

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

623

Vragen van het lid **Dassen** (Volt) aan de Ministers van Economische Zaken en Klimaat en van Binnenlandse Zaken en Koninkrijksrelaties over *de urenlange storing bij Facebook en Instagram op 4 oktober 2021* (ingezonden 7 oktober 2021).

Antwoord van Minister **Blok** (Economische Zaken en Klimaat), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 10 november 2021).

Vraag 1

Heeft de grootschalige storing impact gehad op de bedrijfsvoering van de Nederlandse overheid (op de verschillende lagen)? Zo ja, op welke manier? Heeft de Nederlandse overheid daarbij schade geleden?

Antwoord 1

Facebook, Whatsapp en Instagram zijn voornamelijk berichtenplatforms. Voor de rijksoverheid is de Gedragsregeling Digitale Werkomgeving van toepassing, waarin staat dat dergelijke berichtenapps alleen gebruikt mogen worden voor informele zaken, zoals een interessant artikel delen, een hulpvraag stellen of sparren met collega's. Er is geen standaard voor berichtenapps vastgesteld, waardoor een dergelijke storing niet direct leidt tot een belemmering in de bedrijfsvoering.

Voor zover mij bekend heeft de storing niet geleid tot belemmering van de bedrijfsvoering bij gemeenten, waterschappen en provincies. Overheidsorganisaties zijn zelf verantwoordelijk voor hun bedrijfsvoering en de beveiliging van informatie en informatiesystemen, zij hanteren daarbij vergelijkbare gedragsregelingen als bij de rijksoverheid.

Vraag 2

Heeft het demissionaire kabinet berichten van Nederlandse burgers, bedrijven en organisaties gehad, die last hebben ervaren van de storing? Zo ja, hoeveel? Wat was de inhoud van deze berichten? Welk algemeen beeld kan hieruit worden afgeleid?

Antwoord 2

Er zijn op dit moment geen signalen bekend over dergelijke aan het kabinet gerichte berichten. In algemene zin kan worden gesteld dat Nederlandse burgers, bedrijven en organisaties hinder en/of ongemak zullen hebben ervaren als gevolg van deze storing, die optrad als gevolg van een menselijke

fout. Het betrof immers uitval van diensten die door Nederlandse burgers en bedrijven veel gebruikt worden, waaronder sociale-media platforms Facebook en Instagram en berichtendiensten WhatsApp en Facebook Messenger. Hoewel het een grote communicatiestoring betrof in termen van gebruikers-uren (duur uitval * getroffen gebruikers), lijkt in dit geval de maatschappelijke en economische schade in Nederland mee te vallen.

Het betrof uitval van diensten die door Nederlandse burgers en bedrijven veel gebruikt worden, waaronder sociale-media platforms Facebook en Instagram en berichtendiensten WhatsApp en Facebook Messenger. Vanzelfsprekend zullen burgers en organisaties die meer gebruik maken van Facebook-diensten meer hinder hebben ondervonden.

Zo lijkt een deel van de gebruikers zonder grote problemen te zijn uitgeweken naar alternatieve diensten. Diverse andere sociale-media platforms en berichtendiensten gaven aan dat het gebruik van hun diensten tijdens en na de storing is toegenomen. Voor zover organisaties en bedrijven tijdelijk verminderd bereikbaar waren, is de verwachting dat dienstverlening over het algemeen op een later moment alsnog heeft kunnen plaatsvinden.

Vraag 3

Hoe is het demissionaire kabinet voornemens in de (recente) toekomst om te gaan met zulke grootschalige digitale storingen?

Antwoord 3

Het is in eerste instantie primair aan Facebook zelf om de benodigde technische en organisatorische maatregelen te treffen om een storing als deze te voorkomen, of wanneer deze zich toch voordoet, zo snel mogelijk te verhelpen.

Parallel daaraan hebben gebruikers een eigen verantwoordelijkheid om voor zichzelf na te gaan in hoeverre het voor hen verantwoord is om van één dienst of één bedrijf afhankelijk te zijn en zo nodig alternatieven te verkennen en te gebruiken.

Voor zover het de storing van de berichtendiensten WhatsApp en Facebook Messenger betreft: deze diensten zijn zogeheten nummeronafhankelijke interpersoonlijke communicatiediensten. Zij vallen daarmee onder de verbrede definitie van een elektronische communicatiedienst zoals gedefinieerd in het wetsvoorstel tot wijziging van de telecomwet ter implementatie van Richtlijn 2018/1972 (de Telecomcode) (Kamerstuk 35 865, nr. 2) zoals deze op dit moment bij uw Kamer voorligt. Dat betekent dat na inwerkingtreding van bovenvermelde wijziging van de telecomwet (TW) de aanbieders van deze diensten straks ook een meldplicht van incidenten (TW art. 11.a2) en een zorgplicht (treffen van passende beveiligingsmaatregelen onder meer om, als het gaat om dergelijke storingen, in bepaalde mate bestand te zijn tegen acties die de beschikbaarheid van de dienst in gevaar brengen, (TW art. 11.a1) opgelegd krijgen, zoals dat nu al geldt voor aanbieders van traditionele elektronische communicatiediensten als spraaktelefonie en berichtenverkeer (SMS). Agentschap Telecom is hiervoor de aangewezen toezichthouder.

Op Europees niveau wordt gewerkt aan een herziening van de richtlijn (2016/1148) ter bevordering van de beveiliging van netwerk- en informatiesystemen, NIB2. De huidige richtlijn is in Nederland geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Op grond van de huidige NIB-richtlijn is de Ierse toezichthouder exclusief bevoegd om toe te zien op Facebook-clouddiensten daar de Europese vestiging van het bedrijf in Ierland is gevestigd. Met betrekking tot het herzieningsvoorstel¹ heeft de Europese Commissie voorgesteld om in deze herziening ook sociale media op te nemen. Over deze richtlijn wordt momenteel onderhandeld.

In het ECASEC²-overleg van ENISA³ en de Europese toezichthouders die toezien op de telecomveiligheid worden ook incidenten en te nemen maatregelen besproken. Dit gebeurt nu voor de meer traditionele elektronische communicatiediensten en zal naar verwachting straks ook gaan gelden voor de interpersoonlijke communicatiediensten. Hierdoor kunnen vroegtijdig

¹ COM (2020) 823

² European Competent Authorities for Secure Electronic Communications

³ Het agentschap van de Europese Unie voor cyberbeveiliging

trends en ontwikkelingen in incidenten worden gesignaleerd. Dat kan er bijvoorbeeld toe leiden dat de toezichthouders bij het uitoefenen van het toezicht op de zorgplicht extra aandacht gaan besteden aan de bepaalde oorzaken van incidenten. ENISA publiceert jaarlijks⁴ de grote incidenten die nationale toezichthouders doormelden aan ENISA.

Ter voorbereiding op een digitale crisis is er het Nationaal Crisisplan Digitaal.⁵ Het plan is een leidraad om op hoofdlijnen snel inzicht en overzicht te krijgen in de bestaande afspraken op nationaal niveau over de beheersing van incidenten in het digitale domein met aanzienlijke maatschappelijke gevolgen. Het plan sluit daarmee aan op het Nationaal Handboek Crisisbesluitvorming. In dit geval is er geen aanleiding geweest om op te schalen binnen de nationale crisisstructuur.

Vraag 4

Is het demissionaire kabinet voornemens tijdens de Europese wetgevingsonderhandelingen inzake de Digital Services Act, de Digital Markets Act en de Artificial-Intelligence-verordeningen, en direct al bij de komende Europese top, het belang van het vernieuwen en updaten van de Border Gateway Protocol aan te kaarten? Zo ja, hoe gaat het demissionaire kabinet dit aanpakken? Zo niet, waarom niet?

Antwoord 4

Deze casus heeft geen invloed op de Nederlandse positie in de onderhandelingen aangaande de Europese wetsvoorstellen voor een Digital Services Act, een Digital Markets Act en een AI Act, omdat de casus buiten de reikwijdtes van deze voorstellen valt. Wel ziet het kabinet het belang van het doorontwikkelen van internetstandaarden zoals het Border Gateway Protocol (BGP). Facebook heeft na afloop van de storing verklaard dat deze veroorzaakt is door een menselijke fout in de BGP-configuratie van het Facebook-netwerk die niet tijdig is opgemerkt.⁶ Het BGP is het belangrijkste routeringsprotocol van het internet. Het zorgt ervoor dat zogenaamde Autonome Systemen (AS) elkaar kunnen vinden op het internet. Het BGP zorgt voor de koppeling tussen verschillende AS-netwerken. In dit geval heeft Facebook, door een interne (menselijke) fout, abusievelijk alle routes tussen haar netwerk en de rest van het wereldwijde Internet opgeheven, waardoor de Facebook-servers voor de rest van het Internet niet meer bereikbaar waren. Het BGP-protocol heeft in deze correct gefunctioneerd.

Het BGP wordt ontwikkeld onder de vlag van de Internet Engineering Task Force (IETF). De doorontwikkeling van een dergelijke essentiële standaard is complex en vereist een wereldwijde consensus tussen betrokken en deskundige partijen. De IETF is een grote, open, internationale gemeenschap van netwerkontwerpers, -operators, -leveranciers en -onderzoekers die zich bezighoudt met de evolutie van de internetarchitectuur en de soepele werking van het internet. Om bij deze casus te blijven, ook Facebook neemt deel aan de IETF. Nederland staat voor het multi-stakeholder model van internet governance, waarvan de IETF een goed voorbeeld is. Het kabinet ziet naar aanleiding van deze casus geen noodzaak de werkwijze van de IETF ter discussie stellen.

Wel laat ik de ontwikkelingen rond dergelijke standaardisatievraagstukken volgen en duiden. Agentschap Telecom voert daartoe op dit moment een onderzoek uit naar de belangrijkste vraagstukken rond technische internetstandaardisatie.

Vraag 5

Deelt het demissionaire kabinet de mening dat dit incident wederom aantoont hoe groot de afhankelijkheid van slechts enkele tech-grootmachten op dit moment is en dat deze buitenproportionele afhankelijkheid, middels Europese wetgeving, noodzakelijkerwijs en spoedig ingeperkt dient te worden ter bescherming van Europese burgers en bedrijfsleven? Zo ja, hoe gaat het demissionaire kabinet dit aanpakken? Zo niet, waarom deelt het demissionaire kabinet deze mening niet?

⁴ <https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020>

⁵ Nationaal Crisisplan Digitaal, bijlage bij Kamerstuk 30 821, nr. 660

⁶ More details about the October 4 outage – Facebook Engineering (fb.com)

Antwoord 5

Het kabinet heeft al een tijd zorgen over de afhankelijkheid van een aantal grote platforms waar ondernemers en consumenten nauwelijks meer omheen kunnen. Vandaar dat het kabinet sinds 2019 pleit voor aanvullende regelgeving om met de macht van deze poortwachters om te gaan (Kamerstuk 27 879, nr. 71 en Kamerstuk 35 134, nr. 13). Dit heeft zijn vruchten afgeworpen. De Europese Commissie heeft in december 2020 een voorstel gedaan voor de Digital Markets Act (DMA) waarmee zij dit soort problematiek wil aanpakken. Dit voorstel is voor een groot deel in lijn met de Nederlandse inzet voor de DMA, die in februari per BNC-fiche naar uw Kamer is verzonden (Kamerstuk 22 112, nr. 3049). Ook is deze inzet tijdens de Technische Briefing over de DMA met de Commissie Digitale Zaken van eind september toegelicht. De onderhandelingen in de Raad over het voorstel lopen in een ambitieus tempo door. Er wordt gestreefd naar het aannemen van een algemene oriëntatie in de Raad voor Concurrentievermogen eind november.

Vraag 6

Welke maatregelen gaat het demissionaire kabinet treffen naar aanleiding van de grootschalige storing?

Antwoord 6

In de beantwoording van vragen 3, 4 en 5 is de inzet van het kabinet uiteengezet.