DeNederlandscheBank
EUROSYSTEEM

Uitsluitend per email

Aan: bestuur / directie

De Nederlandsche Bank N.V.
Toezicht Pensioenfondsen
Expertisecentrum Operationele & IT-risico's

Postbus 98
1000 AB Amsterdam
+31 20 524 91 11
www.dnb.nl

Handelsregister 3300 3396
BTW: NL003569056B01

Onderwerp
Benchmarkbrief informatiebeveiliging 2022

Geacht(e) bestuur, directie,

Ter informatie ontvangt u de benchmarkrapportage informatiebeveiliging 2022.

DNB voert structureel onderzoeken uit op het gebied van informatiebeveiliging (IB) en cybersecurity. Eén van de onderzoeken die DNB uitvoert betreft het IB fundament onderzoek. Betrokken instellingen ontvangen na afronding van de onderzoeksperiode een benchmarkrapportage, waarin de resultaten zijn vergeleken met het sectorbeeld.

Uw instelling was in 2022 niet betrokken bij een IB-fundament onderzoek. Ter informatie deelt DNB dit jaar een algemene versie van de benchmarkrapportage 2022 om uw instelling in staat te stellen om benchmarks en analyses ook op uw instelling te betrekken. Tenzij anders is aangegeven hebben de benchmarks betrekking op (zelfadministrerende) **pensioenfondsen, PUO's en PPI's** (kortweg: pensioensector).

De benchmarkrapportage kent de volgende onderdelen:

1. **Benchmark volwassenheid van IB-beheersmaatregelen** in uw sector naar aanleiding van IB-fundament onderzoeken.
2. **Analyse van indicatoren** voor informatiebeveiligingsrisico's in uw sector in 2022.
3. **DNB Toezichtsactiviteiten 2023** in uw sector in 2023.
4. Het nieuwsbericht **"DNB ziet cyberdreiging toenemen terwijl basismaatregelen niet altijd op orde zijn"**

Datum
18 april 2023

Uw kenmerk

Ons kenmerk
T039-2108800697-719

Behandeld door
EC-OPIT

Telefoonnummer

Mailadres
info@dnb.nl

DeNederlandscheBank
EUROSYSTEEM

Vervolgacties
Op basis van deze brief verwacht DNB geen vervolgacties van u. We verzoeken u deze benchmarkrapportage te bespreken met uw Bestuur en/of Directie en een kopie van deze brief te delen met uw interne toezichthouders.

Neem bij vragen of suggesties contact op met ondergetekende.

Hoogachtend,
De Nederlandsche Bank N.V.

ing. J. Jacobs RE CRISC
Afdelingshoofd Expertisecentrum Operationele- en IT-risico's

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

DeNederlandscheBank
EUROSYSTEEM

1. Benchmark volwassenheid van IB-beheersmaatregelen

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

Inleiding
In deze benchmarkrapportage treft u het sectorgemiddelde aan voor de volwassenheidsniveaus van de beheersmaatregelen op het gebied van Informatiebeveiliging (IB) en Cybersecurity.

DNB voert elk jaar onderzoeken uit bij een selectie van instellingen om vast te stellen op welk volwassenheidsniveau informatiebeveiliging bij die instellingen wordt beheerst: de 'IB-fundament onderzoeken'. Voor IB-fundament onderzoeken selecteert DNB een aantal instellingen dat niet eerder is onderzocht (0-metingen) en een aantal instellingen voor vervolgmetingen.

Aanpak onderzoek
Het DNB toezicht op informatiebeveiliging is 'principle based'. Hierbij houdt DNB rekening met de aard, omvang en complexiteit van de instelling. In deze onderzoeken wordt de instellingen gevraagd een self-assessment uit te voeren ten aanzien van de beheersing van het cyber-risico. Onderdeel van de beoordeling uitgevoerd door DNB is een documentatiereview van het door de instelling opgeleverde dossier om de volwassenheidsniveaus te onderbouwen, alsmede waarnemingen ter plaatse bij de instelling (op basis van interviews en deelwaarnemingen). Ook wordt de onafhankelijke opinie van een onafhankelijke functionaris (een sleutelfunctiehouder internal audit of externe audit opinie van een IT-auditor) betrokken bij deze beoordeling. Indien de instelling onvoldoende heeft kunnen onderbouwen dat het IB-risico adequaat wordt beheerst, wordt gevraagd een verbeterplan op te stellen en wordt door DNB een mitigatietraject gestart.

In de Good Practice informatiebeveiliging[1] reikt DNB handvatten aan ten aanzien van de inrichting van informatiebeveiliging om daarmee aantoonbaar 'in control' te zijn. Onderdeel van de beheersing van IB-risico's is het op voldoende volwassenheidsniveau hebben van alle (58) in de Good Practice opgenomen beheersmaatregelen[2].

Tenzij anders is aangegeven, zijn de overzichten en data in deze benchmarkrapportage gebaseerd op de door DNB verwerkte volwassenheidsniveaus bij instellingen uit de IB-fundament onderzoeken in de drie jaars periode 2020-2022. Dit betreffen de definitief vastgestelde volwassenheidsniveaus na onderzoek door DNB.

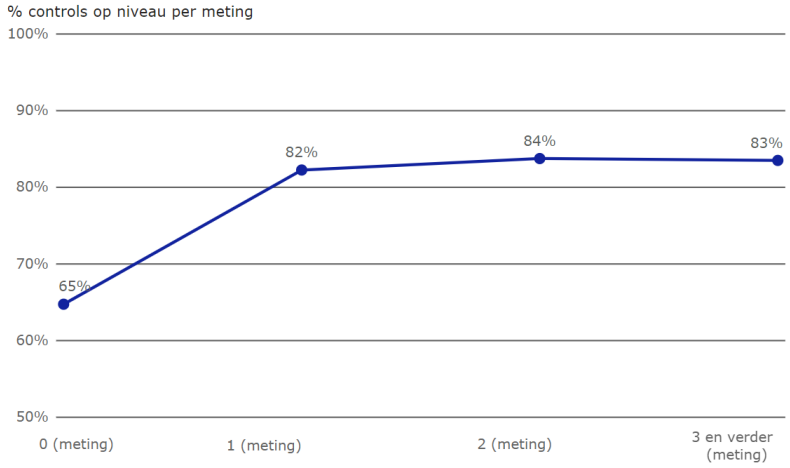
Benchmarkresultaten van de pensioensector
In onderstaand *figuur 1* ziet u het percentage van beheersmaatregelen dat zich op of boven het in de Good Practice opgenomen volwassenheidsniveau bevond bij de 0-, 1-, 2-, 3- (en verder) metingen in uw sector. Dit betreft het sectorgemiddelde.

[1] Zie Good Practice Informatiebeveiliging
[2] Zie Q&A Informatiebeveiliging (dnb.nl)

DeNederlandscheBank
EUROSYSTEEM

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

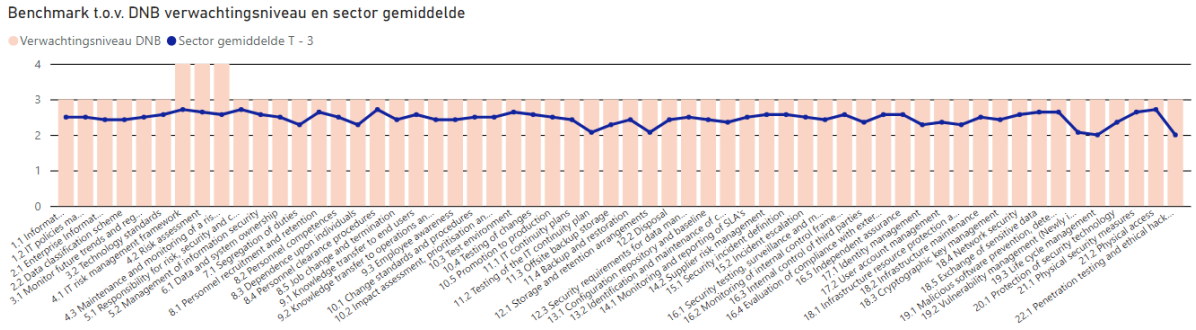


Figuur 1- gemiddeld percentage beheersingsmaatregelen op niveau voor uw sector

Toelichting figuur 1:

- Lijn: het gemiddelde percentage van de beheersingsmaatregelen dat zich per meting op het verwachte volwassenheidsniveau bevond in uw sector.
- Metingen: uitkomsten van IB-fundament onderzoeken bij instellingen vanaf 2010 (0-meting is het initiële onderzoek).
- Waarneming: na de 0-meting verbeteren instellingen zich op de IB-controls. Tegelijkertijd blijkt uit de vervolgmetingen dat instellingen op deelgebieden nog in volwassenheid kunnen groeien.

In onderstaande *figuur 2* ziet u het gemiddelde in uw sector van de volwassenheidsniveaus van alle 58 beheersingsmaatregelen over de laatste drie jaar (T-3), 2020-2022 (blauwe lijn).



Figuur 2 – totaaloverzicht van alle 58 beheersingsmaatregelen van uw sector

Toelichting figuur 2:

- Lijn: het gemiddelde van de gerapporteerde volwassenheidsniveaus binnen uw sector, over de afgelopen drie jaren (T-3).
- De roze staven: het door DNB verwachte volwassenheidsniveau.
- Waarneming: uit de figuur blijkt dat veel van de controls gemiddeld niet voldoende aantoonbaar volwassen zijn.

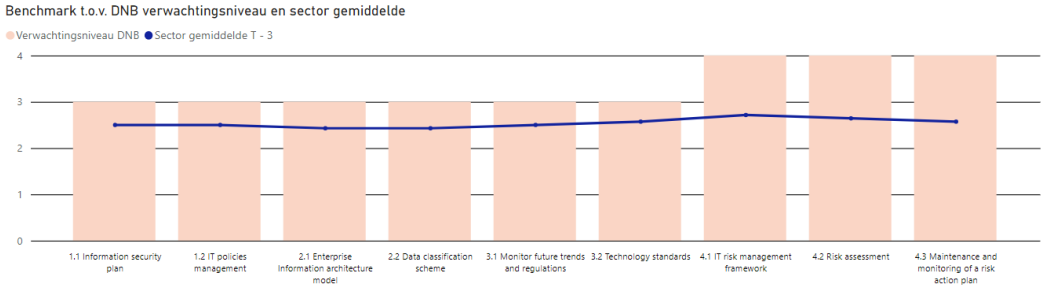
DeNederlandscheBank
EUROSYSTEEM

Voor de leesbaarheid zijn de 58 beheersingsmaatregelen hierna gecategoriseerd naar aandachtsgebied[3], te weten:

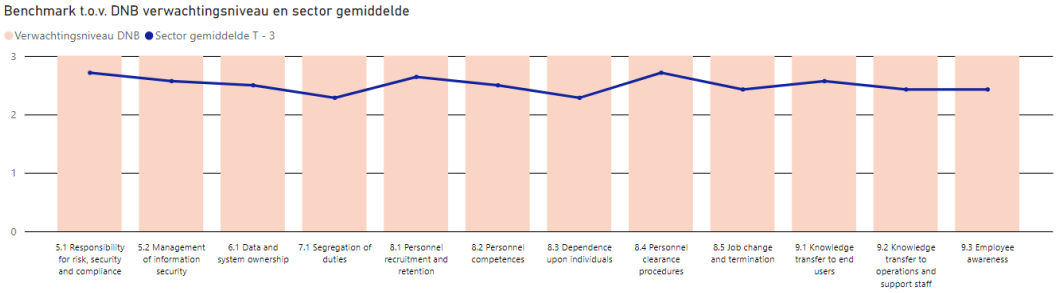
- Governance and Risk management (*figuur 3*);
- Organisation & People (*figuur 4*);
- Processes and Outsourcing (*figuur 5*);
- Technology, Facilities & Testing (*figuur 6*).

Datum
18 april 2023

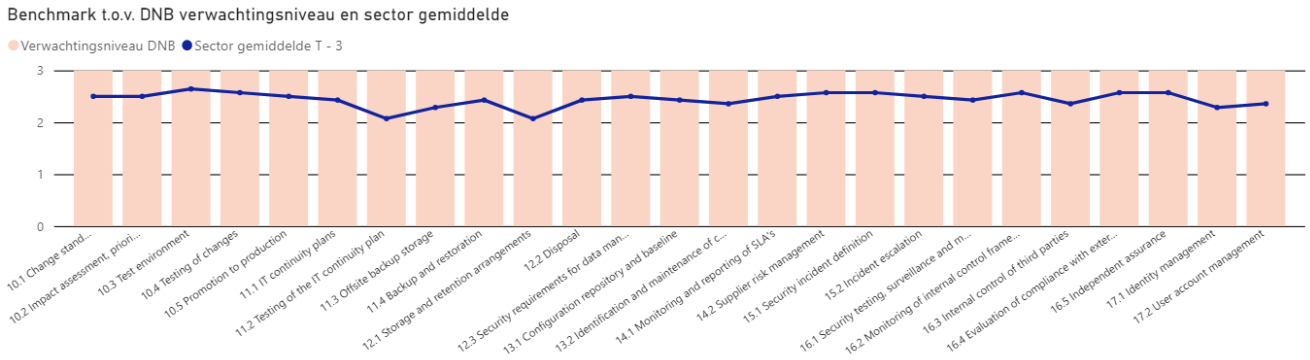
Ons kenmerk
T039-2108800697-719



Figuur 3 – Governance and Risk management

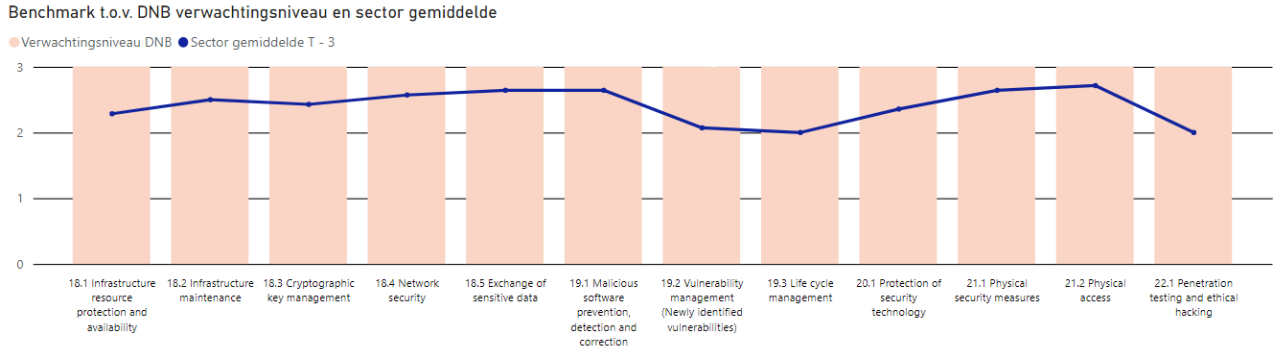


Figuur 4 – Organisation and people



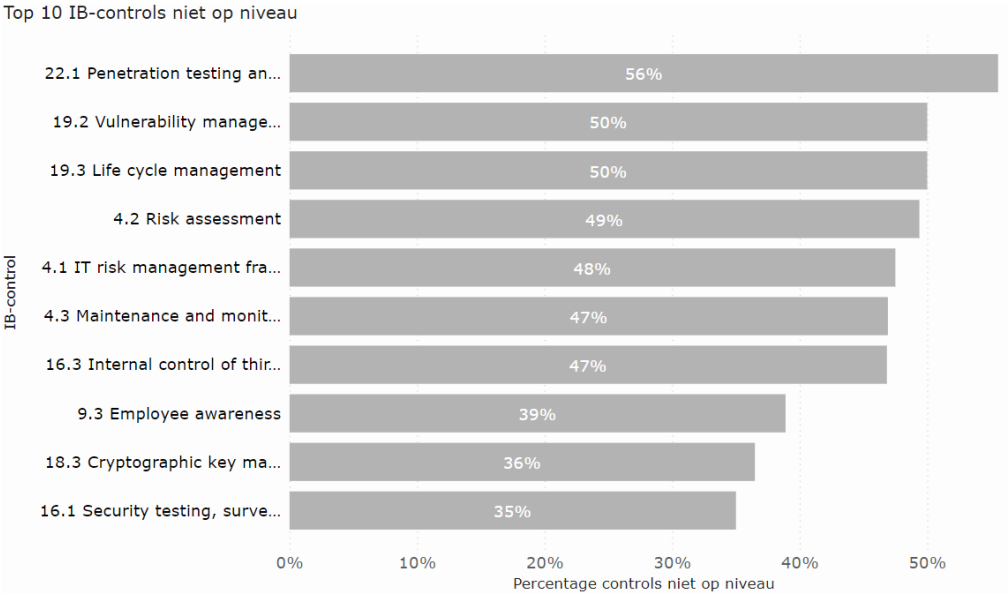
Figuur 5 – Processes and Outsourcing

[3] De aandachtsgebieden volgen uit de Good Practice Informatiebeveiliging DNB 2019-2020.



Figuur 6 – Technology, Facilities & Testing

In *figuur 7* ziet u de top 10 IB-controls (grijze staven) binnen uw sector die niet op het verwachte volwassenheidsniveau zijn.



Figuur 7 – Top 10 controls niet op niveau

Waarneming: In de pensioensector zijn de maatregelen die zien op (#22.1) Penetration testing and ethical hacking met 56% het vaakst niet aantoonbaar op het door DNB verwachte volwassenheidsniveau gebracht.

DeNederlandscheBank
EUROSYSTEEM

2. Analyse van indicatoren

Op basis van eigen onderzoeken bij instellingen en de jaarlijkse uitvraag gericht op informatiebeveiliging (de SBA-IB) verkrijgt DNB inzicht in de kwaliteit van specifieke informatiebeveiligingsprocessen en bijbehorende indicatoren bij instellingen. Hieronder delen wij een aantal inzichten gericht op de pensioensector.

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

De informatie is gegroepeerd naar inzichten op het gebied van:

1. IT-beveiliging
2. IT-beschikbaarheid en continuïteit
3. IT-uitbesteding

Waar relevant is deze aanvullende informatie verder onderverdeeld naar de drie prudentiële impactklassen[4] binnen uw sector. De impactklasse geeft een indicatie van de mate van toezicht door DNB op dit type instellingen. De impactklassen en de mate van toezicht zijn:

- Impactklasse 1 – Adaptief toezicht
- Impactklasse 2 – Actief toezicht
- Impactklasse 3 – Proactief toezicht

2.1 IT-beveiliging

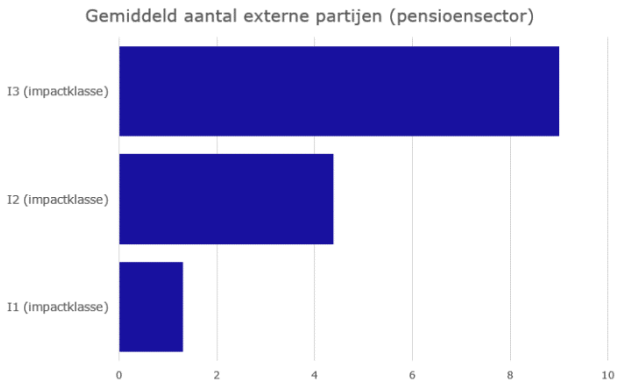
Waarneming: 5% van de Nederlandse verzekeraars, pensioenfondsen, PUO's en PPI's hebben het in 2022 te maken gehad met ongeautoriseerde toegang tot interne IT-systemen en gegevens door een kwaadwillende. Dit beeld is nagenoeg gelijk aan 2021.

Hieronder delen wij aanvullende informatie op het gebied van IT-beveiliging.

2.1.1 Hoeveelheid externe partijen met toegang tot uw systemen of gegevens

Toelichting: Dit figuur geeft het gemiddeld aantal externe partijen dat toegang heeft tot systemen. Hierbij valt te denken aan het aantal dienstverleners dat toegang heeft tot uw interne systemen of gegevens via IT-middelen die niet onder beheer van uw instelling vallen. De data betreffen gemiddelden, verdeeld naar impactklasse van de instellingen.

Waarneming: de I3 instellingen in de pensioensector hebben te maken met het beheersen van toegang van gemiddeld 9 externe partijen.



Figuur 8 – Gemiddeld aantal externe partijen met toegang tot uw systemen / gegevens

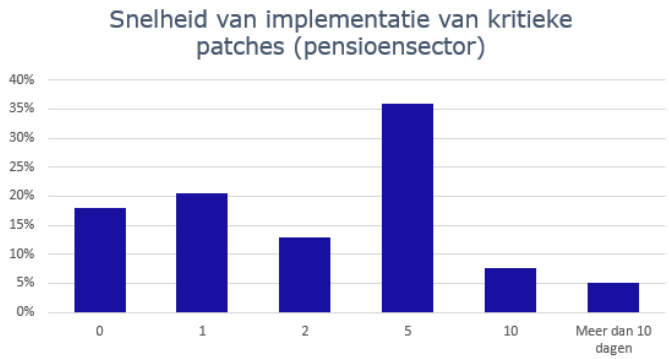
[4] De indeling in de prudentiële impactklasse hangt onder meer af van de omvang van de activiteiten, de nationale systeemrelevantie van een instelling en de maatschappelijke functie van de activiteiten. Zie voor verdere informatie over de impactklassen en toezichtaanpak van DNB de brochure: ATM - de vernieuwde toezichtaanpak

DeNederlandscheBank
EUROSYSTEEM

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

2.1.2 Snelheid van implementatie van patches



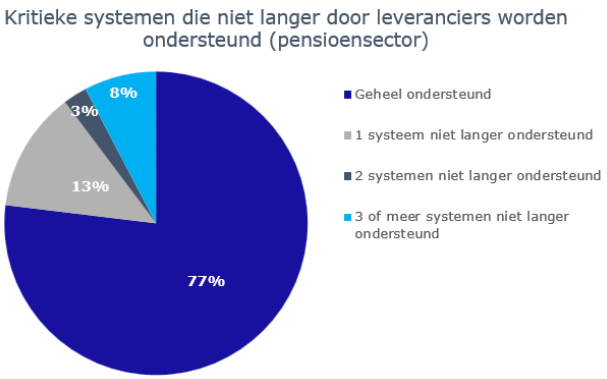
Figuur 9 – snelheid van implementatie van kritieke patches (in dagen)

- Toelichting: In figuur 9 is de gemiddelde snelheid van patchen getoond voor instellingen in uw sector. De snelheid van implementatie van kritieke patches is een belangrijke indicator om te bepalen hoelang een instelling blootgesteld is aan reeds bekende kwetsbaarheid in het systeemlandschap.
- Waarneming: Bijna 5% van de instellingen geeft aan dat de gemiddelde snelheid van kritieke patches langer is dan 10 dagen. Naar mate kwetsbaarheden gedurende langere tijd open staan neemt het risico toe dat hackers deze kwetsbaarheden vinden en daarvan misbruik maken. Het niet snel doorvoeren van kritieke patches maakt IT-systemen langer kwetsbaar voor aanvallers.

2.1.3 Kritieke systemen niet langer door leveranciers ondersteund

Toelichting: Instellingen hebben te maken met kritieke IT-systemen die niet langer door leveranciers worden voorzien van beveiligingsupdates. Bijgaand overzicht maakt inzichtelijk in hoeverre instellingen hiermee te maken hebben. Het niet langer updaten van IT-systemen kan leiden tot een verhoogd beveiligingsrisico.

Waarneming: 23% van de instellingen in de pensioensector heeft te maken met kritieke systemen die niet langer worden ondersteund met beveiligingsupdates door de leveranciers.



Figuur 10 – kritieke systemen niet langer ondersteund door leveranciers

DeNederlandscheBank
EUROSYSTEEM

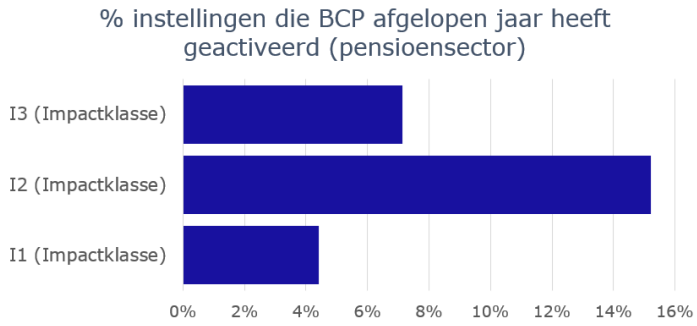
Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

2.2 IT-beschikbaarheid en continuïteit

Beschikbaarheid en continuïteit van de IT-systemen is van groot belang voor de bedrijfsvoering van de instellingen. Hieronder geven wij inzicht in een aantal waarnemingen op dit vlak.

2.2.1 Activering van BCP of IT continuity in de afgelopen 12 maanden

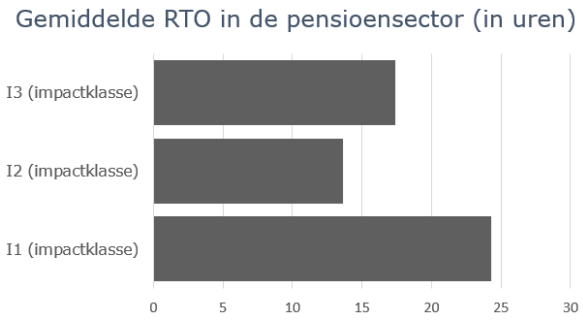


Figuur 11 – % instellingen die BCP afgelopen jaar heeft geactiveerd

- Toelichting: dit overzicht maakt inzichtelijk of instellingen in het afgelopen jaar een Business Continuity Plan (BCP) heeft geactiveerd als gevolg van een operationele verstoring.
- Waarneming: ongeveer 15% van de I2 instellingen hebben hun BCP geactiveerd in periode van onderzoek.

2.2.2 De RTO van meest kritieke bedrijfsprocessen

Toelichting: De volgende figuur geeft inzicht in door de instelling bepaalde Recovery Time Objective (RTO) verdeeld naar I-klassen. De RTO is de tijd waarbinnen de instelling streeft om te herstellen na een ernstige verstoring, bijvoorbeeld een cyberaanval.



Figuur 12 – Gemiddelde RTO van de meest kritieke bedrijfsprocessen

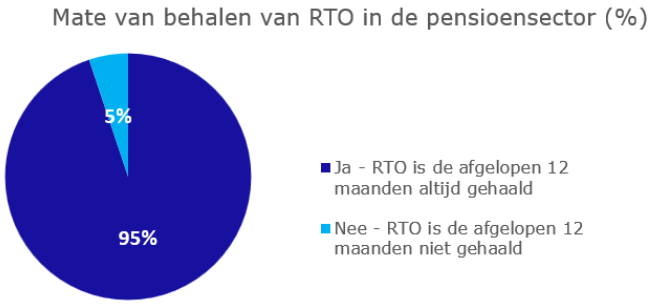
Waarneming: In de pensioensector hanteren de I2-instellingen de laagste RTO met gemiddeld bijna 14 uur.

DeNederlandscheBank
EUROSYSTEEM

2.2.3 In hoeverre heeft u de RTO gehaald voor uw kritieke bedrijfsprocessen?

Toelichting: voor instellingen is het voor haar dienstverlening van belang om de vastgestelde RTO's te behalen. De mate waarin instellingen hun RTO hebben gehaald is zichtbaar in dit figuur.

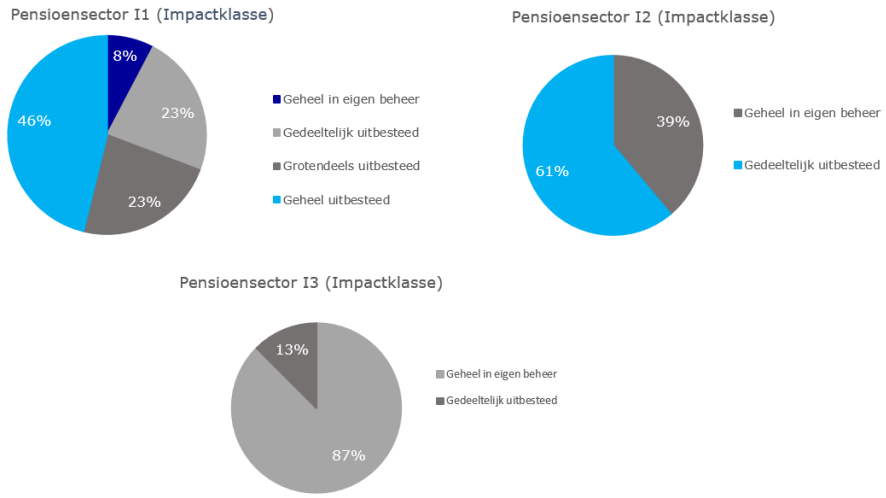
Waarneming: 5% van de instellingen in de pensioensector heeft te maken gehad met incidenten of verstoringen in de bedrijfsvoering die langer duurden dan wat de instelling zelf acceptabel vindt.



Figuur 13 – Mate waarin RTO is behaald door instelling

2.3 IT-uitbesteding

Toelichting: Onderstaande figuren geven inzicht in de mate van afhankelijkheid van de instelling van kritieke uitbestede IT-diensten verdeeld naar impactklassen in uw sector.



Figuur 14 – mate van IT-uitbesteding

Waarneming: In de pensioensector kennen de I1 instellingen de hoogste mate van gehele uitbesteding van hun IT (46%). Van de I2 instellingen hebben 39% kritieke of belangrijke IT-processen geheel in eigen beheer. I3 instellingen besteden hun kritieke of belangrijke IT-processen niet geheel uit.

DeNederlandscheBank
EUROSYSTEEM

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

3. DNB Toezichtsactiviteiten 2023

Het beheersen van risico's op het gebied van informatiebeveiliging, uitbesteding en cybersecurity blijft onverminderd belangrijk voor een beheerste en integere bedrijfsvoering door financiële instellingen. DNB ziet er ook in 2023 op toe dat instellingen hun cyberweerbaarheid op orde hebben en houden. Dit doen wij door het uitvoeren van IB-fundament onderzoeken, gesprekken met instellingen en sectorbrede data-uitvragen op het gebied van informatiebeveiliging met de SBA-IB van 2023.

Ook hebben we aandacht voor de beheersing van de uitbestedingsrisico's en de voorbereidingen op de implementatie van de nieuwe wet- en regelgeving op dit gebied, in het bijzonder de Digital Operational Resilience Act (DORA). Hierbij doet DNB een selectie van pensioenfondsen en verzekeraars onderzoek in de vorm van uitvragen en gerichte onderzoeken op locatie. Daarnaast verwacht DNB aandacht te besteden aan de ontwikkelingen op het gebied van Quantum-computing en de invloed hiervan op huidige en toekomstige systemen.

4. Nieuwsbericht: “DNB ziet cyberdreiging toenemen terwijl basismaatregelen niet altijd op orde zijn”

(30 november 2022, DNB nieuwsbericht, *sectoren: pensioenfondsen, premiepensioeninstellingen en verzekeraars*)

Cyberrisico’s zijn reëel. DNB ziet dat cyberdreigingen in de maatschappij toenemen. Dat geldt ook voor de instellingen onder ons toezicht. Voortdurende aandacht voor dreigings- en risicoanalyse blijft daarom voor instellingen belangrijk om hun basismaatregelen, het fundament, op niveau te houden. Dit wordt bevestigd in de door DNB uitgevoerde onderzoeken in 2022.

Op basis van eigen onderzoeken bij instellingen en de jaarlijkse uitvraag gericht op informatiebeveiliging (de SBA-IB) verkrijgt DNB inzicht in dit fundament bij verzekeraars, pensioenfondsen, PUO’s en PPI’s. Hieruit blijkt dat niet alle basismaatregelen bij instellingen effectief zijn ingericht en functioneren. Basismaatregelen die aandacht vragen zijn:

- Actieve monitoring op cyberrisico’s binnen de IT-omgeving;
- Noodzakelijk onderhoud op de beveiliging van IT-systemen; waarin de uitbestedingsketen betrokken wordt;
- Testen van en oefenen met een cyberaanval.

In 2021 heeft DNB een IB-monitor uitgebracht waarin aandacht is besteed aan de belangrijke rol van bestuur voor het op orde krijgen en houden van informatiebeveiliging- en cyberrisico’s. Actieve bestuurlijke betrokkenheid en een toereikend kennisniveau over dit onderwerp is ook dit jaar onderwerp in onze onderzoeken. Het belang van kennis en aandacht op het gebied van informatiebeveiliging en cyberrisico’s wordt aan veel bestuurstafels onderschreven. Bestuurlijke verankering van dit onderwerp en het op orde brengen en houden van kennis bij bestuurders en intern toezicht behoeft nadrukkelijke aandacht.

DeNederlandscheBank
EUROSYSTEEM

Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

Hieronder volgt een toelichting op deze waarnemingen en de bestuurlijke aandacht die instellingen hebben ten aanzien van cyberrisico's. Dit artikel sluit af met een vooruitblik op toezicht door DNB op informatiebeveiliging en cyberrisico's in 2023.

Monitor actief op cyberrisico's binnen de huidige IT-omgeving
Opnieuw heeft 5% van de Nederlandse verzekeraars, pensioenfondsen, PUO's en PPI's het afgelopen jaar te maken gehad met ongeautoriseerde toegang tot interne IT-systemen en gegevens door een kwaadwillende. Dit beeld is gelijk aan 2021. De sector geeft aan dat deze trend blijvend is en geslaagde aanvallen zelfs kunnen toenemen. Daarom is het van belang dat instellingen, naast het op orde houden van preventieve basismaatregelen, zich ook richten op de situatie wanneer een kwaadwillende daadwerkelijk ongeautoriseerd toegang heeft gekregen. Uit ons onderzoek blijkt dat meer dan een kwart van de instellingen minder goed in staat is om logging te verzamelen en te analyseren en daarmee mogelijke inbreuken daadwerkelijk te detecteren en/of de impact van een inbreuk te achterhalen.

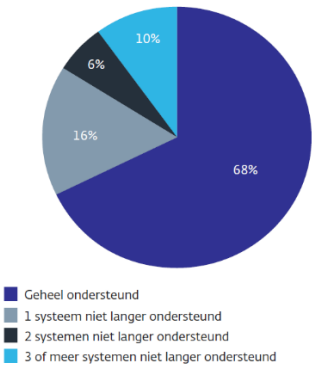
Onderhoud van systemen blijft een belangrijk aandachtspunt
Uit ons onderzoek blijkt dat de volgende aspecten belangrijk zijn om de basismaatregelen op orde te houden:

- Inzicht in de staat van onderhoud van kritieke IT-systemen;
- Snel kunnen patchen is zeer belangrijk;
- Het betrekken van de gehele uitbestedingsketen in de risicoanalyse.

Deze drie aspecten zijn hieronder verder toegelicht.

<u>Inzicht in de staat van onderhoud van kritieke IT-systemen</u>
DNB ziet dat 32% van de instellingen gebruik maken van één of meer kritieke IT-systemen die niet langer door leveranciers worden voorzien van beveiligingsupdates. In 2021 was dit percentage hoger, namelijk 42%. Een voorzichtige conclusie is dat instellingen aandacht hebben voor deze verouderde systemen en deze bijvoorbeeld uitfaseren.

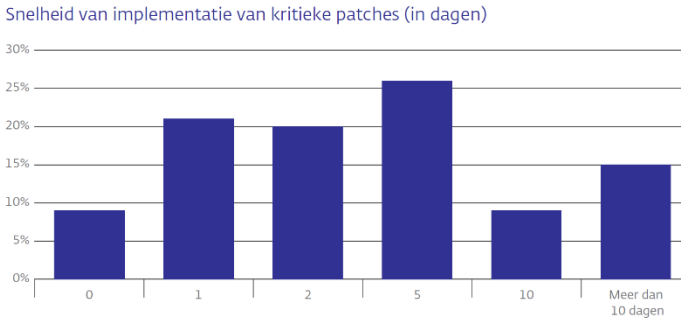
Instellingen waarvan systemen niet langer door leveranciers worden onderhouden



DNB ziet dat instellingen meer aandacht hebben voor het vernieuwen van het applicatielandschap. Binnen de pensioensector is dit vooral gedreven door het kunnen administreren van de nieuwe pensioenregeling. Dit heeft een positief effect op het uitfaseren van systemen die niet langer (door de leverancier) zijn onderhouden.

<u>Snel kunnen patchen is zeer belangrijk</u>
Instellingen hebben al naar gelang hun omvang en complexiteit van IT-systemen te maken met vele honderden zo niet duizenden (kritieke) security-patches op jaarbasis. Uit onderzoek blijkt dat kritieke security-patches de afgelopen jaren sneller worden doorgevoerd. Deze patches zijn na het uitbrengen door de leveranciers gemiddeld binnen 7 werkdagen geïmplementeerd in de productiesystemen. In de onderstaande figuur wordt de gemiddelde snelheid van patchen door instellingen getoond.

DeNederlandscheBank
EUROSYSTEEM



Datum
18 april 2023

Ons kenmerk
T039-2108800697-719

Bijna 20% van de instellingen geeft aan dat één of meer kritieke patches langer dan 30 dagen heeft openstaan. Het niet snel doorvoeren van kritieke patches maakt IT-systemen langer kwetsbaar voor aanvallers. Uit onderzoek blijkt dat het merendeel van geslaagde aanvallen te relateren is aan misbruik van reeds bekende zwakheden in IT-systemen waarvoor al een security patch beschikbaar is.

Inzicht in de uitbestedingsketen
Systemen die niet zijn voorzien van de laatste beveiligingsupdates zijn een mogelijke 'ingang' voor aanvallers. In het geval dat die systemen zijn uitbesteed kan dat ook gebeuren via leveranciers.

Uit ons onderzoek blijkt dat ruim een derde van de instellingen geen inzicht heeft in de uitbestedingsketen. Daarmee ontbreekt een goed beeld van de staat van onderhoud van kritieke systemen in de keten. Deze instellingen zijn sterk afhankelijk van maatregelen in de gehele uitbestedingsketen, zoals end-to-end monitoring en de mogelijkheid tot isolatie van delen van systemen.

DNB benadrukt het belang dat instellingen zicht hebben op de gehele uitbestedingsketen en dat ketenpartners worden betrokken in het uitvoeren van testen en sturen op het aantoonbaar op orde houden van basismaatregelen bij alle kritieke dienstverleners.

Test van cyberweerbaarheid
Instellingen hechten veel belang aan het uitvoeren van goede beveiligingstesten om daarmee op zoek te gaan naar zwakheden in de beveiliging en deze te verbeteren. Ook zijn continuïteitstesten belangrijk om weerbaar te zijn.

Uitvoeren continuïteitstesten
Uit ons onderzoek blijkt dat instellingen diverse maatregelen treffen om zich voor te bereiden op mogelijke cyberaanvallen die verstorend kunnen zijn voor hun operationele bedrijfsvoering. Een van de maatregelen is het houden van een continuïteitstest. In het algemeen wordt het uitvoeren van een jaarlijkse test door de sector als minimum frequentie gezien.

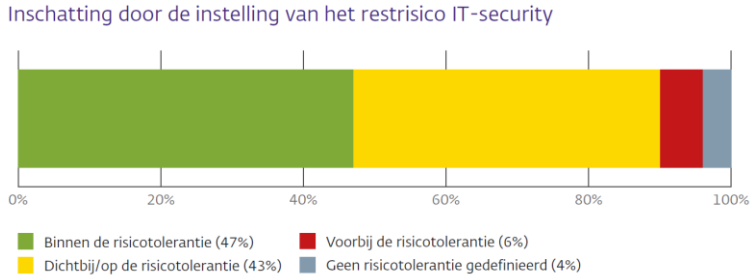
Het afgelopen jaar heeft ruim een kwart van de instellingen geen continuïteitstest uitgevoerd. Dit percentage lijkt daarmee opvallend hoog. Een aantal instellingen heeft aangegeven deze testen te hebben uitgesteld. Reden hiervoor was dat de geplande (jaarlijkse) testen samenvielen met de oorlog in Oekraïne, waardoor het dreigingsniveau veranderde en een bestuurlijke afweging is gemaakt de test niet op dat moment uit te voeren.

De keuze voor de timing van een continuïteitstest ligt bij de instelling. Het belang van deze testen is groot; het betrekken van diverse relevante scenario's helpen bij het opsporen van mogelijke tekortkomingen. Een veelgebruikt scenario is het simuleren van een ransomware aanval en de wijze waarop de instelling hierop anticipeert en herstelt.

Maximale hersteltijd bedrijfsprocessen
Eén van de indicatoren die DNB uitvraagt is de door de instelling gestelde maximale hersteltijd van primaire bedrijfsprocessen na calamiteiten, zoals een cyberaanval: de Recovery Time Objective (RTO).

De gemiddelde RTO ligt gemiddeld tussen 15 en 20 uur. Overigens verschilt de RTO sterk per instelling en per bedrijfsproces. DNB ziet dat 10% van de instellingen aangeeft de interne RTO's niet te hebben gehaald in het afgelopen jaar. Deze instellingen hebben te maken gehad met incidenten of verstoringen in de bedrijfsvoering die langer duurden dan wat de instelling zelf acceptabel vindt.

Bestuurlijke aandacht voor cyberrisico's
DNB heeft instellingen gevraagd hoe zij het cyberrisico inschatten (restrisico) en in hoeverre dat past binnen de eigen risicotolerantie. De helft van de instellingen (49%) signaleert belangrijke IT-security risico's in hun bedrijfsvoering.



Uit bovenstaande figuur blijkt dat bijna de helft (48%) van de instellingen zich bevinden binnen hun risicotolerantie. 43% van de instellingen signaleert dat ze op of dichtbij haar risicotolerantie zit en 6% zit daarboven. Ongeveer 4% van de instellingen heeft geen risicotolerantie vastgesteld. Wel ziet DNB een positieve ontwikkeling dat IT-security risico's worden gemeten ten opzichte van tolerantiegrenzen en steeds meer onderdeel uitmaken van (operationele) managementinformatie. Het beheersbaar houden van deze risico's krijgt zo de voortdurende en nodige bestuurlijke aandacht, gezien deze zich dichtbij de vastgestelde risicotolerantie bevinden.