Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

36 740 VI Jaarverslag en slotwet Ministerie van Justitie en Veiligheid 2024

Nr. 16

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 23 juni 2025

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Ministers van Justitie en Veiligheid en van Asiel en Migratie en de Staatssecretaris van Justitie en Veiligheid over het jaarverslag 2024 van het Ministerie Justitie en Veiligheid (Kamerstuk 36 740 VI, nr. 1), over het Rapport resultaten verantwoordingsonderzoek 2024 Algemene Rekenkamer bij het Ministerie van Justitie en Veiligheid (Kamerstuk 36 740 VI, nr. 2), beantwoording vragen commissie over het Jaarverslag 2024 van het Ministerie van Justitie en Veiligheid (Kamerstuk 36 740 VI, nr. 1), over het Jaarverslag 2024 van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 36 740 VII, nr. 1), over het Jaarverslag 2024 van het Ministerie van Economische Zaken (Kamerstuk 36 740 XIII, nr. 1) voor zover het onderwerpen betreft die zien op digitalisering, beantwoording vragen commissie over het rapport Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Justitie en Veiligheid (Kamerstuk 36 740 VI, nr. 2), over het rapport Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 36 740 VII, nr. 2) en over het rapport Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Economische Zaken (Kamerstuk 36 740 XIII, nr. 2).

De vragen en opmerkingen zijn op 12 juni 2025 aan de Minister van Justitie en Veiligheid van Justitie en Veiligheid voorgelegd. Bij brief van 23 juni 2025 zijn de vragen beantwoord.

De voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller

kst-36740-VI-16
ISSN 0921 - 7371
's-Gravenhage 2025

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van PVV-fractie

De leden van de PVV-fractie hebben met interesse kennisgenomen van de stukken behorende bij het schriftelijk overleg over de behandeling van de Jaarverantwoording 2024 voor zover het onderwerpen inzake JenV betreft die zien op digitalisering. Naar aanleiding hiervan hebben zij de volgende vragen.

De leden van de PVV-fractie lezen dat de Nederlandse Digital Travel Credential (DTC)-pilot succesvol is afgerond, al zijn er terechte vraagtekens geplaatst door de Autoriteit Persoonsgegevens over de representativiteit van de toets in haar schrijven van d.d. 11 juli 2024, en onderhandelingen zijn gestart over de DTC-verordeningen van de Europese Commissie. Wat is de insteek van het kabinet bij de onderhandelingen over de DTC-verordeningen van de Europese Commissie?[1]

Daarnaast constateren de leden van de PVV-fractie dat voor de digitale achterstanden bij het Openbaar Ministerie het afgelopen jaar een aparte taskforce is opgezet. Met tooling zijn de digitale achterstanden op verschillende netwerkschijven in kaart gebracht. Blijkens het jaarverslag staan er ook voor komend jaar nieuwe organisaties op de rol, de inhoudelijke en technische randvoorwaarden worden momenteel ingeregeld. Graag vernemen deze leden expliciet welke middelen en inzet verstaan worden onder «tooling» en tevens vragen zij welke acties de Minister concreet wil gaan uitvoeren om de digitale achterstanden in de informatiehuishouding weg te werken.[2]

Ook merken de leden van de PVV-fractie op dat er een aanbesteding is uitgevoerd voor de verwerving van kunstmatig intelligente document herkenningssoftware voor de bouw van een «Digitale Archivaris». Deze zou straks grote documentcollecties sneller kunnen voorzien van de juiste metadata en ze in het daarvoor bestemde systeem plaatsen, waardoor stukken sneller en beter vindbaar worden. Deze leden vinden dat een veelbelovend en vernuftig idee, maar vragen wat de status is van deze aanbesteding. Ook vragen zij welke randvoorwaarden voor het te gebruiken taalmodel (large language model), de opslag van de data en de gebruikte algoritmen gesteld zijn en of hier de nodige impact assessments en risicoanalyses voor zijn uitgevoerd. Is er borging dat documentcollecties die gevoelige of gerubriceerde informatie kunnen bevatten ook daadwerkelijk in autonoom beheer blijven?[3]

Voorts lezen de leden van de PVV-fractie dat in 2023 15,6% van de bevolking van 15 jaar of ouder aangaf slachtoffer te zijn geweest van

---

[1] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p.20
[2] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p.30
[3] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p.30

online criminaliteit. Dit is iets minder (1,3 procentpunt) dan in 2021.[4] Om cybercrime te voorkomen hebben in 2024 bewustwordingscampagnes plaatsgevonden om veiliger gedrag van personen online te stimuleren. Het betreft een campagne over social engineering en een campagne over het gebruik van tweefactorauthenticatie. Hoe wordt de effectiviteit van deze bewustwordingscampagnes gemeten?[5]
Bovendien lezen deze leden dat er bij het hele ministerie een grote achterstand is in het accrediteren van belangrijke informatiesystemen. Kan de Minister aangeven om welke systemen dit concreet gaat? Kan de Minister ook komen met een «roadmap» met deadlines voor het accrediteren van belangrijke informatiesystemen?[6]

De leden van de PVV-fractie merken ten slotte op dat het op centraal niveau inzicht houden van wat op decentraal niveau gebeurt, afhankelijk is van de volledigheid en tijdigheid waarmee de JenV-organisaties informatie delen en dat zonder goede informatie-uitwisseling de Minister van JenV zijn coördinerende rol niet goed kan vervullen. Een voorbeeld dat werd genoemd is de vraag vanuit het kerndepartement aan JenV-organisaties om in de jaarplannen 2025 te beschrijven hoe ze invulling willen geven aan de NIS2-richtlijn. Het decentrale niveau heeft beperkt gereageerd op deze vraag. Hierdoor heeft de centrale leiding onvoldoende inzicht in de status van de informatiebeveiliging en extra te nemen beveiligingsmaatregelen. Welke stappen gaat de Minister zetten om ervoor te zorgen dat de status van de informatiebeveiliging en de te nemen beveiligingsmaatregelen vanuit de decentrale organisaties inzichtelijk wordt gemaakt voor de centrale leiding? Hoe zal hier vervolgens op worden gehandeld?[7] Of algemener: Welke stappen gaat de Minister zetten om de informatie-uitwisseling tussen centraal en decentraal niveau te verbeteren?

Vragen en opmerkingen van de leden van GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de verantwoordingsstukken van het Ministerie van Justitie en Veiligheid over 2024. Deze leden pleiten al lange tijd voor een meer integrale behandeling van begrotingen en de verantwoording van uitgaven voor digitalisering. Over de verantwoordingsstukken hebben zij enkele vragen en opmerkingen.

De leden van de GroenLinks-PvdA-fractie wijzen vooral op de verantwoording van de uitgaven aan het Nationaal Cyber Security Centrum (NCSC). Het is moeilijk te controleren of de middelen voor deze organisatie doelmatig, doeltreffend en effectief zijn. Deze leden vragen de Minister daarom om duidelijk te maken wat het totaalbudget voor het NCSC was in 2024 en wat de betrokken departementen hebben ingelegd. Wat waren de doelstellingen voor 2024 en zijn die behaald? Zij wensen dit in de toekomst beter te controleren en vragen de Minister om dit voortaan standaard inzichtelijk te maken. Welke mogelijkheden ziet u om de uitgaven beter controleerbaar te maken?

De leden van de GroenLinks-PvdA-fractie maken zich zorgen over het grote aantal extern ingehuurde medewerkers bij het NCSC. Het is van groot belang dat publieke organisaties specialisten weten aan te trekken en te behouden. Wat doet de Minister om het aandeel extern ingehuurde

[4] Rapport verantwoordingsonderzoek 2024, Kamerstuk 36 740 VI, nr. 2, p. 11
[5] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p. 58 en 83.
[6] Rapport verantwoordingsonderzoek 2024, Kamerstuk 36 740 VI, nr. 2, p. 33.
[7] Rapport verantwoordingsonderzoek 2024, Kamerstuk 36 740 VI, nr. 2, p. 79.

krachten te verminderen en meer vast personeel aan te trekken binnen het NCSC? Hoe enthousiasmeert u extern ingehuurde krachten om vast in dienst te komen of elders in de publieke sector hun kennis en expertise in te zetten? Deze leden benadrukken dat er een schrijnend tekort aan ICT-experts is en dat het demissionaire kabinet zich moet inzetten om meer specialisten langjarig in dienst te nemen. Dat is nodig om het kennisniveau over cyberveiligheid binnen de overheid op peil te brengen.

De leden van de GroenLinks-PvdA-fractie zijn blij dat de Cyberbeveiligingswet eindelijk aan de Kamer is toegestuurd. Deze leden vragen u of het NCSC nu voldoende is uitgerust voor de implementatie van deze wet en zo niet, welke aanvullende middelen er volgens het NCSC nodig zijn. Zij maken zich zorgen over de voorbereidingen van alle organisaties en overheden die straks aan de wet moeten voldoen. Met name gemeenten, die al te maken hebben met grote financiële uitdagingen, hebben vragen over de implementatie en voorziene kosten van de Cyberveiligheidswet. Per wanneer kunt u organisaties en overheden duidelijkheid geven over welke middelen zij moeten reserveren om te voldoen aan hun nieuwe verplichtingen? Is er een systematiek voor deze organisaties om te berekenen waar zij ongeveer rekening mee moeten houden?

Tot slot zijn de leden van de GroenLinks-PvdA-fractie bezorgd over de alsmaar toenemende afhankelijkheid van Amerikaanse techleveranciers binnen de overheid en de publieke sector. Deze leden vrezen dat als de marktdominantie van enkele Amerikaanse bedrijven niet afneemt, er aanzienlijke risico's zijn voor de onafhankelijkheid van instituties en overheden. Dit is in lijn met veel aangenomen Kamermoties op dit onderwerp. Zij vragen daarom om uit te leggen hoe u in 2024 binnen uw ministerie werk heeft gemaakt van digitale soevereiniteit en of u de afhankelijkheid succesvol heeft teruggedrongen. Kunt u dit uitdrukken in cijfers, bijvoorbeeld het aandeel soft- en hardware dat is ingekocht van Europese bedrijven, of de uitgaven die u heeft gedaan aan niet-Europese soft- en hardware ten opzichte van Europese alternatieven? Ziet u het als uw rol om de digitale soevereiniteit binnen uw departement te versterken?

De leden van de GroenLinks-PvdA-fractie vragen ook aandacht voor de digitale soevereiniteit van de justitieketen. Het is riskant om een aanzienlijk deel van onze justitieketen afhankelijk te maken van niet-Europese bedrijven. In uiterste gevallen kunnen zij als speelbal worden gebruikt in geopolitieke conflicten; dit zet de vrijheid van onze rechtsstaat onder druk. Kunt u toelichten hoe groot de digitale afhankelijkheid van niet-Europese leveranciers is binnen organisaties in de justitieketen, zoals de politie, het Openbaar Ministerie, de Raad voor de Rechtspraak, en de Hoge Raad? Wat doet u om hun digitale soevereiniteit te borgen en versterken? Zijn hier middelen en capaciteit voor beschikbaar gesteld over 2024? Zo niet, bent u bereid dit alsnog te doen?

Vragen en opmerkingen van de leden van VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de stukken geagendeerd voor het schriftelijk overleg aangaande de Jaarverantwoording 2024 van het Ministerie van Justitie en Veiligheid (voor zover het digitaliseringsonderwerpen betreft). Deze leden stellen nog enkele vragen naar aanleiding van de beantwoording van de vragen inzake Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Justitie en Veiligheid[8].

[8] Kamerstuk 36 740 VI, nr. 2.

De leden van de VVD-fractie onderschrijven de waarde van een snelle accreditatie bij ingebruikname van gevoelige informatiesystemen zodat een juist beveiligingsniveau kan worden gewaarborgd. Deze leden lezen in de genoemde beantwoording dat bij het wegwerken van de achterstanden in het accrediteren van belangrijke informatiesystemen wordt ingezet op het tijdelijk beschikbaar stellen van meer capaciteit om het proces van accreditatie te faciliteren en de accreditaties uit te voeren, en dat er een actualiseringsslag heeft plaatsgevonden op de lijst met kritieke of bedrijfskritische systemen waarna op basis van risicomanagement een shortlist met systemen die prioriteit in de accreditering benodigen is gemaakt. Deze leden vragen de Minister wanneer de achterstanden op accreditaties van gevoelige informatiesystemen naar verwachting ingehaald zullen zijn. Zij vragen de Minister verder hoe het departementaal accreditatiebeleid van het Ministerie van Justitie en Veiligheid in lijn gaat worden gebracht met het interdepartementale accreditatiebeleid van het Rijk en wat de verwachting is op welke termijn dit volbracht kan worden.

In het verlengde van bovenstaande vragen de leden van de VVD-fractie of de Minister een overzicht kan geven van innovatieve ICT-toepassingen bij het Ministerie van Justitie en Veiligheid? Welke innovaties worden momenteel verder uitgewerkt ten behoeve van efficiëntere dienstverlening en efficiënter werken binnen het ministerie? Wordt er bijvoorbeeld gewerkt aan innovatieve ICT-toepassingen voor de afhandeling van WOO-verzoeken? En welke ICT-projecten hebben voor de Minister de hoogste prioriteit bij het verbeteren van de doorlooptijden in de strafrechtketen en specifiek bij de politie? Zij vragen ook hoe zorg wordt gedragen dat bevindingen die volgen uit «red teaming» sneller gedeeld worden en opvolging genieten bij uitvoeringsorganisaties. Deelt de Minister de mening dat red teaming weinig nut heeft als vervolgens recent uitgevoerde beveiligingstests deels vergelijkbare bevindingen opleveren als bij eerdere testen?

Ten slotte vragen de leden van de VVD-fractie hoe zorg wordt gedragen voor een beter informatie-uitwisseling tussen het kerndepartement en organisaties gelieerd aan het ministerie, zodat het kerndepartement zijn coördinerende rol kan vervullen.

Vragen en opmerkingen van de leden van NSC-fractie

De leden van de NSC-fractie hebben met belangstelling kennisgenomen van de Jaarverantwoording 2024 van het Ministerie van Justitie en Veiligheid, voor zover het onderwerpen betreft die zien op digitalisering. Deze leden hebben naar aanleiding hiervan nog een aantal vragen en opmerkingen.
De leden van de NSC-fractie willen de Minister vragen hoe hij aankijkt tegen de recente reflectie van de Algemene Rekenkamer, waarin wordt geconcludeerd dat bewindspersonen van het kabinet onvoldoende concrete en meetbare doelstellingen formuleren. Dit bemoeilijkt het inzicht in de behaalde resultaten, ook op het terrein van digitalisering binnen het Ministerie van Justitie en Veiligheid. Deze leden vragen de Minister naar aanleiding hiervan om aan te geven welke concrete doelen op het gebied van digitalisering het afgelopen jaar zijn gesteld binnen het ministerie en in hoeverre deze doelen daadwerkelijk zijn behaald. Wat waren de belangrijkste resultaten op dit terrein in het afgelopen jaar en hoe dragen deze bij aan het verbeteren van de digitale weerbaarheid en de dienstverlening van het ministerie?

De digitale dreiging tegen Nederland is groot en voortdurend in ontwikkeling, zo blijkt uit het *Cybersecuritybeeld Nederland 2024*. De leden van de NSC-fractie willen de Minister vragen welke leerpunten het ministerie heeft getrokken uit incidenten met datalekken en kwesties rond cyberveiligheid in het afgelopen jaar. Op welke wijze worden deze lessen structureel meegenomen in beleid en uitvoering?

De leden van de NSC-fractie vernemen graag van de Minister welke behoeften hij op dit moment signaleert in de markt als het gaat om cybersecurity. Zijn er volgens de Minister specifieke knelpunten, zoals een tekort aan kennis, technologie of capaciteit, die het realiseren van digitale veiligheid belemmeren? Daarnaast constateren zij dat er op het gebied van informatiebeveiliging binnen het Ministerie van Justitie en Veiligheid nog stappen nodig zijn. De Algemene Rekenkamer signaleert onder andere een grote achterstand in de accreditatie van belangrijke systemen, trage opvolging van bevindingen uit beveiligingstesten, en onvoldoende informatie-uitwisseling tussen het kerndepartement en de onderliggende organisaties. De leden vragen de Minister hoe hij deze structurele tekortkomingen beoordeelt, welke concrete maatregelen er worden of zijn genomen om deze aan te pakken, en op welke termijn verbeteringen zichtbaar moeten zijn.

II Antwoord/reactie van de bewindspersoon

Vragen en opmerkingen van de leden van PVV-fractie

De leden van de PVV-fractie hebben met interesse kennisgenomen van de stukken behorende bij het schriftelijk overleg over de behandeling van de Jaarverantwoording 2024 voor zover het onderwerpen inzake JenV betreft die zien op digitalisering. Naar aanleiding hiervan hebben zij de volgende vragen.

De leden van de PVV-fractie lezen dat de Nederlandse Digital Travel Credential (DTC)-pilot succesvol is afgerond, al zijn er terechte vraagtekens geplaatst door de Autoriteit Persoonsgegevens over de representativiteit van de toets in haar schrijven van d.d. 11 juli 2024, en onderhandelingen zijn gestart over de DTC-verordeningen van de Europese Commissie. Wat is de insteek van het kabinet bij de onderhandelingen over de DTC-verordeningen van de Europese Commissie?[9]

Antwoord
Op 8 oktober 2024 heeft de Europese Commissie twee voorstellen gepresenteerd om het gebruik van digitale reiscredentials (DTC) Uniebreed te reguleren. Het eerste voorstel betreft een verordening voor een EU-reisapplicatie gericht op het stroomlijnen van grensoverschrijdend verkeer van en naar het Schengengebied, AenM heeft hier in nauwe samenwerking met BZK een BNC-fiche voor opgesteld. Het tweede voorstel betreft een verordening die digitale reiscredentials gebaseerd op een identiteitskaart reguleert. BZK heeft hier in nauwe samenwerking met AenM een BNC-fiche voor opgesteld.

Nederland staat in algemene zin positief tegenover de voorstellen en het doel daarvan:
het verhogen van de doeltreffendheid en doelmatigheid van grenscontroles en de bevordering van de veiligheid en mobiliteit van reizigers. Dit sluit aan bij de kabinetsinzet op dit terrein en de noodzaak om te investeren in innovaties voor optimaal

[9] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p.20

grensbeheer. Het kabinet zet zich tijdens de onderhandelingen in voor een technische oplossing die voldoet aan de randvoorwaarden inzake gegevensbescherming en informatiebeveiliging. Daarbij dienen ook de achterliggende processen van uitgifte, creatie en het gebruik zo effectief en efficiënt mogelijk ingericht te worden. Voor een uitgebreide toelichting inzake de kabinetsinzet ten aanzien van voorstellen, verwijs ik u naar de BNC-fiches.

Daarnaast constateren de leden van de PVV-fractie dat voor de digitale achterstanden bij het Openbaar Ministerie het afgelopen jaar een aparte taskforce is opgezet. Met tooling zijn de digitale achterstanden op verschillende netwerkschijven in kaart gebracht. Blijkens het jaarverslag staan er ook voor komend jaar nieuwe organisaties op de rol, de inhoudelijke en technische randvoorwaarden worden momenteel ingeregeld. Graag vernemen deze leden expliciet welke middelen en inzet verstaan worden onder «tooling» en tevens vragen zij welke acties de Minister concreet wil gaan uitvoeren om de digitale achterstanden in de informatiehuishouding weg te werken.[10]

Antwoord
De ingezette techniek betreft een zogenaamde RM-tool, waarbij RM staat voor record management. De tool is goedgekeurd door de Chief Privacy Officer (CPO) en de Chief Information Security Officer (CISO) en wordt gebruikt om op diverse netwerkschijven een grove schifting te maken van bestanden die weg kunnen of archiefwaardig zijn en bewaard moeten blijven. De tool geeft informatie over dubbellingen, de leeftijd van documentcollecties, de data waarop het bestand voor de laatste keer is geraadpleegd, etc. Op basis van de analyse gaan de JenV/AenM-organisaties zelf aan de slag met het opschonen van hun netwerkschijven.
De tooling is/wordt momenteel door de zogenaamde «Taskforce Digitale Achterstanden» ingezet bij het Openbaar Ministerie, de Raad voor Strafrechtstoepassing en Jeugdbescherming, het WODC en de Raad voor Rechtsbijstand. Daarna volgen onder andere het NFI, de Justitiële ICT Organisatie, het COA, de Raad voor de Kinderbescherming en Justis.

Ook merken de leden van de PVV-fractie op dat er een aanbesteding is uitgevoerd voor de verwerving van kunstmatig intelligente document herkenningssoftware voor de bouw van een «Digitale Archivaris». Deze zou straks grote documentcollecties sneller kunnen voorzien van de juiste metadata en ze in het daarvoor bestemde systeem plaatsen, waardoor stukken sneller en beter vindbaar worden. Deze leden vinden dat een veelbelovend en vernuftig idee, maar vragen wat de status is van deze aanbesteding.

Antwoord
Het afgelopen jaar is een Europees aanbestedingstraject doorlopen voor de zogenaamde Digitale Archivaris: tooling die op basis van AI grote verzamelingen van data voorziet van de juiste metadata. Door het toevoegen van metadata wordt de informatie duurzaam toegankelijk en is JenV/AenM beter in staat om te voldoen aan de eisen van het selectiebeleid.
De offertes zijn beoordeeld en er is een voorlopige leverancier uitgekomen. Volgende stap is een proef (een zogenaamde proof of concept) om te kijken of de door de leverancier geoffreerde tooling voldoende levert wat JenV/AenM voor ogen heeft. Lukt

[10] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p.30

het de leverancier om in de proef 75% (van de testbestanden) correct te vinden en metadateren, is de tool effectief genoeg en gaan we in zee met deze leverancier. Lukt het niet, dan gaan we door met de volgende leverancier met wie we dezelfde proef doen, etc., etc.

Ook vragen zij welke randvoorwaarden voor het te gebruiken taalmodel (large language model), de opslag van de data en de gebruikte algoritmen gesteld zijn en of hier de nodige impact assessments en risicoanalyses voor zijn uitgevoerd. Is er borging dat documentcollecties die gevoelige of gerubriceerde informatie kunnen bevatten ook daadwerkelijk in autonoom beheer blijven?[11]

Antwoord

Voor het te gebruiken taalmodel geldt de randvoorwaarde dat het op de interne JenV/AenM-omgeving moet draaien. De data en algoritmes worden per organisatie opgeslagen binnen de eigen ICT-omgeving van de JenV/AenM-organisatie waar ze worden gegenereerd. Alles blijft daarmee binnen de interne JenV/AenM ICT-infrastructuur. Daaruit voortvloeiend blijven documentcollecties en eventuele gevoelige of gerubriceerde informatie ook in de interne JenV/AenM-omgeving. Een DPIA en QuickScan Informatiebeveiliging worden voorafgaand aan ingebruikname van de tooling ter goedkeuring voorgelegd aan respectievelijk de Privacy Officer en CISO.

Voorts lezen de leden van de PVV-fractie dat in 2023 15,6% van de bevolking van 15 jaar of ouder aangaf slachtoffer te zijn geweest van online criminaliteit. Dit is iets minder (1,3 procentpunt) dan in 2021.[12] Om cybercrime te voorkomen hebben in 2024 bewustwordingscampagnes plaatsgevonden om veiliger gedrag van personen online te stimuleren. Het betreft een campagne over social engineering en een campagne over het gebruik van tweefactorauthenticatie. Hoe wordt de effectiviteit van deze bewustwordingscampagnes gemeten?[13]

Antwoord

Bij alle overheidscampagnes met een mediabudget vanaf € 150.000 per jaar doet Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken een campagne-effectonderzoek. Daarbij worden de volgende zaken onderzocht: het bereik, de waardering, gedragsverandering op de lange termijn en of de boodschap overkomt, kortom: het effect van de campagne. De Commissie Rijksbrede Communicatie evalueert en toetst elke campagne. De Minister-President legt achteraf in de Jaarevaluatie over het totaal van deze overheidscampagnes verantwoording af aan de Tweede Kamer. De campagnes met een mediabudget tot € 150.000 per jaar hoeven niet te worden onderzocht, maar worden wel vermeld in de Jaarevaluatie. Ministeries blijven zelf inhoudelijk verantwoordelijk voor hun campagnes.
De campagne-effectonderzoeken over tweefactorauthenticatie: «Dubbel beveiligd is dubbel zo veilig» en over social engineering: «Laat je niet interneppen» zijn openbaar beschikbaar via *https://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/campagnes/campagneresultaten*.

[11] Jaarverslag 2024 van het ministerie JenV, Kamerstuk 36 740 VI, nr. 1, p.30
[12] Rapport verantwoordingsonderzoek 2024, Kamerstuk 36 740 VI, nr. 2, p. 11
[13] Jaarverslag 2024 van het MMinisterie JenV, Kamerstuk 36 740 VI, nr. 1, p. 58 en 83.

Bovendien lezen deze leden dat er bij het hele ministerie een grote achterstand is in het accrediteren van belangrijke informatiesystemen. Kan de Minister aangeven om welke systemen dit concreet gaat? Kan de Minister ook komen met een «roadmap» met deadlines voor het accrediteren van belangrijke informatiesystemen?[14]

Antwoord

Ja, er is een lijst met betreffende informatiesystemen. Deze informatie is echter vertrouwelijk vanwege de aard en gevoeligheid hiervan. De lijst is beschikbaar en kan desgewenst onder de daarvoor geldende vertrouwelijke voorwaarden met de Kamer worden gedeeld. Het concretiseren en prioriteren ten behoeve van de roadmap van te accrediteren belangrijke informatiesystemen is op dit moment risicogestuurd uitgewerkt en wordt afgestemd met de eigenaren van de verschillende onderkende informatiesystemen.

De leden van de PVV-fractie merken ten slotte op dat het op centraal niveau inzicht houden van wat op decentraal niveau gebeurt, afhankelijk is van de volledigheid en tijdigheid waarmee de JenV-organisaties informatie delen en dat zonder goede informatie-uitwisseling de Minister van JenV zijn coördinerende rol niet goed kan vervullen. Een voorbeeld dat werd genoemd is de vraag vanuit het kerndepartement aan JenV-organisaties om in de jaarplannen 2025 te beschrijven hoe ze invulling willen geven aan de NIS2-richtlijn. Het decentrale niveau heeft beperkt gereageerd op deze vraag. Hierdoor heeft de centrale leiding onvoldoende inzicht in de status van de informatiebeveiliging en extra te nemen beveiligingsmaatregelen.

Welke stappen gaat de Minister zetten om ervoor te zorgen dat de status van de informatiebeveiliging en de te nemen beveiligingsmaatregelen vanuit de decentrale organisaties inzichtelijk wordt gemaakt voor de centrale leiding? Hoe zal hier vervolgens op worden gehandeld?[15] Of algemener: Welke stappen gaat de Minister zetten om de informatie-uitwisseling tussen centraal en decentraal niveau te verbeteren?

Antwoord

De bevinding dat verbetering van de informatie-uitwisseling tussen het kerndepartement en de uitvoeringsorganisaties over informatiebeveiliging nodig is, wordt onderschreven.
Als maatregel is er een actieplan opgesteld dat onder meer de opvolging van de redteamingtesten moet verbeteren. Onderdeel is tevens het versterken van departementaal toezicht op informatiebeveiliging zowel op centraal als decentraal niveau.
Hiervoor zullen de volgende stappen worden genomen:

- **de informatie van de organisaties richten op de hoge risico's die de betrouwbaarheid van de informatievoorziening en de processen bedreigen;**
- **de informatie van de organisaties in elk bestuurlijk overleg met de organisaties te bespreken en de bestuurlijke afspraken op te volgen;**
- **de informatie-uitwisseling te vergemakkelijken.**

[14] Rapport verantwoordingsonderzoek 2024, Kamerstuk 36 740 VI, nr. 2, p. 33.
[15] Rapport verantwoordingsonderzoek 2024, Kamerstuk 36 740 VI, nr. 2, p. 79.

Vragen en opmerkingen van de leden van GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de verantwoordingsstukken van het Ministerie van Justitie en Veiligheid over 2024. Deze leden pleiten al lange tijd voor een meer integrale behandeling van begrotingen en de verantwoording van uitgaven voor digitalisering. Over de verantwoordingsstukken hebben zij enkele vragen en opmerkingen.

De leden van de GroenLinks-PvdA-fractie wijzen vooral op de verantwoording van de uitgaven aan het Nationaal Cyber Security Centrum (NCSC). Het is moeilijk te controleren of de middelen voor deze organisatie doelmatig, doeltreffend en effectief zijn.

Deze leden vragen de Minister daarom om duidelijk te maken wat het totaalbudget voor het NCSC was in 2024 en wat de betrokken departementen hebben ingelegd.

Antwoord
Het totaalbudget van het NCSC was in 2024 71,3 miljoen euro. Het merendeel werd ingelegd door het Ministerie van Justitie en Veiligheid. Voor de voorbereiding op de inwerkingtreding van de Netcode werd 3,2 miljoen euro door het Ministerie van Economische Zaken/Klimaat en Groene Groei ingelegd. Voor de uitvoering van het programma Versterking SOC-stelsel Rijk werd 2,3 miljoen door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties ingelegd.

Wat waren de doelstellingen voor 2024 en zijn die behaald?

Antwoord
In 2024 heeft het NCSC invulling gegeven aan haar wettelijke taken uit de Wet beveiliging netwerk- en informatiesystemen. Het NCSC werkt daarnaast doorlopend aan het verbeteren van haar slagkracht en dienstverlening. In 2024 is in het bijzonder gewerkt aan twee grote veranderopgaven, namelijk de voorbereiding op de inwerkingtreding van de Cyberbeveiligingswet (Cbw) en de transitie naar een vernieuwde cybersecurityorganisatie waarin het NCSC vanaf 2026 samen met het DTC en CSIRT-DSP in op zal gaan.

Zij wensen dit in de toekomst beter te controleren en vragen de Minister om dit voortaan standaard inzichtelijk te maken. Welke mogelijkheden ziet u om de uitgaven beter controleerbaar te maken?

Antwoord
De Minister van Justitie en Veiligheid informeert de Tweede Kamer regelmatig over de taakuitvoering van het NCSC bijvoorbeeld in de voortgangsrapportage van de Nederlandse Cybersecurity Strategie (NLCS). De Minister van Justitie en Veiligheid zorgt daarnaast conform de Regeling Periodiek Evaluatieonderzoek (RPE) voor beleidsdoorlichting/periodieke evaluatie. Ook is het jaarplan van het NCSC openbaar te raadplegen.

De leden van de GroenLinks-PvdA-fractie maken zich zorgen over het grote aantal extern ingehuurde medewerkers bij het NCSC. Het is van groot belang dat publieke organisaties specialisten weten aan te trekken

en te behouden. Wat doet de Minister om het aandeel extern ingehuurde krachten te verminderen en meer vast personeel aan te trekken binnen het NCSC?

Antwoord
Het NCSC wil de afhankelijkheid van externe inhuur graag verkleinen. Het NCSC zet daarom stevig in op het werven van vast personeel, met speciale aandacht voor functies waar de arbeidsmarkt het krapst is – zoals cybersecurityspecialisten. Het NCSC werkt in het kader van de transitie naar de vernieuwde cybersecurityorganisatie aan een nieuw Organisatie- en Formatieplan. De organisatie verbetert de wervingsaanpak, biedt ontwikkelmogelijkheden en zorgt voor een aantrekkelijk loopbaanperspectief. Toch is het NCSC op dit moment, door de krapte op de arbeidsmarkt, nog aangewezen op externe krachten om het werk goed te kunnen doen.

Hoe enthousiasmeert u extern ingehuurde krachten om vast in dienst te komen of elders in de publieke sector hun kennis en expertise in te zetten?

Antwoord
Het NCSC gaat actief in gesprek met externen over de mogelijkheid om in dienst te komen. Het NCSC benadrukt wat het werk bij het NCSC en binnen de Rijksoverheid bijzonder maakt: impactvol, inhoudelijk sterk, en maatschappelijk relevant. Het NCSC biedt hen daarnaast perspectief op interessante opdrachten, doorgroei en een goede balans tussen werk en privé. Tegelijkertijd merken we dat de overstap naar een vast contract vaak knelt als het gaat om verschil in arbeidsvoorwaarden, zeker bij schaarse profielen waar de markt hogere vergoedingen biedt.

Deze leden benadrukken dat er een schrijnend tekort aan ICT-experts is en dat het demissionaire kabinet zich moet inzetten om meer specialisten langjarig in dienst te nemen. Dat is nodig om het kennisniveau over cyberveiligheid binnen de overheid op peil te brengen.

De leden van de GroenLinks-PvdA-fractie zijn blij dat de Cyberbeveiligingswet eindelijk aan de Kamer is toegestuurd.

Deze leden vragen u of het NCSC nu voldoende is uitgerust voor de implementatie van deze wet en zo niet, welke aanvullende middelen er volgens het NCSC nodig zijn.

Antwoord
Het NCSC heeft middels een uitvoeringstoets in kaart laten brengen hoeveel aanvullende middelen nodig zijn voor de implementatie en uitvoering van de Cbw. De beschikbaar gestelde middelen in 2024 waren afdoende voor de werkzaamheden die het NCSC in 2024 in het kader van de implementatie Cbw heeft verricht.

Zij maken zich zorgen over de voorbereidingen van alle organisaties en overheden die straks aan de wet moeten voldoen. Met name gemeenten, die al te maken hebben met grote financiële uitdagingen, hebben vragen over de implementatie en voorziene kosten van de Cyberveiligheidswet.

Per wanneer kunt u organisaties en overheden duidelijkheid geven over welke middelen zij moeten reserveren om te voldoen aan hun nieuwe verplichtingen? Is er een systematiek voor deze organisaties om te berekenen waar zij ongeveer rekening mee moeten houden?

Antwoord
Organisaties zijn zelf verantwoordelijk voor het implementeren van de Cyberbeveiligingswet (Cbw). Het maken van een risicoanalyse is de eerste stap in het verbeteren van de cyberweerbaarheid van een bedrijf of organisatie. Uit een risicoanalyse komt naar voren welke risico's het zwaarst wegen en waar beveiligingsmaatregelen het hardst nodig zijn. Deze set aan maatregelen bepalen onder anderen welke investeringen nodig zijn. Op de overheidswebsite van het NCSC staat wat organisaties nu al kunnen doen om zich voor te bereiden op de Cbw. Daarnaast kunnen organisaties op basis van het wetsvoorstel, dat in de Tweede Kamer ligt, en de consultatieversie van de algemene maatregel van bestuur (AMvB) al een eerste indicatie maken wat het voor hen betekent.
Vanuit de Europese Unie is er een standaardberekening met de richtlijn meegegeven hierover. Deze staat vermeld in de memorie van toelichting van het wetsvoorstel.
Daarnaast is met de regeldruktoets en de MKB-toets een inschatting gemaakt van de uren en de kosten die nodig zijn om de maatregelen uit de wet en de AMvB te implementeren. De resultaten zijn opgenomen in de memorie van toelichting van de wet, en de nota van toelichting van de AMvB. Daarnaast is door het Ministerie van BZK en het Ministerie van IenW bij medeoverheden een Uitvoeringstoets Decentrale Overheden uitgevoerd (UDO) voor de wet en AMvB.

Tot slot zijn de leden van de GroenLinks-PvdA-fractie bezorgd over de alsmaar toenemende afhankelijkheid van Amerikaanse techleveranciers binnen de overheid en de publieke sector. Deze leden vrezen dat als de marktdominantie van enkele Amerikaanse bedrijven niet afneemt, er aanzienlijke risico's zijn voor de onafhankelijkheid van instituties en overheden. Dit is in lijn met veel aangenomen Kamermoties op dit onderwerp. Zij vragen daarom om uit te leggen hoe u in 2024 binnen uw ministerie werk heeft gemaakt van digitale soevereiniteit en of u de afhankelijkheid succesvol heeft teruggedrongen. Kunt u dit uitdrukken in cijfers, bijvoorbeeld het aandeel soft- en hardware dat is ingekocht van Europese bedrijven, of de uitgaven die u heeft gedaan aan niet-Europese soft- en hardware ten opzichte van Europese alternatieven? Ziet u het als uw rol om de digitale soevereiniteit binnen uw departement te versterken?

Antwoord
Departementale versterking van de digitale soevereiniteit is een belangrijke taak waartoe momenteel verschillende mogelijkheden worden onderzocht.
JenV kijkt bewust naar de implementatie van M365 vanuit de gedachte om cloud afhankelijkheid daarin zoveel mogelijk te vermijden. Verder onderzoekt SLM-Rijk alternatieven en samenwerking op Europees niveau zoals StackIT en EuroStack.
Daarnaast is de inzet om AI/Large Language Model in eigen ontwikkeling/beheer uit te voeren i.p.v. AI-tooling aan te schaffen van grote leveranciers.

Binnen het Rijk en daarmee JenV wordt niet bijgehouden welke ingekochte soft- en/of hardware «Europees» is en welke niet. Deze cijfers hebben we op dit moment dan ook niet.
Eventueel kan inzicht worden geboden aan wie opdrachten zijn gegund en aan wie facturen zijn betaald. Daarmee is de herkomst van soft-/hardware en/of de invloed van mogelijk in het

buitenland gevestigde toeleveranciers en/of moederondernemingen niet per definitie gegeven.

De leden van de GroenLinks-PvdA-fractie vragen ook aandacht voor de digitale soevereiniteit van de justitieketen. Het is riskant om een aanzienlijk deel van onze justitieketen afhankelijk te maken van niet-Europese bedrijven. In uiterste gevallen kunnen zij als speelbal worden gebruikt in geopolitieke conflicten; dit zet de vrijheid van onze rechtsstaat onder druk. Kunt u toelichten hoe groot de digitale afhankelijkheid van niet-Europese leveranciers is binnen organisaties in de justitieketen, zoals de politie, het Openbaar Ministerie, de Raad voor de Rechtspraak, en de Hoge Raad? Wat doet u om hun digitale soevereiniteit te borgen en versterken? Zijn hier middelen en capaciteit voor beschikbaar gesteld over 2024? Zo niet, bent u bereid dit alsnog te doen?

Antwoord
In hoeverre en in welke omvang sprake is van digitale afhankelijkheid in de justitieketen van niet-Europese leveranciers kan ik niet toelichten. Deze informatie is niet beschikbaar.
Voor de rechterlijke macht en het Openbaar Ministerie als onafhankelijke organisaties in het staatsbestel geldt dat zij zelf zorgdragen voor aanschaf en beheer van hun hardware en software.
De organisaties in de justitieketen brengen voortdurend wijzigingen aan in de programmatuur, apparatuur, contracten en ICT-systemen om te blijven voldoen aan de laatste ontwikkelingen en nieuwste beveiligingseisen.[16]

Het borgen van de continuïteit en de kwaliteit binnen de justitieketen, zowel voor het strafrecht als voor de andere rechtsgebieden, vergt een zorgvuldige aanpak. Daarom ben ik met organisaties binnen het juridische domein in gesprek over digitale autonomie en in hoeverre dit uitvoerbaar is in de praktijk. Gelet op dit alles zet JenV onverminderd in op weerbaarheid en vitale infrastructuur. Er zijn vanuit JenV geen financiële middelen beschikbaar specifiek voor de digitale soevereiniteit.[17]

Vragen en opmerkingen van de leden van VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de stukken geagendeerd voor het schriftelijk overleg aangaande de Jaarverantwoording 2024 van het Ministerie van Justitie en Veiligheid (voor zover het digitaliseringsonderwerpen betreft). Deze leden stellen nog enkele vragen naar aanleiding van de beantwoording van de vragen inzake Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Justitie en Veiligheid[18].

De leden van de VVD-fractie onderschrijven de waarde van een snelle accreditatie bij ingebruikname van gevoelige informatiesystemen zodat een juist beveiligingsniveau kan worden gewaarborgd. Deze leden lezen in de genoemde beantwoording dat bij het wegwerken van de achterstanden in het accrediteren van belangrijke informatiesystemen wordt ingezet op het tijdelijk beschikbaar stellen van meer capaciteit om het proces van accreditatie te faciliteren en de accreditaties uit te voeren, en

---

[16] *Kamerstukken II*, 2024/25, 26 643, nr. 1314.
[17] Beantwoording Kamervragen van de Vaste Kamer commissie voor Digitale Zaken inzake Wijziging van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2025 (wijziging samenhangende met de Voorjaarsnota), antwoord op vraag 56.
[18] Kamerstuk 36 740 VI, nr. 2.

dat er een actualiseringsslag heeft plaatsgevonden op de lijst met kritieke of bedrijfskritische systemen waarna op basis van risicomanagement een shortlist met systemen die prioriteit in de accreditering benodigen is gemaakt. Deze leden vragen de Minister wanneer de achterstanden op accreditaties van gevoelige informatiesystemen naar verwachting ingehaald zullen zijn.

Antwoord
De Minister streeft ernaar om de meest risicovolle informatiesystemen op zo kort mogelijke termijn geaccrediteerd te krijgen. Op dit moment wordt de uitvoering van de accreditatie van de meest risicovolle systemen ter hand genomen en worden voorbereidingen getroffen voor de accreditatie van de overige systemen. De Minister spant zich maximaal in om dit zo snel en zorgvuldig mogelijk te realiseren. De Minister onderkent de urgentie van het wegwerken van de achterstanden en hoewel de Minister op dit moment nog geen exacte datum kan noemen, benadrukt de Minister dat de Kamer vanzelfsprekend geïnformeerd zal worden over de voortgang van deze operatie.

Zij vragen de Minister verder hoe het departementaal accreditatiebeleid van het Ministerie van Justitie en Veiligheid in lijn gaat worden gebracht met het interdepartementale accreditatiebeleid van het Rijk en wat de verwachting is op welke termijn dit volbracht kan worden.

Antwoord
Het accreditatiebeleid van het ministerie is gebaseerd op het brede interdepartementale accreditatiebeleid alsook het VIRBI 2013 en vigerend BIO. Het ministerie heeft dat beleid verder afgestemd op haar aard en organisatie inrichting. Daar waar dit mogelijk afwijkt vindt het ministeriële accreditatiebeleid de grondslag in het VIRBI 2013 en vigerend BIO.

In het verlengde van bovenstaande vragen de leden van de VVD-fractie of de Minister een overzicht kan geven van innovatieve ICT-toepassingen bij het Ministerie van Justitie en Veiligheid?
Welke innovaties worden momenteel verder uitgewerkt ten behoeve van efficiëntere dienstverlening en efficiënter werken binnen het ministerie?

Antwoord (19 en 20)

doorGROEI
Het Ministerie van JenV werkt voortdurend aan het vergroten van beleidseffectiviteit. Effectief beleid is zoveel mogelijk evidence informed en gebaseerd op wetenschappelijke kennis. JenV ontwikkelt daarom tooling waarmee beleidsmedewerkers eenvoudiger, sneller en vollediger toegang hebben tot wetenschappelijke- en vakliteratuur voor het maken en verantwoorden van beleid. De tooling wordt geïntegreerd in de JenV AI Assistent Robin.

Kennis assistent («Robin»)
Het Ministerie van Justitie en Veiligheid en Asiel en Migratie ontwikkelen een Kennis assistent («Robin») om een veiliger en verantwoorder alternatief te bieden voor (gratis) online applicaties zoals ChatGPT. Robin is een modulaire AI-assistent die gebruik kan maken van geavanceerde Large Language Models (LLM's). Via Robin worden collega's ondersteund in tekstverwerkingstaken en het vinden van relevante (interne) informatie. Daarnaast kan men via Robin andere digitale (AI)-tools

aanroepen, zoals tools voor het samenvatten van documenten, transcriberen van geluidsopnamen of het vertalen van teksten.

Andere innovaties zijn:

PET (Privacy Enhancing Technologieën)
JenV/AenM ontwikkelen en implementeren Privacy Enhancing Technologieën, waarmee het bevragen van gegevens vanuit de keten efficiënter en met inachtneming van de privacy waarborgen plaatsvindt. Hiermee wordt onnodige gegevensdeling voorkomen en worden beschikbare gegevens gerichter gedeeld. Veilige onderlinge bestand uitwisseling Binnen JenV AenM loopt de verkenning naar effectieve bestandsdeling en samenwerking op Open Source technieken die de afhankelijkheid van grote Tech bedrijven op dit vlak verminderd.

Innovatie AI-infrastructuur
Vanuit JenV AenM wordt de ontwikkeling naar een *on premise* infrastructuur onderzocht. Zodat productionele AI-toepassingen daarin (*buiten de cloud)* kunnen landen.

Wordt er bijvoorbeeld gewerkt aan innovatieve ICT-toepassingen voor de afhandeling van WOO-verzoeken?

Antwoord
Het ministerie werkt al met innovatieve ICT-toepassingen voor de behandeling van Woo-verzoeken. De toepassing wordt gebruikt om grote hoeveelheden documenten te ordenen, doorzoeken en redigeren; ook is het programma instaat om automatisch sommige persoonsgegevens te lakken, zoals telefoonnummers en e-mailadressen. Het resultaat is dat het afhandelingsproces hierdoor efficiënter en sneller verloopt dan voorheen.

En welke ICT-projecten hebben voor de Minister de hoogste prioriteit bij het verbeteren van de doorlooptijden in de strafrechtketen en specifiek bij de politie?

Antwoord
Zoals ik uw Kamer in de Voortgangsbrief Strafrechtketen berichtte werken de organisaties in de strafrechtketen aan een meerjarenagenda die moet leiden tot een versterking van de aanpak van voorraden en doorlooptijden. De meerjarenagenda zal later worden aangevuld met afspraken over de andere twee ketendoelen, namelijk ketendigitalisering en implementatie van het nieuwe Wetboek van Strafvordering.

Twee voorbeelden van projecten met een ICT-component die gericht zijn op het verbeteren van de doorlooptijden zijn:
- **Schonen van BOSZ (Betere Opsporing door Sturing op Zaken), een workflow systeem voor misdrijven en verdachten daarvan. Dit is een gezamenlijk project van politie en OM. Doel hiervan is het verkrijgen van beter overzicht en inzicht in zaken door het schonen en standaardiseren van het gebruik van het systeem BOSZ.**
- **Digitale samenwerkingsruimte. Dit is een gezamenlijk project van de politie, het OM en 3RO. Er wordt gewerkt aan een digitale samenwerkingsruimte ZSM waarin informatie wordt verzameld zodat het OM en alle ketenpartners gerichter en sneller kunnen besluiten over de afhandeling van ZSM-zaken.**

Zij vragen ook hoe zorg wordt gedragen dat bevindingen die volgen uit «red teaming» sneller gedeeld worden en opvolging genieten bij uitvoeringsorganisaties.

Antwoord
Om ervoor te zorgen dat bevindingen die volgen uit red teaming sneller gedeeld worden en opvolging genieten, stelt het departement een lijst op met (meest kritische) bevindingen. Bevindingen die een collectieve aanpak behoeven wordt centraal binnen het departement opgepakt. De opvolging van bevindingen door de uitvoeringsorganisaties wordt door deze organisaties periodiek gerapporteerd in het IB beeld. Het departementale programma IB2.0 biedt aan uitvoeringsorganisaties steun met kennis, capaciteit en financiële middelen. Er is daarnaast een actieplan opgesteld en gestart dat onder meer de opvolging van de bevindingen uit red teaming verder verbeterd.

Deelt de Minister de mening dat red teaming weinig nut heeft als vervolgens recent uitgevoerde beveiligingstests deels vergelijkbare bevindingen opleveren als bij eerdere testen?

Antwoord
**De mening wordt gedeeld dat red teaming weinig nut heeft als recent uitgevoerde beveiligingstests deels vergelijkbare bevindingen opleveren als bij eerdere testen. De red teaming onderzoeken bieden inzichten in nieuw soortige risico's op informatiebeveiliging. Daarnaast leidt het aanpakken van bekende testbevindingen tot nieuwe inzichten die vragen om een nadere, soms andere verdiepende aanpak. Een aantal hiervan grijpen diep in op de organisatie en techniek van taakorganisaties en vergen daarom enige tijd en (financiële) capaciteit om op te lossen.
Als maatregel is een actieplan opgesteld dat onder meer de opvolging van de bevindingen uit red teaming moet verbeteren. Onderdeel hiervan is tevens het versterken van departementaal toezicht op informatiebeveiliging zowel op centraal als decentraal niveau.**

Ten slotte vragen de leden van de VVD-fractie hoe zorg wordt gedragen voor een beter informatie-uitwisseling tussen het kerndepartement en organisaties gelieerd aan het ministerie, zodat het kerndepartement zijn coördinerende rol kan vervullen.

Antwoord
**De bevinding dat verbetering van de informatie-uitwisseling tussen het kerndepartement en de uitvoeringsorganisaties over informatiebeveiliging nodig is, wordt onderschreven.
Als maatregel is er een actieplan opgesteld dat onder meer de opvolging van de redteamingtesten moet verbeteren. Onderdeel is tevens het versterken van departementaal toezicht op informatiebeveiliging zowel op centraal als decentraal niveau.**

Vragen en opmerkingen van de leden van NSC-fractie

De leden van de NSC-fractie hebben met belangstelling kennisgenomen van de Jaarverantwoording 2024 van het Ministerie van Justitie en Veiligheid, voor zover het onderwerpen betreft die zien op digitalisering. Deze leden hebben naar aanleiding hiervan nog een aantal vragen en opmerkingen. De leden van de NSC-fractie willen de Minister vragen hoe hij aankijkt tegen de recente reflectie van de Algemene Rekenkamer, waarin wordt geconcludeerd dat bewindspersonen van het kabinet

onvoldoende concrete en meetbare doelstellingen formuleren. Dit bemoeilijkt het inzicht in de behaalde resultaten, ook op het terrein van digitalisering binnen het Ministerie van Justitie en Veiligheid.

Antwoord
De conclusies omtrent het gebrek aan concrete en meetbare doelstellingen worden herkend. In het kader van de opvolging zijn actieplannen opgesteld waar vol op wordt ingezet. Hiermee worden concrete verbeteringen beoogd bij onder meer de opvolging van redteamingtesten en het versterken van het departementaal toezicht op informatiebeveiliging.

Deze leden vragen de Minister naar aanleiding hiervan om aan te geven welke concrete doelen op het gebied van digitalisering het afgelopen jaar zijn gesteld binnen het ministerie en in hoeverre deze doelen daadwerkelijk zijn behaald. Wat waren de belangrijkste resultaten op dit terrein in het afgelopen jaar en hoe dragen deze bij aan het verbeteren van de digitale weerbaarheid en de dienstverlening van het ministerie?

Antwoord
Er is nieuw informatiebeveiligingsbeleid binnen JenV opgesteld en de voorbereiding voor de implementatie van de nationale wetgeving van de Europese NIS2-richtlijn en de BIO2.0 wordt voortgezet. Met het departementale programma Informatiebeveiliging 2.0 (IB2.0) wordt beoogd om de digitale weerbaarheid te vergroten. Het programma biedt steun aan uitvoeringsorganisaties met kennis, capaciteit en financiële middelen. Het programma wordt momenteel verder geoptimaliseerd.

De digitale dreiging tegen Nederland is groot en voortdurend in ontwikkeling, zo blijkt uit het Cybersecuritybeeld Nederland 2024. De leden van de NSC-fractie willen de Minister vragen welke leerpunten het ministerie heeft getrokken uit incidenten met datalekken en kwesties rond cyberveiligheid in het afgelopen jaar. Op welke wijze worden deze lessen structureel meegenomen in beleid en uitvoering?

Antwoord
Binnen het sturingsmodel van JenV en AenM is een cyclus ingericht waarin planning, verantwoording en toezicht plaatsvindt. Binnen deze cyclus worden onder meer incidenten omtrent datalekken en informatiebeveiliging gerapporteerd en geëvalueerd. Deze evaluaties worden gebruikt als stuurinstrument en input voor beleidsevaluatie. Hiernaast beschikken JenV en AenM voor het afhandelen van grote incidenten, datalekken en (cyber-)crisissituaties over incidentbestrijdingsprocedures en een departementaal coördinatiecentrum crisisbeheersing (DCC) die de crisisaanpak waarborgt. Onderdeel van deze procedures is ook het evalueren en leren van deze situaties. Onlangs is de kamer door de Minister van Binnenlandse zaken geïnformeerd over het datalek met metadata. Ook binnen JenV en AenM is hiervoor de crisisorganisatie opgeschaald om schadelijke gevolgen en risico's vanuit deze situatie te mitigeren. Op dit moment wordt de crisisaanpak conform werkwijze geëvalueerd om vanuit hier lessen mee te nemen naar toekomstige situaties en, indien nodig, mee te nemen in beleidsontwikkelingen op deze thema's.

De leden van de NSC-fractie vernemen graag van de Minister welke behoeften hij op dit moment signaleert in de markt als het gaat om cybersecurity. Zijn er volgens de Minister specifieke knelpunten, zoals een

tekort aan kennis, technologie of capaciteit, die het realiseren van digitale veiligheid belemmeren?

Antwoord
Zoals geschetst in het Cybersecuritybeeld Nederland 2024 (CSBN) is de verwachting dat de komende jaren de vraag naar cybersecurity professionals zal toenemen. Dit komt voort uit de combinatie van voortschrijdende digitalisering, toenemende vraag, en toekomstige wet- en regelgeving waaraan moet worden voldaan én waar toezicht op moet worden gehouden. Het is niet alleen de toegenomen vraag die tot schaarste heeft geleid, ook het aanbod groeit niet mee. Het CSBN geeft aan dat dit tekort aan cybersecuritydeskundigen de digitale weerbaarheid van Nederland kan aantasten. Om te waarborgen dat de Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts heeft het Kabinet dit opgenomen in de doelstellingen van de Nederlandse Cybersecurity Strategie 2022–2028.

Daarnaast constateren zij dat er op het gebied van informatiebeveiliging binnen het Ministerie van Justitie en Veiligheid nog stappen nodig zijn. De Algemene Rekenkamer signaleert onder andere een grote achterstand in de accreditatie van belangrijke systemen, trage opvolging van bevindingen uit beveiligingstesten, en onvoldoende informatie-uitwisseling tussen het kerndepartement en de onderliggende organisaties. De leden vragen de Minister hoe hij deze structurele tekortkomingen beoordeelt, welke concrete maatregelen er worden of zijn genomen om deze aan te pakken, en op welke termijn verbeteringen zichtbaar moeten zijn?

Antwoord
De bevinding dat verbetering van de informatie-uitwisseling tussen het kerndepartement en de uitvoeringsorganisaties over informatiebeveiliging nodig is, wordt onderschreven.
Als maatregel is er een actieplan opgesteld dat onder meer de opvolging van de redteamingtesten en accreditatie van informatiesystemen moet verbeteren. Onderdeel is tevens het versterken van departementaal toezicht op informatiebeveiliging zowel op centraal als decentraal niveau.