Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

1570

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Technologieleverancier van Defensie en politie gehackt, losgeld geëist voor vertrouwelijke informatie»* (ingezonden 14 december 2021).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 4 februari 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1242.

Vraag 1
Bent u bekend met het bericht «Technologieleverancier van Defensie en politie gehackt, losgeld geëist voor vertrouwelijke informatie»[1]?

Antwoord 1
Ja. Dit voorval is zeer onwenselijk. Onderdeel van ons beleid is beter te gaan monitoren hoe toeleveranciers van de overheid omgaan met onze data. Het gaat daarbij om een samenhang van de te treffen beveiligingsmaatregelen (in zowel de contracten van de overheid als van de ICT-leverancier) als om het inregelen van toezicht. Ook het beleid van ICT-leveranciers ten aanzien van ransomware moet hierin worden meegenomen.

Vraag 2
Aan welke overheidsorganisaties levert Abiom communicatietechnologie?

Antwoord 2
Voor zover bekend nemen onder andere de Nationale Politie, de Dienst Justitiële Inrichtingen, Rijkswaterstaat, het Centraal Bureau Rijvaardigheidsbewijzen, Luchtverkeersleiding Nederland en het Ministerie van Defensie diensten en producten af van Abiom. Abiom levert in dat verband aan verschillende overheidsorganisaties onder andere C2000 portofoons en communicatietechnologie. Op dit moment is er geen uitputtende lijst bekend van het gebruik van ICT-producten zoals dat van Abiom binnen de overheid. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties werkt aan de wettelijke verankering van en toezicht op informatieveiligheid voor het gehele

[1] https://www.volkskrant.nl/nieuws-achtergrond/technologieleverancier-van-defensie-en-politie-gehackt-losgeld-geeist-voor-vertrouwelijke-informatie~bcc2f42b/?utm_source=browser_push&utm_medium=push&utm_campaign=stdc_vk.

ah-tk-20212022-1570
ISSN 0921 - 7398
's-Gravenhage 2022

openbaar bestuur, waaronder de Baseline Informatiebeveiliging Overheid (BIO) in een volgende tranche van de Wet Digitale Overheid (WDO). Overwogen wordt om in nadere regelgeving op te nemen dat bij iedere bestuurslaag voldoende snel kan worden achterhaald welke organisaties gebruik maken van welke leveranciers en/of software. Met deze informatiepositie kan de overheid haar respons op toekomstige digitale aanvallen beter invulling geven.

Vraag 3
Gelden er bepaalde (veiligheids)eisen voor kritieke toeleveranciers zoals Abiom die technologie leveren aan overheidsorganisaties? Zo ja, welke en in welke mate wordt hierop gescreend bij aanbestedingsprocessen? Zo nee, waarom niet?

Antwoord 3

(Veiligheids)eisen zijn van toepassing op alle leveranciers. Zoals bijvoorbeeld in antwoord op eerdere Kamervragen over het bericht «Litouwen adviseert consument geen Xiaomi-telefoons meer te kopen» is aangegeven, is voor de aanschaf van ICT-producten en diensten, door de overheid de Baseline Informatiebeveiliging Overheid (BIO) van kracht.[2, 3] De uitgangspunten van de BIO zijn onder andere risicomanagement en de eigen verantwoordelijkheid van overheidsorganisaties. Dat betekent dat organisaties zelf risicoafwegingen uitvoeren voordat ICT-producten en diensten van een leverancier worden afgenomen. Op grond van die risicoafwegingen bepalen zij dan de toepassing binnen hun eigen bedrijfsprocessen. De inkopende overheidsorganisatie bepaalt ook aan welke eisen een leverancier moet voldoen om voor verlening van een opdracht in aanmerking te komen. Deze overheidsorganisaties zullen ook tijdens de looptijd van het contract moeten toezien op het naleven van die eisen door de leverancier.
Om de inkopende overheidsorganisatie te helpen bij het bepalen aan welke inkoopeisen op het gebied van informatieveiligheid moet worden voldaan in het geval van ICT-producten en -diensten heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties samen met het Ministerie van Economische Zaken en Klimaat een inkooptool ontwikkeld, de zogenaamde ICO-wizard, Inkoopeisen Cybersecurity Overheid.[4]
Tevens geldt in algemene zin dat bij de inkoop en aanbesteding van producten en diensten binnen de rijksoverheid (eventuele) risico's voor de nationale veiligheid worden meegewogen. Hierbij wordt in het bijzonder gelet op mogelijke risico's ten aanzien van de continuïteit van vitale processen, de integriteit en exclusiviteit van kennis en informatie en de ongewenste opbouw van strategische afhankelijkheden. Bij elke casus wordt bezien hoe risico's beheersbaar kunnen worden gemaakt. Het uitgangspunt is dat maatregelen die hiertoe genomen worden proportioneel zijn. Dit vergt een gedetailleerde analyse van de te beschermen belangen, de dreiging en de (huidige) weerbaarheid.[5] Uiteindelijk is het aan de opdrachtgever om deze risicoafweging te maken en mitigerende maatregelen te implementeren en te monitoren. De term «kritieke toeleveranciers» heeft geen specifieke status binnen de overheid.
In algemene zin biedt het wettelijk kader de mogelijkheid om bij inkoop en aanbestedingen specifieke (veiligheids)eisen als voorwaarden te stellen aan de (mogelijke) opdrachtnemer. Hier kan op worden gecontroleerd tijdens het aanbestedingsproces en gedurende de looptijd van het contract. Ook hier geldt dat de betreffende overheidsorganisatie hier zelf verantwoordelijk voor is.

Politie:
Bij alle Europese aanbestedingen betreffende door de Politie te verlenen opdrachten zijn eisen en contractuele bepalingen opgenomen die zich richten op geheimhouding en de verwerking van persoonsgegevens. Met de

---

[2] Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 578.
[3] *Stcrt.* 2020, 7857.
[4] https://www.bio-overheid.nl/ico-wizard/.
[5] Aanhangsel Handelingen vergaderjaar 2021–2022, nr. 753.

toeleveranciers van de politie worden – indien nodig – verwerkersovereenkomsten gesloten. In deze overeenkomsten staan de eisen met betrekking tot de omgang met informatie opgenomen waaraan een toeleverancier moet voldoen om leverancier van de politie te kunnen zijn. Deze eisen neemt de politie al mee bij de (voor-)selectiekeuzen voor leveranciers. Daarnaast worden, wanneer relevant, bij aanbestedingen eisen opgenomen die betrekking hebben op het beschermen van (digitale) politiegegevens, het vernietigen na gebruik en de plicht tot het melden van datalekken. Recentelijk is door de Korpsleiding van de politie besloten tot het intensiveren van het toezicht tijdens de uitvoeringsfase van een contract waarbij substantiële veiligheidsrisico's zijn voorzien.

Defensie:
Voor Defensie geldt dat de Algemene Beveiligingseisen Defensieopdrachten (ABDO) van toepassing is op gerubriceerde opdrachten die Defensie bij de industrie belegt. De ABDO voorziet in diverse maatregelen om gerubriceerde informatie te beveiligen tegen een dreiging van bijvoorbeeld statelijke actoren. Welke (beveiligings-)eisen van toepassing zijn wordt per opdracht bepaald. ABDO is ook van toepassing op subcontractors en heeft daarmee impact op de beveiliging van de hele keten waar een gerubriceerde opdracht wordt belegd. De MIVD houdt toezicht op het naleven van de ABDO. Er worden in het openbaar geen uitspraken gedaan over welke bedrijven dit betreft.

Vraag 4
Deelt u de mening dat het goed is om de minimale veiligheidseisen voor IT-leveranciers te herzien en wellicht te verhogen om de kans op hacks met grootschalige impact zo klein mogelijk te maken? Zo ja, welke veiligheidseisen heeft u voor ogen en vanaf wanneer? Zo nee, waarom niet?

Antwoord 4
De minimale beveiligingseisen waar IT-leveranciers van overheden zich aan moeten houden liggen vast in de BIO. De uitdaging ligt in het toepassen van de BIO bij bijvoorbeeld inkooptrajecten. Die eisen zullen specifiek ingevuld moeten worden voor de verschillende in gebruik te nemen ICT-producten en -diensten. De inkooptool, de eerdergenoemde ICO-wizard, die ontwikkeld is voor tien inkoopsegmenten, ondersteunt de inkopende overheidsorganisaties bij het bepalen en/of uitwerken van deze beveiligingseisen. Dat ontheft de inkopende organisatie niet van de verantwoordelijkheid om zelf op basis van risicomanagement te bepalen welke eisen in relatie tot de inkoop van ICT-producten of -diensten moeten komen te gelden.
Daarnaast wijs ik er graag op dat er op dit moment binnen de EU wordt onderhandeld over de herziening van de Netwerk- en Informatiebeveiligingsrichtlijn (NIB2-richtlijn). Deze richtlijn regelt onder meer dat entiteiten in 16 sectoren, waaronder de overheid, maatregelen moeten nemen om risico's voor hun netwerk- en informatiesystemen die zij gebruiken bij het leveren van hun diensten te beheersen. Onderdeel van deze zorgplicht is dat zij rekening moeten houden met risico's die voortkomen uit de relatie met hun leveranciers en dienstverleners. Op de naleving van de bepalingen uit de richtlijn moet worden toegezien door de lidstaten via hun nationale toezichthouders.

Vraag 5
Aan welke eisen moeten IT-leveranciers aan de overheid voldoen na een veiligheidsincident zoals een hack? Welk controle of testen worden er uitgevoerd?

Antwoord 5
De BIO schrijft voor dat er na een incident een analyse moet worden gemaakt ter voorkoming van vergelijkbare incidenten in de toekomst. Dit voorschrift geldt voor zowel de proceseigenaar als voor de leverancier. Dergelijke analyses moeten worden gedeeld met relevante partners om herhaling van en toekomstige incidenten te voorkomen. De exacte invulling hiervan is afhankelijk van de aard en het belang van het betreffende ICT-proces en zal voor elke organisatie per geval verschillen. Los hiervan moeten (overheids)organisaties inbreuken in verband met persoonsgegevens bij de Autoriteit

Persoonsgegevens melden, indien die inbreuk een risico vormt voor de rechten en vrijheden van personen.

Vraag 6
Klopt het dat de ransomwaregroep LockBit vertrouwelijke documenten online heeft gezet? Zo ja, om wat voor documenten en gegevens gaat het en komen hierdoor processen van de overheid in gevaar en/of lopen burgers gevaar om eventueel slachtoffer te worden van misbruik met hun gegevens?

Antwoord 6
Nee, burgers en processen van de overheid lopen, voor zover bekend, geen gevaar om door dit lek slachtoffer te worden van misbruik met hun gegevens. In tegenstelling tot de genoemde berichtgeving heeft Abiom geen kopieën van paspoorten van de politieambtenaren, verdachten, verbalisanten en/of benadeelden ontvangen vanuit de politie. De informatie die door de ransomwaregroep LockBit is gepubliceerd betreft – in het geval van de politie – kentekens van voertuigen en een zeer beperkt aantal zakelijke e-mailadressen van medewerkers. Deze informatie heeft Abiom tot zijn beschikking vanwege uitlevering van randapparatuur zoals bijvoorbeeld op maat gemaakte oortjes voor communicatievoorzieningen. Deze informatie stond op facturen van Abiom aan de politie. De vrijgekomen informatie heeft naar verwachting een beperkte impact op het operationele proces. Op basis van de nu beschikbare informatie kunnen politiemedewerkers en andere hulpverleners nog steeds veilig gebruik maken van C2000. Ook de informatie ten behoeve van het primaire proces bij meldkamers en politiediensten is nog steeds beschikbaar en ongewijzigd.
Naar huidig inzicht heeft de vrijgekomen informatie een beperkte impact gehad bij Defensie. Uit onderzoek is gebleken dat van enkele Defensiemedewerkers contactgegevens zijn gelekt en een beperkte hoeveelheid ongerubriceerde informatie. Deze informatie had geen betrekking op operationele eenheden. Ook zijn er geen missies in gevaar gekomen.

Vraag 7
Wat is het bedrag dat LockBit vraagt voor het niet publiceren van deze documenten? Klopt het dat Abiom niet is ingegaan op de eis van de hackers?

Antwoord 7
Zoals aangegeven in een statement van Abiom over het incident is er in overleg met de politie door Abiom besloten om niet in contact te treden met de actor die verantwoordelijk is voor de ransomware-aanval.[6] In verband met het lopende politieonderzoek kan er op dit moment niet nader in worden gegaan op de casus.

Vraag 8
Is bekend waarom een ransomware-aanval bij Abiom is gedaan, wat de werkwijze van de criminelen is en wie hier eventueel achter zit? Zo nee, wordt daar nog onderzoek naar gedaan?

Antwoord 8
Op basis van de beschikbare informatie wordt ervan uitgegaan dat LockBit informatie heeft gestolen met het doel om losgeld te verkrijgen voor het niet publiceren van vertrouwelijke informatie. Vanwege het lopende politieonderzoek kan geen nadere informatie worden gegeven over de casus.

Vraag 9
Wordt er vanuit de overheid toezicht gehouden op gevoelige data van kritieke toeleveranciers van de overheid die online komen te staan? Zo ja, wie verzorgt dit toezicht en wat voor data is tot nu gevonden dat kan worden herleid tot de hack bij Abiom? Zo nee, waarom gebeurt dit niet?

[6] https://abiom.nl/statement-ransomware-aanval/.

Antwoord 9
Nee, zoals genoemd in vraag 3, heeft de term «kritieke toeleveranciers» geen specifieke status van de overheid. Hierop wordt als zodanig vanuit de overheid dus ook geen toezicht gehouden. Wel kan een incident aanleiding vormen voor andere toepasselijke toezichthoudende partijen om een onderzoek in te stellen. Wanneer bijvoorbeeld persoonsgegevens online komen te staan (een zogenaamde datalek) als gevolg van een incident is het aan de Autoriteit Persoonsgegevens om te overwegen of nader onderzoek ingesteld moet worden.
Daarnaast eist de BIO in het algemeen dat overheidsorganisaties beveiligingseisen opnemen in hun contracten met leveranciers en dat ze jaarlijks de prestatie van leveranciers op het gebied van informatiebeveiliging beoordelen op basis van vooraf vastgestelde prestatie-indicatoren. Deze behoren onderdeel te zijn van het contract met de leveranciers. Met een toekomstige wettelijke verankering van de BIO worden deze bepalingen van de BIO ook wettelijk verplicht.

Vraag 10
Deelt u de mening dat het goed om is Abiom te vragen om informatie over de hack te delen met bijvoorbeeld het Nationaal Cyber Security Centre en/of Digital Trust Centre? Zo ja, is dit gevraagd en wat gaat er met deze informatie gebeuren? Zo nee, waarom niet?

Antwoord 10
Het Nationaal Cyber Security Centrum (NCSC) van mijn ministerie 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. Dit betekent onder andere dat het NCSC zich daartoe een zo goed mogelijk beeld vormt van dergelijke dreigingen of incidenten en van de in die gevallen mogelijke mitigerende maatregelen. Het NCSC kan hiervoor informatie opvragen bij betrokken partijen, zoals de leverancier van kwetsbare softwareproducten. DTC heeft vooruitlopend op het wetsvoorstel Bevordering digitale weerbaarheid bedrijven (Wbdwb) de bevoegdheid het als niet-vitaal aangemerkte bedrijfsleven te informeren over serieuze dreigingen indien deze bekend zijn bij het DTC. Daarnaast neemt het DTC in voorkomende gevallen contact op met bedrijven waarbij er sprake is geweest van een serieus incident en DTC hier weet van heeft. In sommige gevallen deelt het DTC de verkregen informatie in meer algemene vorm zodat andere bedrijven hiervan kunnen leren en hun eigen cyberweerbaarheid kunnen vergroten. Het delen van informatie door bedrijven met het DTC over incidenten gebeurt op basis van vrijwilligheid. Het DTC heeft contact gezocht met Abiom om navraag te doen en is nog in afwachting van een reactie. Daarnaast hebben de getroffen overheidsorganisaties contact met Abiom gehad inzake aangifte, onderzoek en herstel, buitgemaakte gegevens, acties van Abiom en acties van de politie zelf.

Vraag 11
Deelt u de mening dat dit soort voorvallen zeer schadelijk kunnen zijn voor het functioneren van kritieke processen van de overheid zoals het functioneren van onze hulpdiensten? Zo ja, welke lessen worden uit deze hack getrokken en welke maatregelen kunnen worden genomen om kritieke toeleveranciers van de overheid (nog) weerbaarder te maken tegen ondermijnende digitale aanvallen zoals ransomware-aanvallen?

Antwoord 11
Als een incident leidt tot de verstoring van een vitaal proces is er een risico op maatschappelijke ontwrichting. Zoals ik in het antwoord op vraag 5 heb vermeld, schrijft de BIO voor dat organisaties incidenten evalueren. Welke lessen er exact worden getrokken zal per organisatie verschillen, omdat iedere organisatie verschilt en ook omdat de verlening van diensten en producten van Abiom op verschillende manieren is ingezet binnen de betrokken overheidsorganisaties. Die organisaties zullen daarbij zelf steeds een afweging moeten maken hoe risico's gemitigeerd kunnen worden en welke eventuele restrisico's blijven bestaan.