Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

1297

Vragen van het lid **Van den Nieuwenhuijzen** (GroenLinks) aan de Minister van Defensie over *de beveiliging van ICT bij het Ministerie van Defensie* (ingezonden 16 december 2020).

Antwoord van Minister **Bijleveld-Schouten** (Defensie) (ontvangen 12 januari 2021)

Vraag 1
Klopt het dat een ICT-journalist op het Ministerie van Defensie alleen is gelaten in een ruimte met een router, UTP-kabel en diverse toegangspoorten tot het netwerk?[1]

Antwoord 1
Op 15 december 2020 ontving Defensie een journalist op het ministerie die kort in een wachtruimte alleen is gelaten. De betreffende wachtkamer is voorzien van een zogeheten *wall-outlet* met internetaansluiting waarop een wifi acces point is aangesloten. Via deze aansluiting kunnen bezoekers alleen gebruik maken van een afgeschermde internetverbinding voor gasten.

Vraag 2
Kunt u uitsluiten dat ook in andere gevallen mensen op het Ministerie van Defensie alleen zijn gelaten in ruimtes waar men zich toegang zou kunnen verschaffen tot het netwerk van uw ministerie?

Antwoord 2
Defensie hanteert een toegangsbeleid en bezoekersregeling op het ministerie waarbij bezoekers begeleid worden door een daarvoor verantwoordelijke gastheer. Het kan voorkomen dat een bezoeker, die in een werk- of wachtkamer wordt ontvangen, korte tijd alleen wordt gelaten. Dit betekent echter niet dat bezoekers in deze kort tijd toegang kunnen verkrijgen tot het netwerk van Defensie. Door het inzetten van technische maatregelen in het netwerk, op outlets en op de werkstations wordt toegang door bezoekers tot het netwerk tegengegaan.

[1] https://twitter.com/danielverlaan/status/1338892475717529606

ah-tk-20202021-1297
ISSN 0921 - 7398
's-Gravenhage 2021

Vraag 3
Kunt u uitsluiten dat bezoekers bij het Ministerie van Defensie militair gevoelige gegevens hebben buitgemaakt?

Antwoord 3
Defensie behandelt gevoelige gegevens overeenkomstig de in het Defensie Beveiligingsbeleid vastgestelde normen en maatregelen. Gevoelige gegevens worden opgeslagen binnen hoger gerubriceerde netwerkomgevingen die zich in beveiligde ruimtes bevinden. Wanneer Defensie een bezoeker ontvangt in een van deze beveiligde ruimtes wordt hij/zij te allen tijde begeleid en voorzien van een gekleurde pas die altijd zichtbaar gedragen dient te worden.

Vraag 4
Zijn er pogingen geweest om informatie van de ICT-systemen van Defensie, op uw ministerie dan wel op andere locaties van Defensie, buit te maken in de laatste jaren, die zijn opgemerkt en/of voorkomen? Zo ja, om hoeveel pogingen gaat het?

Antwoord 4
Elke dag worden er in Nederland cyberaanvallen uitgevoerd. Het JIVC (met oa. het Defensie Cyber Security Centrum), lokale beheerorganisaties en gebruikers beschermen Defensie tegen deze dreiging. Gerubriceerde en/of gemerkte fysieke informatie (documentaire informatie) wordt binnen Defensie opgeslagen in beveiligde werkomgevingen en/of beveiligde ruimten. Al naar gelang de hoogte van de rubricering worden aanvullende beveiligingsmaatregelen getroffen om ontvreemding van die informatie te voorkomen. Doelgerichte pogingen door bezoekers om op locatie informatie buit te maken zijn niet bekend.

Vraag 5 en 6
Zijn er richtlijnen of werkinstructies voor ICT-veiligheid op uw ministerie? Zo ja, zijn die up-to-date en effectief? Zo nee, waarom niet?
Indien u wel richtlijnen of werkinstructies voor ICT-veiligheid op uw ministerie heeft, wat is hierin dan opgenomen over het alleen laten van bezoekers in ruimtes met netwerkpoorten en de omgang met gevoelige informatie op papier, zoals bijvoorbeeld codes en wachtwoorden voor besloten vergaderingen?

Antwoord 5 en 6
Defensie heeft, als onderdeel van het Defensie Beveiligingsbeleid, instructies voor ICT-beveiliging en -veiligheid, die minimaal tweejaarlijks worden geëvalueerd, waaronder op effectiviteit.
Defensie heeft, conform het Defensie Beveiligingsbeleid en in overeenstemming met het Rijksbreed geldende Voorschrift Informatiebeveiliging Rijk – Bijzondere Informatie (VIR-BI), de beveiliging ingericht middels vier lagen die verschillende beveiligingsniveaus kennen (waarbij niveau één «hoog» is en niveau vier «laag»). Zo zijn poorten voor hoger gerubriceerde netwerksystemen bijvoorbeeld niet toegankelijk voor bezoekers in verband met de permanente begeleiding in de beveiligde ruimten. In het geval van besloten vergaderingen treft Defensie de nodige beveiligingsmaatregelen, waaronder ook het tegengaan van opnamen of afluisteren. Wachtwoorden en codes worden regelmatig door de gebruikers gewijzigd omdat dit middels het systeem automatisch wordt afgedwongen.

Vraag 7
Bent u bereid om professionals van bijvoorbeeld de veiligheidsdiensten de Defensieorganisatie te laten doorlichten op ICT-veiligheid? Zo nee, waarom niet?

Antwoord 7
Defensie voert jaarlijks meerdere soorten *security assessments* uit op het gebied van (ICT-) beveiliging. Dit gebeurt ook in samenwerking met de veiligheidsdiensten. Daarnaast staat de IT-beheerder van Defensie in nauw contact met onder meer het Defensie Cyber Security Centrum. Bij vermoedens van incidenten, of om andere veiligheidsredenen, voert Defensie onderzoek uit en worden de systemen doorgelicht.