het opsporen en vervolgen van cybercrimedelicten complex is zetten de politie en het OM in op een bredere bestrijding. Hieronder vallen ook alternatieve interventies, gericht op preventie en verstoring.

Vraag 9

Moet de overheid meer doen om de pakkans bij hacken te vergroten? Zo ja, wat voor maatregelen heeft u in gedachten? Zo nee, waarom niet?

---

[4] StatLine - Geregistreerde criminaliteit; soort misdrijf, regio (cbs.nl)

[5] Kamerstuk 28648, 621

Antwoord op vraag 9

De afgelopen jaren is er geïnvesteerd in de aanpak van cybercrime bij politie en OM. Zo is de politie met 145 fte uitgebreid, waarmee o.a. de regionale cybercrimeteams zijn versterkt. Vanwege de complexiteit van de opsporing vraagt cybercrime een bredere bestrijding. Daarnaast blijft het van belang dat burgers en organisaties voldoende weerbaar zijn tegen cybercrime.

Er worden ook internationaal maatregelen genomen. Nederland neemt actief deel aan de Europese gesprekken over de E-Evidence-verordening en de gesprekken over een tweede protocol bij het Cybercrimeverdrag, ter bevordering van de grensoverschrijdende opsporing, zowel binnen als buiten de EU. Het is belangrijk om te blijven inzetten op de aanpak van cybercrime, zodat het internet geen vrijplaats wordt voor criminelen.