Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

608

Vragen van de leden **Kathmann** en **Stultiens** (beiden GroenLinks-PvdA) aan de Minister van Sociale Zaken en Werkgelegenheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Paniek over veiligheid pensioenen APG: kritisch rapport legt problemen bloot»* (ingezonden 26 september 2024).

Antwoord van Minister **Van Hijum** (Sociale Zaken en Werkgelegenheid), mede namens de Minister van Justitie en Veiligheid (ontvangen 19 november 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 247

Vraag 1
Bent u bekend met de berichtgeving over de kwetsbaarheid van de ICT bij APG en het Schuberg Phyllis-onderzoek waar dit uit bleek?[1]

Antwoord 1
Ja, hier ben ik mee bekend.

Vraag 2
Is het bij u bekend of andere kritieke instellingen met zulke kwetsbaarheden te maken hebben?

Antwoord 2
Instellingen, zoals APG, laten periodiek testen en audits uitvoeren om IT-kwetsbaarheden en verbeterpunten aan het licht te brengen. Hieruit is gebleken dat de beveiliging van APG van zeer hoog niveau is. APG geeft echter aan dat er ook verbeterpunten zijn in de beveiliging van de IT-infrastructuur. Na deze constatering zijn er mitigerende maatregelen genomen tegen de IT-risico's. Dit gebeurt in goed overleg met de belangrijkste stakeholder en toezichthouders. Pensioenuitvoerders staan via hun fondsen onder toezicht, en doen mee aan zeer ingrijpende cybersecuritytesten van DNB. Het doel hiervan is om eventuele kwetsbaarheden tijdig te onderkennen en deze adequaat op te lossen.

[1] De Limburger, 20 september 2024, «Paniek over veiligheid pensioenen APG: kritisch rapport legt problemen bloot», (www.limburger.nl/cnt/dmf20240920_96567875).

ah-tk-20242025-608
ISSN 0921 - 7398
's-Gravenhage 2024

Vraag 3
Deelt u de opvatting dat het veilighouden van álle kritische ICT-infrastructuur waar mensen afhankelijk van zijn, bijvoorbeeld voor hun pensioen, gezondheid of inkomen, een overheidstaak is?

Antwoord 3
De regering hecht waarde aan de vitaliteit van belangrijke (financiële) instellingen zoals pensioenfondsen. Tegelijkertijd zet de regering in de Aanpak vitaal in op het versterken van de weerbaarheid van vitale instellingen[2]. De vitale infrastructuur bestaat uit processen en diensten die essentieel zijn voor de Nederlandse samenleving, waarvan verstoring, uitval of manipulatie grote gevolgen kan hebben voor de Nederlandse economie en maatschappij. De Aanpak vitaal is gericht op het voorkomen van de verstoring van vitale processen en de weerbaarheid aanhoudend te verhogen. In de cyclus vitaal identificeren vakdepartementen welke processen en aanbieders vitaal zijn en welke dreigingen en risico's er binnen de vitale processen bestaan.
Mocht de uitkomst van de Aanpak vitaal zijn dat sommige pensioenuitvoerders als vitaal worden aangemerkt, dan brengt dit rechten en plichten met zich mee. Zo krijgt een vitale aanbieder bij cyberincidenten ondersteuning van het Nationaal Cyber Security Centrum (NCSC) in het geval van grootschalige uitval.

Vraag 4
Hoe bent u betrokken bij het oplossen van de kwetsbaarheden bij APG, gezien het essentiële belang van deze instelling voor het uitkeren van pensioenen?

Antwoord 4
Vanuit mijn positie als Minister van Sociale Zaken en Werkgelegenheid ben ik niet rechtstreeks betrokken bij het oplossen van de kwetsbaarheden bij APG. APG is een private vergunninghoudende entiteit die onder toezicht staat bij de toezichthouders AFM en DNB. APG heeft in samenspraak met de twee toezichthouders zo spoedig mogelijk zelf mitigerende maatregelen getroffen om deze problemen zelf op te lossen.

Vraag 5
Heeft De Nederlandsche Bank (DNB) als toezichthouder eerder deze kwetsbaarheden aangetroffen? Zo nee, hoe kan de toezichthouder beter in staat worden gesteld om op de ICT toe te zien?

Antwoord 5
Informatiebeveiliging en cybersecurity zijn de afgelopen jaren een belangrijk strategisch thema binnen het toezicht van DNB en AFM.
Pensioenuitvoeringsorganisaties staan via hun fondsen onder toezicht en doen mee aan zeer ingrijpende cybersecuritytesten van DNB, waaronder de TIBER-test. TIBER staat voor Threat Intelligence Based Ethical Red-teaming en heeft als doel om te testen hoe weerbaar organisaties zijn tegen geavanceerde cyberaanvallen[3]. Kwetsbaarheden, waar zichtbaar, worden gemitigeerd. Voor zover bij mij bekend zijn er geen gevallen waarbij de IT-veiligheid van pensioenuitvoerders niet op orde is. Er zijn geen signalen vanuit de toezichthouders dat de huidige manier van toezicht op de ICT van pensioenuitvoerders niet voldoet. DNB kan niet ingaan op vragen over individuele instellingen die onder toezicht staan.

Vraag 6
Welk aandeel van het toezicht van de DNB wordt besteed aan cyberveiligheid van pensioenfondsen? Is dit toereikend om structurele kwetsbaarheden grondig te onderzoeken?

---

[2] Kamerstukken II, 2023–2024, 30 821 en 26 643 nr. 203
[3] Voor meer informatie zie: Cyberstrategie DNB

Antwoord 6
Vanwege toezichtvertrouwelijke informatie kan DNB geen uitlatingen doen welk aandeel van het toezicht besteed wordt aan cyberveiligheid van pensioenfondsen. Er zijn mij vanuit de toezichthouders geen signalen bekend dat de huidige capaciteit ontoereikend is om structurele kwetsbaarheden grondig te onderzoeken.
In zijn algemeenheid geldt dat cyberdreigingen toenemen. Dat ziet DNB terug in externe dreigingsanalyses van onder andere het Nationaal Cyber Security Centrum (NCSC). DNB heeft recent ook informatie gedeeld over cyberrisico's voor de financiële stabiliteit in het Overzicht Financiële Stabiliteit (najaar 2024). Dat komt enerzijds door steeds verdergaande automatisering van bedrijfsprocessen die al jarenlang aan de gang is. Dat maakt instellingen potentieel kwetsbaar voor cybercriminaliteit. Anderzijds ziet DNB dat dreigingen toenemen als gevolg van geopolitieke spanningen. Dit maakt instellingen potentieel ook kwetsbaar voor verstoring/sabotage door statelijke actoren.
DNB geeft aan dat maatregelen gelijke tred moeten houden met eventuele toenemende dreigingen. Instellingen moeten voortdurend alert zijn dat hun beheersmaatregelen passend zijn en blijven. DNB vraagt daarvoor aandacht, onder andere met de DNB Good Practice informatiebeveiliging. DNB ziet risico-gebaseerd erop toe dat instellingen aandacht houden voor voortdurende verbetering en dat zij de effectiviteit van hun maatregelen ook regelmatig testen. Voorts heeft DNB binnen de divisie Toezicht Pensioenfondsen een expertisecentrum specifiek gericht op operationele en IT-risico's.

Vraag 7
Hoe zorgt u ervoor dat andere kritieke instellingen zo goed mogelijk lessen trekken uit het Schuberg Phyllis-onderzoek en de stappen die APG zet ter verbetering?

Antwoord 7
Instellingen moeten voortdurend alert zijn dat hun beheersmaatregelen passend zijn en blijven. DNB vraagt daarvoor aandacht, onder andere met de DNB Good Practice informatiebeveiliging. DNB ziet er risico-gebaseerd op toe dat instellingen aandacht houden voor voortdurende verbetering en dat zij de effectiviteit van hun maatregelen ook regelmatig testen. Voorts heeft DNB binnen de divisie Toezicht Pensioenfondsen een expertisecentrum specifiek gericht op operationele en IT-risico's.
De regering hecht waarde aan de vitaliteit van belangrijke (financiële) instellingen zoals pensioenfondsen. Daartoe zet de regering in de Aanpak Vitaal in op het versterken van de weerbaarheid van vitale instellingen.[4] Het doel hiervan is om de weerbaarheid van kritieke instellingen blijvend te verhogen.

Vraag 8
Bent u bereid andere kritieke instellingen aan te moedigen al dan niet financieel te ondersteunen bij het uitvoeren van diepgravende analyses van hun ICT-kwetsbaarheden?

Antwoord 8
Organisaties zijn primair zelf verantwoordelijk voor hun ICT, zo ook de daaruit naar voren komende kwetsbaarheden. Vitale aanbieders dienen bij het in gebruik nemen van producten en diensten goed risicomanagement uit te voeren. Het analyseren van mogelijke risico's is gestoeld op het in kaart brengen van (1) de te beschermen belangen, (2) de dreiging tegen deze belangen te identificeren en (3) de bestaande weerbaarheid van de organisatie te definiëren en (4) op basis van deze analyse aanvullende maatregelen treffen om de risico's te beheersen. Het doel is om uiteindelijk tot een passend niveau van weerbaarheid te komen en de mate van risicoacceptatie te bepalen.
Pijler I van de Nederlandse Cybersecurity Strategie 2022–2028 ziet toe op het verhogen van de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties. Er worden verschillende acties uitgevoerd die

[4] Kamerstukken II, 2023–2024, 30 821 en 26 643 nr. 203

de vergaande publiek-private samenwerking – hetgeen nodig is om deze ambitie te realiseren – te verdiepen en uit te breiden.
Het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) hebben het afgelopen jaar diverse kennis- en adviesproducten ontwikkeld over cybersecurity in het risicomanagementproces, crisispreparatie en incidentrespons. Het gaat daarbij niet alleen om producten die relevant zijn voor organisaties die onder het toepassingsbereik van Cyber beveiligingswet vallen, maar ook voor alle andere organisaties. Daarnaast is er door het NCSC en het DTC een nieuwe set cybersecurity basisprincipes geschreven.
Om in publiek-privaatverband nog sneller en beter samen te werken heeft het NCSC gewerkt aan het digitaliseren van onder andere het delen van kwetsbaarheden. Hierbij wordt gebruik gemaakt van kwetsbaarheidsregisters om zo organisaties snel van advies te kunnen voorzien. Dit gebeurt mede in samenhang met het programma Cyclotron.
Daarnaast is er in 2024 met het publiceren van de toekomstvisie voor het Cyberweerbaarheidsnetwerk (CWN) een belangrijke stap gezet naar het verdiepen en uitbreiden van publiek-private samenwerking op het gebied van cybersecurity.
Tot slot heeft de Cyberbeveiligingswet ook invloed. Organisaties die onder deze wet vallen moeten voldoen aan een zorgplicht, waarin risicomanagement een centrale rol speelt. De verwachting is dat het wetsvoorstel in Q4 2024 aan de Afdeling Advisering van de Raad van State kan worden aangeboden. Op 17 oktober 2024 is de kamer geïnformeerd over de huidige stand van zaken.

Vraag 9
Welke voorzieningen staan er in de Cyberveiligheidswet die nog naar de Kamer komt, die onmisbare (publieke én private) instellingen als het APG zouden helpen?

Antwoord 9
De Cyberbeveiligingswet is de nationale wetgeving die voortkomt uit de Europese Network and Information Security Directive (NIS2-richtlijn). Het wetsvoorstel dat nog naar de Kamer komt heeft als doel om de digitale en economische weerbaarheid te versterken tegen toenemende dreigingen. De wet zal gelden voor bedrijven en organisaties die in specifieke «kritieke» sectoren actief zijn en een bepaalde omvang hebben. Voor financiële instellingen geldt de DORA, waarvoor het Ministerie van Financiën en DNB verantwoordelijk zijn.
De Cyberbeveiligingswet is horizontale wetgeving en schrijft voor de organisaties die daaronder vallen een zorgplicht voor. De zorgplicht verplicht organisaties zelf een risicoanalyse uit te voeren, op basis waarvan zij passende en evenredige maatregelen nemen voor de beveiliging van hun netwerk- en informatiesystemen die worden gebruikt voor de verlening van hun diensten. De leden van het bestuur van die entiteiten moeten de maatregelen goedkeuren en toezicht houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen.
De organisaties waarop de Cyberbeveiligingswet van toepassing is, moeten met advies en bijstand worden ondersteund door een CSIRT (Computer Security Incident Response Team). De ondersteuning vanuit de overheid kan verder bestaan uit informatie-uitwisseling, richtlijnen en kennisuitwisseling over maatregelen met als doeleinde het verhogen van cyberweerbaarheid. Daarnaast zal worden toegezien op de naleving van de Cyberbeveiligingswet door de verantwoordelijke toezichthouders.

Vraag 10
Erkent u evenals bronnen uit het artikel dat het versterken van de ICT-kennis in de besturen van grote instellingen direct bijdraagt aan de cyberveiligheid van die organisaties?

Antwoord 10
De leden van het bestuur van organisaties moeten de maatregelen in het kader van de risicoanalyse goedkeuren en toezicht houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen. Deze verplichting is onderdeel van de eerder benoemde NIS2-richtlijn en hier zal ook op worden toegezien.

Vraag 11
Op welke manier gaat u ervoor zorgen dat er meer ICT-kennis komt aan de top van kritieke instellingen? Is het versterken van de rol van de functionaris gegevensbescherming hiervoor voldoende? Kan er desnoods vanuit het Rijk bijgesprongen worden met ICT-expertise als die expertise aan de bestuurstafel mist?

Antwoord 11
De NIS2-richtlijn schrijft het bestuur van organisaties voor dat zij een cybersecurity-opleiding volgt. We hanteren in Nederland het principe dat er met de vertaling van EU-richtlijnen naar Nederlandse wet- en regelgeving zo dicht mogelijk bij de richtlijn wordt gebleven.
Een functionaris gegevensbescherming kan indien nodig ingezet worden, als dit nodig wordt geacht vanuit toezicht & handhaving. De precieze invulling hiervan volgt uit de Cyberbeveiligingswet en de bijbehorende AMvB.
Organisaties zijn zelf verantwoordelijk en dus is het niet mogelijk dat de overheid deze rol aan de bestuurstafel overneemt. Wel kunnen organisaties indien nodig een beroep doen op bijstand en expertise van de CSIRT.

Vraag 12
Kunt u deze vragen afzonderlijk van elkaar beantwoorden?

Antwoord 12
Ja.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Joseph (Nieuw Sociaal Contract),ingezonden 25 september 2024 (vraagnummer 2024Z14247).