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

2226

Vragen van het lid **Van Nispen** (SP) aan de Minister voor Rechtsbescherming over *het bericht dat de Autoriteit Persoonsgegevens de noodklok luidt om de stijging van het aantal hacks bij datalekken* (ingezonden 2 maart 2021).

Antwoord van Minister **Dekker** (Rechtsbescherming) (ontvangen 1 april 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 2106.

Vraag 1
Heeft u kennisgenomen van het bericht dat het aantal meldingen van hacking, phishing en malware bij datalekken het afgelopen jaar met 30% is gestegen ten opzichte van het voorgaande jaar?[1]

Antwoord 1
Ja.

Vraag 2
Hoe verklaart u dat de overheid, meer dan ooit, persoonsgegevens heeft afgegeven of verstuurd aan de verkeerde ontvanger? Wat wordt er concreet aan gedaan om dit soort fouten te voorkomen?

Antwoord 2
Deze vraag ziet op de constatering in de Rapportage datalekken 2020 van de AP dat het aantal meldingen van datalekken vanuit de overheid is gestegen en dat deze stijging vooral komt doordat er meer persoonsgegevens zijn afgegeven of verstuurd aan een verkeerde ontvanger.
De constatering heeft betrekking op de openbare sector als geheel, waardoor het moeilijk is om dit punt toe te schrijven aan een specifiek deel daarvan. Ook wordt uit de rapportage niet duidelijk wat de oorzaak is van (de stijging van) het verkeerd versturen van persoonsgegevens; het kan bijvoorbeeld een menselijke fout betreffen of een onjuiste registratie van een e-mailadres. Dat neemt niet weg dat bij de overheid wordt geïnvesteerd in het verhogen van de beveiliging van informatie en dus ook in de beveiliging van persoonsgegevens. Concreet loopt bij de overheid de implementatie van de Baseline

[1] Autoriteit Persoonsgegevens, 1 maart 2021, «AP luidt noodklok: explosieve toename hacks en datadiefstal», https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-luidt-noodklok-explosieve-toename-hacks-en-datadiefstal

ah-tk-20202021-2226
ISSN 0921 - 7398
's-Gravenhage 2021

Informatiebeveiliging Overheid (BIO). Onderdeel van de BIO is het verhogen van het beveiligingsbewustzijn van medewerkers.

Vraag 3, 4
Hebben de Autoriteit Persoonsgegevens en de politie genoeg capaciteit om alle meldingen van hacks, phishing en malware goed te onderzoeken? Zo ja, waaruit blijkt dat?
Hoeveel fte hebben de Autoriteit Persoonsgegevens en politie om zelf actief op zoek te gaan naar hacks en datadiefstallen?

Antwoord 3, 4
Het opsporen van cybercriminaliteit is geen taak van de AP. De AP houdt toezicht op de uitvoering van de AVG. Als door een datalek inbreuk wordt gemaakt op de persoonlijke levenssfeer van burgers, dan is een bedrijf verplicht daarvan een melding te doen bij de AP. De AP kan naar aanleiding van de melding onderzoek doen naar het datalek en eventueel een boete opleggen. In het onderzoek dat door KPMG is uitgevoerd naar de capaciteit en de financiële middelen van de AP is geconcludeerd dat er nog te veel onzekerheden aanwezig zijn om voor de AP tot een eenduidige, meerjarige, vooruitkijkende capaciteitsraming te komen. Ik voer gesprekken met de AP om te zorgen dat haar datapositie wordt verbeterd, om zodoende meer zicht te krijgen op de benodigde capaciteit (brief aan TK van 1 maart 2021, kenmerk 3218059).
Indien aan het datalek een misdrijf – zoals een hack, phishing, malware of een datadiefstal – ten grondslag ligt dan wordt het bedrijf aangemoedigd daarvan aangifte te doen bij de politie. Voor de opsporing van cybercrime beschikt de politie over het Team High Tech Crime van de Landelijke Eenheid en de cybercrimeteams in de regionale eenheden. Deze laatste zijn met gelden uit het Regeerakkoord de afgelopen jaren met 100 fte uitgebreid. Daarnaast is 45 fte ingezet om de aanpak verder te versterken, bijvoorbeeld voor het verbeteren van de intelligence. De politie werkt met een fenomeen-aanpak, waarbij zij proactief kijkt naar de brede bestrijding van specifieke cybercrime-fenomenen. Zeker gezien de digitalisering van onze samenleving is het aannemelijk dat cybercrime zal toenemen. Daarom wordt naast opsporing ook ingezet op alternatieve interventies met publieke en private partners, zoals verstoring en preventie.

Vraag 5
Hoeveel van de in het bericht genoemde 1173 meldingen van hacks en datadiefstallen hebben opvolging gekregen bij de politie? In hoeveel van die gevallen zijn ook daadwerkelijk daders opgespoord en straffen opgelegd?

Antwoord 5
De meldplicht van datalekken staat los van een mogelijke aangifte van datadiefstal. Het is daarom niet mogelijk om vast te stellen welke meldingen bij de AP hebben geleid tot opsporing en/of vervolging. Uiteraard worden burgers, organisaties en bedrijven die het slachtoffer zijn van datadiefstal aangemoedigd om aangifte te doen, zodat daders opgespoord kunnen worden.

Vraag 6
Wat is uw reactie op de suggestie dat veel schade beperkt of zelfs voorkomen had kunnen worden als «meerfactorauthenticatie» was gebruikt bij het inlogproces? Zou meerfactorauthenticatie dan niet de standaard moeten zijn om in te loggen? Bent u bereid te kijken naar manieren om meerfactorauthenticatie de norm te maken bij online inlogprocedures?

Antwoord 6
Meerfactorauthenticatie is in beginsel veiliger dan toegangscontrole waarbij een enkele factor voor authenticatie wordt gebruikt. Daarom adviseren het Nationaal Cyber Security Centrum (NCSC), het DTC en www.veiliginternetten.nl meerfactorauthenticatie te gebruiken waar dat wordt aangeboden en wordt hier aandacht aan besteed in bewustwordingsactiviteiten bij specifieke doelgroepen. Daarnaast adviseert het NCSC aan systeemeigenaren meerfactorauthenticatie zo veel mogelijk aan te bieden. In het kader van het publieke-private Convenant Preventie Cybercriminaliteit spreken de ministe-

ries van Economische Zaken en Klimaat en Justitie en Veiligheid met diverse publieke en private partijen onder meer over hoe meerfactorauthenticatie breder kan worden gebruikt.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Kuiken (PvdA), ingezonden 1 maart 2021 (vraagnummer 2021Z03983).