Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Vragen gesteld door de leden der Kamer

2020Z15381

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»* (ingezonden 2 september 2020).

Vraag 1
Bent u bekend met het bericht «Hack bij Apollo Vredestein toont zwakke cyberbeveiliging Nederlandse bedrijven»[1] en het bericht «Overheid wist wie kwetsbaar was, maar liet bedrijven toch gehackt worden»?[2]

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)?

Vraag 3
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?

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

[1] Het Financieele Dagblad, 4 augustus 2020, https://fd.nl/ondernemen/1353014/hack-apollo-vredestein-legt-zwakke-cyberbeveiliging-bij-bedrijven-bloot.
[2] Het Financieele Dagblad, 17 augustus 2020, https://fd.nl/ondernemen/1353350/overheid-wist-wie-kwetsbaar-was-maar-liet-bedrijven-toch-gehackt-worden.

dusver voorgekomen dat de overheid heeft ingegrepen ingeval bedrijven kwetsbaar bleken op het gebied van (cyber)beveiliging, en op welke manieren?

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?

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)?

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 hier van 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?

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 om dit risico te mitigeren?

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?