#3

SEPTEMBER 2021

P&P

pensioen & praktijk

Alle facetten van een duurzaam pensioen

Pensioenfondsen echt in control als het gaat om cyberrisico's?

De levensloopregeling – een opera in drie akten

Overcompensatie door de brutoprofijtmethode

Risicobeheer en de praktijk

De VTE-normering als maatstaf voor voldoende beschikbare tijd

Is de verkrijger gebonden aan op de Wet Bpf 2000 gebaseerd pensioen?

Wat pensioenfondsen moeten weten over de energietransitie

VAKMEDIANET

Over de auteurs

Drs. Elroy Coltof AAG is sinds 2014 werkzaam bij Vermaase Insurance Automation. Voorheen heeft hij onder meer gewerkt bij PWC. Bij Vermaase is hij verantwoordelijk voor de actuariële berekeningen die ten grondslag liggen aan de pensioensoftware ontwikkeld voor diverse Pensioenverzekeraars en Pensioennavigator BV.

Mr. Drs. Corey Dekkers MFP FFP CFP® is senior pensioenjurist op de afdeling fiscaal- en juridische zaken bij Pensioennavigator BV.

Mr. Jim Kaldenberg CPL is pensioenadvocaat bij Delissen Martens advocaten in Den Haag. Zijn artikel gaat over de vraag of een verkrijger na overgang van onderneming gebonden is aan op de Wet Bpf 2000 gebaseerd pensioen. Zeker in verband met due diligence, waarmee Jim met regelmaat te maken heeft, een belangrijke en actuele vraag.

Mr. Paul de Koning is partner bij TriVu. Daarvoor heeft hij diverse functies in de pensioenbranche vervuld. Hij heeft met name veel ervaring en expertise op het gebied van pensioenrecht, governance, (niet-financieel) risicomanagement en compliance.

Mr. Onno de Lange RPB is secretaris van Stichting IVP – Instituut voor Pensioeneducatie. Deze stichting is opgericht in 2012 om een kwaliteitsimpuls te geven aan de pensioensector via onder andere opleidingen, boeken en evenementen.

Scott Martens RPA CFE is Registerpensioenadviseur, gecertificeerd fraudeonderzoeker, onafhankelijk fondsbestuurder en interim-manager bij Martens Management BV.

Mr. Ruben Stam CPL is fiscalist en pensioenjurist bij Nationale-Nederlanden Bank. Hij is tevens als vaste medewerker of redacteur verbonden aan diverse uitgaven, waaronder Pensioen & Praktijk. Verder is hij docent voor de beroepsorganisatie RB, SOB en verzorgt hij regelmatig cursussen en masterclasses over pensioen- en fiscaalrechtelijke onderwerpen. Hij schrijft het artikel 'Passende compensatie bij uitfasering van pensioen in eigen beheer' op persoonlijke titel.

Bas J.W. van Vliet MSc AAG is Director en senior actuaris bij Phenox Consultants. Met 25 jaar werkervaring is hij een allround pensioenspecialist met een pragmatische aanpak, o.a. op het gebied van pensioenadvisering aan zowel lokaal als internationaal opererende ondernemingen. Hieronder vallen strategie – let op met het nieuwe pensioenstelsel!! – en (her)ontwerp van collectieve pensioenregelingen, maar ook internationale accounting waarderingen zoals IFRS en USGAAP. Daarnaast adviseert Bas sinds jaar en dag pensioenfondsen.

Natascha Westen MSc CISO CDPO is gecertificeerd Data Protection Officer, gecertificeerd Information Security Officer (CISO) en MSc Cyber Security. Natascha is partner bij Compliance-i-Consultancy BV en heeft jarenlange ervaring als compliance- en privacy-officer bij meerdere pensioenfondsen en uitvoeringsorganisaties.

Scott Martens RPA CFE
Registerpensioenadviseur, gecertificeerd fraudeonderzoeker, onafhankelijk fondsbestuurder en interim-manager bij Martens Management BV

Natascha Westen MSc CISO CDPO
Gecertificeerd Data Protection Officer, gecertificeerd Information Security Officer (CISO) en MSc Cyber Security. Natascha is partner bij Compliance-i-Consultancy BV

Door de voortdurende technologische groei maken we voor de communicatie en dataverwerking steeds meer gebruik van één of meerdere digitale omgevingen. Hierdoor is veel data op een of andere wijze vaak gekoppeld met het internet. Organisaties zijn daardoor steeds meer afhankelijk van deze informatie- en communicatietechnologie. Dit brengt ook meer risico's met zich mee op het gebied van het verwerken en beschermen van gegevens en in het bijzonder op het gebied van cyberaanvallen. Een belangrijke vraag die bij ons opkomt is of pensioenfondsen (hierna: fondsen) en pensioenuitvoeringsorganisaties (hierna: puo's) voldoende in staat zijn om cyberaanvallen of datalekken te voorkomen.[1] Voor het gemak beschouwen we de bestuursondersteuning even als de uitvoeringsorganisaties van de fondsbesturen en de puo's als uitvoeringsorganisaties voor de pensioenadministratie.

Zijn pensioenfondsen en puo's écht *in control* als het gaat om cyberrisico's?

DE DOELEN VAN CYBERCRIMINELEN EN (INTER)NATIONALE RISICO'S

Wij werpen eerst een blik op de cybercriminelen en hun motieven. De hoofddoelen van cybercriminelen zijn veelal: het stelen van officiële valuta of cryptovaluta, het vernietigen of lamleggen van een infrastructuur, het afpersen van geld met de verkregen informatie en het uitvoeren van spionageactiviteiten bij overheden of innovatieve industrieën. Soms worden cybercriminelen ingezet om politieke of maatschappelijke invloed op burgers en/of belangorganisaties uit te oefenen.

Zo schatten de autoriteiten van Zuid-Korea in dat Noord-Korea met een leger van ongeveer 6.000 cybercriminelen dagelijks zo'n 1,5 miljoen aanvallen lanceert op Zuid-Korea om het dagelijkse leven aldaar te ontregelen. Dat geeft iets om over na te denken als we weten dat Zuid-Korea 24 kerncentrales in gebruik

1 Een datalek wordt in algemene zin omschreven als een inbreuk op de beveiliging die op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

heeft.[1] In geopolitieke zin valt een machtsverschuiving waar te nemen van 'massavernietigingswapens' (de Koude Oorlog) naar 'massaverstoringswapens' (de internationale cyberoorlog).

Omdat een cyberaanval in de meeste gevallen niet met volledige zekerheid is toe te schrijven aan één agressor, spreekt men over een zogenoemd 'attributieprobleem'. Dit maakt het indienen en innen van een schadeclaim nagenoeg onmogelijk. De vijand heeft geen officiële identiteit. Als toch een dader wordt geïdentificeerd, werpt zich een probleem op als het gaat om de bewijsvoering. Zal een claimende organisatie daarbij de digitale technieken prijsgeven, zodat zij wellicht andere (openstaande) deuren toont voor nieuwe hackers? Waarschijnlijk niet. Het bedrijf Northwave, medeoprichter van brancheorganisatie Cyberveilig Nederland, schat in dat zo'n 80 % van de bedrijven losgeld betaalt om zo van *ransomware* (gijzelsoftware) af te komen.[2] Een kosten-batenafweging die hacken profijtelijk maakt voor cybercriminelen. Criminelen die bij een nieuw soort slachtoffer (zoals fondsen en puo's) minder inventief hoeven te zijn dan bij financiële instellingen die inmiddels weten hoe ze zich moeten verweren.

Bij een hack of datalek kan toch sprake zijn van een integere bedrijfsvoering

IT-GOVERNANCE MET EEN AANSCHERPING OP CYBERRISICO'S

Alhoewel de mogelijke impact op puo's en fondsen van een andere orde is, is evident dat een platgelegde IT-structuur of data in handen van criminelen schadelijke gevolgen kan hebben. Bedrijfs- of fondsgevoelige informatie (reputatieschade) kan openbaar gemaakt worden of deelnemers (identiteitsfraude) worden slachtoffer van zogenoemde *spearfishers*. Bij deze laatste vorm wordt met gebruikmaking van zeer specifieke (vertrouwd ogende) data getracht het slachtoffer te overtuigen dat het contact legitiem is. Het datalek bij de Blue Sky Group[3] zal naar verwachting niet leiden tot een wereldcrisis, maar je hebt als organisatie veel werk aan een evaluatie van, communicatie over en het managen van mogelijke risico's. Een boete van de Autoriteit Persoonsgegevens (AP) en reputatieschade door de negatieve media-aandacht kan funest zijn voor het imago en daarmee het gestelde vertrouwen in de goede dienstverlening van een bedrijf.

Eén van de vragen die wij onszelf de laatste jaren stellen is: "Zijn bestuurders, bestuursondersteuners, fondsadviseurs en managers van puo's zichzelf wel voldoende bewust van de digitale dreigingen van buitenaf en van de mogelijke inrichtings- of handelingsfouten binnen hun organisatie?". Door in dit artikel te wijzen op de kaders van toezichthouders, te wijzen op het risicobewustzijn en enkele praktische vragen te belichten die een bestuur en de puo kan stellen, hopen we in ieder geval de betrokkenen mee te nemen in een bewustwording. Ook zal worden ingegaan op handreikingen die DNB doet voor een fonds op basis van haar richtlijn informatiebeveiliging en delen we enkele van onze observaties.

Het is ons inziens niet zo dat kwaadwillenden vaak beslag proberen te leggen op de financiële middelen van fondsen, zoals bijvoorbeeld bij banken het geval is. Maar als dat toch gebeurt, dan kan de financiële schade en de veelal bijbehorende reputatieschade groot zijn. Medewerkers van puo's, adviseurs van fondsen hebben immers toegang tot grote hoeveelheden data waar cybercriminelen steeds meer in geïnteresseerd zijn. Wij zijn van mening dat een fonds of puo met (veelal) duizenden deelnemers een potentieel doelwit kan zijn en zal worden voor cybercriminelen. De vraag is niet óf het ooit op grote schaal gebeurt, maar eerder: wannéér. Als fondsbestuur en management van een puo wil je de beheersmaatregelen op orde en op een goed volwassenheidsniveau hebben. Het voeren van een zogenoemd *vulnerability management* is één van die maatregelen. Door het inrichten van je *vulnerability management* analyseer je de zwakheden in je systemen en software die erop

1 National Geographic, Inside North Korea: The Cyber State, 2020.
2 Bron: "Ook met internetcrimineel valt te onderhandelen", Brabants Dagblad, 1 juli 2021.
3 Bron: https://www.blueskygroup.nl/nl/nieuws/blue-sky-group-getroffen-door-datalek, 10 augustus 2021.

draait. Onze verwachting is dat binnen de vereiste IT-governance de onderwerpen cyberrisico's en datalekken extra aandacht gaan vragen.

Fondsen moeten meer alert zijn op cyberrisico's

De complexiteit van deze cases wordt veroorzaakt doordat fondsen vrijwel al hun diensten, waaronder hun gehele pensioenadministratie, hebben uitbesteed. Fondsen zijn, ondanks hun verantwoordelijkheid voor deze data, sterk afhankelijk van bijvoorbeeld de puo om de data van hun deelnemers goed te beschermen.

TOEZICHTKADER VAN FONDSEN

Omdat fondsen het overgrote deel van de activiteiten uitbesteden, spelen de uitbestedingsorganisaties een cruciale rol bij het beveiligen van data. Desalniettemin blijft het bestuur van een fonds eindverantwoordelijk voor alle uitbestede processen.

Met de vernieuwde Toezichtaanpak (FOCUS!) van 2012 gaf DNB aan dat zij haar toezicht verscherpte op de toezichtcyclus. Zij benadrukte toen dat 'een integere bedrijfsvoering wordt verlangd die risico's doeltreffend beheerst en dat er integere en deskundige bestuurders aan het hoofd van de instelling staan'. De brief die fondsen ontvingen met de mededeling dat de onderwerpen cybersecurity en uitbesteding in 2021 de nodige aandacht krijgen, is niet toevallig. DNB verwacht dat blijvend wordt voldaan aan het minimaal verwachte volwassenheidsniveau voor informatiebeveiliging. Een bestuur dient volgens de opinie van DNB de (onder)uitbestedingsrisico's te beheersen en zicht te hebben op kritieke en belangrijke partijen.

Aanvullend wordt databeveiliging steeds belangrijker, mede door de Algemene Verordening Gegevensbescherming (AVG) en door de Gedragslijn Verwerking Persoonsgegevens Pensioenfondsen. Fondsen dienen jaarlijks verantwoording af te leggen over de naleving van de gedragslijn. Als verwerkingsverantwoordelijke blijft het fonds verantwoordelijk voor de uitbestede gegevensverwerkingen. In de AVG zelf wordt overigens geen definitie gegeven van een datalek maar spreekt men van 'een inbreuk in verband met persoonsgegevens'. Uitbestedingspartners zoals puo's worden hiermee indirect gedwongen om ook hun organisatie compliant te krijgen op de eisen die toezichthouders stellen.

Bij een eventuele hack of datalek voldoet een fonds, in de optiek van de wetgever, niet aan artikel 143 van de Pensioenwet. In dat artikel is bepaald dat een fonds een beheerste en integere bedrijfsvoering dient te waarborgen met name voor bedrijfsprocessen en bedrijfsrisico's. In geval van uitbesteding geldt dat ook voor de (onder)uitbestedingspartners van een fonds. In de AVG zijn immers niet alleen verplichtingen opgenomen voor de verwerkingsverantwoordelijke (het fonds) maar ook voor de verwerker.

VERHOGEN VAN RISICOBEWUSTZIJN FONDBESTUURDERS

Een goede beveiliging tegen cyberaanvallen is essentieel. Het bestuur moet echter kunnen aantonen dat het zoveel als mogelijk *in control* is en dat het ook toezicht houdt op de uitvoerder. Van belang is dat bestuurders van fondsen weten wat mogelijke risico's zijn en hoe deze risico's gemitigeerd worden door de puo.

Op dit moment is een veelvoorkomend probleem dat fondsbestuurders onvoldoende weten hoe bijvoorbeeld puo's met deze risico's omgaan. Enerzijds omdat er bij de bestuurders onvoldoende kennis en *knowhow* aanwezig is, anderzijds omdat de puo deze informatie onvoldoende deelt of wil delen. De reden hiervan kan zijn dat de puo's niet willen dat informatie over kwetsbaarheden met betrekking tot hun IT-structuur in handen van kwaadwillenden of concurrenten terechtkomt.

DNB verwacht van fondsbestuurders dat ze weerstand bieden aan cyberrisico's, ondanks het feit dat de meeste besturen niet op deze rol zijn voorbereid. Een belangrijk streven van een fonds is dus om voldoende kennis te hebben van IT-risico's. Indien bestuurders van fondsen te weinig kennis hebben van IT, is het lastig om kritische vragen te stellen of rapportages adequaat te beoordelen, om zo grip te krijgen op cybersecurity. Fondsen kunnen daardoor moeilijk aantonen dat ze controle hebben over cyberrisico's en deze houden in de toekomst. Sterk ontwikkelende technologieën maken dat extra lastig.

Ook beschouwen organisaties (en daarmee hun bestuurders) beveiliging als een ongewenste kostenpost. Inmiddels investeren Amerikaanse bedrijven 41 % meer in beveiliging dan Europese ondernemingen.[1] Het nadrukkelijk beleggen van taken en verantwoordelijkheden binnen het bestuur op het specifieke IT-beveiliging domein kan een belangrijke eerste stap zijn. Veel private ondernemingen die met data- en gegevensbescherming werken, hebben een *chief information officer* aangesteld of op zijn minst een *security officer*. Het toebedelen van een soortgelijke rol aan een fondsbestuurder zou een goede tweede stap kunnen zijn.

Gijzelsoftware kan het pensioenfonds lam maken

CONCRETE RISICO'S BIJ DOCUMENTGEBRUIK

Een ander – meer concreet – punt als het gaat om het risicobewustzijn van bestuurders, is de zogenoemde 'persoonlijke hygiëne' omtrent IT-beveiliging. Deze is volgens ons erg laag. Veel bestuurders, bestuursondersteuners of adviseurs werken voor meerdere fondsen en hebben daarbij hun bestuursdocumenten en mailcorrespondentie op één of meerdere devices staan. Denk aan een laptop, desktop, smartphone en/of tablet. Deze devices zijn niet altijd optimaal beschermd met een goed wachtwoord of worden niet altijd exclusief door alleen de betrokkene gebruikt. Soms worden devices gebruikt op een open wifi-kanaal. Daarnaast valt ons op dat veel toeleveranciers van documentportalen voor fondsen geen tweetrapsauthenticatie hanteren en dat uitbestedingspartijen niet altijd e-mails en documentbijlages versturen met een versleuteling.

VERHOGEN VAN RISICOBEWUSTZIJN PUO'S

Hetgeen op bestuurders en hun staf van toepassing is, is naar ons inziens in het bijzonder van toepassing op puo's. Zij zijn immers de hoofdbewaarder van privacygevoelige data van (gewezen) deelnemers. Kortom: als de puo niet zichtbaar een adequaat risicoraamwerk voor cybersecurity kan bieden aan fondsen en daar niet adequaat over rapporteert, dan laat ze onvoldoende zien hoe de beheersing van bijvoorbeeld cyberrisico's is ingeregeld en wordt gemonitord.

Ten tijde van het schrijven van dit artikel werd in het Financieele Dagblad[2] aangekondigd dat banken en investeerders overwegen om bij kredietverstrekking een speciale verklaring van ondernemingen te verlangen aangaande hacking en het voeren van een degelijk IT-beleid. Kennelijk is bij schuldeisers doorgedrongen dat een goed doordacht IT-beleid het *vulnerability management* aanzienlijk verstevigt. We verwachten dat *cyber security monitoring* steeds meer een eis wordt van afnemers en hun auditors.

Een puo moet het fonds in staat stellen controle uit te kunnen oefenen door inzicht te verstrekken in het complexe en vaak zeer gedetailleerde vraagstuk van cybercrime. Dit kan bijvoorbeeld middels scenario's, waarmee wordt verduidelijkt wat er mis kan gaan. Maar ook door passende beheersmaatregelen in te regelen, 'hoe mitigeren we bepaalde risico's?'. Door scenario's in een risicoraamwerk vast te leggen heeft het fonds een sturingsmechanisme in handen en heeft het bestuur inzicht in de risico's. Vervolgens kan het fonds bepalen wat het aan beheersing en rapportages verwacht van de puo. Als de puo weet met welke risico's het fonds rekening houdt en hoe zij deze wil beheersen, kan een puo veel beter haar verantwoordelijkheid nemen als het gaat om cybersecurity. De puo bepaalt vervolgens hoe ze dit verder gaat inrichten. Hiermee is het bestuur in de lead en hoeft zij niet slechts eenzijdig van de puo te vernemen wat de puo zelf denkt aan maatregelen nodig te hebben. Het fonds kan dan het functioneren van de puo via dit raamwerk beoordelen, het kan via dit raamwerk *assurance* vragen met behulp van testen die worden uitgevoerd. Een fondsbestuur kan ook vragen om over het raamwerk gerapporteerd te krijgen. Om *in control* te zijn, dient het fondsbestuur duidelijke afspraken te maken met de puo. Het gaat daarbij niet om hoe de puo haar cybersecurity moet inrichten, maar wel om wat het bestuur aan resultaten verwacht.

1 Bron: "Niet wachten op de digitale vuile bom", Elsevier Weekblad, 7 augustus 2021.

2 Bron: "Nieuwe IT-check kan voorwaarde worden voor krediet aan bedrijf", Het Financieele Dagblad, 13 augustus 2021.

De vragen die een fonds aan zichzelf en een puo kan stellen, kunnen bijvoorbeeld zijn:

- In hoeverre beheerst het fonds via de puo zijn cybersecuritymanagement? Denk hierbij aan netwerkverbindingen, wachtwoorden, databeheer en het gebruik van diverse digitale apparaten.
- Met welke cyberrisico's zijn het fonds en de puo bekend?
- Hoe groot wordt de kans ingeschat dat het fonds en de puo met bovengenoemde cyberrisico's te maken krijgen?
- In hoeverre maakt het fonds via de puo gebruik van beveiligde netwerken?
- Welke beheersmaatregelen heeft de puo voor het fonds genomen om deze cyberrisico's te managen?
- Hoe effectief zijn de securitymaatregelen van het fonds via de puo?
- Wat doen het fonds en de puo aan bewustwording in het kader van cybersecurity?
- Hebben het fonds en de puo een noodplan?
- Worden de toegangsrechten direct vergrendeld of verwijderd wanneer iemand het fonds en de puo niet meer bedient?
- Worden gevoelige of vertrouwelijke bestanden versleuteld in het mailverkeer van het fonds en de puo?

Het streven is om na te gaan in hoeverre cybersecuritymanagement op het niveau is aan de eisen die hieraan gesteld worden. Door het verkrijgen van rapportages op het gebied van cybersecurity krijgt het fonds tevens een duidelijk beeld van de risicohouding, de risicobereidheid en de identificatie van de risico's bij de puo. Dit vormt uiteindelijk de basis voor de lopende processen en voor het evalueren, beheersen en bewaken van de uitbestede activiteiten door het fonds.

VERTROUWEN IS GOED, CONTROLE IS BETER!

Het *in place* hebben van beheersmaatregelen voor cyberrisico's is slechts één van de aspecten van integraal risicomanagement. Rapportages begrijpen, laten aanpassen en het stellen van doortastende vragen is voor veel fondsbestuurders (nog steeds) onbekend terrein. Een bestuur kan echter in overleg treden met haar puo om meer gevoel te krijgen bij het achterliggende IT-landschap en de mogelijke risico's en risiconiveaus. Zo kan zij de vraag stellen of de puo haar cybersecuritymanagement geïntegreerd heeft op een gedetailleerd controleniveau om een effectieve controlecyclus voor het fonds zichtbaar te maken.

Om een goede samenwerking in de bestrijding van cybercrime te creëren, is het essentieel dat de puo ook openheid toont over haar kwetsbaarheden. Niets doen is geen optie omdat de risico's steeds groter worden en vaak van ver over de grens komen. Dit betekent dat er een duidelijk beeld moet worden geschetst van preventie-, detectie- en responsmaatregelen en de restrisico's waaraan men blootgesteld is.

Fondsen dienen hun uitbestede processen periodiek te evalueren aan de hand van vooraf gestelde doelen en de wijze van beheersing daarvan. Hierdoor kan het fonds kritische vragen stellen en een oordeel vellen of de vooraf gestelde doelen en beheersing zijn gehaald. Bij het vaststellen van IT-beleid en het bijbehorende cybersecuritymanagement bij het fonds wordt bepaald wat het fonds verwacht van de risicobereidheid bij de puo. De risicobereidheid van de puo moet passen binnen de kaders die het fonds hieraan heeft gesteld. Hierdoor kunnen fondsen conclusies trekken over huidig beleid en gerichte eisen stellen.

> Fondsen hebben grote hoeveelheden data waar cybercriminelen steeds meer in geïnteresseerd zijn

Een fonds zou als sluitstuk een overzicht van alle kwetsbaarheden, bedreigingen en beheersmaatregelen moeten vastleggen in haar cybersecuritybeleid. Hierdoor krijgt zij een duidelijk beeld van de concrete verbeterpunten en die van de uitbestedingspartner. Zo kan bijvoorbeeld een puo zelf bepalen hoe zij de beheersing hiervan inregelt en monitort. Wanneer dit vastligt op een zo gedetailleerd mogelijk controleniveau, zal dit fondsen helpen om op een effectieve manier op de controlecyclus te sturen.

De puo moet het fonds derhalve in staat stellen om:
1 bedreigingen en kwetsbaarheden bij de puo te begrijpen;
2 inzicht te geven hoe groot de kans is dat informatie-incidenten plaatsvinden bij de puo;
3 duidelijkheid te verschaffen over de vervolgstappen die moeten worden genomen om informatie in het systeem of de dienst te beschermen.

Fondsen moeten weten waar cyberrisico's zich kunnen manifesteren voor zowel inherente cyberrisico's als grove risico's. Met andere woorden, ook voor de (reeds) bestaande risico's als er geen beheersmaatregelen zouden zijn genomen.

HANDREIKINGEN DNB

DNB heeft cybersecurity en uitbesteding in de Visie op Toezicht opgenomen.[1] Daarnaast wordt in haar richtlijn voor informatiebeveiliging een aantal activiteiten genoemd die in dit kader moeten worden ondernomen.[2] Hoe dit concreet moet gebeuren, wordt niet nader toegelicht. DNB doet wel de volgende handreikingen aan een fonds:
- Het doen van een risicoanalyse.
- Het uitvoeren van beveiligingstests.
- Het toewijzen van taken en verantwoordelijkheden.
- Het inrichten van communicatie, bewustwording en training.
- Het realiseren van de uitvoering, monitoring en de rapportage.
- Het instellen van incidentdetectie, -beheer en -respons.

ONZE OBSERVATIES

Nieuwe ontwikkelingen volgen elkaar in rap tempo op en hackers blijven nieuwe kwetsbaarheden in de IT-componenten ontdekken. Fondsen moeten ervoor zorgen dat ze controle hebben over de extra detectie van incidenten en dat die, zodra ze zich voordoen, direct kunnen worden geïntervenieerd. Daarnaast is het een *must* om de beheersmaatregelen van zowel het fonds als de uitbestedingspartner periodiek onder de loep te nemen.

Het geven van trainingen, het creëren van bewustwording als het gaat om cybercrime en het helpen opzetten van de juiste beheersmaatregelen zijn activiteiten die op korte termijn moeten worden opgepakt door fondsen en puo's. Een aantal zaken die opvielen tijdens observaties bij fondsen en puo's:
- Observatie 1: een geïntegreerde roadmap voor ICT in relatie tot cyberalertheid ontbreekt veelal.
- Observatie 2: er is geen specifieke aandacht voor bewustwording voor cybersecurity in de IT-visie en de IT-strategie.
- Observatie 3: er is geen integrale SWOT-analyse met betrekking tot cybersecurity.
- Observatie 4: er is geen geïntegreerd communicatieplan voor de IT-strategie.
- Observatie 5: in de meeste gevallen heeft een fonds wel een IT-beleid maar wordt dit beleid niet gemonitord.

ONZE CONCLUSIES

Op het gebied van cybersecuritymanagement zouden fondsbesturen een meer proactieve en meer kritische houding mogen en zelfs móéten aannemen als eigenaar van de data. Cybersecurity moet onderdeel worden van de risicomanagementcyclus. Het is belangrijk dat de puo deze aanbeveling draagt en ook daadwerkelijk informatie uitwisselt, ook als er onverhoopt iets misgaat. Aansluitend dient de informatie inzake cybersecurity een zo goed mogelijk beeld te geven over de prestaties van alle uitbestedingspartners. Deze informatie moet gerelateerd zijn aan de door het bestuur gestelde doelen. Daarnaast moet ook aandacht worden besteed aan elementen zoals de cultuur en omgeving waarin het fonds en de puo opereert. Alleen dan kan worden voorkomen dat 'de put pas gedempt wordt als het kalf eenmaal verdronken is'.

1 Bron: "Visie op Toezicht 2021 – 2024", DNB.
2 Bron: "Good Practice Informatiebeveiliging 2019/2020", DNB.