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

609

Vragen van het lid **Joseph** (Nieuw Sociaal Contract) 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 25 september 2024).

Antwoord van Minister **Van Hijum** (Sociale Zaken en Werkgelegenheid) (ontvangen 19 november 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 248

Vraag 1
Bent u bekend met het bericht «Paniek over veiligheid pensioenen APG: kritisch rapport legt problemen bloot»?[1]

Antwoord 1
Ja, hier ben ik mee bekend.

Vraag 2
Bent u, evenals De Nederlandsche Bank (DNB), op de hoogte van de uitkomsten van het onderzoek van de consultants van het bureau Schuberg Philis naar de kwetsbaarheid van pensioenuitvoerder APG voor cyberaanvallen?

Antwoord 2
Naar aanleiding van de berichtgeving in De Limburger heb ik hierover contact opgenomen met APG. Uit deze contacten is gebleken dat APG en andere pensioenuitvoerders met regelmaat laten onderzoeken wat de impact is van een significante cyberaanval. Uit het meest recente onderzoek is gebleken dat de beveiliging op hoog niveau is. Op een aantal punten heeft het rapport geleid tot verdere aanscherpingen. Deze werkwijze is in lijn met de wettelijke taak om te zorgen voor een beheerste en integere bedrijfsvoering. Hier wordt ook door DNB en AFM in hun respectievelijke verantwoordelijkheden toezicht op gehouden.

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

ah-tk-20242025-609
ISSN 0921 - 7398
's-Gravenhage 2024

Vraag 3
In het bericht staat dat APG voor vier miljoen mensen pensioenen regelt, kunt u aangeven hoeveel mensen momenteel via APG een maandelijkse pensioenuitkering ontvangen?

Antwoord 3
APG verzorgt op dit moment voor circa 4,6 miljoen mensen hun pensioen (jaarverslag APG 2023). Op het moment van schrijven ontvangen ruim 1,4 miljoen mensen een maandelijkse pensioenuitkering via APG.

Vraag 4-7
Hoe kijkt u naar de uitkomst van het onderzoek van Schuberg Philis dat APG mogelijk zes tot twaalf maanden nodig zou hebben om de digitale infrastructuur weer op de rit te krijgen in een zogenoemde «no-IT-situatie», een situatie waarin hackers alles platleggen?
Hoe kijkt u aan tegen het geschetste scenario dat een groot aantal mensen in Nederland in geval van zo'n «no-IT-situatie» bij APG mogelijk plots – tijdelijk – geen aanvullende pensioenuitkering ontvangen en daardoor bijvoorbeeld de huur niet meer kunnen betalen?
Wat is uw visie op de stelling in het bericht dat de huidige kwetsbare situatie niet alleen een bedreiging is voor APG en APB, maar zelfs voor de «BV Nederland»?
Vindt u het in dat licht ook zorgelijk dat uit het onderzoek naar voren komt dat de grootste kwetsbaarheden in de IT-beveiliging in de programma's en applicaties zitten waar dagelijks mee wordt gewerkt bij APG?

Antwoord 4-7
Gezien de onderlinge samenhang van gestelde vragen zal ik deze hieronder gezamenlijk beantwoorden.
Met het toenemend belang van cybersecurity laat APG met regelmaat onderzoeken wat de impact is van een significante cyberaanval waarbij de IT volledig wordt stilgelegd (no-IT scenario) en welke mogelijkheden er zijn om de impact te verkleinen. In april jl. is het rapport opgeleverd waarnaar in de publicatie werd verwezen. Een belangrijke nuance is dat er uitgegaan is van het meest extreme denkbare scenario. De kans dat dit scenario zich voordoet is uitermate klein. Dit is mede zo omdat APG al mitigerende maatregelen heeft getroffen. Ook in het geval van een no-IT scenario kan APG een groot deel van haar primaire processen uitvoeren, zo geeft het desgevraagd aan. Het rapport heeft geleid tot verdere aanscherping van APG's noodprocedures en maatregelen.
Een belangrijk voorbeeld van een primair proces is het uitbetalen van de pensioenuitkeringen. De hiervoor ingerichte noodprocessen worden voortdurend getest en zijn betrouwbaar gebleken. De pensioenen kunnen dus ook in een no-IT scenario uitbetaald worden, zo geeft APG aan op basis van de uitgevoerde onderzoeken.
Pensioenuitvoeringsorganisaties, zoals APG, laten periodiek testen en audits doen 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 heeft APG maatregelen genomen om de IT-risico's te mitigeren. Dit gebeurt in goed overleg met de belangrijkste stakeholder en toezichthouders. Pensioenuitvoerders staan via hun fondsen onder toezicht, en doen mee aan zeer ingrijpende cybersecurity testen van DNB waarbij het verplicht is dat instellingen scenario's uitwerken en testen uitvoeren tegen cyberdreigingen, zoals ransomware aanvallen, DDoS-aanvallen en in een uiterst geval ook een no-IT scenario. Daarbij is het van belang dat de instellingen die scenario's meenemen die passen bij de aard, het risicoprofiel en de vastgestelde «risk appetite» van de instellingen. DNB laat pensioenuitvoeringsorganisaties, zoals APG, bovendien meedoen aan de zogenaamde TIBER-test, een intensieve test georganiseerd door DNB, om digitale veiligheid van financiële instellingen te toetsen en verbeteringen aan het licht te brengen. TIBER staat voor Threat Intelligence Based Ethical Red-teaming. De tekst heeft als doel om te testen hoe weerbaar organisaties

zijn tegen geavanceerde cyberaanvallen[2]. Kwetsbaarheden, waar zichtbaar, worden gemitigeerd. De betreffende instelling zal de testresultaten evalueren, meenemen en – daar waar van toepassing – omzetten in verbeteracties.

Vraag 8
Is bij u bekend of er andere pensioenuitvoerders zijn waarbij de IT-veiligheid niet op orde is? Zo ja, hoe gaat u pensioenuitvoerders aansporen om die IT-veiligheid te verbeteren?

Antwoord 8
Pensioenuitvoeringsorganisaties, zoals APG, laten periodiek testen en audits doen om IT-kwetsbaarheden en verbeterpunten aan het licht te brengen. Wanneer daaruit blijkt dat er verbeterpunten zijn, worden maatregelen genomen om de IT-risico's te mitigeren. Na deze constatering heeft APG maatregelen genomen om de IT-risico's te mitigeren. Dit gebeurt in goed overleg met de belangrijkste stakeholders en toezichthouders. Pensioenuitvoerders staan via hun fondsen onder toezicht, en doen mee aan zeer ingrijpende cybersecuritytesten van DNB, waaronder de bovengenoemde TIBER-test.

Vraag 9-14
Bent u van mening dat het in het grootste belang is dat een pensioenuitvoerder zoals APG zo snel mogelijk weer operationeel kan zijn in het geval van een cyberaanval?
Hoe beoordeelt u de uitkomst van het onderzoek dat de back-ups van APG op dit moment niet zodanig zijn ingericht dat APG weer snel operationeel kan zijn in het geval van een cyberaanval?
Wat kunt u vanuit uw rol als bewindspersoon doen om bij te dragen aan een oplossing voor deze kwetsbaarheid in de IT-systemen van APG, nu uit het bericht blijkt dat er veel discussie is over hoe de problemen opgelost moeten worden?
Bent u van mening dat het van groot belang is dat de regie over IT-systemen en digitale infrastructuur zoveel mogelijk intern blijft ten opzichte van uitbesteding aan externe partijen/experts? Zo niet, waarom niet?
Deelt u de observatie uit het bericht dat het een enorme impact heeft, en zelfs maatschappelijk ontwrichtend werkt, als het misgaat door bijvoorbeeld een cyberaanval bij een instelling als APG? Zo niet, waarom niet?
Hoe gaat u zich vanuit uw rol als bewindspersoon inzetten om dit risico zoveel mogelijk te minimaliseren?

Antwoord 9-14
Gezien de onderlinge samenhang van gestelde vragen zal ik deze hieronder gezamenlijk beantwoorden.
In artikel 14 BuPw staat dat een pensioenfonds zorgdraagt voor een systematische analyse van de risico's die samenhangen met de uitbesteding van werkzaamheden en deze risico's vastlegt (lid 1), in het kader van een beheerste en integere bedrijfsvoering.
Een situatie waarin een APG of een andere pensioenuitvoerder te maken krijgt met een no-IT scenario en hierdoor ook mogelijk tijdelijk geen aanvullende pensioenuitkering kan uitkeren is ten allen tijde hoogst onwenselijk. Daarom nemen pensioenfondsen en de pensioenuitvoerders ook diverse mitigerende maatregelen, waaronder het hebben van noodsystemen, om dit te voorkomen.
Instellingen zijn primair zelf verantwoordelijk voor een beheerste en integere bedrijfsvoering, daarbij hoort ook informatiebeveiliging en cybersecurity. Dit geldt ook bij uitbesteding van werkzaamheden. Het is aan instellingen zelf om binnen deze eigen verantwoordelijkheid, rekening houdende met geldende wet- en regelgeving, te bepalen of werkzaamheden worden uitbesteed of niet en bij uitbesteding voldoende «regie» te voeren over de uitbestede dienstverlening. Toezichthouders DNB en AFM houden hier in op hun respectievelijke verantwoordelijkheden toezicht op. Op grond van artikel 3.17 Wet financieel toezicht, in verband met artikel 20 Besluit prudentiële regels en artikel 143 (lid 1) van de Pensioenwet en artikel 18 besluit FTK beschikken instellingen onder

[2] Voor meer informatie zie: Cyberstrategie DNB

toezicht van DNB over adequate procedures en maatregelen ter beheersing van ICT-risico's. Hieronder valt het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van de geautomatiseerde gegevensverwerking. Met ingang van 17 januari 2025 zal ook de Digital Operational Resilience Act (DORA) van kracht worden voor de financiële sector, die erop ziet dat financiële organisaties IT-risico's beter beheersen en daarmee weerbaarder worden tegen cyberdreigingen.[3] DORA stelt eisen ten aanzien van IT-risicomanagement, IT-incidenten, periodieke testen van digitale weerbaarheid en de beheersing van risico's bij uitbesteding aan (kritieke) derden.
Aanvullend hecht de regering grote waarde aan de vitaliteit van belangrijke (financiële) instellingen zoals pensioenfondsen.[4] Tegelijkertijd zet de regering in de Aanpak Vitaal in op het versterken van de weerbaarheid van vitale instellingen. De Aanpak vitaal is gericht op het voorkomen van de verstoring van vitale processen en de weerbaarheid aanhoudend te verhogen. In de beleidscyclus vitaal, onderdeel van de Aanpak Vitaal, wordt door vakdepartementen geïdentificeerd welke processen en aanbieders vitaal zijn en welke dreigingen en risico's binnen die vitale processen bestaan.[5]

Vraag 15
Hoe beoordeelt u tenslotte dit bericht over kwetsbaarheden in de IT-systemen van een grote pensioenuitvoerder in het licht van de druk op de IT-systemen van pensioenuitvoerders in de transitie naar het nieuwe pensioenstelsel?

Antwoord 15
De transitie naar het nieuwe pensioenstelsel vraagt veel van de sector. Om deze reden houdt mijn ministerie een vinger aan de pols tijdens de stelseltransitie. Met behulp van signalering, gesprekken met de sector, de monitoring en de onafhankelijke adviezen van de regeringscommissaris wordt gewogen of de transitie haalbaar blijft binnen de voorgestelde termijnen. De regeringscommissaris heeft in haar eerste advies gesignaleerd dat in het kader van de transitie rekening moet worden gehouden met een realistische planning en commitment van de betrokken partijen aan die planning, waaronder ICT-leveranciers. In de Wtp staat vastgelegd dat tijdens de transitie van pensioenuitvoerders wordt verwacht in het implementatieplan op welke wijze en in welk tijdspad de pensioenuitvoerder voorbereidingen treft voor de uitvoering van de nieuwe pensioenregeling, op welke wijze er invulling zal worden gegeven aan de uitvoering van de nieuwe pensioenregeling en de wijze waarop zal worden omgegaan met opgebouwde pensioenaanspraken en pensioenrechten.
In het implementatieplan gaat de pensioenuitvoerder onder meer in op de technische uitvoerbaarheid, de kosten en de risico's van de uitvoering van de pensioenregeling en de risicobeheersingsmaatregelen die getroffen worden. In het bijzonder wordt door de pensioenuitvoerder aandacht gegeven aan de datakwaliteit voor, na en tijdens de transitie naar het nieuwe pensioenstelsel, en aan de geschiktheid van het pensioenadministratiesysteem. Voor datakwaliteit en de risico's daaromtrent zijn extra waarborgen gesteld in de Wtp. Aanvullend is er ook het «Kader Datakwaliteit» van de Pensioenfederatie dat tot doel heeft te faciliteren dat pensioenuitvoerders die wensen in te varen op een consistente en aantoonbare wijze de datakwaliteit onderbouwen en borgen.[6] Deze wettelijke kaders dragen bij aan het zo klein mogelijk houden van de risico's op het gebied van IT-veiligheid en datakwaliteit.
Er zijn naar mijn weten geen signalen bekend dat IT-systemen van pensioenuitvoerders niet tijdig gereed zullen zijn om de transitie naar het nieuwe pensioenstelsel te maken.

---

[3] Verordening (EU) 2022/2554 betreffende digitale operationele weerbaarheid voor de financiële sector
[4] Kamerstukken II, 2023–2024, 30 821 en 26 643 nr. 203
[5] Kamerstukken II, 2023–2024, 32 013 nr. 207
[6] Kader datakwaliteit (pensioenfederatie.nl)