Verhaallijn Themabijeenkomst “Digitaal veilig Pensioenfonds”, 6 oktober 2020

DeNederlandscheBank
EUROSYSTEEM

Introductie – wie zijn wij

Jacco Jacobs

Afdelingshoofd Expertisecentrum Operationele & IT-risico's bij DNB

Noor Witteveen

Senior toezichthouder specialist Expertisecentrum Operationele & IT-risico's

Twee handvaten voor bestuurders van Pensioenfondsen

- DNB heeft vorig jaar het Toetsingskader Informatiebeveiliging geactualiseerd en omgevormd naar de Good Practice IB. De rol van de bestuurder wordt in de good practice specifiek benoemd

- DNB heeft april dit jaar haar “Jaarlijkse informatiebeveiligingsmonitor-2020” weer gepubliceerd. Met daarin zes waarnemingen over Informatiebeveiliging voor de financiële instellingen, waaronder ook de ‘Rol van de Directie’

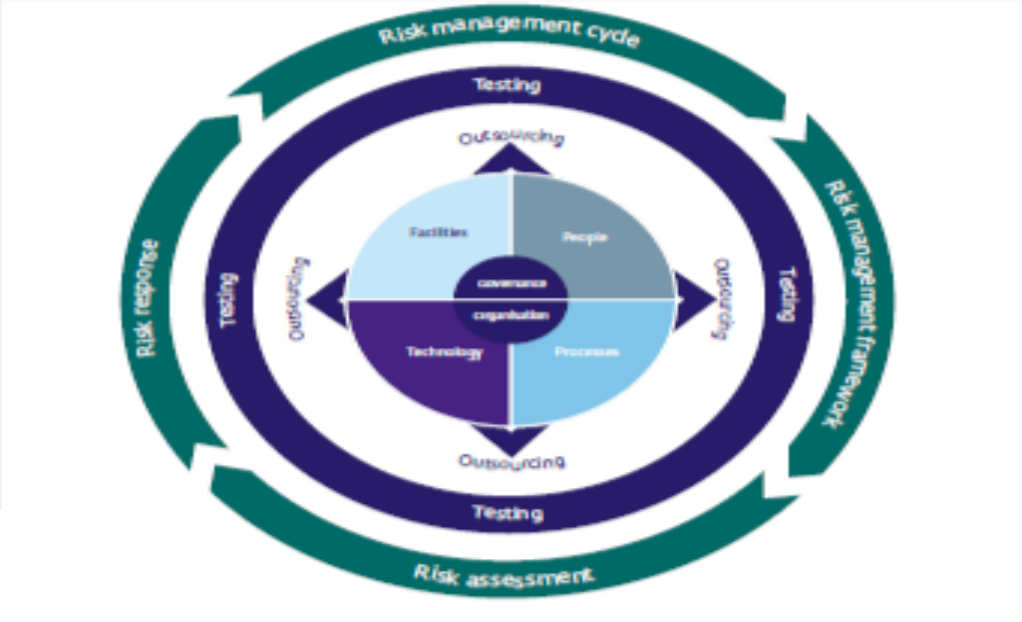
Achtergrond Good Practice IB

- De Good Practice IB biedt pensioenfondsbestuurders, naast een minimum norm waaraan voldaan moet worden, concrete handvatten hoe pensioenfondsen de beheersing van de risico's op het gebied van informatiebeveiliging en cybersecurity kunnen vormgeven.

- Deze beheersingsmaatregelen zijn niet alleen gericht op technologische oplossingen (Technology), zij zijn ook gericht op menselijk handelen (People), inrichting van processen (Processes) en faciliteiten (Facilities).

Model achter de Good Practice IB

- De Good Practice IB is vormgegeven aan de hand van het volgende model.



Wat is nieuwe aan de Good Practice IB

- In deze Good Practice is zoveel mogelijk aangesloten op de reeds bestaande indeling van de voorgaande ‘Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek’

- De Good practice is toegankelijker voor bestuurders en beleidsbepalers gemaakt en geeft meer concrete voorbeelden. Daarnaast zijn er vier nieuwe beheersingsmaatregelen toegevoegd:

1. Employee awareness: Het actief bevorderen van bewustzijn voor cyberrisico’s bij medewerkers.
2. Vulnerability management: Het actief monitoren en oplossen van kwetsbaarheden in de IT-infrastructuur en IT-applicaties.
3. Application Life cycle management: Borgen dat applicaties tijdig worden onderhouden en uitgefaseerd.
4. Penetration testing and ethical hacking: Testen van de weerbaarheid van de instelling tegen cyberdreigingen.

De rol van de bestuurder in de Good Practice IB

- In de Good practice zijn de beheersingsmaatregelen per element uit het model, samengevat voor bestuurders en beleidsbepalers. De beheersingsmaatregelen zijn toegespitst op respectievelijk de instelling en op de rol van het bestuur bij het implementeren van en het toezien op die beheersingsmaatregelen.

- Voorbeelden daarvan zijn:
  - het bestuur zorgt er binnen de Risk Management cycle voor dat periodiek in het bestuur wordt nagegaan in hoeverre de informatiebeveiligings- en cybersecurity risico's van de instelling passen binnen de risicobereidheid van het bestuur. Hierbij kan worden afgewogen in hoeverre een effectieve mix van maatregelen – People, Processes, Technology en Facilities – is getroffen om risico's van de instelling te beheersen.
  - Het bestuur heeft aantoonbaar trainingen en opleidingen gevolgd om de belangrijkste IT-risico's en beheersingsmaatregelen voor haar instelling te kunnen begrijpen.

Achtergrond IB-monitor

- Basis voor deze jaarlijkse IB-monitor zijn de IB-onderzoeken bij pensioenfondsen en verzekeraars uitgevoerd in 2019.

- Verder is de IB-monitor aangevuld met informatie vanuit standaard uitvragen en doorlopend account toezicht, meldingen van cyber-incidenten, beelden uit het TIBER-programma en uit werkgroepen van EBA en EIOPA die aan Europese Guidelines op het gebied van IT en Cybersecurity hebben gewerkt.

Zes waarnemingen uit de IB-monitor

De belangrijkste zes waarnemingen uit deze IB-monitor voor financiële instellingen zijn:

1. Cyberhygiëne en met name vulnerability management blijft cruciaal.
2. Testen van maatregelen draagt bij aan continue verbeteren van Cyberweerbaarheid.
3. Geef met uitbesteden niet de verantwoordelijkheid uit handen, blijf zelf in control.
4. Preventie alleen is niet genoeg, de focus verschuift naar samenwerking, detectie en response.
5. Wees u bewust van de rol die u als bestuurder heeft bij informatiebeveiliging.
6. Houd rekening met specifieke risico's die naar aanleiding van de pandemie COVID-19 naar voren komen.

Recente ervaringen met IB en COVID-19

- In het begin leek het erop dat COVID-19 ook een springplank was voor meer cyberaanvallen. DNB ziet momenteel wel dat het thema COVID-19/Corona wordt gebruikt bij aanvallen, zoals bij Spearphising. Er is echter geen significante toename van aanvallen en de modus operandi van de aanvallen is veelal hetzelfde als voorheen.

- Verder ziet DNB een gemengd beeld als het om het uitstellen van kritische patches door COVID-19 gaat. Bij sommige instelling is spraken van uitstel bij anderen helemaal niet.

Enkele recente relevante voorbeelden van aanvallen

- Wereldwijde DDos aanval via dreigmail die meerdere financiële instellingen heeft geraakt.

- Geslaagde gerichte aanval op postbussen van één financiële instelling. Het algoritme heeft na het klikken door de medewerkers, de mailbox van de instelling gebruikt om de aanvalsmail te verbeteren en een nieuwe mail met malware naar alle medewerkers gestuurd. Doel was het achterhalen van wachtwoorden die toegang geven tot het netwerk.

- Data-breach bij een grote software ontwikkelaar Cognizant. Zij ontwikkelen ook voor enkele grote verzekeraars en banken en zitten daarvoor soms ook op het netwerk van enkele kanten.

Verdere boodschappen uit de IB-monitor

- Naast deze adviezen komt uit de IB-monitor naar voren dat instellingen steeds vaker onderling samenwerken, hetgeen DNB als essentieel ziet voor de financiële sector om cyberdreigingen het hoofd te kunnen bieden.

- Verder geeft de IB-monitor een Dreigingsbeeld, waarin DNB op basis van de verschillende door haar opgedane beelden en ervaringen voor 2020 een aantal dreigingen 'high light' die vaak voorkomen, kansrijk en van potentieel grote impact op de financiële sector zijn.

- De IB-monitor sluit af met een vooruitblik hoe zij met verscheidende onderzoeksmethoden toezicht gaat houden op IB.