Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 360 VI Jaarverslag en slotwet Ministerie van Justitie en Veiligheid 2022

36 360 VII Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2022

36 360 XIII Jaarverslag en slotwet Ministerie van Economische Zaken en Klimaat 2022

Nr. 13 **LIJST VAN VRAGEN EN ANTWOORDEN**

Vastgesteld 9 juni 2023

De vaste commissie voor Digitale Zaken heeft een aantal vragen voorgelegd aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over de brieven van de Algemene Rekenkamer van 17 mei 2023 inzake aanbieding van de rapporten Resultaten verantwoordingsonderzoek 2022 bij het Ministerie van Justitie en Veiligheid (Kamerstuk 36 360 VI, nr. 2), Resultaten verantwoordingsonderzoek 2022 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 36 360 VII, nr. 2) en Resultaten verantwoordingsonderzoek 2022 bij het Ministerie van Economische Zaken en Klimaat (Kamerstuk 36 360 XIII, nr. 2) voor zover het onderwerpen betreft die zien op digitalisering voor zover het onderwerpen betreft die zien op digitalisering.

De Minister heeft deze vragen beantwoord bij brief van 8 juni 2023. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
Kamminga

De adjunct-griffier van de commissie,
Muller

kst-36360-VI-13
ISSN 0921 - 7371
's-Gravenhage 2023

Vragen en antwoorden

Vragen en antwoorden inzake het rapport Resultaten verantwoordingsonderzoek 2022 bij het Ministerie van Justitie en Veiligheid

1
Hoeveel algoritmes heeft het Ministerie van J&V aangemeld bij het algoritmeregister?
Antwoord:
Op 6 april jongstleden zijn de eerste zeven algoritmen uit het domein van Justitie en Veiligheid gepubliceerd. Deze zijn te vinden op rijksoverheid.nl en zijn aangemeld om ook in het landelijke algoritmeregister opgenomen te worden.

2
Zijn er andere algoritmes binnen het Ministerie van J&V die vergelijkbare risico's met zich meebrengen zoals Ritax?
Antwoord:
Justitie en Veiligheid werkt stapsgewijs aan het realiseren van meer algoritmeregisters bij uitvoeringsorganisaties. Zo is er een project gestart om de komende jaren bij alle JenV-onderdelen algoritmeregisters op te zetten vooruitlopend op de (wettelijke) verplichting die de Staatssecretaris Koninkrijksrelaties en Digitalisering hiervoor in voorbereiding heeft. Doel van dit project is om per organisatie algoritmes te inventariseren, het selecteren van de risicovolle algoritmes daarbinnen, het beoordelen van de genomen risicomitigerende maatregelen en het publiceren ervan in het algoritmeregister.

3
Hoe vaak is een Data Protection Impact Assessment (DPIA) in 2022 en in 2023 ingezet bij de beoordeling van algoritmes?»
Antwoord:
Bij (de start van) het verwerken van persoonsgegevens wordt een DPIA uitgevoerd. Er wordt echter niet bijgehouden/ geregistreerd of de betreffende verwerking een algoritme betreft. Daarnaast bevat niet ieder algoritme persoonsgegevens, waardoor voor het betreffende algoritme geen DPIA nodig. Hoewel JenV bij verwerking van persoonsgegevens altijd een DPIA uitvoert, is niet aan te geven hoe vaak een dergelijke verwerking een algoritme betrof.

4
Welke ministeries zijn betrokken bij de besteding van de extra middelen ten aanzien van de versterking van J&V diensten met betrekking tot vergroting van de weerbaarheid en veiligheid tegen dreigingen?
Antwoord:
De Ministeries van EZK, IenW, JenV, OCW, VWS, BZK, DEF en BZ ontvangen een deel van de extra middelen ten aanzien van de versterking van de digitale weerbaarheid. Zie voor de acties van de verschillende departementen en de verdeling van de extra middelen de Nederlandse Cybersecuritystrategie (NLCS).[1]

5
Welke maatregelen worden de komende jaren uitgevoerd om de weerbaarheid tegen dreigingen te vergroten? Hoe staat het met de uitvoering van deze maatregelen?
Antwoord:
De maatregelen die de komende jaren worden uitgevoerd om de weerbaarheid tegen digitale dreigingen te vergroten staan beschreven in

[1] Bijlage bij Kamerstuk 26 643, nr. 925.

de Nederlandse Cybersecuritystrategie (NLCS) en het bijbehorende actieplan. De kamer wordt dit najaar middels de jaarlijkse voortgangsrapportage geïnformeerd over de voortgang van de uitvoering van deze maatregelen.

6
Welke maatregelen als onderdeel van het vergroten van de weerbaarheid tegen dreigingen worden getroffen om de vitale infrastructuur beter te beschermen en weerbaarder te maken?
Antwoord:
Het kabinet werkt aan een versterkte aanpak voor de bescherming van de vitale infrastructuur. Over de hoofdlijnen heb ik de Kamer op 30 mei 2023 geïnformeerd in de Kamerbrief Versterkte aanpak bescherming vitale infrastructuur.[2] Een belangrijk element van deze aanpak is dat wordt ingezet op minder vrijblijvendheid en het verankeren van de aanpak in wet- en regelgeving. De implementatie van de Europese richtlijnen – de herziening van de richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de richtlijn veerkrachtige kritieke entiteiten (de CER-richtlijn) is hier een belangrijk onderdeel van (zie daarvoor ook het antwoord op vraag 181). Daarnaast is het beleidsinstrumentarium voor het weerbaar houden van de vitale infrastructuur tegen dreigingen herzien en aangescherpt. Hierbij is er meer aandacht voor het veilig inkopen van producten en diensten, risicovolle afhankelijkheden, sectoroverstijgende risico's en cascade-effecten.

7
Kunt u aangeven welke beleidsmaatregelen u voornemens bent te treffen of reeds worden getroffen per omschreven bestedingsdoel?
Antwoord:
Zie hiervoor het antwoord op vraag 5.

8
Kunt u een overzicht geven van het extra budget dat beschikbaar wordt gesteld tussen 2023 en 2027, uitgesplitst per begrotingsjaar? Hoe wordt dit budget verdeeld onder de 9 betrokken ministeries?
Antwoord:
Zie voor de uitsplitsing van het extra budget dat beschikbaar wordt gesteld voor cybersecurity de financiële onderbouwing bij de Nederlandse Cybersecurity Strategie (NLCS)[3] zoals opgenomen in de bijlage van de NLCS.

9
Welke subsidies zijn in 2022 verleend om tot realisatie van de omschreven beleidsdoelen te komen? Kunt u dit uitsplitsen per beleidsdoel en per betrokken ministerie?
Antwoord:
De Minister van Justitie en Veiligheid coördineert de verdeling van de extra cybersecurity middelen en monitort de voortgang van de Nederlandse Cybersecuritystrategie (NLCS). Over de NLCS ontvangt uw Kamer jaarlijks een voortgangsrapportage op beleidsmaatregelen. In de besteding per departement heeft de Minister van JenV geen inzicht, dit valt onder de verantwoordelijkheid van de verschillende vakministers. Uit het Verantwoordingsonderzoek JenV 2022 van de Algemene Rekenkamer blijkt dat de middelen uit het Coalitieakkoord conform de bestedingsplannen zijn overgeboekt naar de betrokken departementen. Conform de begrotingsvoorschriften leggen de desbetreffende Ministers in de jaarverantwoording verantwoording af over de realisatie.

---

[2] Kamerstuk 30 821, nr. 182.
[3] Bijlage bij Kamerstuk, 26 643, nr. 925, p. 51.

10
Kunt u een overzicht geven van de bestedingsplannen per betrokken ministerie en de daarbij behorende financiële middelen?
Antwoord:
Zie hiervoor de antwoorden op vraag 5 en vraag 8.

Bijlage bij 26 643, nr. 925, p. 51.

11
Onder welk bestedingsdoel valt het beleid dat wordt gevoerd ten aanzien van crisisbeheersing in het digitale domein? Hoeveel middelen zijn begroot voor de komende jaren om de weerbaarheid ten aanzien van digitale ontwrichting te vergroten?
Antwoord:
Crisisbeheersing valt onder de (Nederlandse Cybersecuritystrategie) NLCS doelstelling «Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en -crises». Alle maatregelen die in de NLCS worden aangekondigd zijn gericht op het vergroten van de digitale weerbaarheid en dragen daarmee bij aan het voorkomen van digitale ontwrichting. Aan de realisatie van de NLCS wordt oplopend tot € 111 mln. structureel vanaf 2027 extra uitgegeven, dit zijn middelen die dit kabinet beschikbaar heeft gesteld bij het coalitieakkoord.[4] Naast deze extra structurele middelen hadden de verschillende departementen al verschillende posten voor het vergroten van hun digitale weerbaarheid. De Minister van Justitie en Veiligheid heeft geen overzicht van deze middelen.

12
Kunt u een overzicht geven van de uitvoering van de bestedingsplannen in 2022 uitgesplitst per betrokken ministerie? Hoeveel is uitgegeven van het beschikbare budget in 2022 per ministerie?
Antwoord:
De Minister van JenV coördineert de verdeling van de extra cybersecurity middelen en monitort de voortgang van de Nederlandse Cybersecuritystrategie (NLCS). De Minister van JenV heeft geen inzicht in de besteding per departement, dit valt onder de verantwoordelijkheid van de verschillende vakministers. Voor het Ministerie van JenV zelf geldt dat in 2022 72% van de € 9,2 mln. toegekende Coalitieakkoord middelen is besteed. De krapte op de arbeidsmarkt heeft er toe geleid dat een deel van de middelen onbenut is gebleven. Ook het aantrekken van IT deskundigheid is lastig gebleken. Naast de coalitiemiddelen hadden de verschillende departementen al posten voor het vergroten van digitale weerbaarheid op hun begrotingen. Het Minister van JenV heeft geen overzicht van deze uitputting van deze posten.

13
Onder welk beleidsdoel valt het cross-sectoraal publiek-privaat oefenen op cyberaanvallen om zo de digitale weerbaarheid te vergroten? Hoeveel budget is begroot voor de komende jaren om een structurele oefenagenda op te zetten?
Antwoord:
Cross-sectoraal publiek-privaat oefenen op cyberaanvallen valt onder de Nederlandse cybersecuritystrategie doelstelling «organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en crises». Voor het opstellen van een interdepartementale oefenagenda, zoals aangekondigd in het actieplan van de Nederlandse Cybersecurity Strategie, zal in eerste instantie een overzicht worden gemaakt van reeds bestaande en begrootte cyber- en hybride-oefeningen. Een voorbeeld

[4] Bijlage bij Kamerstuk 26 643, nr. 925.

betreft de tweejaarlijkse landelijke cyberoefening ISIDOOR, georganiseerd door het Nationaal Cyber Security Centrum. Daarnaast organiseren departementen op sectoraal niveau soortgelijke oefeningen. Het daarvoor bestemde budget kan (ten dele) afkomstig zijn uit de extra financiële middelen onder de Nederlandse Cybersecurity Strategie.
Het extra budget voor de uitvoering van de Nederlandse Cybersecurity Strategie (oplopend tot structureel € 111 mln. vanaf 2027) is onderverdeeld bij de departementen, met een eigen verantwoordelijkheid voor de toekenning van voldoende capaciteit en financiële middelen om, in de strategie en het actieplan vastgelegde beleidsdoelen en acties, te realiseren. Crisispreparatie en oefenen vormt hier een belangrijk onderdeel van. Naast de extra middelen die beschikbaar zijn gekomen met het coalitie akkoord hebben de verschillende departementen ook nog andere structurele middelen beschikbaar voor het vergroten van de digitale weerbaarheid en daarmee crisispreparatie, het Ministerie van JenV heeft hier geen overzicht van.

14
Wat is de laatste stand van zaken ten aanzien van de realisatie en uitvoering van bestedingsplannen voor 2023?
Antwoord:
Er zijn verschillende uitdagingen in de uitvoering van de bestedingsplannen. Zo maakt de krapte op de arbeidsmarkt het lastig om geschikt personeel te werven. Daarnaast leggen de verschillende Europese wetgevingstrajecten zoals de Network and Information Security (NIS2) richtlijn en de Critical Entities Resilience (CER) richtlijn een flink beslag op de beleids- en uitvoeringscapaciteit. Er zijn echter geen signalen dat de realisatie en uitvoering van de bestedingsplannen voor 2023 hierdoor vastlopen. De kamer wordt dit najaar geïnformeerd over de voortgang van de acties en doelstellingen in de NLCS.

15
Wat is de laatste stand van zaken ten aanzien van de implementatie van de Europese CER en NIS richtlijn? Wanneer verwacht u deze implementatie af te ronden?
Antwoord:
Op dit moment werkt het kabinet aan wetsvoorstellen om de herziening van de richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de richtlijn veerkrachtige kritieke entiteiten (de CER-richtlijn) te implementeren. De verwachting is dat deze wetsvoorstellen in het najaar in consultatie gaan. Het kabinet verwacht de implementatie van de richtlijnen eind 2024 af te ronden.

16
Worden er maatregelen getroffen om de besteding van de extra begrote middelen voor 2023 te realiseren? Zo ja, welke? Zo nee, waarom niet?
Antwoord:
Zie hiervoor het antwoord op vraag 14.

17
Klopt het dat er monitoringsinstrumenten in ontwikkeling zijn om de realisatie van de bestedingsplannen te verbeteren? Zo ja, welke? Wanneer zullen deze monitoringsinstrumenten gereed zijn voor gebruik en wanneer verwacht u deze in te kunnen zetten?
Antwoord:
Vanuit het coalitieakkoord zijn met behulp van bestedingsplannen middelen verstrekt om de beleidsinzet over de hele breedte van het cybersecurity domein te versterken. In het verlengde van deze versterking is samen met betrokkenheid van publieke, private en maatschappelijke organisaties de Nederlandse Cybersecuritystrategie tot stand gekomen. In

de Nederlandse Cybersecuritystrategie staan de doelstellingen en de acties van het kabinet voor een digitaal veilig Nederland. In opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) is Dialogic Innovatie en Interactie gestart met een beleidsmatige nulmeting van de beleidsdoelstellingen en de acties in de Nederlandse Cybersecuritystrategie.[5] De oplevering van de nulmeting staat eind 2023 gepland. De nulmeting wordt openbaar gepubliceerd op de website van het WODC. Doel van de nulmeting is om duidelijk te krijgen wat de vertreksituatie is van de beleidsmaatregelen en om de voortgang van de maatregelen te kunnen monitoren in de tijd. Uw Kamer wordt jaarlijks geïnformeerd over de voortgang van de Nederlandse Cybersecuritystrategie

18
Worden er maatregelen getroffen om de ontstane achterstand in de uitvoering in te halen, dan wel te herstellen? Zo ja, welke? Zo nee, waarom niet?
Antwoord:
Het kabinet investeert in de werving van extra personeel voor de uitvoering. Momenteel is al extra personeel geworven en zal het kabinet blijven inzetten op de werving van extra personeel. Het aantrekken van extra IT-expertise blijkt lastig. Daarnaast werkt het kabinet aan wetsvoorstellen om de herziening van de richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en de richtlijn veerkrachtige kritieke entiteiten (de CER-richtlijn) te implementeren. In het verantwoordingsonderzoek JenV 2022 van de Algemene Rekenkamer wordt gerefereerd naar deze implementatie en dat de uitvoering vertraging heeft opgelopen omdat de wetgeving in 2022 nog niet geïmplementeerd was. De afronding van implementatie was niet voorzien voor 2022 en er is dan ook geen sprake geweest van belemmering van de uitvoering in 2022 door vertraging van de implementatie. Op dit moment wordt gewerkt aan de benodigde voorbereiding op de uitvoering van deze richtlijnen. De verwachting is dat deze wetsvoorstellen in het najaar in consultatie gaan en de implementatie van de richtlijnen eind 2024 is afgerond.

Vragen en antwoorden inzake het rapport Resultaten verantwoordingsonderzoek 2022 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

19
In hoeverre wordt het doel van een laagdrempelig, bereikbaar stelsel van Informatiepunten Digitale Overheid (IDO's) behaald als naar schatting slechts 1% van de doelgroep wordt bereikt?
Antwoord:
Er zijn verschillende maatregelen genomen om het bereik te vergroten. Zo hebben gemeenten per 2023 een regierol en zij bepalen:
– welke doelgroepen en lokale maatschappelijke opgaven prioriteit hebben;
– welke partners opgenomen worden in het lokale netwerk.
Daarnaast stimuleert het ministerie dat er meer Informatiepunten Digitale Overheid komen buiten de muren van de bibliotheek. Bijvoorbeeld in buurt- en wijkcentra of koffiehuizen. En werkt BZK samen met onder andere de VNG, de KB en de Alliantie Digitaal Samenleven samen aan de inrichting en bestendiging van solide lokale netwerken, waarbij de Informatiepunten Digitale Overheid lokale partners zijn.
Ik doe onderzoek naar de samenstelling en behoefte van de groep mensen die (al dan niet tijdelijk) niet in staat zijn om zelfstandig gebruik te maken

[5] Zie ook WODC.nl, Projectnummer 3368, Nulmeting Nederlandse Cyber Security Strategie (NLCS).

van de (digitale) publieke dienstverlening. Ik zal de Kamer na de zomer informeren over de voortgang.
Mijn departement werkt, vanuit haar coördinerende rol op publieke dienstverlening, aan een beleidstheorie voor passende ondersteuning aan de (al dan niet tijdelijk) kwetsbare burger en ondernemer. De rol die het Informatiepunt Digitale Overheid in deze ondersteuning kan spelen wordt hierin meegenomen, net als de overheidsbrede loketten die ik aan het inrichten ben.

20
Hoe kan beter in beeld worden gebracht tegen welke problemen burgers aanlopen bij contact met de overheid en welke subdoelgroepen daarin moeten worden onderscheiden en hoe helpt het opstellen van een beleidstheorie hierbij?
Antwoord:
Er worden analyses uitgevoerd op alle inzichten die zijn verkregen uit bestaande en lopende onderzoeken en nieuw berekende cijfers en programma's, waarna er een behoefte en doelgroepenonderzoek wordt opgestart. Daarnaast heeft de beleidsvisie van BZK tot doel om samen met de mensen waar het om gaat te komen tot passende ondersteuning voor ieder type vraag en die aansluit op de behoefte van (al dan niet tijdelijk) kwetsbare burgers en ondernemers

21
Kan een overzicht worden gegeven van alle doelen en subdoelen van de IDO's?
Antwoord:
– De IDO's zijn herkenbaar, goed bereikbaar, laagdrempelig en toegankelijk.
– Iedere burger krijgt snel begrijpelijke informatie en passende hulp via een IDO in de buurt.
– Eerste hulp en ondersteuning bij (online) overheidsdienstverlening wordt vanuit overheden georganiseerd in een IDO.

22
Wordt de aanbeveling van de Algemener Rekenkamer dat alle grote uitvoeringsorganisaties van het Rijk een vast aanspreekpunt krijgen voor medewerkers van IDO's die burgers proberen te helpen opgevolgd en, zo ja, hoe en wanneer?
Antwoord:
Nee, niet voor de IDO-medewerkers, zij helpen niet met persoonlijke casuïstiek, maar verwijzen wel door. Maar wel voor de overheidsdienstverlener in de overheidsbrede loketten die momenteel ingericht worden. Deze overheidsdienstverlener neemt de coördinatie op zich als meer uitvoeringsorganisaties betrokken zijn. Door middel van directe lijnen met de uitvoeringsorganisaties kan de overheidsdienstverlener burgers helpen.
Door middel van 3 praktijkinitiatieven met overheidsbrede loketten in Amsterdam, Utrecht en Enschede wordt getoetst wat werkt en wat niet. En datgene wat werkt, wordt meteen toepast. Eind dit volgt een advies over de inrichting van de loketten en eventuele landelijke uitrol.

Vragen en antwoorden inzake het rapport Resultaten verantwoordingsonderzoek 2022 bij het Ministerie van Economische Zaken en Klimaat

23
Wordt de aanbeveling van de Algemene Rekenkamer over het kwetsbaarhedenbeheer bij de Dienst ICT Uitvoering (DICTU) opgevolgd en, zo ja, hoe?

Antwoord:
DICTU heeft de aanbeveling van de Algemene Rekenkamer, om het kwetsbaarhedenmanagement te verbeteren, waarbij het proces uniformen consistent wordt uitgevoerd waardoor kwetsbaarheden en bijbehorende mitigerende maatregelen en geaccepteerde risico's centraal inzichtelijk zijn, overgenomen.
In 2022 heeft DICTU een extern onderzoek laten uitvoeren naar het kwetsbaarhedenmanagement waarbij de belangrijkste conclusies overeenkomstig zijn aan de conclusies van de Algemene Rekenkamer, aangevuld met procesmatige en operationele aandachtspunten.
Het rapport als resultaat van het onderzoek, heeft naast bevindingen een gewenste toekomstige situatie en mogelijk aanpak opgeleverd. In 2023 is intern een project gestart om kwetsbaarheden management aan de hand van de gegeven richtlijnen vorm te geven. Hieronder staat kort toegelicht over vier vlakken hoe we dit willen verbeteren:

1. Techniek: Implementatie van geautomatiseerde detectie en oplossing van beveiligingsincidenten (SOAR)
2. Proces: Inrichten van een eenduidig, organisatie breed en integraal kwetsbaarheden proces.
3. Governance: Implementeren van een integrale rapportage naar zowel het management als de oplosteams.
4. Operatie: Inrichten van een kwetsbaarheden beheer team.

Op dit moment bevindt het project zich in de opstartfase en wordt er een haalbaarheidscheck uitgevoerd. De verwachting is dat er op 1 september 2023 een plan van aanpak is opgesteld waarin bovenstaande punten zijn uitgewerkt.

Overkoepelende / overige en antwoorden vragen die betrekking hebben op bovenstaande rapporten Resultaten verantwoordings-onderzoek 2022

Geen vragen.