IB Monitor 2021

DeNederlandscheBank

EUROSYSTEEM

Inhoud

Waarnemingen

Dreigingsanalyse financiële sector

Vooruitblik

Bronnen

Inleiding

DNB ziet informatiebeveiliging en daarmee samenhangende cyberrisico's als één van de belangrijke operationele risico's bij financiële instellingen. Niet alleen het aantal cyberaanvallen neemt toe, ook de ontwrichtende impact van aanvallen wordt steeds groter. Cyberaanvallen hebben de potentie om de continuïteit van de bedrijfsvoering ernstig te schaden. Daarom deelt DNB voorbeelden voor de beheersing van deze risico's in Q&A's en Good Practices, voert DNB sectorbrede en individuele onderzoeken uit bij instellingen en werkt zij op onderdelen samen met de financiële sector om de weerbaarheid van instellingen verder te versterken.

In deze IB-monitor 2021 treft u de meest recente waarnemingen aan op het gebied van IT- en cyberrisico's, gebaseerd op toezichtonderzoeken en -uitvragen bij pensioenfondsen en verzekeraars. Daarnaast zijn een dreigingsanalyse en een vooruitblik op geplande toezichtactiviteiten in 2022 opgenomen. Uit onze toezicht-gesprekken en onderzoeken bij bancaire instellingen blijkt dat de waarnemingen benoemd in deze IB-monitor ook relevant zijn voor de gehele Nederlandse financiële sector.

De basis voor de waarnemingen in deze IB-monitor zijn de in 2020-2021 uitgevoerde onderzoeken en sectorbrede uitvragen bij pensioenfondsen[1] en verzekeraars. Deze bronnen zijn aangevuld met signalen en incidentmeldingen van instellingen en onze informatie-uitwisseling met andere toezichthouders en samenwerkingsverbanden. Waar relevant, zijn deze informatiebronnen ook in deze IB-monitor verwerkt, uiteraard op anonieme basis.

Waarnemingen die vaak terugkomen in onze onderzoeken zijn opgenomen in deze IB-monitor. Die hebben wij samengevat tot de navolgende drie belangrijke waarnemingen die wij onder de aandacht willen brengen van zowel bestuursleden als interne en externe toezichthouders (bijvoorbeeld sleutelfunctiehouders, leden van raden van toezicht en commissarissen) van de onder ons toezicht staande instellingen:

De risicomanagementcyclus gericht op informatiebeveiliging is onvoldoende effectief

Het beheersen van informatiebeveiliging in de keten is cruciaal

De weerbaarheid tegen cyberaanvallen moet worden versterkt

Deze waarnemingen zijn verder uitgewerkt en concreet gemaakt in de onderdelen van deze IB-monitor.

1 Wanneer pensioenfondsen hun pensioenbeheer hebben uitbesteed, zijn ook hun pensioenuitvoeringsorganisaties betrokken in het onderzoek.

Aandacht voor kennis van het bestuur en intern toezicht

DNB ziet een belangrijke en groeiende rol weggelegd voor de bestuurder, de sleutelfunctiehouder, de (externe) toezichthouder en de commissaris voor het op orde krijgen en houden van de risicomanagementcyclus ten aan zien van informatiebeveiliging- en cyberrisico's. In de Good Practice Informatiebeveiliging[2] zijn per element van informatiebeveiliging voorbeelden gegeven die ingaan op de rol van bestuurders en beleidsbepalers. Voldoende kennis en aandacht bij bestuurders en interne toezichthouders draagt in de praktijk bij aan het borgen van dit onderwerp. DNB ziet ruimte voor groei in kennisontwikkeling aan de bestuurstafel op dit gebied. Meedenken en het stellen van kritische vragen door bestuurders en interne toezichthouders helpt de instelling op dit onderwerp goede strategische en tactische keuzes te maken.

Samenwerking

DNB ziet verdere samenwerking tussen alle partijen in de financiële sector als essentieel om de weerbaarheid van instellingen te vergroten. De bestaande samenwerkingsverbanden binnen de sectoren zoals de ISAC's[3] zijn hierbij van toegevoegde waarde. Waar mogelijk is het intensiveren van samenwerking of aangaan van nieuwe samenwerkingsverbanden niet alleen aan te bevelen, maar zelfs essentieel.

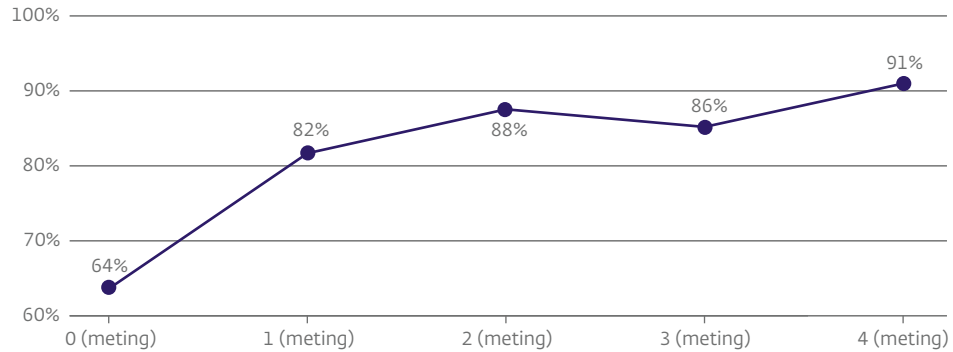
De toenemende complexiteit van de cyber-aanvallen maakt het voor individuele instellingen namelijk moeilijk om zelf over de juiste en actuele kennis en ervaring te blijven beschikken, terwijl die sectorbreed wel beschikbaar is. Zeker nu aanvallers steeds verder hun kennis specialiseren, samenwerken en diensten 'inkopen'. DNB constateert dat de samenwerking niet binnen alle sectoren even effectief is als het gaat om het delen van informatie en best practices op het gebied van cybersecurity.

DNB roept daarom de instellingen op om binnen én buiten de verschillende sectoren de samenwerking op te zoeken of te intensiveren.

Informatiebeveiliging inbedden in het internal control framework

Naast de inhoudelijke waarnemingen constateren we, evenals in voorgaande jaren, dat het uitvoeren van een 0-meting door de toezichthouder vaak een startpunt is voor de instelling om informatiebeveiliging structureel te gaan verbeteren en te borgen. De volwassenheid van informatiebeveiligingsmaatregelen verbetert naar mate de maatregelen onderdeel zijn van een bij de instelling ingerichte en geformaliseerde planning- en control cyclus. Op basis van onze onderzoeken vanaf 2010 is een opgaande trend waarneembaar in het percentage aantoonbaar werkende beheersmaatregelen na een eerste beoordeling door de toezichthouder, zie figuur 1.

Figuur 1 % controls op niveau per meting



2 Zie de Good Practice Informatiebeveiliging en bijbehorende Q&A: Q&A Informatiebeveiliging (dnb.nl)
3 Een Information Sharing and Analysis Centre (ISAC) betreft een sectorale samenwerking met als doel de digitale weerbaarheid te verbeteren.

In de praktijk zien we een positieve ontwikkeling dat bij instellingen waar verschillende metingen zijn uitgevoerd, de systematiek van meten, rapporteren en verbeteren van informatiebeveiligingsmaatregelen een vast onderdeel is geworden van het internal control framework in de organisatie. Tegelijkertijd zien we bij vervolgmetingen dat ook deze instellingen op deelgebieden in volwassenheid kunnen groeien. Bij deze instellingen zien wij veelal een verschuiving van het implementeren van beveiligingsstandaarden naar onderhoud daarop en het (efficiënter) aantonen van de werking van het beveiligingsraamwerk.

Slot

In alle activiteiten van financiële instellingen speelt technologie een belangrijke rol. Om het hoofd te kunnen bieden aan ontwikkelingen in cyberdreigingen is het voor de instellingen van groot belang dat zij kunnen steunen op een sterk fundament van informatiebeveiliging. Een fundament dat enerzijds een solide structuur vormt om de beheersing van risico's te organiseren maar anderzijds ook meebeweegt met actuele ontwikkelingen. Beheersmaatregelen hierin zijn niet statisch. Van belang blijft een risicogebaseerde aanpak die ertoe leidt dat beheersmaatregelen worden aangepast aan de trend van toenemende cyberdreigingen. Net als de ESG-factoren is de Technologie ('T')-factor een onderwerp die bij instellingen het afgelopen jaar meer centraal stond in het bepalen van (beleids)beslissingen.

Waarnemingen

Waarneming 1: De risicomanagementcyclus gericht op informatiebeveiliging is onvoldoende effectief

Het beeld bij pensioenfondsen en verzekeraars is dat IT-risicomanagement aandacht nodig heeft om door te kunnen groeien naar het vereiste volwassenheidsniveau. Niet altijd wordt geëvalueerd of het risicomanagement-raamwerk toereikend en van voldoende diepgang is om daadwerkelijk fundamentele verbeteringen in de beheersing door te voeren en het effect daarvan op informatiebeveiligingsrisico's te meten. Ook maakt het informatiebeveiligingsrisico vaak geen integraal onderdeel uit van het overkoepelende risicomanagement-raamwerk van een organisatie.

In de Good Practice Informatiebeveiliging (GP IB) is beschreven wat DNB verstaat onder de risicomanagementcyclus, namelijk:

> Het is belangrijk dat de instelling regelmatig de voor haar relevante risico's op het gebied van informatiebeveiliging en cybersecurity identificeert en analyseert. Op grond van deze risicoanalyse bepaalt de instelling haar reactie, treft maatregelen om risico's te beperken en accepteert (tijdelijk) eventuele restrisico's. Geaccepteerde restrisico's worden periodiek opnieuw geëvalueerd en ter acceptatie aangeboden.

Ook beschrijft de GP IB welke handvatten en volwassenheidsniveaus een goede invulling kunnen geven aan de risicomanagementcyclus. DNB ziet goed risicomanagement als een belangrijke voorwaarde om informatiebeveiliging structureel te borgen en bij te sturen. Dit koppelt DNB aan een hoger volwassenheidsniveau, namelijk niveau '4' voor de risicomanagement beheersmaatregelen. In de GP IB staat beschreven dat de risicomanagementcyclus aantoonbaar werkt (niveau 3) en dat de effectiviteit van risicomanagement zelf door instellingen regelmatig wordt geëvalueerd (niveau 4). Oftewel: er is sprake van een aantoonbaar volwassen proces dat regelmatig wordt geëvalueerd.

> In de Good Practice Informatiebeveiliging (GP IB) reiken we handvatten aan om volwassenheidsniveaus van 0 tot 5 te bepalen. Om volwassenheidsniveau 4 te behalen, is het nodig dat de instelling periodiek de inrichting van de beheersmaatregelen evalueert. Hierbij verwacht DNB dat er geëvalueerd wordt of de risicobeheersing beter of anders ingericht kunnen kan worden en of de mix aan beheersmaatregelen effectief is of misschien aanpassing behoeft.[4]

Bij een evaluatie komen vragen aan de orde als: Is het zinvol dat we dit proces nog zo vormgeven? Zijn alle deelstappen nog functioneel? Is rekening gehouden met actuele (aanvals-)scenario's? Welke alternatieve Best Practices kennen we? Passen die alternatieven beter bij ons?

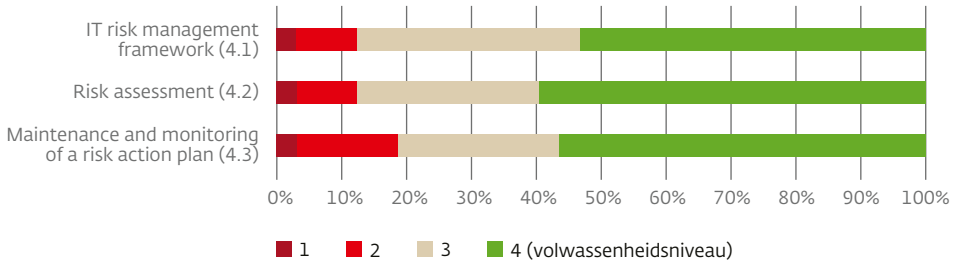
Ook het bestuur heeft een rol in de evaluatie van de risicomanagementcyclus. Te denken valt hierbij aan het passend zijn van de governance van informatiebeveiliging en de afweging in hoeverre de mix van maatregelen effectief is om binnen de risicobereidheid van de instelling te blijven.

4 Een uitgebreide beschrijving van de criteria per volwassenheidsniveau is te vinden in de Good Practice Informatiebeveiliging. Zie de Good Practice en bijbehorende Q&A: Q&A Informatiebeveiliging (dnb.nl)

Uitkomsten van onderzoeken

De resultaten van de uitgevoerde onderzoeken geven het beeld dat ruim 40% van de onderzochte instellingen niet het volwassenheidsniveau '4' heeft bereikt voor de drie beheersmaatregelen in de risicomanagementcyclus.

Figuur 2 Risicomanagement cyclus



Voorbeelden van waarnemingen bij instellingen met een lager volwassenheidsniveau zijn:

- De evaluatie van de risicomanagementcyclus ontbreekt in het geheel.
- Het raamwerk voor informatiebeveiliging maakt geen deel uit van het overkoepelende risicomanagement raamwerk van de organisatie.
- Onvoldoende diepgang in evaluaties om daadwerkelijk tot verbeteringen te komen, bijvoorbeeld door geen scenario-analyses in te zetten als instrument voor risicomanagement.
- Gebruikte scenario-analyses sluiten niet aan op het recente dreigingsbeeld van de instelling. Bijvoorbeeld door het ontbreken van een specifiek scenario voor een geslaagde ransomware aanval of onvoldoende operationele uitwerking hiervan. Bijvoorbeeld in de vorm van een runbook, testplannen en/of uitgevoerde oefeningen.

Het onvoldoende of niet tijdig evalueren van het IT-riskmanagement-framework vergroot de informatiebeveiliging- en cyberrisico's voor de instelling. Een instelling selecteert, implementeert of wijzigt interne beheersmaatregelen op basis van de uitkomsten van risicoanalyses, met als doel te kunnen blijven opereren binnen de vastgestelde risicobereidheid. Deze risicoanalyses vormen daarmee een belangrijk uitgangspunt om te komen tot een maatwerk IT-riskmanagement-framework dat de belangrijkste specifieke risico's mitigeert. Door deze risicoanalyses periodiek bij te werken kunnen instellingen evalueren of de huidige ingerichte set aan beheersmaatregelen toereikend is en blijft.

Cyberdreigingen kenmerken zich als sterk veranderlijk. Wanneer deze evaluatie niet of niet tijdig plaatsvindt, bestaat het risico dat instellingen steunen op beheersmaatregelen die de gewijzigde (cyber)dreigingen niet (afdoende) mitigeren. Beheersmaatregelen hierin zijn niet statisch. Van belang blijft een risicogebaseerde aanpak die ertoe leidt dat beheersmaatregelen worden aangepast aan de trend van toenemende cyberdreigingen. Net als de ESG-factoren is de Technologie ('T')-factor een onderwerp die bij instellingen het afgelopen jaar meer centraal stond in het bepalen van (beleids)beslissingen; het integraal opnemen van informatiebeveiligingsrisico's in interne controleraamwerken ondersteunt hierbij.

Ervaringen op basis van TIBER-testen[5]:

Uit TIBER-testen is naar voren gekomen dat instellingen bij het identificeren van risico's hoofdzakelijk vanuit het perspectief van de instelling zelf denken en veel minder vanuit het perspectief van mogelijke aanvallers. Dit leidt tot 'interne tunnelvisie'. TIBER-testen hebben inzichtelijk gemaakt dat aanvallers regelmatig andere doelwitten nastreven dan waar de financiële instelling zelf rekening mee houdt.

Bijvoorbeeld: een significant gedeelte van de instellingen houdt met name rekening met aanvallers die uit zijn op financieel gewin, terwijl veel aanvallers ook andere intenties hebben, zoals sabotage, verstoring en economische of politieke spionage. Penetratietesten gebaseerd op actuele dreigingsinformatie zijn een waardevol instrument bij het bepalen van relevante risico's. Ook wordt hiermee de inrichting en werking van het risicomanagement raamwerk getest.

In de GP IB zijn voorbeelden opgenomen op het gebied van de risico-management-cyclus. Onderstaande voorbeelden zijn daarvan afgeleid:

- Een instelling inventariseert en evalueert de getroffen maatregelen aan de hand van scenario's. De instelling past de scenario's periodiek aan op basis van op de instelling toegespitste dreigingsanalyses. Een goed voorbeeld is een ransomware aanval scenario.
- Bij de evaluatie van het risicoraamwerk evalueert het bestuur nadrukkelijk de vraag in hoeverre het risicomanagement op informatiebeveiliging onderdeel is van - en in samenhang is met - het integraal risicomanagementraamwerk van de organisatie.
- Een instelling brengt haar 'kroonjuwelen' in kaart, evalueert deze periodiek en relateert deze aan actuele dreigingen en getroffen beheersmaatregelen. Daar waar nodig treft de instelling aanvullende beheersmaatregelen. Maatregelen die niet (meer) effectief werken worden aangepast, vervangen door andere maatregelen of uitgefaseerd.
- Een instelling betrekt de risico's in de uitbestedingsketen volledig in haar risicoanalyse. De instelling beoordeelt periodiek de actieplannen van dienstverleners in de keten op relevantie en stelt vast dat de dienstverlening nog voldoet (of kan voldoen) aan de eisen van de instelling. Bij afwijkingen maakt de instelling afspraken met die partijen om het risico te beperken naar een acceptabel niveau dat past binnen de risicobereidheid van de instelling.

5 Threat Intelligence Based Ethical Red-teaming, zie paragraaf 5.2

Waarneming 2: Het beheersen van informatiebeveiliging in de keten is cruciaal

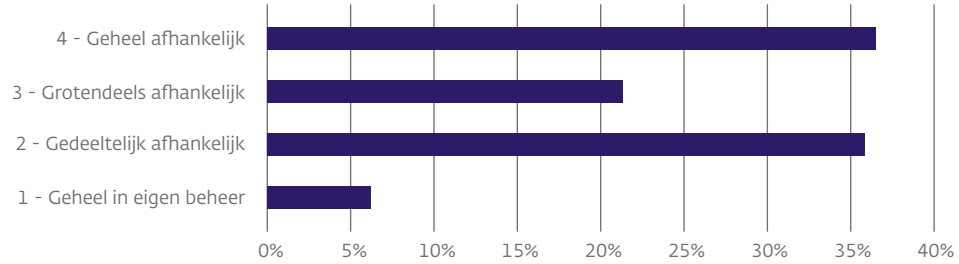
Uitbesteding en ketensamenwerking zijn niet meer weg te denken uit de bedrijfsvoering van financiële instellingen. Het beheersen van informatiebeveiliging bij uitbesteding vergt specifieke kennis en maatregelen. Onderzoeken laten zien dat instellingen moeite hebben om deze beheersing van de gehele keten inzichtelijk en adequaat in te richten.

Door ontwikkelingen zoals het opzetten van partnerships, ontvlechting van de waardeketen en uitbesteding[6] is de beheersing van informatiebeveiliging voor instellingen een opgave die over de grenzen van de eigen organisatie reikt.
Door horizontale ontvlechting kan bijvoorbeeld het contact tussen de consument en een traditionele financiële instelling via een omgeving van een Fintech-partij gaan verlopen. Consumenten krijgen dan via één partij een overzicht van al hun rekeningen bij verschillende banken.

Door verticale ontvlechting in de waardeketen nemen dienstverleners één of meer schakels in de waardeketen over van financiële instellingen, bijvoorbeeld door uitbesteding van werkzaamheden. Het aandeel uitbesteding neemt jaarlijks toe. Uit een vergelijking tussen DNB onderzoek uit 2017 en 2021 blijkt dat de uitgaven aan uitbesteding bij verzekeraars bijna is verdubbeld in vier jaar van 20% naar 36% als percentage van de totale operationele kosten. Dit is een stijging die overeenkomt met het beeld in de praktijk. In 2017 waren veel verzekeraars gestart met projecten op het gebied van uitbestedingen. Het is waarschijnlijk dat deze projecten zijn opgeschaald en structureel hebben geleid tot deze stijging. Bij pensioenfondsen zien we deze sterke stijging in de gehele keten (nog) niet, echter ligt de uitbestedingsgraad in de eerste schakel van de keten al vrij hoog (bijvoorbeeld het uitbesteden van pensioen- en vermogensbeheeractiviteiten).

Uit sectorbrede analyses door DNB blijkt dat kritieke of belangrijke processen van veel instellingen in hoge mate afhankelijk zijn van IT-dienstverleners. Dit is weergeven in onderstaande figuur 3.

Figuur 3 Mate van afhankelijkheid van IT-dienstverleners



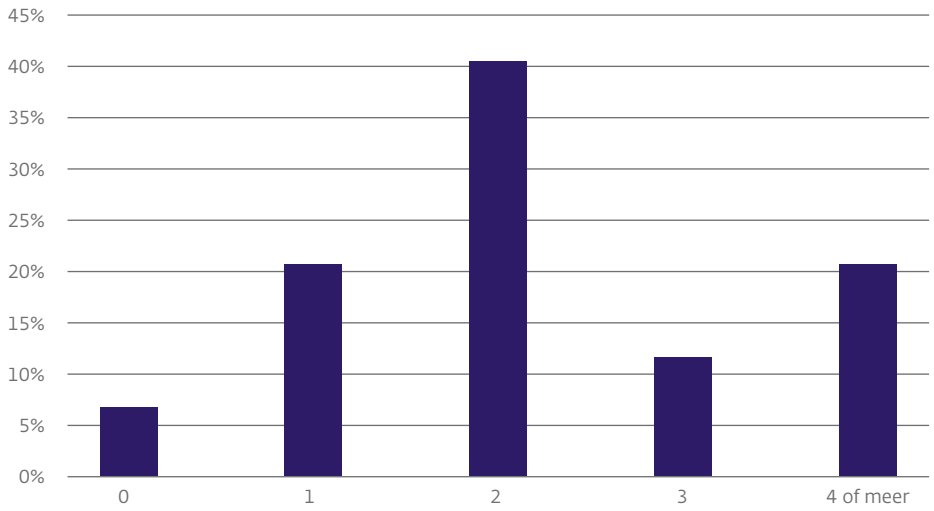
Uit figuur 3 is op te maken dat ruim 35% van de instellingen voor het functioneren van hun kritieke of belangrijke IT-processen geheel afhankelijk is van IT-dienstverleners. Verder is een tendens zichtbaar dat instellingen sterk afhankelijk zijn van één of meer cloudserviceproviders (CSP's) voor het functioneren van een kritiek of belangrijk bedrijfsproces. In onderstaande figuur 4 is dit inzichtelijk gemaakt.

Uit figuur 4 is op te maken dat ruim 20% van de instellingen te maken heeft met vier of meer CSP's die betrokken zijn bij kritieke of belangrijke bedrijfsprocessen.

Door de verticale en horizontale ontvlechting zijn de instellingen steeds meer onderdeel én afhankelijk van een keten van dienstverleners om hun primaire taken te kunnen uitvoeren. Als gevolg van deze ontwikkelingen veranderen de risico's op het gebied van informatiebeveiliging ook richting de keten waar instellingen onderdeel van uitmaken. Instellingen zullen hun beheersmaatregelen en volwassen-

6 Zie hiervoor ook het rapport: Veranderend landschap, veranderend toezicht- Ontwikkelingen in relatie tussen Big Techs en financiële instellingen, "Opkomst BigTechs zorgt voor gebruiksgemak, maar er zijn ook risico's" (dnb.nl)

Figuur 4 Aantal cloud service providers betrokken bij kritieke of belangrijke bedrijfsprocessen (% instellingen)



heidsniveaus op deze risico's moeten afstemmen en ook uitbestedingsrelaties moeten sturen op het aantoonbaar op orde houden van hun volwassenheidsniveaus van beheersingsmaatregelen. In de GP IB is dit als volgt beschreven:

> Instellingen blijven eindverantwoordelijk voor de door dienstverleners uitgevoerde activiteiten. Voor een adequate invulling van deze verantwoordelijkheid is het van belang dat de instelling afspraken maakt met de dienstverleners over passende beheersmaatregelen en deze controleert, monitort en periodiek test op effectiviteit passend bij het risicoprofiel. Zo nodig implementeert de instelling aanvullende beheersmaatregelen.

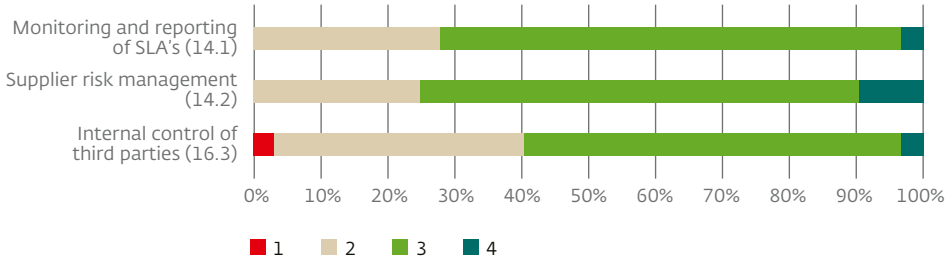
Uitkomsten van onderzoeken

Uit onderzoeken van DNB komen de volgende belangrijke bevindingen op het gebied van uitbesteding naar voren:

1. **Instellingen controleren, monitoren en meten onvoldoende aantoonbaar in hoeverre dienstverleners en onderaannemers hun afspraken nakomen op het gebied van informatiebeveiliging, cybersecurity en business continuïteit.** Instellingen hebben maatregelen met een onvoldoende volwassenheidsniveau op dit vlak. Een voorbeeld is dat de instelling niet vaststelt of contractuele afspraken voldoende zijn uitgewerkt in processen en maatregelen bij de dienstverlener en hierover een rapportage ontvangt. Een ander voorbeeld is dat de instelling onvoldoende zicht heeft op de waarborgen met betrekking tot business continuïteit en mogelijkheden voor vertrek bij de dienstverlener.
2. **Instellingen hebben onvoldoende risicomanagement-processen ingeregeld rondom hun dienstverleners.** Als gevolg van de corona pandemie en het massale thuiswerken zagen we dat instellingen aanvullende risicoanalyses op hun kritieke dienstverleners hebben uitgevoerd. Desalniettemin blijkt dat de instellingen onvoldoende volwassen zijn op dit gebied. Eén veel voorkomende waarneming is dat de dienstverlener waaraan is uitbesteed, de instelling geen inzicht kan geven in de specifieke risico's waarmee het te maken heeft.
3. **Er is bij de onderzochte instellingen onvoldoende inzicht in opzet, bestaan en de effectieve werking van beheersmaatregelen bij kritieke dienstverleners en eventuele onderaannemers die zijn betrokken bij de uitbestedingsketen.** Hierbij kan worden gedacht aan het opvragen en beoordelen van assurance-rapportages of door het uitvoeren van onderzoek bij de dienstverlener. Een aandachtspunt bij assurancerapportages is dat de verklaringen van dienstverleners, vaak delen van de keten buiten beschouwing laten (carve out), terwijl daar wel kritieke data en informatie van de instellingen is opgeslagen. Hierdoor dekt de scope van de verklaring niet alle controls t.a.v. informatiebeveiliging over de gehele keten.

Dit betreffen de controls #14.1, #14.2 en #16.3 van de GP IB. In figuur 5 treft u de volwassenheidsniveaus aan van deze controls.

Figuur 5 Controls over de keten



Te beperkte expertise en kennis op bestuurlijk niveau bij instellingen en te beperkte beheersmaatregelen in relatie tot het risicoprofiel, kunnen leiden tot:

- Het risico dat een instelling bij het aangaan van het contract onvoldoende waarborgt dat de IT-ketens rondom kritieke of belangrijke processen volledig in beeld zijn, vastgelegd zijn en hierover adequate contractuele afspraken maakt. Met als gevolg dat de risico's van onder-uitbestedingen onvoldoende zijn beheerst.
- Het risico dat instellingen onvoldoende inzicht hebben in de uitvoering van het contract en de beheersing van cyberrisico's bij hun dienstverleners. Bijvoorbeeld door ontoereikende afspraken over performance en interne controle en de rapportages daarover.

Hierdoor worden instellingen mogelijk blootgesteld aan risico's die hun risicobereidheid overschrijden.

Waarneming op basis van TIBER-testen

Ook binnen het TIBER-programma wordt de groeiende invloed van derde partijen op instellingen waargenomen. Wanneer deze derde partijen niet worden meegenomen bij het testen, geven de uitkomsten minder goed inzicht in de daadwerkelijke staat van de cyberweerbaarheid van deze instellingen. Immers, het aanvalsoppervlak wordt met de introductie van meer en meer derde partijen steeds groter, maar het gedeelte dat getest kan worden bij de instelling zelf wordt relatief steeds kleiner. Daarom wordt de rol en functie van derde partijen steeds vaker een integraal onderdeel van TIBER-scenario's en -testen.

Praktijkvoorbeeld

In februari 2021 werd bekend dat een significant aantal vertrouwelijke medische gegevens ('patient records') van Amerikaanse burgers enige tijd publiek toegankelijk zijn geweest. De gegevens waren in beheer bij een medisch onderzoeksbureau en bevatten onder andere vertrouwelijke patiënt-informatie en scans van identificatiebewijzen. De oorzaak voor dit datalek bleek een verkeerde configuratie van een webserver bij een cloud-serviceprovider. Volgens beveiligingsonderzoekers komen dergelijke fouten vaker voor vanwege onduidelijkheid over de verantwoordelijkheid voor de beveiliging van de data tussen cloud-serviceprovider en haar klanten.

In de GP IB zijn voorbeelden opgenomen op het gebied van uitbesteding. Onderstaande voorbeelden zijn daarvan afgeleid.

- Een instelling heeft een risicoanalyse opgesteld over de continuïteit en betrouwbaarheid van de dienstverlening waarbij zij gebruik kan maken van de expertise van de dienstverlener. Risico's bij partijen waaraan diensten zijn onder-uitbesteed zijn meegenomen in de risicoanalyse.
- Een instelling test jaarlijks de cruciale systemen en processen, waarbij de onderdelen die zijn uitbesteed deel uitmaken van deze testen.
- Een instelling neemt specifieke bijlagen op in de uitbestedingscontracten gericht op compliance en informatiebeveiliging. Hierin zijn afspraken gemaakt om de IT-ketens rondom kritieke of belangrijke processen volledig in beeld te brengen en vast te leggen, zodat er zicht is op belangrijke onder-uitbesteding. Tevens zijn adequate contractuele afspraken gemaakt met dienstverleners zodat wordt voldaan aan toepasselijk wetgeving en het eigen beleid.
- Een instelling ontvangt en beoordeelt zekerheidsrapportages, zoals onafhankelijke audit- en assurancerapportages over de beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity bij de dienstverlener en de betrokken belangrijke onderaannemers. De rapportages sluiten aan bij de afgesproken dienstverlening waarin de beheersmaatregelen uit de GP IB zijn opgenomen.
- Een groep van instellingen besluit hun kennis te bundelen voor het beheersen van haar uitbestedingsrisico's. Good en best practices worden onderling uitgewisseld en ervaringen gedeeld. Het resultaat hiervan is dat de monitoring door de instellingen beter is afgestemd op de uitbestedingsrisico's en dat de gemeenschappelijke dienstverlener op veel onderdelen meer gestandaardiseerd kan rapporteren. Ook worden gezamenlijk audits uitgevoerd op de gemeenschappelijke dienstverleners (pooled audits).

Waarneming 3: De weerbaarheid tegen cyberaanvallen moet worden versterkt

De combinatie van preventieve, detectieve en correctieve maatregelen én het uitvoeren van cyber resilience testen is voor een instelling van groot belang om weerbaar te zijn tegen cyberaanvallen en de gevolgen hiervan te beperken. Een deel van de instellingen heeft hiervoor echter (op onderdelen) geen volwassen beheersmaatregelen ingericht.

Om digitale aanvallen af te weren of de gevolgen te beperken zijn de volgende zaken van belang: een goede cyberhygiëne als fundament voor preventie, adequate detectie van een aanval, het inrichten van recovery processen en regelmatig uitvoeren van cyber resilience testen.

- Preventieve maatregelen zorgen ervoor dat een digitale aanval minder kans van slagen heeft door het toepassen en onderhouden van security standaarden. De mix aan deze maatregelen wordt hieronder samengevat onder de noemer Cyberhygiëne.
- Detectie en response bestaat uit tooling en processen om te monitoren of, en zo ja, hoe een aanval plaatsvindt en hierop te reageren.
- Recovery processen stellen de instelling in staat om de toegebrachte schade te beperken en de continuïteit van de bedrijfsvoering niet in gevaar te laten brengen.
- Bij cyber resilience testen wordt de weerbaarheid versterkt door digitale aanvallen op productiesystemen na te bootsen en daarvan te leren.

Deze elementen sluiten sterk op elkaar aan. We hebben ze daarom samengevoegd tot één waarneming. Een aantal elementen wordt hieronder achtereenvolgens uitgewerkt.

Met cyberhygiëne bedoelen we dat het fundament van maatregelen voor informatiebeveiliging goed op orde en volwassen is en blijft. Dit zijn bijvoorbeeld basismaatregelen als: awareness van personeel, toegangsbeveiliging, virus/malware scans, changemanagement en het maken van back-up's. Een belangrijk onderdeel hierbinnen is het verkrijgen van inzicht in, en zo snel mogelijk oplossen van, potentiele zwakheden. Mogelijke zwakheden kunnen zijn: achterstanden in patchmanagement van systemen en systemen die niet meer worden onderhouden door leveranciers.

De GP IB beschrijft op het gebied van vulnerability management (#19.2) het volgende:

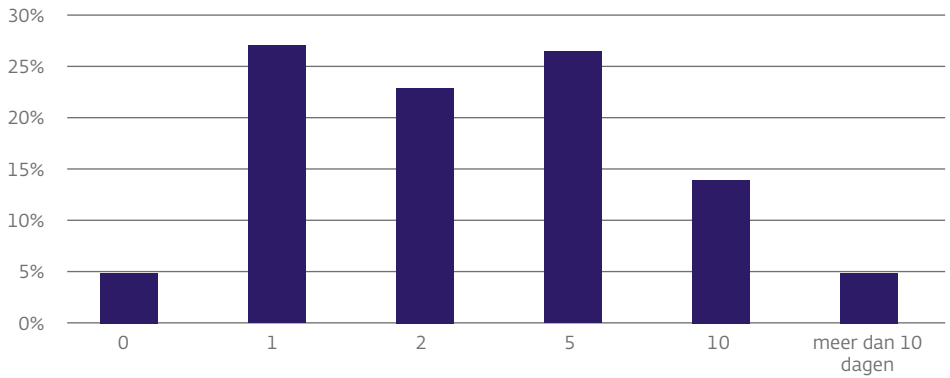
> De belangrijkste IT-assets zijn op basis van een risicoanalyse geïdentificeerd. Periodiek worden aan de IT-assets gerelateerde (cyber)kwetsbaarheden vastgesteld mede op basis van threat intelligence en vulnerability scans en de impact hiervan op de (bedrijfs)processen van de instelling bepaald. Op basis van de impact worden risicomitigerende acties bepaald voor bedreigingen die buiten de risicotolerantie van de instelling vallen.

Inzicht in mogelijke kwetsbaarheden in IT-systemen, en de risico inschatting van deze kwetsbaarheden, is een proces dat meer aandacht verdient. Uit onze onderzoeken blijkt dat de volwassenheid op het gebied van vulnerability-management onvoldoende is. In veel gevallen is hierbij sprake van het niet hebben van een goed overzicht van de belangrijkste IT-middelen (IT-assets) of een goed inzicht in de mogelijke (cyber)kwetsbaarheden daarvan.

Als de IT-assets in kaart zijn gebracht is het van belang om deze op kwetsbaarheden te blijven monitoren. Eén van de aspecten waarop gemonitord kan worden, is de snelheid van doorvoeren van kritieke patches om kwetsbaarheden in IT-systemen op te lossen. De snelheid van patchen verkleint het risico dat de systemen vatbaar(der) zijn voor aanvallen van buitenaf.

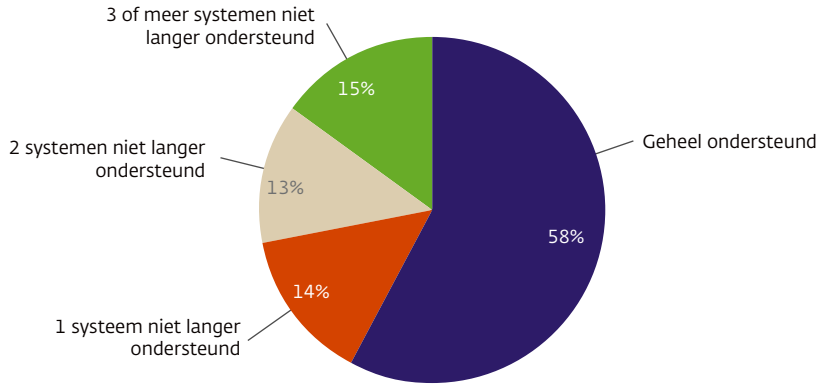
In figuur 6 is de snelheid van patchen inzichtelijk gemaakt op basis van onze sectorbrede analyse van 2021. In vergelijking met onze onderzoeken over voorgaande jaren zien we een verbetering in de snelheid van patchen. Op basis van dit figuur is echter ook duidelijk dat 5% van de instellingen zegt gemiddeld meer dan 10 dagen nodig hebben om kritieke security patches door te voeren op de IT productiesystemen.

Figuur 6 Snelheid van implementatie van kritieke patches (in dagen)



Een juiste, volledige en actuele registratie van alle IT-systemen waar een organisatie gebruik van maakt, is van belang om te zorgen dat die systemen tijdig worden onderhouden en/of uitgefaseerd, zodat het gewenste informatiebeveiligingsniveau niet in gevaar komt. DNB signaleert dat er nog (grote) ruimte is voor verbetering, zowel bij de registratie als bij het tijdig onderhouden en uitfaseren van IT-systemen. Instellingen lopen risico's wanneer zij gebruik maken van IT-systemen die niet langer ondersteund worden door leveranciers met beveiligingsupdates waardoor (blijvend) security kwetsbaarheiden kunnen optreden. Van de instellingen geeft 58% aan dat alle door haar geïdentificeerde kritieke systemen[7] worden ondersteund door leveranciers; 42% van de instellingen heeft te maken met één of meer kritieke systemen die niet langer worden ondersteund, zogenoemde End of life systemen (zie figuur 7).

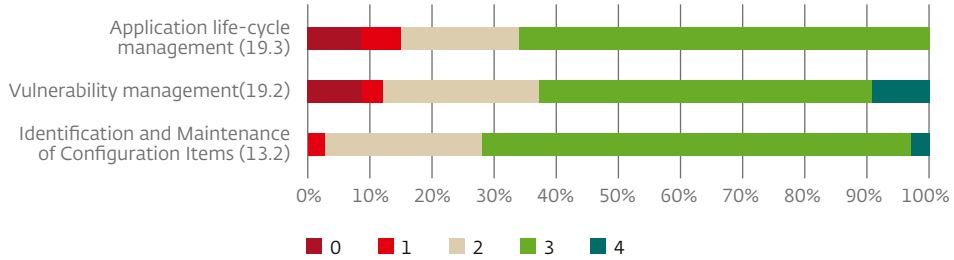
Figuur 7 Instellingen waarvan systemen niet langer door leveranciers worden ondersteund



Genoeg aanleiding om aandacht te (blijven) besteden aan het beheersen van deze risico's. Ter illustratie zijn hieronder de uitkomsten opgenomen van de onderzochte instellingen (figuur 8).

7 Dit betreffen in de o.a. besturingssystemen, databasesystemen, netwerksystemen en (polis)administratiesystemen

Figuur 8 Volwassenheidsniveau cyberhygiëne



Om aanvallen af te weren dan wel de gevolgen te beperken moet je deze kunnen signaleren. Hiervoor is adequate monitoring een basisvoorwaarde. Historisch hebben organisaties veel aandacht voor maatregelen die toezien op preventie op het gebied van informatiebeveiliging en cyberrisico's. Op het moment dat deze maatregelen niet voldoende blijken, is het van belang dat detectieve maatregelen zijn ingericht om een aanval of een ongeoorloofde handeling van een medewerker tijdig te signaleren.

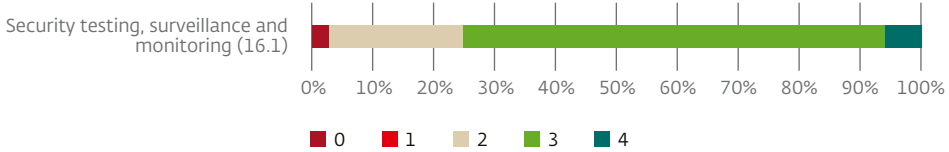
5% van de Nederlandse verzekeraars en pensioenfondsen heeft in 2021 aangegeven doelwit te zijn geweest van een succesvolle cyberaanval hetgeen heeft geleid tot daadwerkelijke ongeautoriseerde toegang tot interne systemen of gegevens.

Voor de weerbaarheid van de instelling is het daarom van belang om in haar beheersraamwerk nadrukkelijk aandacht te besteden aan de monitoring op haar netwerk en systemen. In de GP IB zijn beheersmaatregelen opgenomen die ingaan op deze monitoring. Een belangrijke control op dit gebied betreft "16.1 Security-testing, surveillance and monitoring". Hierin wordt een beschrijving gegeven van het proces die de instelling op dit gebied kan inrichten om de risico's te beheersen:

> Monitoring van ongebruikelijke activiteiten in IT-systemen vindt plaats. Uitzonderingen worden gesignaleerd en opgevolgd. De instelling zet bijvoorbeeld tooling in om aan de hand van logging afwijkende patronen te kunnen herkennen en daarop snel in te spelen.

Uitkomsten van de onderzoeken laten zien dat een kwart van de onderzochte instellingen geen volwassen proces heeft op het detecteren van een mogelijke inbreuk op het netwerk (zie figuur 9).

Figuur 9 Volwassenheidsniveau security testing, surveillance and monitoring



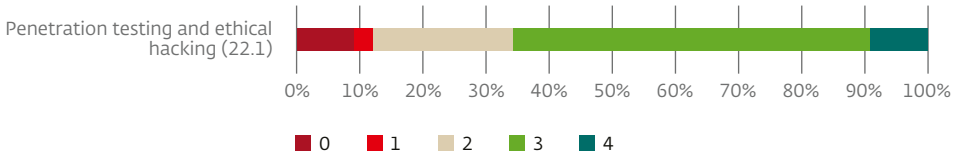
Dit heeft mogelijk als gevolg dat aanvallers lang onopgemerkt kunnen blijven en informatie verzamelen over de werking van IT-systemen en/of data onttrekken zonder dat de instelling dit signaleert.
De impact van zo'n aanval is daardoor groter dan in die gevallen waarin de organisatie in staat is nauwgezet te monitoren en snel inbreuken te signaleren in haar omgeving.

Naast aandacht voor cyberhygiëne is het voor de instelling van belang regelmatig te testen. Een goede manier om periodiek de cyberweerbaarheid van de instelling te toetsen is het testen op basis van een risicoanalyse en actuele cyberdreigingen met als doel zwakheden op te sporen en de mogelijke impact inzichtelijk te maken. Dit soort testen wordt ook wel penetration testing and ethical hacking genoemd. De GP IB beschrijft onder meer:

> De instelling bepaalt op grond van een risicoanalyse en actuele cyberdreigingen welke soorten beveiligingstests worden uitgevoerd alsmede de scope en diepgang van die tests. De aard en frequentie van deze tests zijn afhankelijk van het risicoprofiel van de instelling.

Op grond van de uitkomsten van onze onderzoeken heeft ongeveer 34% van de instellingen onvoldoende beheersmaatregelen op dit gebied ingericht. Een deel van de instellingen (9%) voert in het geheel nog geen testen uit. 25% van de instellingen voert dit onvoldoende gestructureerd uit waardoor geen sprake is van een volwassen proces (zie figuur 10).

Figuur 10 Volwassenheidsniveau Pentesting and ethical hacking



Een mogelijk risico is dat instellingen steunen op beheersmaatregelen die niet meer up-to-date zijn en die – onopgemerkt – omzeild kunnen worden op basis van (bekende) aanvalstechnieken.

Waarneming op basis van **TIBER-testen**

Als een aanvaller gemotiveerd en geavanceerd genoeg is, dan weet deze uiteindelijk binnen te komen. Dit is een kernbevinding uit 5 jaar TIBER-testen. Instellingen moeten daarom inzetten op meerdere verdedigingslagen.
Deze 'in depth' verdediging moet aanvallers niet alleen buiten houden (preventie), maar tevens adequate detectie bieden en een aanpak om aanvallers weer uit systemen te kunnen verwijderen (response).

Zo is (spear)phishing een aanvalsvector die regelmatig bij het TIBER-programma, op basis van intelligence, wordt toegepast. Maar uit evaluaties van deze testen komt naar voren dat (spear)phishing niet volledig kan worden gemitigeerd door nog meer nadruk te leggen op awareness-campagnes. Training en bewustwording reduceert het aantal mensen dat op phishing-mails klikt, maar 0% zal het nooit worden. Ervaring leert daarom dat het gevaarlijk is om uit te gaan van een waterdichte verdediging tegen (spear)phishing. Een verdediging in de diepte met meerdere barrières, waaronder een intern anomalie detectiesysteem, is dus essentieel om binnengedrongen aanvallers te kunnen detecteren en de gevolgen te beperken.

Enerzijds is het aanwezig zijn van deze 'basismaatregelen' cruciaal voor het weerstaan van digitale aanvallen. Anderzijds is het net zo belangrijk om de verdedigingslagen en -plannen periodiek te testen en te evalueren. Immers, door 'papieren maatregelen en plannen' in de praktijk te testen wordt pas echt inzichtelijk in hoeverre een instelling weerbaar is tegen cyberaanvallen.

Praktijkvoorbeeld: testen in samenwerking met DNB

Naast de toezichtfunctie van DNB werkt DNB in het TIBER programma samen met instellingen uit de banken-, pensioen- en verzekerings- sector om de digitale weerbaarheid van de financiële sector te verbeteren door het gezamenlijk uitvoeren van testen. Zie paragraaf 5.2 van deze IB-Monitor voor meer informatie over het TIBER programma van DNB.

Praktijkvoorbeeld: logging

Na een geslaagde poging tot phishing blijkt een hacker toegang te hebben verkregen tot het account van een medewerker. Na het vaststellen van de inbreuk op het account, wil de instelling de activiteiten van de hacker beoordelen. De instelling heeft echter nauwelijks logging en specifieke tools op dit gebied. De instelling kan hierdoor nauwelijks bepalen wat de hacker op haar systemen en netwerk heeft uitgevoerd. De instelling ziet zich hierdoor genoodzaakt ervan uit te gaan dat de hacker toegang heeft gehad tot alle data en systemen en op basis daarvan de mogelijke impact in te schatten en passende maatregelen te nemen.

In de GP IB zijn voorbeelden opgenomen om (mogelijke) kwetsbaarheden te monitoren. Onderstaande voorbeelden zijn daarvan afgeleid.

- Een instelling voert verschillende typen beveiligingstests uit en betrekt haar dienstverleners in de keten hierin, waaronder pentests gericht op de beveiliging van infrastructuur en applicaties, red teaming, het testen van de fysieke beveiliging en het testen van menselijk handelen in relatie tot informatiebeveiliging en cybersecurity.
- Een instelling inventariseert frequent (dagelijks) kwetsbaarheden op basis van Threat Intelligence en gebruikt tools om kwetsbaarheden geautomatiseerd te inventariseren (vulnerability scanning).
- Potentiële aanvalsmethoden kunnen worden vastgelegd in scenario's die de basis vormen voor generieke en instellings-specifieke use cases waarmee de monitoringsapplicaties gevoed worden. Door het vastleggen van use cases wordt inzichtelijk hoe, wat, waar en welke drempelwaarden gemeten moeten worden om mogelijke aanvallen snel te kunnen opsporen en actie te kunnen ondernemen.
- Naast veel aandacht voor het vaststellen en monitoren van kwetsbaarheden besluit een instelling de mogelijke impact van een eventuele geslaagde cyberaanval verder te beperken door micro-segmentering van haar netwerk toe te passen. Hierbij worden de rechten verder teruggebracht waarbij nadrukkelijk ook aandacht wordt besteed aan de rechten van beheerders. Het netwerk wordt hierbij ingedeeld in lagen en op zichzelf staande omgevingen. Hiermee wordt voorkomen dat een aanvaller – eenmaal binnen – ook overal bij kan.
- Beveiligingstesten geven ook zeer bruikbare informatie voor andere instellingen. Enerzijds om de gebruikte scenario's ook op de eigen organisatie toe te passen maar met name ook om de (generieke) bevindingen uit de testen ook te toetsen op de eigen organisatie. In verschillende samenwerkingsverbanden (zoals in de ISAC's) worden deze inzichten gedeeld.

Dreigingsanalyse financiële sector

Dit hoofdstuk geeft een beeld van een aantal dreigingen voor de Nederlandse financiële sector. DNB houdt in haar onderzoeken rekening met de dreigingen opgenomen in deze dreigingsanalyse zoals het verloop van risico's door de tijd heen en de richting waarin risico's zich bewegen. Het is hierdoor een belangrijke indicator voor het bepalen van prioriteiten in de gehanteerde toezichtaanpak.

Adequate digitale weerbaarheid is cruciaal voor het functioneren van de Nederlandse financiële sector. Door de toenemende digitalisering worden financiële instellingen meer en meer 'IT-bedrijven met activiteiten in de financiële sector'. Het zwaartepunt van dreigingen voor de financiële sector ligt daarom ook steeds meer in het digitale domein. Op basis van meerdere bronnen[8] en contacten met instellingen ziet DNB de volgende vier dreigingen als een prioriteit voor de sector:

- Ransomware
- Aanvallen op of via derde partijen in de uitbestedingsketen
- Long term compromise
- DDoS

Ransomware

De hoeveelheid aanvallen met ransomware is sinds het begin van de coronacrisis sterk gestegen, zo blijkt onder andere uit het Cybersecuritybeeld Nederland 2021[9]. Ook instellingen in de internationale financiële sector en/of relevante derde partijen worden regelmatig geraakt. Het opzetten van een ransomware-aanval wordt steeds bereikbaarder voor een steeds grotere groep criminelen door de beschikbaarheid van ransomware-as-a-service-diensten (RaaS).

Op het darkweb[10] is de afgelopen jaren een 'diensteneconomie' van gespecialiseerde criminelen ontstaan die tegen een vergoeding gedeeltes van een (ransomware) aanval uitvoeren. Zo zijn er criminelen die toegang tot bedrijven verkopen, terwijl andere criminelen zich specialiseren in de ontwikkeling en uitrol van ransomware. Op deze manier kunnen grote gedeeltes van een aanval soms modulair worden gekocht. Er zijn zelfs criminele aanbieders die complete 'aanvalspakketten' verkopen. Het is echter niet alleen de hoeveelheid aanvallen die ransomware een grote dreiging maakt, maar ook de veranderende aard. Waar voorheen primair data werd versleuteld tijdens ransomware-aanvallen, wordt nu ook regelmatig geprobeerd om vitale data weg te sluizen. Vervolgens dreigt de aanvaller met het publiceren of verkopen van deze data, tenzij de losgeldsom wordt betaald. Dit is de zogenaamde 'double extortion'. Een andere belangrijke reden voor de 'populariteit' van ransomware is de potentiële winstgevendheid. Door de beschikbaarheid van RaaS is de investering voor criminelen relatief beperkt, terwijl de potentiele opbrengst zeer groot is. Losgeldbedragen lopen soms tot in de tientallen miljoenen euro's.

8 Drie primaire bronnen voor de IB-monitor zijn (1) de EC3 van Europol, (2) het CSBN van het NCSC en (3) het 1Financial Threat Landscape for The Netherlands (1FTL-NL). Het 1FTL-NL is een dreigingsbeeld via de FI-ISAC wordt gemaakt door en voor de Nederlandse financiële sector.
9 Het Cybersecuritybeeld Nederland is uitgebracht door de Nationaal Coördinator Terrorismebestrijding en Veiligheid, zie https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021
10 Het darkweb is het verborgen collectief van internetsites die alleen toegankelijk zijn via een gespecialiseerde webbrowser. Het wordt gebruikt om internetactiviteiten anoniem en privé te houden.

Aanvallen op of via derde partijen

Zoals hierboven gesteld hebben niet alleen digitale aanvallen op financiële instellingen een potentieel grote impact, maar ook aanvallen op derde partijen. Een toenemend aantal diensten, systemen en processen wordt door financiële instellingen uitbesteed aan grotere en kleinere digitale partners. Voorbeelden zijn dataopslag, betaalsystemen, software en werkplekfaciliteiten. Deze digitale afhankelijkheid heeft een aantal gevolgen voor de cyberweerbaarheid van de financiële sector. De paradox hierbij is dat derde partijen enerzijds gespecialiseerd zijn in wat ze doen en veiligheid doorgaans hoog in het vaandel hebben. Anderzijds lijken ze regelmatig een aantrekkelijk doelwit te zijn voor digitale aanvallers. Er zijn verschillende verklaringen voor de recente stijging in aanvallen op of via derde partijen. Ten eerste is sprake van een concentratierisico. Eén enkele derde partij kan door aanvallers als springplank worden gebruikt om toegang te krijgen tot meerdere klanten. Aanvallen zijn hierdoor gemakkelijk schaalbaar. Ten tweede vergroot het gebruik van derde partijen het aanvalsoppervlak voor cybercriminelen. Zij kunnen meerdere routes of meerdere derde partijen kiezen om ergens binnen te komen. Een derde verklaring is dat financiële instellingen de controle over de cyberweerbaarheid deels uit handen geven. Vaak leveren derde partijen hoog gespecialiseerde diensten. Juist daardoor is het voor financiële instellingen lastig om de kwaliteit van de cyberweerbaarheid bij de derde partij objectief te bepalen en te toetsen door middel van ontvangen rapportages of het uitvoeren van audits. Sommige derde partijen geven beperkt openheid over beveiliging of incidenten.

Long term compromise

Een dreiging die niet vaak wordt waargenomen, maar toch relevant blijft voor financiële instellingen, is long term compromise. Hiermee wordt bedoeld dat geavanceerde groeperingen – vaak op het niveau van een natiestaat – langdurig aanwezig zijn in de netwerken en systemen van een financiële instelling. Door het hoge niveau van de aanvaller is een dergelijke inbreuk vaak zeer lastig te detecteren. Aanvallers kunnen zodoende over een langere periode veel kennis opdoen over de instelling en haar klanten, zonder dat de instelling zich hiervan bewust is en actie kan ondernemen. Hoewel een long term compromise zelden gedetecteerd wordt of in de openbaarheid verschijnt, is dit geen garantie dat het ook daadwerkelijk niet plaatsvindt. Financiële instellingen moeten derhalve alert blijven op dit soort onzichtbare, maar uitermate verstrekkende aanvallen.

DDoS

Hoewel Nederlandse financiële instellingen de afgelopen jaren veel maatregelen hebben genomen tegen DDoS-aanvallen, blijft deze dreiging relevant. Dat komt voornamelijk door de onvoorspelbaarheid van DDoS-aanvallen. Soms wordt maandenlang geen DDoS-aanval waargenomen, op andere momenten volgen de aanvallen elkaar in hoog tempo op. Ook hier is de toegankelijkheid voor criminelen tot tools om een DDoS aanval uit te kunnen voeren reden tot zorg. Deze cyclus speelt al zolang financiële instellingen diensten via het internet aanbieden. Vaak ontbreekt hierbij een eenduidige motivering om een DDoS-aanval te starten. Het is voor instellingen daarom van belang waakzaam te blijven op mogelijke oplevingen hiervan, zodat zij de tegenmaatregelen snel kunnen aanpassen.

Vooruitblik toezicht op cyberrisico's

Vanwege de voortdurende ontwikkelingen op het gebied van informatiebeveiliging en cybersecurity dienen instellingen permanent aandacht te besteden aan het op niveau brengen en houden van de kwaliteit van de inrichting van hun informatiebeveiliging. DNB heeft de beheersing van risico's op het gebied van Technologie een prominente plaats gegeven in de Visie op Toezicht 2021-2024[11]. In het onderdeel 'Inspelen op technologische vernieuwing' zijn drie aandachtspunten gedefinieerd:

1. Instellingen en hun dienstverleners moeten kunnen aantonen dat zij hun informatiebeveiliging op orde hebben en zij moeten regelmatig hun cyberweerbaarheid testen.
2. Instellingen dienen aandacht te geven aan het verhogen en up-to-date houden van het kennisniveau van, en betrokkenheid van bestuursleden en commissarissen op het gebied van IT- en cyberrisico's. Om de toenemende cyberrisico's te beheersen is het van belang dat er op bestuursniveau voldoende kennis aanwezig is.
3. Instellingen brengen hun data en IT-processen steeds vaker onder bij derde partijen die niet onder direct toezicht staan[12]. Instellingen blijven echter altijd zelf verantwoordelijk voor de veiligheid van de data en het voldoen aan regelgeving. Daarbij heeft DNB bijzondere aandacht voor specifieke vormen van uitbesteding, waarbij bedrijfs- of IT-processen via een oplossing extern zijn ingericht bij bijvoorbeeld bigtechs. DNB zal de komende jaren gerichter toezicht houden op deze vormen van uitbestedingen en of deze voldoen aan de geldende wet- en regelgeving en aan de uitbestedingsrichtlijnen zoals gepubliceerd door EBA[13] en EIOPA[14].

Naast de bovengenoemde drie items uit de Visie op Toezicht benadrukt DNB dat samenwerking tussen instellingen in de financiële sector een positieve uitwerking kan hebben op de beheersing van informatiebeveiliging- en cyberrisico's in alle schakels van de uitbestedingsketen. In de praktijk zien we dit op verschillende manieren terug. Bijvoorbeeld door informatie uitwisseling tussen instellingen over actuele dreigingsinformatie en gezamenlijk lering trekken uit incidenten en oefeningen. Dit kan ervoor zorgen dat instellingen beter voorbereid zijn op mogelijke dreigingen. Ook zien we dat instellingen die al een relatief hoge volwassenheid hebben op het gebied van informatiebeveiliging consistente eisen stellen aan dienstverleners en ook andere instellingen met een lagere volwassenheid ondersteunen om te verbeteren door het uitwisselen van best practices.

11 Visie op toezicht 2021-2024 (dnb.nl)
12 Op 24 september 2020 heeft de Europese commissie een wetgevingsvoorstel gepubliceerd, de Digital Operational Resilience Act (DORA), voor het stellen van uniforme eisen aan financiële instellingen en derde partijen die kritische dienstverlening aanbieden aan financiële instellingen (tot het gebruik en de beveiliging van ICT). Hierbij is het de intentie om een vorm van Europees toezicht (oversight) in te richten op aangewezen significante dienstverleners.
13 European Banking Authority (EBA) is de Europese prudentiële toezichthouder voor de bancaire sector.
14 European Insurance and Occupational Pensions Authority (EIOPA) is de Europese prudentiële toezichthouder voor de sector verzekeringen en pensioenen.

Actualisering toezichtmethodologie

In december 2020 informeerden wij onze onder toezicht staande instellingen over de actualisering van de toezichtmethodologie[15] waarbij de intensiteit van ons toezicht toeneemt naarmate de negatieve impact van de risico's op het vertrouwen groter is. De toezicht activiteiten worden daarom samengesteld op basis van de aan de instelling toegekende impactklasse en de hoogte van de vastgestelde risicoscores. Daarnaast kan een instelling – onafhankelijk van de toegekende impactklasse en risicoscore – geselecteerd worden voor een onderzoek als onderdeel van een toezichtthema. Het cyberrisico is voor 2022 een belangrijk toezicht thema.

Daarnaast kunnen toegekende risicoscores (bijvoorbeeld t.a.v. het operationeel en IT risico) aan een instelling een aanleiding zijn voor risico identificerende of risico mitigerende opvolging van DNB. Risico-identificatie vindt plaats via een risico-identificerend gesprek, een deep dive of een on-site. Ook zijn (wederkerende) data-uitvragen en ronde tafels/seminars onderdeel van het toezicht.

Toezicht thema 2022: Cybersecurity over de hele keten

Een ontwikkeling die de financiële sector raakt, is het cyberrisico, dat door de steeds groter wordende afhankelijkheid van digitale diensten, processen en systemen en een toenemende mate van (onder)uitbesteding sterk toeneemt. De trend naar uitbesteding van digitale bedrijfsprocessen leidt tot toenemende afhankelijkheid van derde partijen. Dit maakt instellingen kwetsbaar voor verstoringen bij hun dienst-verleners. DNB zet ook in 2022 haar onderzoeken bij de instellingen risicogebaseerd voort om te beoordelen of zij voldoende en structurele aandacht hebben voor effectieve beheersmaatregelen in de gehele (outsource) keten op dit gebied.

Ook zal de impact van nieuwe wet- en regelgeving, zoals DORA worden betrokken in het toezicht. Daarnaast wordt in 2022 bijzondere aandacht besteed aan de rol en het kennisniveau van bestuurders en (interne) toezichthouders op dit onderwerp.

15 Deze toezichtmethodologie geldt niet voor bancaire instellingen die vallen onder SSM-toezicht. Zie voor meer informatie de brochure van DNB: "geactualiseerde toezichtaanpak: ATM"; Brochure ATM (dnb.nl)

Bronnen

Onderzoeksbronnen vanuit onze Toezichtfunctie

IB Fundament onderzoeken
Sinds een groot aantal jaren onderzoekt DNB de beheersing van informatie-beveiliging en cybersecurity binnen de Nederlandse financiële sector. Dit doen we sinds 2010, steeds op basis van periodieke self-assessments bij de onder ons toezicht staande instellingen. Als handvat voor het invullen van deze self-assessments is in 2019 de Good Practice en bijbehorende Q&A Informatiebeveiliging geactualiseerd.

Sector Brede Analyse Informatiebeveiliging (SBA-IB)
In 2021 is DNB gestart met het structureel uitvragen van de volwassenheid van Informatiebeveiliging bij verzekeraars en pensioenfondsen aan de hand van de SBA-IB. De SBA-IB bevat vragen die ingaan op de mate waarin de instelling is blootgesteld aan IT-risico's inclusief risico's op het gebied van informatiebeveiliging. Daarnaast gaat de SBA-IB in op de volwassenheid van de beheersmaatregelen op het gebied van informatiebeveiliging. Informatie uit deze SBA-IB wordt gebruikt om het risicoprofiel van een instelling te identificeren.

Inspecties en on-site onderzoeken bij onder toezicht staande instellingen
DNB voert, risicogebaseerd, gerichte inspecties en on-site onderzoeken uit op het gebied van IT- en cyber-risico's bij onder toezicht staande instellingen. De waar-nemingen ter plaatse bij deze instellingen tezamen met de rapporten van de inspecties hebben bijgedragen aan de waarnemingen in deze IB-Monitor.

Rapportages, signalen en incidentmeldingen vanuit onder toezicht staande instellingen
Op dagelijkse basis staan account toezichthouders van DNB in contact met onder toezicht staande instellingen. Zij zijn binnen DNB het eerste aanspreekpunt voor instellingen en ontvangen daarom frequent informatie over operationele zaken waaronder IT- en cyberrisico's.
Daarnaast zijn instellingen conform sectorale wetgeving verplicht om majeure (cyber-) incidenten zo spoedig mogelijk te melden bij de toezichthouder.

Onderzoeksbronnen vanuit onze centrale bankfunctie

Resultaten van TIBER testen
Sinds juni 2016 is DNB vanuit haar centrale bankfunctie samen met de sector gestart met TIBER-NL (Threat Intelligence Based Ethical Red Teaming), een programma om financiële instellingen weerbaarder te maken tegen cyberaanvallen.
Belangrijk onderdeel zijn hacktests op productiesystemen, op basis van actuele dreigingsinformatie.

Uit deze testen blijkt dat de cyberweerbaarheid over het algemeen hoog is. Tegelijkertijd maken deze testen inzichtelijk dat geraffineerde aanvallers in potentie veel schade kunnen aanrichten bij instellingen die essentieel zijn voor de financiële stabiliteit. Indien het niet om gecontroleerde testen zou gaan, maar om echte aanvallen, zou er in enkele gevallen sprake zijn geweest van uitval van essentiële functies, verlies van hoog-vertrouwelijke informatie, financiële verliezen of marktmanipulatie.

Relevante ervaringen en beelden opgedaan uit dit programma zijn ook meegenomen in deze IB-monitor.

Disclaimer

Deze IB-monitor bevat enkele voorbeelden of good practices. Good practices geven niet-verplichtende aanbevelingen voor de toepassing van de wetgeving op het gebied van beheerste en integere uitvoering (o.a. art. 18 Besluit FTK, art. 3.17 WFT en art. 143 PW) aan de onder toezicht staande instellingen. Met behulp van een good practice draagt de Nederlandsche Bank N.V. haar opvattingen uit over de door haar geconstateerde of verwachte gedragingen in de beleidspraktijk, die naar ons oordeel een goede toepassing inhouden van de regels waarop deze good practice betrekking heeft.

Met een good practice beogen we te bereiken dat de onder toezicht staande het daarin gestelde, de eigen omstandigheden in aanmerking nemende, in hun afweging betrekken, zonder dat zij verplicht zijn dat te doen. Een good practice geeft inzicht in de door ons geconstateerde of te verwachten gedraging in de beleidspraktijk, is indicatief van aard en sluit daarmee niet uit dat voor instellingen een afwijkend, al dan niet strengere toepassing van de onderliggende regels geboden is. De afweging betreffende de toepassing berust bij deze instellingen zelf.